SAFECARE

Integrated cyber-physical security for health services

Report on best practices for security standards

Deliverable 8.5

Lead Author: KEMEA

Contributors: EOS, ISEP, PEN, MS, ACS, FST, SPF, LINKS, FMI, AP-HM

Deliverable classification: (PU)

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

Version Control Sheet

Title	*Report on best practices for security standards*
Prepared By	*Vasiliki Mantzana, Ilias Gkotsis*
Approved By	*AP-HM, EOS*
Version Number	*Version 5*
Contact	v.mantzana@kemea-researh.gr; i.gkotsis@kemea-research.gr

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
V0.1	21.06.2021	Initial ToC draft sent to the consortium.	KEMEA	V0.1
V0.2	03.06.2021	Initial Executive Summary and deliverable's description sent to the consortium.	KEMEA	V0.2
V0.3	10.06.2021	Partners' contributions.	All partners	V0.3
V0.4	21.10.2021	Draft sent to reviewers.	APHM, EOS	V0.4
V0.5	05.11.2021	Review comments considered. Final deliverable.	KEMEA	V0.5

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

Table of Contents

List of Figures

LIST OF TABLES

1 The SAFECARE Project

Over the last decade, the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons to impact the population. As Europeans, we know now that we must increase our awareness against these attacks that can strike the places we rely upon the most and destabilise our institutions remotely. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analysed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such a combination of threats. Health services are at the same time among the most critical infrastructures and the most vulnerable ones.

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

2 Executive Summary

The challenge of SAFECARE is to bring together the most advanced technologies from the physical and cyber security spheres to achieve a global optimum for systemic security and for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects. The project focuses on health service infrastructures and works towards the creation of a comprehensive protection system, which will cover threat prevention, detection, response and, in case of failure, mitigation of impacts across infrastructures, populations and environment. Over a 39-month time frame, the SAFECARE Consortium will design, test, validate and demonstrate 13 innovative elements (IEs), developed in the Description of Actions (DoA), which will optimize the protection of critical infrastructures under operational conditions. These elements are interactive, cooperative and complementary, aiming at maximizing the potential use of each individual element. The consortium 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.

In this Deliverable, and based on the normative literature, SAFECARE partners' and external stakeholders' knowledge and experience, gaps, recommendations and best practices on cyber and physical security standards in the healthcare sector, are identified and presented; and the cyber and physical security certification related issues are analysed. Moreover, the importance of standards' adoption is highlighted and their consideration in the cyber and physical insurance process and contracts is explained, as it can be a proof of an organization's competence and quality as well it can support risk management during the overwriting process.

3 Introduction

Healthcare organisations should adopt processes, products and services standards, as it has been proved that they affect the quality of services offered to the public. Moreover, their adoption creates a strong health care structure that the public, providers and policy makers can rely on, assuring high quality health services. In this way, it is ensured from one hand that all patients are treated with dignity and respect, and that they receive adequate services, but also a safe and secure environment to be hospitalized in. In addition, their adoption should be considered by insurance companies when tackling with healthcare organisations, as it can be a proof of their competence and quality and can support risk management during the overwriting process.

The aim of the Deliverable is to extract and present best practices on cyber and physical security standards in healthcare organisations. In meeting this aim, initially (Chapter 0) the standardization landscape is described, with a focus given to the relative legal framework, the Standards Developing Organisations (SDOs), as well as the relative standardisation process. In Chapter 5 the cyber and physical security standards in the healthcare sector, as well as the gaps, recommendations and best practices, are identified and presented (based on the normative literature, SAFECARE partners' and external stakeholders' knowledge and experience). In Chapter 6, cyber and physical security certification related issues are presented. Finally, in Chapter 7 the importance of cyber and physical standards is identified and highlighted and the adoption and consideration of these standards in the insurance process (overwriting, cost etc.) is analysed.

4 Cyber and physical security standardisation framework

In this Chapter, initially the cyber and physical rules and policies, selected for addressing the security and safety needs of SAFECARE are presented. Moreover, the Standards Developing Organisations (SDOs) and the standards' development process are analysed.

