SAFECARE

Integrated cyber-physical security for health services

Dissemination and Communication Strategy

Deliverable 8.1

Lead Author: EOS

Contributors: All Partners

Deliverable classification: PU

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

Version Control Sheet

Title	*Dissemination and Communication Strategy*
Prepared By	*Elodie Reuge*
Approved By	
Version Number	*Version 1*
Contact	Elodie.reuge@eos-eu.com

Revision History:

Version	Date	Summary of Changes	Initials
V0.1	17.10.2018	Initial draft sent to the Consortium	ER
V0.2	5.11.2018	Integration of the Partners' contributions	ER
V0.3	14.11.2018	Review of KEMEA	IG - VM
V.04	15.11.2018	Internal review of EOS	KT
V0.6	16.11.2018	Second draft sent to the consortium	ER
V0.7	20.11.2018	Second Review of KEMEA	IG - VM
V0.8	27.11.2018	Review of SGSP	PG
V0.9	28.11.2018	Second Internal Review EOS	KA
V1	30.11	Final Deliverable	ER

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
DPIA	Data Protection Impact Assessment
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

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, we know that we must increase our awareness since these attacks can affect and destabilize critical infrastructures we depend 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 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 to achieve a global optimum for systemic security and for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects. The project focuses on health service infrastructures and works towards the creation of a comprehensive protection system, which will cover threat prevention, detection, response and, in case of failure, mitigation of impacts across infrastructures, populations and environment.

Over a 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). An explanation on when to use these tools and for which purpose is also provided. Hence, Section 6 describes a set of measures to respect 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 is required which should be the key point of the D&C Strategy for SAFECARE as a whole. This approach should also fully understand the objectives, and ensure that the Dissemination and Communication activities will occur at the right time.

SAFECARE's objectives and outputs should also be perfectly understood by different internal and external stakeholders. The first step of knowing what has to be reached and understand why it has to be reached, helps with the implementation of the engagement process in a meaningful way, defines the appropriate messages for the right stakeholders, selects adequate tools and uses suitable channels, respecting the appropriate timing.

An explanation of what is expected from D8.1 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 8.1

According to the Description of Action, the Dissemination and Communication Strategy will address the relevant user communities through several channels: web-oriented solutions and social networks, awareness and commercial events, communication and participation in national, European and international standard bodies as well as project documentation and reports in collaboration with the Quality Manager (QM).

The development of a proper D&C Strategy early enough in the project (M3) aims to reach impact levels that can be considered satisfactory. The Key audiences for SAFECARE, 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 strategy will also include key messages and means of approaching the aforementioned stakeholders.

1.2 Methodology

The goal of this deliverable is to specify the overall Dissemination and Communication Strategy of SAFECARE that will be used to increase the engagement of the relevant stakeholders for the purposes of the project. The effective implementation of the Dissemination and Communication activities is key for the successful project implementation and a proper strategy definition is the starting point of it. It focuses on two major lines:

- promoting and increasing the visibility of the relevant activities to be carried out by SAFECARE;
- fostering the participatory engagement with key stakeholder groups to enhance the project's impact and ensure the adoption of its main outcomes.

During the second phase of the project these activities will also evolve to ensure market uptake.

The SAFECARE stakeholder engagement approach described in D8.1 defines:

- The reasons for developing an effective stakeholder engagement approach;
- The stakeholders to be engaged with;
- The key messages to be shared;
- The means/methods to use;
- The best timing to maximize the level of engagement.

Engaging different stakeholders is crucial for SAFECARE. The right techniques and media tools should be appropriately selected, knowing that they will vary depending on the stakeholders' groups targeted as well as the messages disseminated or communicated.

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. For this reason, two updates of the strategy are foreseen, namely:

- D8.2 Initial dissemination and communication report (M13)
- D8.3 Final dissemination and communication report (M35)

D8.2 and D8.3 aim at reflecting the activities and results achieved by SAFECARE and informing about the adjustment of the strategy. This will ensure that the right measures are taken at the appropriate time, enhancing SAFECARE's impact. The revisions will benefit from dedicated monitoring, as well as evaluation tools and mechanisms applied in SAFECARE that are also detailed in the strategy.

The engagement approach developed for SAFECARE and the supporting Dissemination and Communication Strategy presented herein describe the corresponding activities relevant for stakeholders. This approach will be described in the following sections.

In section 2, the necessity for SAFECARE to engage with the Critical Infrastructure Protection (CIP) ecosystems is elaborated and proper objectives for that specific engagement are well defined. Section 3 identifies and defines the relevant stakeholder groups SAFECARE is willing to engage with. Then Section 4 and 5 define the objectives leading to key messages that are shared (Section 4) as well as tools and channels (Section 5) that will be used to relay the defined messages. Section 6 describes the monitoring and evaluation mechanisms ensuring, as explained above, the appropriateness of the activities to implement.

2. Engaging with the Critical Health Infrastructure Protection ecosystem

2.1 Objectives for engaging

Clarifying the logic behind stakeholders' engagement is a crucial initial step for the definition of a clear and well defined engagement strategy. It supports the selection of appropriate tools to be used. In the following paragraphs, an overview of benefits, starting from a general vision and concluding with a more specific and relevant approach to SAFECARE is presented.

2.1.1 General objectives for engaging

- **Extend and enhance SAFECARE's reputation:** communicating on SAFECARE can improve its image and gain stakeholders' trust;
- **Boost awareness** of SAFECARE's aims, objectives and subsequent outcomes at different geographical levels (local, national, European and international);
- **Intensify SAFECARE's impact:** a personalized, and efficient communication with stakeholders can support the project outcomes uptake and increase their relevance;
- **Collect relevant ideas:** pertinent stakeholders, with their expertise, can provide insights on SAFECARE, and may contribute with suggestions that might enhance project's activities impact and strategy;
- **Collect and gather information:** Information about SAFECARE's stakeholders needs and requirements can be shared. Hence SAFECARE is better formatted to address them and increase their interest in the appropriation of its outcomes.
- **Build a European solution:** Engaging in SAFECARE serves to (a) protect Critical Infrastructures with and through European solutions and (b) enhance partnerships for future projects on Critical Infrastructure across Europe.

2.1.2 Specific objectives for engaging with the Critical Health Infrastructure Protection ecosystem

Critical infrastructure "*means an **asset**, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, **health,** safety, **security**, economic or social well-being of people, and the **disruption or destruction of which would have a significant impact** in a Member State as a result of the failure to maintain those functions."*[1]

Critical Health Infrastructure Protection ecosystem is a very complex and sensitive sector, involving organizations from various sectors. Nowadays, reducing the vulnerabilities of Healthcare Critical Infrastructures should be one of the main societal objectives. An adequate protection level must be ensured and the detrimental effects of disruptions on the society and citizens must be limited. Indeed, Europe needs a systematic approach and knowledge to better manage evolving roles, risks, threats and vulnerabilities. Stakeholders' involvement in Critical Health Infrastructure Protection ecosystem, through a project responding to critical health infrastructure threats, is essential for improving the dissemination of the project results. Better dissemination means that the results are more likely to be used to better protect European hospitals and other critical health infrastructures.

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of need to improve their protection – Article 2 - Definitions

2.1.3 Specific objectives for engaging with the Critical Health Infrastructure Protection ecosystems in the frame of SAFECARE

The main stakeholder engagement objective which is also the key goal of SAFECARE is to achieve a global optimum for systemic security and to enhance the management of combined cyber and physical threats, and incidents, their interconnections and potential cascading effects.

By identifying and considering needs, concerns and requirements of stakeholders, the Critical Health Infrastructure protection in operational conditions will be optimized. Therefore, it will support the development of advanced technologies in the areas of physical and cyber security that will better meet stakeholders' requirements, involving the health critical infrastructures.

Engaging with the stakeholders in the project will ensure that SAFECARE's global solution developed is flexible, scalable and adaptable to the operational needs of various hospitals across Europe and meet the requirements of newly-emerging technologies and standards. SAFECARE's results will be disseminated to the critical infrastructure stakeholders through the establishment of a bi-directional communication channel.

2.2 Levels of engagement

Similarly, to other EU funded projects, SAFECARE follows the Spectrum of Public[2] Participation developed by the International Association of Public Participation (IAP2)[3]: informing, consulting, involving, collaborating and empowering (representing the five levels of engagement). The table below disclosed in an opportune way the meaning of such division and its use within SAFECARE:

[2] To be understood as the community, the citizens

[3] "IAP2 is an international association of members who seek to promote and improve the practice of public participation / public engagement in relation to individuals, governments, institutions, and other entities that affect the public interest in nations throughout the world », https://www.iap2.org/ , consulted on the 12th of November 2018

Table 1 Level of engagement

	Informing	Consulting	Involving	Collaborating	Empowering
Public Participation Goal	To provide with balanced and objective information, that will assist the public in understanding the opportunities and solutions of SAFECARE	To obtain its feedback on analysis done and/or decisions reached within SAFECARE	To work directly with it throughout the process, ensuring that its concerns and aspirations about SAFECARE are understood and considered	To partner with it in each aspect of the decision, including the development of alternatives and the identification of preferred solution within SAFECARE	To place final decision making, regarding SAFECARE, in their hands
Promise to the Public	To keep it informed about the outcomes of SAFECARE	To keep it informed, listen to and acknowledge concerns and aspirations, and provide feedback on how its input influenced a decision taken within SAFECARE	To work with it, ensure that its concerns and aspirations are directly reflected in the alternatives developed, and provide feedback on how its input influenced the decision taken in SAFECARE	To work together with it in formulating solutions and incorporating its advice and recommendations, into the decisions, to the maximum extent possible	To implement what it decides within and through SAFECARE

3. Stakeholder engagement

To better engage stakeholders, the stakeholders' categories, needs and groups are identified below.

3.1 Identification of stakeholder categories

The different stakeholders' categories identified for SAFECARE's purposes are the following:

Practitioners

As end-users, public hospitals must collect requirements, needs and opinions of different categories of professionals.

The **Medical and Pharmacy staff** must also be consulted as they have knowledge on Crisis management in Health Structures. They also understand how, when and what the consortium has to communicate. Because they have deep knowledge of the healthcare system and the care path, they can describe many scenarios of risks (incidents into patient circuit in the care structure or emergency management). They also have experience on the management of violent persons, particularly in several od sensible sectors (emergencies / Psychiatric emergencies) and can offer some solutions to detect them and provide a more secure approach.

Then the **biomedical staff and the IT and cyber security staff** could be consulted because of their experiences and knowledge on cyberattacks on hospital networks, coming directly from the use of internet or from the biomedical equipment installed in the premises. The biomedical staff can provide information about the requirements of equipment (e.g. functionality or connections). The IT and cyber security staff can identify scenarios of risks, responses and means of protection such as specific components or architecture of firewall.

Finally, the **physical security and technical staff** can provide valuable information about physical security. The technical staff can identify the sensible technical components of a health structure, such as energy, elevators, technical gas/fluid, temperature, air control systems and building management. The physical security staff can provide scenarios of risk concerning the flow of persons in the hospital such as security at the entrances/exits.

Scientific and research community

It is beneficial for the project to engage with the scientific community to broaden the understanding of critical assets and the requirements of a mitigation solution. This category is composed by researchers and academics in the domain of critical infrastructure protection, cybersecurity, privacy and data protection as well as related fields within the health sector. SAFECARE aims to impact the scientific community by expanding the existing knowledge through, the examination of the compliance of new information technologies with the European legal framework on data protection and information sharing infrastructures.

Public/Policy bodies/ Standardization bodies

In this category, experts or organizations working in the public sector, policy and standardization bodies using SAFECARE outputs for the achievement of their duties to serve the society, are targeted.

This involves funding agencies, EU DGs (Directorate Generals), Crisis management centres, Ministries (and their subdivisions) and decisions makers who define health policy and deal with its impact on the population.

Different public administration units responsible for crisis management issues, rescue departments, police departments and civil security are also in charge of first responses in case of a major attack on critical health infrastructures or major health related risks (such as an infectious outbreaks). These bodies aren't responsible only for health crises, compared to hospitals emergency response teams which are health professionals that can be called at any time and sent on the spot in case of major health crises.

This category also involves standardization bodies, such as the European Committee for Standardization (CEN), the International Organization for Standardization (ISO), the European Telecom Standards Institute (ETSI), the National Standardization Body of Greece (ELOT), the British Standards Institution (BSI), Deutsches Institut für Normung (DIN) for example, whose main aim is to issue standardization documents and to ensure easy penetration and widespread acceptance of products in the market.

Private sector

There are several potential stakeholders in the private sector SAFECARE's results could be disseminated to. The private sector has been classified in four categories based on the type of their involvement in the healthcare sector: providers, suppliers, Insurance companies and others[4], which are analysed below:

- Providers include the entities that directly provide health services to the public, for instance, private hospital and clinics, online health service providers, pharmacies and civil society organizations. This category also includes the healthcare infrastructure providers that enable the afore-mentioned service providers to function.
- Suppliers include medical equipment vendors, online healthcare software vendors, SMEs that provide healthcare technologies or solutions and pharmaceutical companies.
- Financers (i.e. payers) are those, who pay for the services provided and include private healthcare financing companies, health insurance companies and non-profit entities among others.
- These three categories stated above include the stakeholders on the healthcare industry context. As SAFECARE focuses on physical and cyber security solutions, a fourth category has been considered: other actors such as security industry, trade unions representing healthcare service providers or suppliers, and academic experts in physical networks and information security.

Related projects and initiatives

EU Projects and initiatives (past or ongoing) are important vehicles for requirements' identification and validation. They consist an important stakeholders' category as they can be involved in the area of critical infrastructure, health critical infrastructure or healthcare in general. Their environment needs to be aligned with SAFECARE's approach, to avoid possible

[4] « Assessing Private Sector Involvement in Health Care and universal Health Coverage in Light of the Right to Health », 18th of December 2016 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5394993/)

overlaps and enhance complementary synergies. SAFECARE will especially establish links with INFRA01 projects which were awarded prior to and after 2017.

These bodies can provide knowledge, capacity and understanding for more advanced technologies in Member States, in order to improve resilience at European Level. They also can embrace new technologies according to their fields of expertise or contribute to improve the functioning of emergency services for citizens.

Civil society

The protection of critical health infrastructures (and critical infrastructures in general) concerns the civil society and its existing sub-entities.

As interested as the entities may be, they also may not have the right expertise to take full advantage of SAFECARE and its outputs or use them in an appropriate way.

For example, hospitals' patients comprise an interesting stakeholder, as their involvement might enhance SAFECARE developed solution awareness. Understanding patients' perception will help the consortium get a different point of view.

Citizens in general have the opportunity to organize themselves into networks (at regional, international, national or local levels) as they have a direct interest in the protection of critical infrastructures and critical health infrastructures. Feeding these networks with correct information on what is really happening in the field of critical infrastructures can lead to a stronger community; and a well-informed civil society can lead to a better governance.

Security Managers and Critical Infrastructures Security Liaison Officers (SLO)

Security managers are practitioners that can support the identification of an organisation's assets (including people buildings, machines, systems and information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets.

It is imperative for SAFECARE to engage with Security Managers and critical infrastructures Security Liaison Officers (SLO) to broaden the understanding of critical assets definition, security response procedures and the spectrum of SAFECARE solutions. This category is composed by healthcare security managers and SLOs (SLO would function as the point of contact for security issues between the ECI and the relevant CIP authorities in the Member States) in the field of critical infrastructure protection, healthcare security (physical and cyber), privacy and data protection as well as other fields within the health and security sector. SAFECARE aims to impact them by expanding the existing knowledge with regards to critical infrastructure security issues, focusing on those of the health sector.

Critical Infrastructure operators and owners

It is imperative for SAFECARE to engage with healthcare critical infrastructures operators and owners to broaden the understanding of critical assets and the security requirements of SAFECARE solutions. This category includes all types of critical infrastructures owners and operators (identified in the EU Directive 114/2008: energy and transport, in the ongoing discussions for its revision (SWD (2013) 318 final) and national policies), Member States NCP for the critical infrastructure protection and EU officials from different DGs related to critical infrastructure resilience programs and regulatory work, and the scientific community. SAFECARE

aims to impact them by expanding the existing knowledge with regards to critical health infrastructure security issues.

Law Enforcement Agencies and Emergency Response Agencies

The protection of critical health infrastructures (and critical infrastructures in general) concerns Law Enforcement Agencies (LEAs) and Emergency Response Agencies (ERA), which are public safety agencies and have varying roles and responsibilities in handling and responding to crisis incidents or criminal activity. Emergency response entities include fire departments, civil protection, ambulance, rescue services, and dispatch centers. A law enforcement agency is any agency which enforces the law, such as a special, local, or state police, federal agencies or international organizations. These agencies and organisations can provide and get knowledge, capacity and understanding in security issues, in order to enhance resilience at European Level.

3.2 Identification of stakeholders needs

Stakeholders' engagement is directly affected by their needs which should be better identified and/or declared. This point is crucial to deliver well-oriented messages that may differ from one group to another.

Practitioners

For each practitioner, the needs are the same. They have to identify risks and understand their scenarios. They must be able to reach a well-informed decision (access reliable information to be integrated in the daily work). They have to adopt a behavior in conformity with the state of security and have a clear line of conduct in case of danger. In case of a crisis, the communication must be mastered. The practitioners must select SAFECARE solutions' components to be communicated to different security events, should be selected based on pre-defined guidelines.

Research and Scientific Community

SAFECARE is particularly pertinent for the scientific research community in the domains of critical infrastructure protection, cybersecurity, privacy and data protection. The latest developments and legal reforms that have occurred in these domains should be analysed from a scientific/academic perspective. Such analysis – that will result in academic contributions, e.g. white papers, conference papers, articles, etc. – will aim at advancing the state-of-art of legal literature and improving the already existing knowledge with respect to the abovementioned domains. The research will also support the: i) provision of guidance for the interpretation of existing and new legal requirements in scope; ii) identification of the main gaps/loopholes of the relevant legislation that may be further addressed by law- and/or policy-makers. Results will be therefore not only beneficial for the scientific research community, but also for any other stakeholder (e.g. public bodies, policy-makers practitioners, private sector, etc.) that may access the relevant guidance and/or information in the research outcomes.