4.1 Cyber and physical security legal framework

In the following paragraphs, the cyber and physical rules and policies, selected for addressing the security and safety needs of SAFECARE are presented. It shall be kept in mind that the aim is not the elaboration of an exhaustive list of all available rules and policies but rather to outline a refined selection of those perceived to best suit the needs of the project activities and systems of interest.

Table 4.1 - Cyber and physical security legal framework

Cyber and physical security legal framework		
Framework	**Description**	**Webpage**
NIST Framework for Improving Critical Infrastructure Cybersecurity (1)	The Cybersecurity Framework provides a prioritised, flexible, repeatable, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties. The Framework does not prescribe particular technological solutions or specifications to enable technical innovation and account for organisational differences. Part of the Framework are the informative references, some of them provided by NIST as Special Publications, such as: (a) SP800-100, aiming to assist managers in understanding and implementing an Information Security Program; (b) NIST 800 -30, aiming to provide guidance for conducting risk assessments of federal information systems and organisations.	https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity
Directive on Security of Network and Information Systems (NIS	On July 6, 2016, the European Parliament set into policy the Directive on Security of Network and Information Systems (the NIS Directive). The Directive went into effect in August 2016, and all member states of the European Union were given 21 months to incorporate the Directive's	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc

Cyber and physical security legal framework		
Framework	**Description**	**Webpage**
Directive) (2)	regulations into their own national laws. The aim of the NIS Directive is to create an overall higher level of cybersecurity in the EU. The Directive significantly affects digital service providers (DSPs) and operators of essential services (OESs). The member states of the EU are required to create a NIS directive strategy, which includes the CSIRTs, in addition to National Competent Authorities (NCAs) and Single Points of Contact (SPOCs). Security requirements include technical measures that manage the risks of cybersecurity breaches in a preventative manner. Both DSP and OES must provide information that allows for an in depth assessment of their information systems and security policies. All significant incidents must be notified to the Computer Security Incident Response Teams (CSIRT).	=OJ:L:2016:194:TOC
EU General Data Protection Regulation (GDPR) (3)	The EU General Data Protection Regulation (GDPR) was set into place on 14 April 2016, but the current date of enforcement is set to be on 25 May 2018. The GDPR aims to bring a single standard for data protection among all member states in the EU. Changes include the redefining of geographical borders. It applies to entities that operate in the EU or deal with the data of any resident of the EU. Regardless of where the data is processed, if an EU citizen's data is being processed, the entity is now subject to the GDPR	https://eur-lex.europa.eu/eli/reg/2016/679/oj
Regulation (EU) No 1025/2012 of the European Parliament (4)	It is the current legal basis for the interaction between the Commission and the European Standardisation Organisations (ESOs). It lays the foundation for the development of voluntary standards in support of European legislation and policies. It also serves as the Legal Framework for the use of standardisation in products and services. The Regulation affords the Commission the key role in standardisation governance, both in the planning and implementation phases. The annual planning cycle results in the EU Work Programme for standardisation, in which it is explained how the Commission intends to leverage standardisation to foster	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02012R1025-20151007

Cyber and physical security legal framework		
Framework	**Description**	**Webpage**
	legislation and policies. The implementation phase is carried out mainly via 'Standardisation Requests' (previously known as mandates) issued to the three European Standardisation Organisations. The requests are issued, following a consultation phase with relevant stakeholders and the go-ahead by the Committee on Standards, and formally via a Commission Implementing Decision. The requests can be accepted or refused by the ESOs. Once accepted, the ESOs are bound to develop specific standardisation deliverables – most importantly European Standards – in a specified timeframe. While the adoption of the final standards is voluntary, national standardisation organisations are required to transpose the newly developed European standards into national standards, superseding if necessary previous national ones. The standardisation process follows the principles laid out in the Regulation. The process must be transparent and promote broad participation among stakeholders interested. Work programmes are publicly available – this does not apply to the internal processes and documents during the development itself. Also, it must be noted that while final published ETSI standards are available freely, this is not usually the case for CEN-CENELEC. A final note on the ICT technical standards, so crucial in Cyberspace, and not developed usually by the recognised ESOs: the Regulation provides a mechanism by which these standards can be referenced and incorporated into the European process. Under article 12, a notification system for all stakeholders (including European standardisation organisations and European stakeholder organisations), has been established.	
EU Cybersecurity Act (5)	The EU Cybersecurity Act establishes an EU-wide cybersecurity certification framework for digital products, services and processes. It complements the NIS Directive. ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework. The	https://eur-lex.europa.eu/eli/reg/2019/881/oj

Cyber and physical security legal framework		
Framework	**Description**	**Webpage**
	certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. This will be based on agreement at the EU level for the evaluation of the security properties of a specific ICT-based product or service, e.g. smart cards. It will attest that ICT products and services which have been certified in accordance with such a scheme comply with specified requirements. In particular, each European scheme should specify: a) the categories of products and services covered, b) the cybersecurity requirements, for example, by reference to standards or technical specifications, c) the type of evaluation (e.g. self-assessment or third-party evaluation), and d) the intended level of assurance (e.g. basic, substantial and/or high).	
Regulation (EU) No 2017/746 of the European Parliament (6)	Directive 98/79/EC of the European Parliament and of the Council (3) constitutes the Union regulatory framework for in vitro diagnostic medical devices. However, a fundamental revision of that Directive is needed to establish a robust, transparent, predictable, and sustainable regulatory framework for in vitro diagnostic medical devices, ensuring a high level of safety and health whilst supporting innovation. (2) This Regulation aims to ensure the smooth functioning of the internal market regarding in vitro diagnostic medical devices, taking as a base a high level of protection of health for patients and users, and taking into account the small and medium-sized enterprises that are active in this sector. At the same time, this Regulation sets high standards of quality and safety for in vitro diagnostic medical devices to meet common safety concerns regarding such products.	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0746&from=EN

In order to support policies and legislation in the field of privacy and security, standards are often developed. Standards have been defined as "technical specifications defining requirements for products, production processes, services or test-methods. These specifications are voluntary. They are developed by industry and market actors following some basic principles such as consensus, openness, transparency and non-discrimination. Standards ensure interoperability and safety, reduce costs and facilitate companies' integration in the value chain and trade." (7). Regulation (EU) No 1025/2012 (8) provides a legal basis to use European standards for products and services, identify ICT technical specifications, and finance the European standardisation process. It also sets an obligation for European Standardisation Organisations (European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), and the European Telecommunications Standards Institute (ETSI)) and National Standardisation Bodies on transparency and participation.

In that way, they are achievable performance measurements in products and services in order to advance safety and security, and promote the competitiveness of the European industry worldwide. Standardisation could also enhance the collaboration of stakeholders, giving the baseline and prerequisites that should be followed either at procedural or technical level, improving the compatibility and interoperability of products and services. The exploitation of research results could assist and speed up this process of standards fostering crisis management, by building institutional resilience and best practices that will increase efficiency, readiness, and operability. In the following paragraphs, European and International standardisation organisations, as well as European bodies involved in this process, are presented.

4.2 Standards Developing Organisations (SDOs)

Standards are developed through the responsibility of the European Standardisation Organisations: CEN, CENELEC, ETSI and can be used to support legislation and policies (as presented in Table below). The European Standardisation Organisations are officially recognised by Regulation (EU) No 1025/2012 (9) as providers of European standards. The internal governance of the ESOs represents the first side of the wider European governance framework for Cybersecurity standardisation, the other being the interaction between ESOs and the Commission when standardisation is developed in support of the policy.

Table 4.2 - European Standardisation Organisations

European Standardisation Organisations		
SDO	**Description**	**Webpage**
European Committee for Standardisation (CEN) (10)	CEN is one of the three European Standardisation Organisations (ESO). CEN is set up as an association under the Belgian law. Participation in CEN is based on national representation, via the national standardisation bodies of the European Union Member States, and other countries participating in the European Single Market, such as Switzerland and Turkey. CEN develops consensus-based voluntary European standards (EN), but also other deliverables of softer nature in the form of CEN Workshop	https://www.cen.eu/Pages/default.aspx