Public/Policy bodies/Standardization bodies

Public Bodies have to identify and deploy a global security model for a better understanding of the situation. A security model dedicated to Health sector's CIs must be created and deployed on the national territory initially, and then on the European one. For better reaction and to limit the impacts of potential risks, only well-known means must be used. To start with, Public bodies have to identify opportunities of getting new tools (such as powerful IT tools), that will be integrated

into their strategy; then it is also important for them to get the correct information (respective to the level of alert) and finally to act accordingly. For the above reasons, they should be aware of results and knowledge gained through SAFECARE, as this can prepare the roadmap for future standardization activities.

As stated in 2015 by the OECD, if "Scientific advice is playing an increasing role in the formulation of policy and decision-making (…)",[5] it is also clear that "the interface between science, politics and society at large can be a treacherous area for both policy-makers and scientists". The needs that can be taken into consideration for the public bodies are quite wide and they require advice coming from the research and scientific community, having also in mind the impact on such action on the civil society**.** Considered as a crucial user of the project outputs, the citizens are often organized into networks that need to be well informed. To enhance their interest, the way of communicating needs to be clear, accessible and usable. The integration of inputs coming from diverse stakeholders can also be used to support the implementation of related projects and initiatives.

Private sector

Private sector stakeholders' needs which will be used to formulate a strategy and plan for dissemination, are described below.

Providers need to be aware of the potential threats and risks (both physical and cyber) in the healthcare domain and implement appropriate security solutions to prevent the risks and to mitigate the adverse impact of some security incidents to the public and their business. It is important for providers to reduce the operational risks to provide better care for the people and to be successful. Security Industry needs insights into risks, context and environment of critical infrastructure in healthcare. It further needs opportunities to validate novel security solutions in such eco-systems.

Suppliers need guidance and insights into security requirements and examples of security solutions proven to be effective in the target context to improve the security provided by their products and services.

Financers need to know how secure and reliable the healthcare systems and services are before they make an investment. Better security and less risk can be viewed as a competitive advantage among providers and suppliers in the healthcare market. Thus, the financers may be interested to know at some level about the best security practices and practical security solutions in the healthcare domain.

Trade unions can benefit from insights to find out if the existing laws are sufficient to address all the physical and cyber security risks and guide them towards improving or even devising new laws in this sector.

Academics and researchers in healthcare or security fields thrive on unsolved problems for new avenues for research or opportunities to validate approaches.

[5] OECD (2015), « Scientific Advice for Policy Making : The role and Responsability of Expert Bodies and Individual Scientists », In OECD Science, Technology and Industry Policy Papers, No.21, OECD Publishing, Paris

Security Managers and Critical Infrastructures Security Liaison Officers (SLO) need to gain knowledge from SAFECARE project outputs into physical and cyber risks management, context and environment of critical infrastructure in healthcare, as it will support them in better assessing and mitigating risks, and allocating properly their resources in the healthcare environment

Critical Infrastructure operators and owners should be aware of SAFECARE outcomes, as they can gain knowledge that might support them in enhancing the protection of critical infrastructures. Also, the decision takers within the critical infrastructures that are not related to the security field (e.g. administrative, financial, marketing, technical, etc.) will help them understand the security needs of their organization and the interconnection/interdependency with the rest of the departments/needs

Law Enforcement Agencies and Emergency Response Agencies should get a better understanding of healthcare security issues (physical and cyber), as this will help them cooperate and keep communities safe. Moreover, it will provide the overall picture and a complete situational awareness in each type of event, as it will enhance their knowledge with specific needs and requirements that the health sector includes (e.g. security/ethical characteristics of personal data within a hospital).

3.3 Identification of Priority Groups

In the next paragraphs, priority groups are identified and specific action plans for the project activities of each target group are provided. For the purpose of SAFECARE, the following three priority groups are identified:

3.3.1 Very Important

This group encompasses those stakeholders that are directly connected with the SAFECARE concept, objectives and expected outcomes. Several dissemination activities with this group will be initiated at the beginning of the project and will continue throughout the project's lifetime. The consortium has identified as members of this group the following target groups:

- Practitioners involved in healthcare services (such as public hospitals, medical practitioners, health professionals, pharmacists and healthcare emergency services),
- Practitioners involved in the security domain (physical and cyber), such as private security organisations, local security agents, Security Operations Centres (SOC) operators, first-responders, police and fire-fighters and civil protection agencies;
- Initiatives, related projects and organizations currently engaged in related research areas for dissemination of project's activities and results, such as ILEAD, FIRE-IN or DARENET, the CNIL (the Commission Nationale de l'Informatique et des Libertés in France), EENA (which is the European Emergency Number Association, and proved to be a valuable source to understand communication between emergency services and citizens), BSI (Bundesamt fuer Sicherheit in der Informationstechnik in Germany) or the ANSSI (Agence nationale de la securité et des systems d'information).

3.3.2 Mid important

This group of stakeholders could have a big impact on SAFECARE, but for different reasons they might not be aware of the project's existence or might not realize its importance. But SAFECARE needs their contributions occasionally.

- Critical Infrastructures owners and operators from other sectors, such as transport, water, energy and telecommunications services and that support the provision of healthcare services
- Scientific community and standardization bodies in order to support the establishment of certification mechanisms
- Private sector: Industry, including SMEs. SAFECARE partners with their networks or contacts with the security industry in Europe have to promote the project and raise awareness to those stakeholders. Important links also need to be made with the European Cyber Security Organisation (ECSO,) and the private end-users of the PPP and the European Organisation for Security (EOS), which is one of the main partners within SAFECARE.

3.3.3 Other Stakeholders

The consortium will identify any opportunity with the following stakeholders for communicating project results throughout the project lifetime:

- Coordinators and key actors of the projects dealing with similar topics, both within the same and other programmes, will ensure visibility and uptake of results, and provide opportunities to receive feedback, share experiences and discuss potential joint problems and issues
- Internal audiences of each Partner's organizations are considered important too. The members of the project consortium will be well informed about the progress of the project. Adequate internal dissemination will also ensure that SAFECARE has a high profile
- Public bodies, such as DG HOME, DG SANTE (Directorate C – Public health, country knowledge, Crisis management, C3: Crisis management and Preparedness in health), REA, National Ministries of Health, Member state Emergency services, DG CONNECT (Directorate D: Policy Strategy and Outreach, Directorate G: Data Policy and Innovation / Directorate H: H3. E-Health, Well-being & Ageing as well as Cybersecurity and Digital Privacy), the European Parliament, the Technical Committee for Cyber Security and ENISA (with a special focus on the critical infrastructures and services: Subtopic health on the security challenges and risks of ICT of the health sector)
- Civil society, such as volunteers organizations or networks that may support healthcare services provision, or the general public in a wide sense.

4. Objectives leading to Key messages

Key messages are the cornerstones of the engagement part. To properly connect with the stakeholders, the messages need to be adapted for their interest and wishes: they have to be customized for each targeted group and relevant to the idea that the consortium wants to share. The key messages will have the following characteristics:

- Clear and simple
- Straight to the point
- Adapted to each audience/stakeholder

For a question of clarity, the communicable outputs and results will be divided and presented per work package together with the corresponding value proposition for each targeted Stakeholders group.

Table 2 Objectives leading to Key messages

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
WP1 Ethics requirements									
Output related to the Ethics requirements									
Achieve the SAFECARE project respecting Ethics requirements	For all the stakeholders: To be sure that all ethic/privacy/legal requirements are covered in each dissemination/communication activity								
WP2 Project Management									
Outputs related to the project management									
Achieve the SAFECARE project toward its objectives (strategic, technical and socio-technical)	To have access to the achievement of SAFECARE objectives	To gain a better understanding of SAFECARE for future influence on policies	To be aware and give feedback on the global protection system and on the tested solutions as such	To have access to opportunities to further improve products/services already tested within SAFECARE	To receive feedback of the achievement of objectives directly relevant for projects or activities		To have access to the achievement of SAFECARE objectives	To gain a better understanding of SAFECARE for future influence on policies	To gain a better understanding of SAFECARE for future influence on policies
WP3 Risk assessment and requirements									
Outputs related to critical assets to improve health services availability									
Product a list of Critical assets (according to the level of confidentiality)	To be able to give feedback on the listed assets from	To have access to the critical assets listed	To be able to give feedback on the listed assets from a scientific point of view				To have access to the critical assets listed	To have access to the critical assets listed	To have access to the critical assets listed