European Standardisation Organisations		
SDO	**Description**	**Webpage**
	Agreements. Approximately 1/3 of the CEN's European Standards are developed in response to standardisation requests coming from the European Commission. CEN has been working on privacy standards since 1997, when the CEN Information Society Standardization System (CEN/ISSS) was established. The CEN/ISSS was focused on Information and Guidance and gaps analysis for European standardisation Communication Technologies (ICT), with a working group on privacy and data protection. Recently, CEN created a new Technical Committee on Data Protection.	
European Committee for Electrotechnical Standardisation (CENELEC) (11)	CENELEC is a non-for profit organisation operating under the Belgian law. It develops voluntary standards in the field of electrotechnical engineering and collaborates closely with the IEC. Like CEN, the participation in CENELEC is through national representation. The IEC is mainly involved in privacy and data protection related standards in the information security context through its collaboration with CEN. An example is the Standardisation request by the European Commission M/530 to develop privacy management standards for security technologies.	https://www.cenelec.eu/index.html
European Telecommunications Standards Institute (ETSI) (12)	ETSI is a non-for-profit organisation established in France. Stakeholders-members of ETSI may join ETSI's standardisation work via direct participation. In addition, the standards developed by ETSI are made publicly available free of charge. ETSI develops standards on different technology clusters: security, interoperability, connecting things, wireless systems and networks, and others. ETSI's Technical Committee on Cyber security (TC Cyber) is mostly active in privacy standardisation for information security. The constituency of ETSI is quite different than CEN-CENELEC's. Industry can be directly represented as the membership is not based on national representatives. The development process is usually nimbler and more focused; the great majority of standards developed are technical in nature. ETSI is also open to non-European members, an important aspect to be considered when global application of standards is	https://www.etsi.org/

European Standardisation Organisations		
SDO	**Description**	**Webpage**
	desired.	

The close collaboration between CEN and CENELEC was consolidated at the start of 2010 by the creation of a common CEN-CENELEC Management Centre (CCMC) in Brussels (13). CEN-CENELEC is composed of National Standardisation Bodies, representing both EU and EFTA countries, and other stakeholders. The National Bodies that form the membership of CEN and CENELEC are usually also part of the ISO worldwide standardisation system and transposition of ISO work items to CEN deliverables is assured under the Vienna agreement, whilst IEC work items are transposed to CENELEC deliverables under the provisions of the Dresden agreement.

The recognised standard-setting organisations conduct collaboration agreements that address issues of participation to each other's work, but also the avoidance of duplication of work. The Vienna Agreement between ISO and CEN, underlines that international standardisation takes precedence over national standardisation, but also recognises that the Single European Market has particular needs for European standards (14). A similar agreement is signed between IEC and CENELEC (15).

European Commission aims to align European standards (as much as possible) with the international standards adopted by the recognised International Standardisation Organisations [e.g. International Organisation for Standardisation (ISO), International Electrotechnical Committee (IEC) and International Telecommunication Union (ITU)]. Some of the most recognised International Standardisation Organisations are presented in the Table below.

Table 4.3 – International Standardisation Organisations

International Standardisation Organisations		
SDO	**Description**	**Webpage**
International Organisation for Standardisation (ISO) (16)	The ISO is a non-governmental organisation, operating under the Swiss law. ISO develops international standards through its Technical Committees. Today, approximately 160 national standardisation bodies are members of ISO and collaborate in over 750 Technical Committees. The ISO standards are voluntary, even though it is also possible they sometimes "*carry more weight*" than a mere voluntary agreement; international standards may be required to be followed as in the case of the World Trade Organisation (WTO). ISO and IEC have a longstanding tradition in developing information security standards.	https://www.iso.org/home.html