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
Identify requirements with regards to organizational and process-related aspects	To give feedback on the requirements identified and on the process related aspects	To understand the requirements identified and to the process related aspects To take actions on policy/regulations accordingly	To adapt the research to the requirements identified and to the aspects related to the process	To be aware of the requirements identified and of the process-related aspects	To be aware of the requirements identified and of the process-related aspects		To understand the requirements identified and to the process related aspects To take actions on policy accordingly	To understand the requirements identified and to the process related aspects To take actions on policy/regulations accordingly	To understand the requirements identified and to the process related aspects To take actions on policy/regulations accordingly
Outputs related to security and known vulnerabilities									
Analyse the State-of-the art about security and known vulnerabilities	To inform about the vulnerabilities			To be aware of the vulnerabilities declared and identified in the analysis	To be informed about the vulnerabilities identified within SAFECARE		To be aware of the vulnerabilities declared and identified in the analysis	To be aware of the vulnerabilities declared and identified in the analysis	
Explore and list of health and security practitioners' requirements, physical security solutions, cyber security solutions, CM communication and coordination strategies	To define the requirements		To support the definition of the requirements	To be aware of the requirements listed by the practitioners	To be informed of the requirements listed within SAFECARE		To support and be informed of the requirements listed within SAFECARE	To support and be informed of the requirements listed within SAFECARE	To support and be informed of the requirements listed within SAFECARE
Outputs related to the scenarios									
Define the cyber-physical scenarios of threat	To identify and formalize the use-cases and attack scenarios		To support the definition and formalize the use-cases, attack	To understand/ be aware whether the integrated security solutions	To be aware of the outputs of the use-cases		To be aware of the outputs of the use-cases	To be aware of the outputs of the use-cases	To be aware of the outputs of the use-cases

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
	against critical health infrastructure		scenarios and response strategies	should be refined					
Outputs related to Cyber-physical risk assessment and impact analysis									
Analyse Cyber-physical risk assessment and impact	To identify the assets (and context) and identify threats To assess the risks To support the definition of security objectives To propose relevant controls	To be aware of the risk assessment and impact analysis To take appropriate actions in terms of policy/regulations to define security objectives	To provide IT, physical and cyber-security expertise about the scenarios of threats and potential impacts on the target infrastructures	To provide security expertise about the scenarios threat	To be aware of the cyber-physical risk assessment and impact analysis		To be aware of the risk assessment and impact analysis To take appropriate actions in terms of policy to define security objectives	To be aware of the risk assessment and impact analysis To take appropriate actions in terms of policy/regulations to define security objectives	To be aware of the risk assessment and impact analysis
WP4 Physical security solutions									
Outputs related to the specifications of physical security solutions									
Develop a suspicious detection system	To be aware of the possibilities of increased automation in this area	To promote increased use of machine learning-based automation and drive consolidation	To provide examples of leading-edge machine learning techniques making an impact on the real world, and promote further development of the state of the art	To lead the way, as planned in our exploitation strategy, in moving the physical security industry forward in application of machine learning techniques		To promote increased use of machine learning-based automation	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
Develop an Intrusion and fire detection system	To be aware of the possibilities of increased aggregation of these	To promote holistic video of physical security and the advantages of including intrusion and fire detection,	To promote physical security, especially intrusion and fire detection, as a fertile area	To lead the way, as planned in our exploitation strategy, in moving the physical	The partners are already moving toward providing an open platform in	To be aware of the possibilities of increased aggregation of these	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
	(fire and intrusion) systems	and promote standardizatio n through bodies to which partners are already members, e.g. OSSA	of application for state of the art techniques	security industry forward in aggregation of intrusion and fire detection	which intrusion detection can be integrated and will provide for integration of fire detection	(fire and intrusion) systems			
Develop data collection from physical subsyste ms	To be aware of the possibilitie s of increased aggregatio n from these (ICS, SCADA and smart building) systems	To promote holistic video of physical security and the advantages of including other physical sensors/syste ms and promote standardizatio n through bodies to which partners are already members, e.g. OSSA	To promote physical security, especially in the rapidly developing smart building context, as a fertile area of application for state of the art techniques	To lead the way in moving the physical security industry forward in aggregation of further sensors and recent development in smart building technology		To promote holistic video of physical security and the advantages of including other physical sensors/sy stems	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
Develop a Ubiquitou s services for integrated alert system	To be aware of how a domain (health) specific mobile interface can increase usability of usefulness of alerting	To promote accessibility of holistic physical security and its adoption especially in the healthcare domain	To lead the way in demonstrati ng best practice in terms of directly addressing to beneficiaries of this type of research, as exemplified by our healthcare use case	To lead the way, as planned in our exploitation strategy, in providing for interfaces that target particular domains, as exemplified by our healthcare use case	The partners already provide an SDK for tailored mobile interface developme nt, the SafeCare tasks in this WP will elaborate further possibilitie s		To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
Build a threat monitorin g system	To be aware of how aggregatio n of video,	To demonstrate that a holistic approach to physical	To demonstrate that bringing together the different	To demonstrate the commercial opportunitie	To be aware of the existence of the		To be aware of such a tool and see its potential	To be aware of such a tool and see its potential	To be aware of such a tool

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
	intrusion, fire and other sensors/systems can lead to increased automation with respect to physical security	security is feasible and beneficial and promote standardization through bodies to which partners are already members, e.g. OSSA	areas of physical security provide a fertile ground for research,	s in bringing together the different aspects of physical security and targeting a specific domain.	threat monitoring system built within SAFECARE		impact on the market	impact on the market	
WP5 Cyber security solutions									
Outputs related to the specifications of cyber security solutions									
Develop the IT threat detection system	To be aware of such a tool that detects anormal behaviours on IT systems	To update on the state of the art and potential of such a tool that uses machine learning algorithms to detect abnormal behaviours	To be able to access additional information for improving threat scenarios and detection To update on the state of the art and potential of such a tool that uses machine learning algorithms	To be aware of such a tool that improves the detection of zero-day attacks	To be aware of such a tool that and the use of machine learning algorithms	To be aware of such a tool that uses AI to ensure the safety of critical health infrastructure	To be aware of the potential of such a tool that can enhance the protection of critical infrastructure	To be aware of the potential of such a tool that can enhance the protection of critical infrastructure	To be aware of such a tool that can enhance the protection of critical infrastructure
Develop the BMS threat detection system	To be aware of such a tool that detects anormal behaviours on BMS systems	To update on the state of the art and potential of such a tool that uses machine learning techniques to detect abnormal behaviours	To update on the state of the art and potential of such a tool that uses machine learning techniques	To be aware of such a tool that improves the detection of attacks on IoT devices	To be aware of such a tool that and the use of machine learning techniques	To be aware of such a tool that uses AI to ensure the safety of critical health infrastructure	To be aware of the potential of such a tool that can enhance the protection of critical infrastructure	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
Develop the Advanced file	To make aware of such a tool that takes into account	To update on the state of the art and potential of such a tool that performs	To update on the state of the art and potential of such a tool that	To be aware of such a tool that demonstrates its effectiveness	To be aware of such a tool that takes into account	To be aware of such a tool that contribute to the	To be aware of the potential of such a tool that an enhance the	To be aware of the potential of such a tool that an enhance the	To be aware of the potential of such a tool that an enhance the potential of

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
analysis system	health-related file formats	static, heuristic and dynamic analyses and can be directly connected to IT and BMS probes to analyze as many files as possible	performs static, heuristic and dynamic analyses and uses specific techniques to improve the detection of threats related to the medical domain	to detect threats related to the medical domain	health-related file formats and can be directly connected to IT and BMS probes	safety of critical health infrastructure	potential of critical infrastructure	potential of critical infrastructure	critical infrastructure
Develop the E-health device security analytics	To be aware of the potential of security monitoring and analytics of equipment.	To update on the state of the art and potential of such approach	To update on the state of the art and potential of such approach	To demonstrate progress in the state of the art of such approach	To update on the state of the art and potential of such approach	To inform and assure that such state of the art approaches contribute to safety and security	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
Develop the Cyber threat monitoring system	To be aware of such a tool that takes into account physical and cyber impacts to display potential cascading effects	To update on the state of the art and potential of such a tool that takes into account physical and cyber impacts to display potential cascading effects	To update on the state of the art and potential of such a tool that takes into account physical and cyber impacts to display potential cascading effects	To make aware of such a tool that takes into account physical and cyber impacts to display potential cascading effects	To be aware of such a tool that takes into account physical and cyber impacts to display potential cascading effects	To be aware of such a tool that contribute to the safety of critical health infrastructure	To be aware of the potential of such a tool that an enhance the potential of critical infrastructure	To be aware of the potential of such a tool that an enhance the potential of critical infrastructure	To be aware of the potential of such a tool that an enhance the potential of critical infrastructure
WP6 Integrated cyber-physical security solutions									
Develop the impact propagation and decision support model	To be aware of the existence of such a tool	To be aware of such a tool	To be aware of the existence of such a tool	To be aware of such a tool and see its potential impact on the market	To be aware of the existence of such a tool developed within SAFECARE		To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
Develop Threat Response and alert system	To be aware of the existence of such a tool	To be aware of such a tool	To be aware of the existence of such a tool	To be aware of such a tool and see its potential impact on the market	To be aware of the existence of such a tool developed within SAFECARE		To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
Develop the Hospital availability management system	To be aware of the existence of such a tool	To be aware of such a tool	To be aware of the existence of such a tool	To be aware of such a tool and see its potential impact on the market	To be aware of the existence of such a tool developed within SAFECARE		To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
Develop the E-heal security risk management model	To be aware of identified vulnerability impact on confidentiality, integrity and availability of critical assets	To be aware of identified vulnerability impact as input for potential follow up action when needed	Use the results for further vulnerability analysis and related mitigations	Use the results in risk assessments in order to define corrective and/or preventive measures	To compare with their models and reach a more realistic quantification of impact, also in different sectors.	To be aware of identified vulnerability impact on confidentiality, integrity and availability of critical assets	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool and see its potential impact on the market	To be aware of such a tool
WP7 Tests and demonstrations									
Outputs related to the test platform									
Build a test platform for the validation of prototypes				To be aware of such a tool and see its potential impact of the market			To be aware of such a tool and see its potential impact of the market. Also to take part in the respective task or get lessons learned	To be aware of such a tool and see its potential impact of the market. Also to take part in the respective task or get lessons learned	To be aware of such a tool. Also to take part in the respective task or get lessons learned
Outputs related to the Test bed and demonstrations									
Product a test bed for	To give feedback on the new		To give feedback on the new test	To analyse potential use of the test-	To be aware of the		To be aware of such a tool and see its	To be aware of such a tool and see its	To be aware of such a tool. Also to take

	Practitioners	Public /Policy bodies/Standardization bodies	Scientific and Research community	Private sector	Related projects and initiatives	Civil society	Security Managers and owners and Security Liaison officers (LSO)	Critical Infrastructure operators	Law Enforcement Agencies and Emergency Response Agencies
monitoring the behavior of medical devices in case of cyber attack	test bed developed from a technical point of view		bed developed from a scientific point of view	bed on the market	existence of such tool		potential impact of the market. Also to take part in the respective task or get lessons learned	potential impact of the market. Also to take part in the respective task or get lessons learned	part in the respective task or get lessons learned
Conduct of project pilots in Turin, Marseille and Amsterdam	To be aware and to give feedback of tested solutions		To be aware of the scientific benefits of the solutions tested	To be aware of the benefits of the solutions tested To be able to take a decision by using a solution on the market	To be aware of the benefits of the solutions tested		To be aware of such a tool To take part in the respective task or get lessons learned	To be aware of such a tool and see its potential impact of the market To take part in the respective task or get lessons learned	To be aware of such a tool To take part in the respective task or get lessons learned
WP8 Dissemination, exploitation and Standardization									
Outputs related to the D&C strategy									
Product D&C means	To be aware of the main results and objectives of the project	To be aware of the main results of the project To have the opportunity to improve actual policy and/or regulations	To be aware of the main results of the project To have the opportunity to give feedback on the solutions a technical point of view	To be aware of the main results of the project and take a position on the market	To be aware of the main results of the projects and avoid duplication of work		To be aware of the main results of the project	To be aware of the main results of the project To learn how to interact with the tools put in place	To be aware of the main results of the project
Outputs related to business plan									
Product the business plan for the marketability of the system developed	To be able to use the solutions/ Systems developed	To have the opportunity to adapt the policy/regulations according to the outputs of the solutions	To be aware of the sustainability of the solutions developed	To have access to the solutions/systems developed	To be aware of the sustainability of the solutions developed		To be able to use the solutions/Systems developed	To be able to use the solutions/Systems developed	To be able to use the solutions/Systems developed. To have the opportunity to adapt the policy/regulations according to the outputs of the solutions

5. Dissemination and Communication means towards engagement

5.1 Dissemination strategy: main means

The online and offline dissemination means will serve common objectives: to create awareness and to engage with stakeholders already identified. Several channels and tools will be described here, as well as the right timing to use them.

The purpose of the following section is to provide an overview of the means that will be used throughout the project lifetime.

5.1.1 Online means

The SAFECARE Project Website

The establishment of a website is crucial in terms of communication. It has a clear impact on the visibility and enhance public engagement as it will be widely accessible by the public and by various platforms.

SAFECARE has its own dedicated website (www.safecare-project.eu, online since October 2018 - M2), having the same graphical identity as the communication tools used within the project as well as representing one of the main tools of the SAFECARE Dissemination and Communication Strategy. Showing an attractive style, the website is modern, using latest state-of-the art functionalities offered by WordPress, it is also optimized for the search engines and ISEP, in charge of providing the website structure, and will include a Google analytics code to monitor user and activities and provenance.

The website serves as both promotional and information tool. On a regular basis, the content of the website will be updated to share the most relevant news, the relevant upcoming events, sponsored or attended by SAFECARE as well as the project outcomes and main achievements. The website will also store and make project resources and publications available to general and specialized reviewers.

Meant to be user friendly, the website is divided into several categories (and subcategories):

1- The Homepage gives a clear overview of the project: "*About SAFECARE*"
2- The description of the consortium of Partners, with their websites and contacts details
3- The resources page, making available all the Public deliverables, the publications and dissemination material. An authentication to access the private documents sharing tool (iPortalDoc) is also included here
4- The news & Events page shares with the reader the most recent information about what is happening in the frame of SAFECARE but also in the frame of the Critical Health Infrastructure Ecosystem
5- The contacts page includes the contact details of the coordinator and technical coordinator of SAFECARE

Figure 1 Homepage of SAFECARE website

Online Media Strategy

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.

The regular sharing of important information related to SAFECARE activities and outputs through media at local, national and international levels will allow the partners to invite the relevant media to the major events. The idea here is to raise interest among the critical health infrastructure community and civil society in general; the consortium using the key messages, beforehand tailored for the pre-identified media. On that purpose a list of online media will be internally established and regularly updated by the Consortium partners (including Local, national, regional and international, general or specialized media).

Electronic contacts

SAFECARE partners must directly be in touch with relevant stakeholders about the project's outputs. This can easily be done by email, using an established database and mailing list. Crucial is to first use already built contacts from the consortium partners, hence establish the stakeholders' engagement on already strong connections.

5.1.2 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: 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. Thanks to this, they are made accessible to a wide audience.

Project publications

Key project findings will be disseminated by the consortium through publications in specialized magazines. Based on specific results, the publications will be linked, amongst other, to the definition of the cyber-physical scenarios of threat, to the analysis of ethics, privacy and confidentiality constraints, to the specification of suspicious behavior detection system, to the specifications of data collection system, to the specification of the mobile alerting system, to the specification of the cyber-physical Building monitoring, to the specifications of the IT threat detection system, to the specification of the advanced file analysis system, to the specification of the E-health devices security analytics.

Third party publications

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.

External channels

SAFECARE's results and activities will be shared on several external websites for awareness purposes. Some of the tools used for dissemination purposes will also be used for communication purposes.

These channels are listed below:

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

On top of that, SAFECARE's partners will contribute on a regular basis to targeted blogs with articles and notes 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 will be put in place to support the consortium in the organization of two main types of events (awareness events and commercial events).The Mass media campaign will be linked to the social media strategy (developed below) and will be divided into three main phases: Before, during and after the event.

Awareness events:

Two awareness events, entirely dedicated to the promotion of SAFECARE and its impact to stakeholders external to the project, will be organized: one in Belgium taking place at KUL's premises at M13 but organized by EOS, one in Athens taking place at KEMEA's premises at M21.

➔ *Awareness event in Leuven at M13 (EOS is the responsible partner)*

M10: Promotional Tools are ready. Invitation letters are created and sent as well as logistics pack (EOS is responsible)

M11: Press Release announcing the event is sent (EOS is responsible)

M11-13: Information about the AE provided on SAFECARE website and opening of registration (EOS is responsible)

M11-13: Start of the Social Media campaign about the AE (EOS is responsible with the support of the consortium)

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

➔ *Awareness event in Athens at M21 (KEMEA is the responsible partner)*

M18: Promotional Tools are ready. Invitations letters are created and sent as well as logistics pack (EOS and KEMEA are responsible)

M19: Press Release announcing the event is sent (EOS is responsible, with the support of KEMEA)

M19-21: Information about the AE provided on SAFECARE Website and opening of registration (EOS is responsible)

M19-21: Start of the Social Media Campaign about the AE (EOS is responsible, with the support of the Consortium)

M22: Press Release summarizing the main outputs is sent (EOS is responsible, with the support of KEMEA)

Commercial events:

Two commercial events, allowing industrial partners and SMEs to find customers and to refine their business plan, will take place at the end of the project: one in Elancourt organized by Cassidian at M34 and one in Brussels organized by EOS at M35.

➔ *Commercial Event in Elancourt at M34 (CCS is responsible)*

M31: Promotional Tools are ready. Invitation letters are created and sent as well as logistics pack (EOS and CCS are responsible)

M32: Press Release announcing the CE is sent (EOS is responsible, with the support of CCS)

M32-34: Information about the CE provided on SAFECARE website (EOS is responsible)

M32-34: Start of the Social Media Campaign about the CE (EOS is responsible, with the support of the consortium)

M35: Press Release summarizing the main outputs is sent (EOS is responsible, with the support of CCS)

➔ *Commercial Event in Brussels at M35 (EOS is responsible)*

M32: Promotional Tools are ready. Invitation letters are created and sent as well as logistics pack (EOS is responsible)

M33: Press Release announcing the commercial event is sent (EOS is responsible)

M33-35: Information about the CE provided on SAFECARE website (EOS is responsible)

M33-35: Start of the Social Media Campaign about the CE (EOS is responsible, with the support of the consortium)

M36: Press Release summarizing the main outputs is sent (EOS is responsible)

5.1.3 Dissemination via events

A clear distinction has to be made between events organized in the frame of SAFECARE and those related to its objectives, called external events.

SAFECARE events

The events organized in the frame of the project are a clear opportunity to disseminate project results and outputs and to receive interesting feedback from targeted stakeholders attending the events.