International Standardisation Organisations		
SDO	**Description**	**Webpage**
International Electrotechnical Committee (IEC) (17)	IEC is focused on international standards for electrical, electronic, and related fields. IEC is a non-for-profit, quasi-governmental organisation, compose of National Committees (one per country) as members. Unlike ISO, IEC also offers conformity assessment via the Conformity Assessment Board.	https://www.iec.ch/
International Telecommunication Union (ITU) (18)	ITU is a United Nations' specialised agency, working on the development of voluntary recommendations (standards) for the telecommunication sector. ITU has numerous publications on cybersecurity and Internet of Things that often address privacy aspects.	https://www.itu.int/en/Pages/default.aspx
Internet Engineering Task Force (IETF) (19)	IETF is the body that is responsible for the development and maintenance of the Internet Standards. The IETF is primarily a volunteer organisation. Its driving force is a group of dedicated high-quality engineers from all over the world. In a structure of working groups, these engineers exchange ideas and experience, and through discussion and collaboration (both electronically and face-to-face) they strive to achieve rough consensus and implement the standards through running code.	https://www.ietf.org/
World Wide Web Consortium (W3C) (20)	The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web.	https://www.w3.org/

While the ESOs are completely independent in their activities regarding which standards to develop and how to do it, including the timing and priorities of their activities, the EC has been interested in how standardisation could support European policy goals since the early 1980s, establishing contacts and cooperation with the standardisation organisations. This is mainly achieved by the EU services, depending on the sector/topics covered by them. In the following table the most relevant DGs are presented.

Table 4.4 - European Union Bodies

European Union Bodies		
SDO	**Description**	**Webpage**
DG for Internal	The Commission's Directorate-General for Internal	https://ec.europa.eu/g

European Union Bodies		
SDO	**Description**	**Webpage**
Market, Industry, Entrepreneurship and SMEs (DG GROW) (21)	Market, Industry, Entrepreneurship and SMEs is responsible for EU policy on the single market, industry, entrepreneurship and small businesses. They hold the main responsibility for standardisation policy in general and initiating the standardisation requests to the ESOs.	rowth/
DG for Communications Networks, Content and Technology (DG CNECT) (22)	The Commission's Directorate-General for Communications Networks, Content and Technology is responsible to develop a digital single market to generate smart, sustainable and inclusive growth in Europe.	https://ec.europa.eu/digital-single-market/
DG for Health and Food Safety(DG SANTE)	DG SANTE develops and carries out the Commission's policies on food safety and public health.	https://ec.europa.eu/info/departments/health-and-food-safety_en
DG Health and Consumer Protection (DG SANCO_	DG Health and Consumer Protection focuses on distance selling, TV-advertising, spam, consumer protection related to electronic communications, eHealth and electro-magnetic fields;	https://ec.europa.eu/jrc/en/science-area/health-and-consumer-protection
DG for Migration and Home Affairs (DG Home) (23)	The Commission's Directorate-General for Migration and Home Affairs is responsible for EU policy on migration and home affairs. They manage policies that aim at ensuring that all activities necessary and beneficial to the economic, cultural and social growth of the EU may develop in a stable, lawful and secure environment. DG Home is also responsible for the European Agenda on Security, cybercrime and cooperates with EC3 (European Cybercrime Centre at EUROPOL).	https://ec.europa.eu/home-affairs/index_en

4.3 Standards development process

The term "standards" covers not only the traditional product standards, system and process standards that are intended to ensure public health, safety, and environment protection, as well as to provide measures to meet the challenges of global competitiveness. The term standards process refers not only to the writing of the standards, but also to the development of the test methods, certification and auditing processes. Within the European framework, the wider objective of standardization is to agree on common specifications and/or procedures that respond to the needs of business and meet consumer expectations (24). In this context CEN, CENELEC and their national Members and Committees work jointly to develop and define standards that are considered necessary by market actors and/or to support the implementation of European legislation.

The European and international standardization bodies use different steps in developing a standard; however standards published are always selected and developed by stakeholders in the area and not by the organisations themselves. A standard can be proposed by any interested stakeholder, such as European industry, technical or scientific associations, international organizations, or the European Commission.