As described below, the two main types of events (Awareness events and Commercial events) will involve both SAFECARE partners and external stakeholders, providing also a perfect ground for sharing meaningful ideas, initiating valued discussion, hence enhancing the qualitative implementation of SAFECARE.

Third Party events

Being present and actively involved in third party events (organized by related EC funded projects, or by the security community in general) is clearly important in terms of networking. SAFECARE partners will be attending events related to their specific field of expertise. The partners involvement in such beforehand targeted events will increase SAFECARE's visibility and impact, develop synergies with related initiatives and strengthen engagement with targeted stakeholders. In addition, they will identify market potential.

5.1.4 Interactions with relevant projects

Interactions between SAFECARE and relevant targeted projects is meant to create long-term collaborations which could be very difficult to reach otherwise, this will encourage enriching exchanges. The main objectives will be the increase of SAFECARE visibility and the maximization of its impacts. One other important point will also be to avoid work duplication (issue that can happen very easily) by sharing knowledge, experience, best practices and lessons learnt coming from the project itself and the related topics in general.

The interaction with relevant projects can be seen as a mutual promotion of events and news, mutual invitation to participate and give presentations at project workshops, joint organization of events, formal or informal exchange of feedback.

5.2 Communication means

According to the EC, "*Commmunication* requires strategic and targeted measures for communicating about the action and its results to the multitude of audiences, including the media and the public, possibly engaging in a two-way exchange".[6]

[6] The European IPR Helpdesk - https://www.iprhelpdesk.eu/sites/default/files/EU-IPR-Brochure-Boosting-Impact-C-D-E_0.pdf , consulted on the 25th of October

Besides the "public disclosure of the project results (…) including by scientific publications in any medium[7]" amongst targeted people, it is crucial to make an effort towards communicating project information to a broad public, including civil society and media.

5.2.1 Visual materials

The SAFECARE visual identity is 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 will be designed by EOS and will be available for use at M3:

- Two SAFECARE roll-up banners to be used during project events and events SAFECARE will participate in[8]
- Promotional brochures with the description of main results and success stories, both in soft and hard copies, to be shared online and during events and conferences if needed
- Flyers to be disseminated during events in general, 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.
- Videos, to be developed

5.2.2 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.

SAFECARE website is intended to serve as a main dissemination as well as communication tool.

5.2.3 SAFECARE social network and social media strategy

Nowadays, developing a strategy for social network and social media is crucial as most of the actors in the security field are using such media. This is most probably explained by the necessity to get and receive the information as fast and as simply as possible.

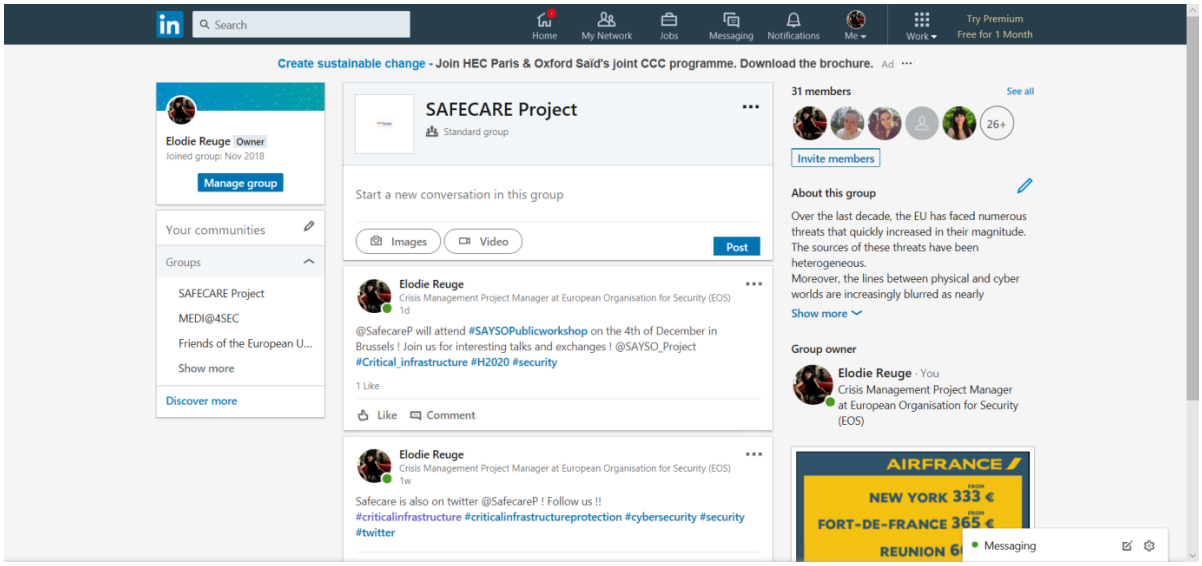
Social Media also tends to enhance a more concrete level of exchange than a simple website, giving an impression of proximity. Social Media Platforms give to the reader the opportunity to "stay in touch" and their use by different stakeholder groups will raise SAFECARE's presence online by the frequency of their interactions. SAFECARE Social Media Channels are operational since October 2018 (M2).

A **LinkedIn Group,** called SAFECARE Project; has been set up, with the main aim to share and promote SAFEARE activities with the different stakeholders connected: practitioners, industry representatives or research and scientific networks. It is managed by EOS with the inputs of the consortium.

[7] The European IPR Helpdesk - https://www.iprhelpdesk.eu/sites/default/files/EU-IPR-Brochure-Boosting-Impact-C-D-E_0.pdf , Consulted on the 25th of October

[8] 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.

Figure 2 Screenshot of the LinkedIn Group



Through a **Twitter account**, @SafecareP, an insight of the SAFECARE's immediate activity is shared with the "Followers"/stakeholders. Twitter is well known to engage with a wide audience on hour-to-hour basis and raise an instant interest on the stories shared. The content of the SAFECARE twitter account needs to be updated regularly and relevant Hashtags are used to enhance the visibility of the Tweets (#SafecareP, #criticalinfrastructure, #healthinfrastructure, #Criticalheathinfrastructure, #healthcare, #e-health, # Criticalassets etc…).

Figure 3 Screenshot of the Twitter Account @SafecareP

The platforms **LinkedIn** and **Twitter** will also be used to promote the 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).

5.2.4 Newsletters

Every six months, SAFECARE newsletter will be shared to the partners, presenting the projects achievements from the past six months and the upcoming activities of the six months to come. Following the tailoring of the website, the newsletter presentation should be dynamic and well formatted:

- It shouldn't exceed 1000 characters including spaces to avoid losing interest of the reader.
- Each division of the newsletter should have understandable and easily reachable tittle and content (no abbreviations or very technical terms should be used)
- Visualisation is crucial and pictures or meaningful graphs should be included whenever it is possible
- The newsletter will be shared in the following two ways:
    - Mailchimp: creating a Mailchimp account will facilitate the registration of interested stakeholders
    - The newsletter will also be shared through each partners network, and in that sense reach an audience that wouldn't have been aware of SAFECARE otherwise.

5.2.5 Press releases

Press releases will also be shared to raise interest in SAFECARE activities. They will be produced at a specific moment and not on a regular basis.

- To communicate about an event, before (date, location, description of the event) and after (to describe results and outcomes and inform on the next event)
- If needed, when a specific milestone is achieved

Following the same ideas than the ones developed for the Newsletter, the following guidelines should be observed:

- It shouldn't exceed one page (A4 format) to avoid losing the interest of the reader
- Each division of the newsletter should have understandable and easily reachable tittle and contents (no abbreviations or very technical terms should be used)
- Visualisation is crucial and pictures or meaningful graphs should be included whenever it is possible

It will be sent using the MailChimp system to the targeted media.

5.3 SAFECARE communication policy

SAFECARE consortium will promote the project, its objectives and results, by sharing targeted messages to a wide audience. This needs to be done according to a strategic and well defined way. Partners will be asked to communicate with interested stakeholders with the final objective being to serve SAFECARE's interests.

What is important is to say that any communication activity led by partners has reflect only the author's point of view and that neither the European Commission nor the Research Executive Agency is responsible for any use that may be made of the information it contains.

Any kind of communication activities should also be reported in the Initial dissemination and Communication report to be submitted at M13 and in the final dissemination and communication

report to be submitted at M35. All external communications should refer to the Grant Number (787002) and use the project visual identity and the European flag.

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.

6. Monitoring and Evaluation process to apply

The stakeholders' Engagement strategy's (defined above) main challenge is to reach the appropriate level of engagement from them and serve SAFECARE objectives.

It is now crucial to present the set of Key Performance Indicators (KPI) defined in the current Dissemination and Communication Strategy. Being the cornerstone of the strategy's assessment, they will need to be constantly reviewed and adapted. Presented in the table below, the KPIs will be established until M13 and then updated in D8.2 Initial Dissemination and Communication Report.

Table 3 KPIs

Key Performance Indicators			Target at M13		
			Level of performance		
Dissemination and Communication tools	**Definition of the indicator**	**Type of data required**	**Poor**	**Good**	**Excellent**
Project Website	Number of visits per month	Google analytics	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
	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
	Average time spent on website		Less than 45 seconds	45 seconds -2min	More than 2min
	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
	Number of posts relayed on partner's internal websites		Less than 250 at M13	250- 450 at M13	More than 450 at M13
	Number of downloads of project reports		Less than 15 at M13	15-50 at M13	More than 50 at M13
Social Media Strategy	Subscribers of the LinkedIn Group	LinkedIn Group Statistics dashboard	Less than 150 at M13	150-250 at M13	More than 250 at M13
	Number of discussion groups on LinkedIn		Less than 5 at M13	5-10 at M13	More than 10 at M13
	Number of Twitter followers	Twitter analytics	Less than 250 at M13	250-450 at M13	More than 450 at M13
	Number of tweets per month		Less than 15	15-30	More than 30
	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	Proceedings	Less than 1	1-2	More than 2
	Number of clicks to open newsletter (for each newsletter)	Google analytic	Less than 100	100-200	More than 200

	Number of subscriptions obtained after each Newsletter release		Less than 13	13-28	More than 28
	Size of the dissemination list	Proceedings	Less than 200	200-400	More than 400
Media campaign, including publications in scientific journals, e-Newsletters and other media	Number of scientific papers submitted	Proceedings	Less than 5	5-10	More than 10
	Number of external websites, e-Newsletters, journals used for dissemination of project outcomes/outputs		Less than 15	15-30	More than 30
	Number of Media partnerships concluded		Less than 3	3-6	More than 6
Contributions to external events	Number of external events in which SAFECARE participates	Proceedings	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
	Number of abstracts/papers submitted and selected		Less than 6 at M13	6-18 at M13	More than 18 at M13
	Copies of the brochure/factsheet distributed		Less than 300 at M13	300-800 at M13	More than 800 at M13
Focus Group	Number of Focus Groups organised	Events timeline	2	2	2
	Number of Tweets during the event	Twitter analytics	Less than 5	5-10	More than 10
	Number of online articles making reference to Focus Groups	Google analytics	Less than 2	2-7	More than 7
Awareness Event (M13 in Leuven)	Number of participants Countries of origin	List of attendees	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 %)	Proceedings	20%	20%-30%	More than 30%
	Number of Tweets during the event	Twitter analytics	Less than 6	6-12	More than 12
	Number of online articles making reference to the awareness event	Google analytics	Less than 5	5-10	More than 10
	Number of hits on the event page		Less than 100	100-200	More than 200
Liaison activities and synergies	Number of relevant projects/initiatives identified and contacted/invited at project events	List of attendees	Less than 8	8-20	More than 20

	Number of relevant organisations/communities /experts identified and contacted/invited at project events		Less than 20	20-50	More than 50
	Number of MoU signed and/or concrete collaboration activities initiated with related initiatives/projects	Proceedings	Less than 10	10-20	More than 20
	Number of cooperation activities (common events and other clustering activities)	Proceedings	Less than 1	2-5	More than 5
Link to the Community of Users	Number of SAFECARE presentations made during plenary meetings and thematic workshops	Proceedings	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
Impact towards Policy Makers	Number of bilateral meetings with Policy makers	Agenda	0-1 at M13	2-4 at M13	More than 4 at M13
	Presentations made during events gathering policy makers	Proceedings	Less than 2 at M13	2-5 at M13	More than 5 at M13
Promotional material	Number of brochures produced	Proceedings	500 brochures at M13	650 brochures at M13	800 brochures at M13
	Number of brochures distributed		400 brochures at M13	600 brochures at M13	750 brochures at M13

Annexes

Annex 1 – SAFECARE Logo and Visual identity

Several points need to be taken into consideration:

1- Orientation: The logo must remain horizontal . any inclination, even minimal, is prohibited. The different elements cannot be divided, separated .
2- Restrictions: Visual effects (gradients, volumes, shadows) are also prohibited.
3- Colors:

Primary	Grayscale
#999999 RGB: 153, 153, 153 CMYK: 43, 35, 35, 1	#999999 RGB: 126, 126, 126 CMYK: 52, 44, 44, 8
#3584c5 RGB: 53, 132, 197 CMYK: 77, 41, 0, 0	#6c6d6d RGB: 108, 109, 109 CMYK: 58, 49, 49, 16

Annex 2: List of external events

INTERNATIONAL / EUROPEAN External Publications			
Name of the event	**Description**	**Date**	**Location**
13th International Conference on Critical Infrastructure Security (CRITIS)	CRITIS 2018 presents innovative research and exploring new challenges in the field of critical (information) infrastructure protection (C(I)IP) and fostering the dialogue between all C(I)I stakeholders. CRITIS 2018 aims at bringing together researchers and professionals from academia, C(I)I operators, industry, defence sector and governmental organisations working in the field of the security of critical (information) infrastructures.	24th-26th of September 2018	Kaunas, Lithuania
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.	2nd – 4th of October 2018	The Hague, Netherlands
European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIC)	European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS) is an annual research event addressing the IS discipline with 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.	4th – 5th of October 2018	Limassol, Cyprus
European Brokerage Event on Resilience from disaster	http://www.seren-project.eu/index.php/events/future-events/87-european-brokerage-event-on-resilience-from-disaster-2019	24th October 2018	Paris, France

(H2020 SU-DRS)			
2nd Europol ENISA Internet of things security conference	https://www.enisa.europa.eu/events/2nd-europol-enisa-iot-security-conference	24th - 25th October 2018	Hague, Netherlands
The European Cyber Week (ECW)	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.	19th – 22th of November 2018	Rennes, France
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 we face. 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.	3rd – 4th of December 2018	Brussels, Belgium
ICT 2018	This research and innovation event will focus on the European Union's priorities in the digital transformation of society and industry. It will present an opportunity for the people involved in this transformation to share their experience and vision of Europe in the digital age.	4-6 December 2018	Vienna, Austria
Security Research Event (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	5th – 6th of December 2018	Brussels, Belgium

	security research in Europe, and where a selection of EU funded security-related projects are displayed in a large exhibition area. Under the theme "Making Europe a safer place - demonstrating the impact of EU-funded security research", SRE 2018 will demonstrate the strength and inspiring results of security related research and innovation activities. The event will bring together 800 participants, representing a wide range of security stakeholders: researchers, industry representatives, public security providers and practitioners (i.e. fire departments, police, border guards, intelligence agencies, etc.), as well as policymakers from across Europe.		
Black Hat Europe 2018	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.	3rd-6th December 2018	London, UK
International Confernce In Information Security and Digital Forensics	International Conference In Information Security And Digital Forensics focuses on Anti-Forensics and Anti-Anti-Forensics Techniques, Data leakage, Data protection and Database forensics, Executable Content and Content Filtering, Forensics of Virtual and Cloud Environments, Investigation of Insider Attacks, Malware forensics and Anti-Malware techniques, New threats and Non-Traditional approaches, Business Continuity & Disaster Recovery Planning, Critical Infrastructure Protection, Digital Rights Management and Intellectual Property Protection, Fraud Management, Laws and Regulations Threats, Vulnerabilities, and Risk Management etc.	7th – 9th of December 2018	Thessaloniki, Greece

14th International Conference on Information Assurance and Security	The conference is expected to provide an opportunity for the researchers to meet and discuss the latest solutions, scientific results and methods in solving intriguing problems in the fields of IAS. The conference programme will include workshops, special sessions and tutorials, along with prominent keynote speakers and regular paper presentations in parallel tracks. Like previous years, we expect the IAS 2018 proceedings to be published by Springer subject to fulfilling of all quality requirements of Springer.	13th – 15th of December 2018	Porto, Portugal
International Cybersecurity Forum (FIC 2019)	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	22nd – 23rd January 2019	Lille, France
International Cybersecurity Forum (FIC 2019)	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 tradeshow, 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	22nd-23rd January 2019	Lille, France

	our network of experts and like minded throughout the year		
12th International Conference of Health Informatics (HEALTHINF 2019+)	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 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.	22nd – 24th of February 2019	Prague, Czech Republic
13th Annual IFIP WG 11.10 International conference 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 twelve conferences, the Thirteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will again provide a forum for presenting original, unpublished research results and	11th – 13th of March 2019	Arlington, USA