As regards to the European approach in standardization, this consists of 6 distinct sequential procedural steps consisting of (a) New Proposal -evaluation and decision, (b) Drafting and consensus building, (c) Public enquiry, (d) Consideration of comments, (e) Approval of the standard and (f) Publication. The aforementioned chain of procedural actions is carried out among a hierarchy of organizational entities as listed below (in descending order) [REF]:

- **Technical Boards:** Responsible for (among others) advising and deciding on technical matters (organization, procedures coordination, overlaps and planning), examining and deciding on new projects.
- **Technical Committees:** Established by supervising technical boards, they are responsible for the title and scope of the new standard under study, drafting deliverables (including Technical Specifications, Technical Reports and CWAs (13)), supporting the negotiations during the standardisation process as well as supervising the timely execution of the standardization request deliverables.
- **Working Groups:** They are established by the supervising technical committee, composed by individual experts and is focused to prepare a first draft of Standards, Technical Specifications and Technical reports

Provided the above, the technical basis of a new standard is usually established through research undertaken prior to standardization (Pre-Normative Research (PNR)). This research aims to demonstrate the feasibility and reliability of the technique or process to be standardized and to investigate its limitations. This process aims at composing a proposal for a new standard that constitutes the initiation of the standardization process and usually originates from (a) Existing Technical Committees, (b) European Commission or Agency, (c) National Standardization Bodies and /or (d) CEN Partner Organizations. After the research has been established, for new areas of technology, it would be normal to prepare a 'pre-standard', such as a Publicly Available Specification (PAS) or Technical Specification (TS), so as to provide a document in a relatively short time frame for evaluation by potential users (25).

After the proposal is made, the relevant Technical Committee (TC) needs to approve the proposal. Following the approval, the relevant TC (e.g. the respective CEN/TC or an assigned WG) starts drafting. Whilst the development of a particular standard is the responsibility of a Technical Committee, the actual work of developing the ‘final working draft’ is assigned to either a Sub-Committee (SC) or a Working Group (WG) of the main TC. Like Technical Committees, Sub-Committees take their own decisions, such as approving the proposals, drafts, establishing and disbanding Working Groups, etc., and, like TCs, each SC has its own chairman and secretary, together with a number of Working Groups in which related work items are developed. Within a TC, WGs are able to make recommendations on technical and organizational matters to their parent TC or SC but cannot make decisions.

The next step is to publish the draft for commenting and voting by all stakeholders, and not only those represented in the standardization process. If the votes cast by member states and the received comments show that the draft standard needs technical revision, the TC can decide to revise the draft and conduct a second vote. If the results of the previous CEN Enquiry show approvals only, the TC can publish the standard. In conjunction with the publication of the European standard, member states are obliged to give it the status of a national standard and to withdraw national standards conflicting with it. As such, it is important to take into consideration when assessing time planning issues in the context of introducing new standards to address specific operational needs.

European standards are reviewed at least every five years after their publication, or earlier following a request. Through this process, for each standard is decided whether it is still valid, should be revised, amended, or withdrawn. For international standards, which were adopted as European standards, systematic reviews are not carried out. ISO carries out the systematic reviews on the corresponding, identical ISO standards and If ISO confirms the ISO standard, the corresponding EN ISO standard is considered as confirmed; If ISO decides to amend or revise the ISO standard, a corresponding project (work item) is registered in the CEN programme of work under the Vienna Agreement and ISO lead. If ISO decides to withdraw the ISO standard, CEN can consider withdrawing the standard as well.

Standards produced can be categorized in formal and informal, with formal standards having processes that operate through national representation and are approved or adopted by one of the National, Regional or international standards bodies; while informal standards operate through individual representation and get published by Standards Development Organisations. Both formal and informal processes are based on the principle of consensus, which has been defined as a 'general agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments' (26).

Throughout the standardization process, there exist several types of standardization deliverables that differ in the levels of transparency, consensus and approval required before issue, thus offering flexible means to meet different market needs. The main different types of standards are presented below:

- **Standard**: "A standard is a document that provides rules, guidelines or characteristics for activities or their results, for common and repeated use. Standards are created by bringing together all interested parties including manufacturers, users, consumers and regulators of a particular material, product, process or service. Everyone benefits from standardization through increased product safety and quality as well as lower transaction costs and prices" (13).
- **Technical Specification (TS):** "A Technical Specification addresses work still under technical development, or where it is believed that there will be a future, but not

immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard" (27).