	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.		
Paris Healthcare Week 2019	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.	21st – 23rd of May 2019	Paris, France
International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2019) Theme – Cyber Situational Awareness for Predictive Insight and Deep Learning	IEEE is the Technical Co-Sponsor (TCS) of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2019), an international refereed conference dedicated to the advancement of the principles, methods and applications of situation awareness on Cyber Systems, Business Information Systems (BIS), Computer Network Defence (CND), Critical National Infrastructures (CNI), Cyber Physical Systems (CPS) and Internet of Things (IoTs). The aim of the CyberSA 2019 is to encourage participation and promotion of collaborative scientific, industrial and academic inter-workings among individual researchers, practitioners, members of existing associations, academia, standardisation bodies, and including government departments and agencies. The purpose is to build bridges between	3-4 June 2019	Oxford, UK

	academia and industry, and to encourage interplay of different cultures. This conference is co-located with: International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2019); International Conference on Cyber Incident Response, Coordination, Containment & Control (Cyber Incident 2019)		
IoT Week 2019	https://iotweek.org/	17-21 June 2019	Aarhus, Denmark
CEBIT 2019	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.	24 - 28 June 2019	Hannover, Germany
ICT systems Security and Privacy Protection – IFIP SEC 2019 (IFIP)	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 we are facing today and will be facing in the future.	25th – 28th of June 2019	Lisbon, Portugal
2019 ICON-S Conference "Public Law in Times of Change?"	Countries around the world are witnessing the reversal of longstanding democratic gains, and new authoritarian threats. Yet there are signs of resilience in the global and national public law order: popular referenda have delivered gains as well as losses for democracy; women and young people have marched in defence of public law values; and justice is being crowd-sourced and data-driven, not just undermined by foreign cyber-attacks and "fake news". Under the strain of technological changes and shifts in economic globalisation, the world is also confronting large-scale changes in the structure and scope of global governance and of the "administrative" state. The Welfare State is under "siege" and	1-3 July 2019	Santiago de Chile, Chile

	at both international and domestic levels the problem of economic injustice is dominating the political and socio-economic debate around the globe.		
International Conference on Informatics, Management and Technology in Health Care (ICIMTH)	TBC	5th – 7th of July 2019	Athens, Greece
32th IEEE CBMS International Symposium Computer-Based Medical Symposium	Attracting a worldwide audience, CBMS is the premier conference for computer-based medical systems, and one of the main conferences within the fields of medical informatics and biomedical informatics. CBMS allows the exchange of ideas and technologies between academic and industrial scientists. The scientific program of IEEE CBMS 2019 will consist of regular and special track sessions with technical contributions reviewed and selected by an international programme committee, as well as, keynote talks and tutorials given by leading experts in their fields. The CBMS 2019 edition also aims to host high-quality papers about industry and real case applications as well as allow to researchers leading international projects to show to the scientific community the main aims, goals and results of their projects.	5th – 7th of July 2019	Cordoba, Spain
Biomedical Engineering ranging from wellness to intensive care	The IEEE Engineering in Medicine and Biology Society is pleased to announce the 41st International Engineering in Medicine and Biology Conference, to be held in Berlin, Germany from July 23–27, 2019. The overarching theme is "Biomedical engineering ranging from wellness to intensive care". Consistent with our theme, we have arranged plenary keynotes from leading academic and industrial scientists, who will present aspects of innovation and translational engineering in biomedicine.	23rd – 27th of July 2019	Berlin, Germany

	The scientific tracks will cover the standard topics of the EMBS technical committees. Beside the scientific sessions, the congress exhibition will show biomedical companies, start-ups, biomedical institutes, universities, and provide networking opportunities for engineers, clinicians, other scientists, entrepreneurs and students. Cutting-edge research and innovation in biomedical engineering, healthcare technology and medical informatics will all be covered in this large conference. The conference program consists of mini symposia, workshops, invited sessions, oral and poster sessions, sessions for students and young professionals, sessions for clinicians and entrepreneurs, and a large exhibition. The conference will be held in Berlin, which is currently developing a major healthcare hub in Germany with three universities, the Berlin Institute of Health (BIH), Healthcapital, and more than 100 regional companies active in the healthcare business.		
The 17th World Congress of Medical and Health Informatics	Branded by the International Medical Informatics Association (IMIA), MedInfo is a worldwide key event in digital health that gathers scientists, physicians, teachers, students, companies, institutions, and decision-makers. After having hosted its previous editions in Brazil and China, in 2019, MedInfo is back to Europe. For the first time, the event will be held in France, in Lyon, also called the "French Tech metropolis". The city is located in the heart of the Auvergne-Rhône-Alpes region, which also happens to be a major player in health technologies.	26th – 30th of August 2019	Lyon, France
24th European Symposium on Research in Computer Security	TBC	September 2019 (TBC)	TBC

(ESORICS 2019)			
International Defense and Homeland Security Wokrshop (DHSS 2019)	TBC	September 2019 (TBC)	TBC
Internet and Mobile World (IMWORLD 2019)	Support Southeast European business environment to adopt digitisation in all industries to increase efficiency and productivity. We all know that digital transformation is no longer a matter of "if," but "when". IMWorld's role is to speed up the process and make it more accessible both through the know-how delivered by the brightest minds in tech and the IT & digital solutions providers.	2-3 October 2019	Bucharest, Romania
Smart City Expo World Congress 2019	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 November 2019	Barcelona, Spain
OWASP Bucharest AppSec Conference 2019	The objective of the OWASP's Bucharest AppSec Conference is to raise awareness about application security and to bring high-quality security content provided by renowned professionals in the European region. Everyone is free to participate in OWASP and all our materials are available under a free and open software license.	TBC	Bucharest, Romania
ICT 2019	This research and innovation event will focus on the European Union’s priorities in the digital transformation of society and industry. It will present an opportunity for the people involved in this transformation	TBC	TBC

	to share their experience and vision of Europe in the digital age.		

Annex 3 – SAFECARE Partners social media account

Partners	Linkedin		Twitter	
	Account	Subscribers	Account	Followers
APHM	APHM LinkedIn	10023	@aphm_actu	4943
CCS	Airbus CyberSecurity LinkedIn	4698	@AirbusCyber	1068
UG	UG LinkedIn	6652	@wissen_lockt	2781
ENC	ENC LinkedIn	2175	@enovacom_fr	922
SPF	SPF LinkedIn	13209	@santeprevention	53.8K
ISEP	ISEP LinkedIn	24941	N/A	N/A
CNAM	CNAM LinkedIn	129850	@LeCnam	11.2k
KUL (CITIP)	N/A	N/A	@CiTiP_KULeuven	1004
ISMB	ISMB LinkedIn	1263	@IsmbOnweb	2265
CSI	CSI Piemonte LinkedIn	4453	@csipiemonte	2312
ASLT05	N/A	N/A	N/A	N/A
EOS	EOS LinkedIn	708	@EOS_EU	637
AMC	AMC LinkedIn	46006	@VUmcAmsterdam	19.4K
MS	Milestone Systems	21960	@milestonesys	14409
SM	Security Matters LinkedIn	2947	@sec_matters	7975
PEN/PMS	Philips LinkedIn	1107981	@Philips	341K
FMI/Civipol	FMI LinkedIn	46297	@Place_Beauvau @PoliceNat13	496K 5438
KEMEA	KEMEA LinkedIn	552	N/A	N/A
BEIA	BEIA LinkedIn	119	@beiaconsult	272
SGSP	N/A	N/A	N/A	N/A

Annex 4 - SAFECARE Partners internal Publication

Partners Internal Publications				
Partners	Website	Blog	Newsletter	Journal Magazines
APHM	www.ap-hm.fr	N/A	N/A	N/A
CCS	www.airbus-cyber-security.com/	www.airbus-cyber-security.com/	Yes, Monthly	N/A
UG	www.uni-greifswald.de	N/A	N/A	N/A
ENC	www.enovacom.fr	N/A	N/A	N/A
SPF	www.santepubliquefrance.fr	N/A	N/A	N/A
ISEP	www.gecad.isep.ipp.pt/GECAD/Pages/Presentation/AllNews.aspx	N/A	N/A	N/A
CNAM	www.cnam.fr/portail/conservatoire-national-des-arts-et-metiers-821166.kjsp	N/A	N/A	N/A
KU Leuven	www.law.kuleuven.be	www.law.kuleuven.be/citip/blog	N/A	N/A
CSI	www.csi.it	N/A	N/A	N/A
ASLT05	www.aslto5.piemonte.it	N/A	N/A	N/A
EOS	www.eos-eu.com	N/A	Yes, every six months	N/A
AMC	www.amc.nl/web/home.htm	N/A	N/A	N/A
MS	www.milestonesys.com	N/A	news.milestonesys.com/	N/A
SM	www.secmatters.com	www.forescout.com/company/blog	N/A	N/A

PEN/PMS	www.research.philips.com www.medical.philips.com	N/A	N/A	N/A
FMI/Civipol	www.interieur.gouv.fr www.police-nationale.interieur.gouv.fr www.civipol.fr	N/A	N/A	N/A
KEMEA	www.kemea.gr	N/A	N/A	N/A
BEIA	www.beiaro.eu/category/news	N/A	Yes, monthly	N/A
SGSP	www.sgsp.edu.pl	N/A	N/A	Scientific Papers of the Main School of Fire Service

Annex 5 – 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	Jan.messerschmidt@uni-greifswald.de
ENC	Melanie Dufrou	information@enovacom.fr	N/A	N/A
SPF	Valérie Derrey	Velerie.DERREY@santepubliquefrance.fr	N/A	N/A
ISEP	Isabel Parça	Icp@isped.ipp.pt	Yes	GCI@ispe.ipp.pt
CNAM	Samira Si-Said Cherfi	samira.cherfi@cnam.fr	N/A	N/A
KUL	Elisabetta Biasin Pierre Notermans	elisabetta.biasin@kuleuven.be pierre.notermans@kuleuven.be	N/A	N/A
ISMB	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	Konstantinos.andreopoulos@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
SM	Mario Dragada	mario.dagrada@secmatters.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	i.gkotsis@kemea-research.gr	N/A	N/A
BEIA	George Suciu	George@beia.ro	Yes	marketing@beia.ro
SGSP	Tadeusz Keson	tkeson@sgsp.edu.pl	Yes	mglowka@sgsp.edu.pl