- **Technical Report (TR):** "A Technical Report is an informative document that provides information on the technical content of standardization work. It may be prepared when it is considered urgent or advisable to provide additional information" (13).
- **Workshop Agreement (WA):** "A WA is an agreement developed and approved in Workshop; the latter is open to the direct participation of anyone with an interest in the development of the agreement. There is no geographical limit on participation; hence, participants may be from outside Europe" (13). Agreements have a limited lifespan (three years, with the possibility of one three year extension), at the end of which, or earlier if appropriate, they are either transformed into another type of standards deliverable, such as a Technical Specification or full standard, or withdrawn.
- **Guides: "**Guides support readers understand more about the main areas where standards add value" (27).
- **Harmonization Document (HD): "**A Harmonization Document is a normative document and its elaboration includes a public enquiry, followed by an approval by weighted vote of national members and final ratification. The Harmonization Document is announced at national level and every conflicting national standard is withdrawn. Having fulfilled these obligations, a member is free to maintain or issue a national standard dealing with a subject within the scope of the HD, provided that it is equivalent in technical content" (13).

Despite the several benefits of standardisation, it remains a challenging process. Managing a standardisation project along its lifecycle is difficult due to the long and complex procedures facing the drawback of sensitive information in some topics; the lack of understanding of the standardisation benefits; as well as the high standardisation costs. Moreover, despite the fact that it is a voluntary process, in some cases, the stakeholders, instead of collaborating they compete with each other as standards are market-driven and business-led. The antidote to this is the standards developed by independent organisations that follow open and transparent processes. Also, to enjoy the benefits of the harmonisation offered by standardisation, a robust national commitment is mandatory to withdraw the conflicting national standards from member states. Nevertheless, in order for the European standards to be highly aligned with the International one, a consensus-based approach among all interested parties, including industry, SMEs & societal stakeholders, is needed.

5 Cyber and physical security standards in healthcare sector

In the previous paragraphs, the standardization landscape has been described, with a focus given to the relative legal framework, the Standards Developing Organisations as well as the relative standardisation process. The aim of this chapter is to identify the cyber and physical security standards in the healthcare sector, and present the gaps, recommendations and best practices, based on SAFECARE partners' knowledge and experience, but also on external stakeholders that KEMEA has interviewed. In meeting the aim of this chapter, the authors followed the methodological steps below:

- Initially reviewed the **normative literature** and identified the cyber and physical standards in healthcare sector, thus developing an understanding of the relative research **(Section 5.1**).
- Following the review, a **questionnaire** was designed, aiming to identify SAFECARE's technical partners' and end-users' best practices for cyber and physical security standards in healthcare sector. The questionnaire as well as the data collected, are presented and analysed in **Section 5.2**.
- The above steps have been combined with several interviews / open-discussions with external stakeholders (e.g. hospitals, health regulatory authorities, insurance companies etc.) on the identification of standards' gaps, recommendations and best practices (**Section 5.3)**, but also on certification mechanisms and insurance contracts (the two later issues are further analysed in **Sections 6 and 7**).

5.1 SDOs and security standards in the healthcare sector

In the following paragraphs, the authors will present the healthcare sector's cyber and physical security standards, as identified from the normative literature. In doing this, initially the partners identified the most relevant SDOs and respective committees.

5.1.1 SDOs and relevant Committees for the healthcare sector

Through the initial research conducted the following SDOs have been identified:

- European Committee for Standardisation (CEN) (10)
- European Committee for Electrotechnical Standardisation (CENELEC) (11)
- European Telecommunications Standards Institute (ETSI) (12)
- International Organisation for Standardisation (ISO) (16)
- International Electrotechnical Committee (IEC) (17)

After that, a list of all SDO's Committees (at least 1.191) was identified from the aforementioned SDOs. As the list created was too extensive (included all SDO's committees) ,related to several sectors and covering different topics, the authors processed it and identified at least 111 committees relevant to cyber (Table 10.1) and approximately 202 relevant to physical security (

Table 10.2), as well as related to the healthcare sector (nearly 43 directly related to healthcare sector and approximately 100 related to different CIs), which are presented in the Table below.

Moreover, in order to further narrow down the aforementioned Committees list, we identified Committees related to the aim of SAEFACARE and the scenarios used to test the SAFECARE platform. Thereafter, we ended up with 49 Committees relevant to SAFECARE, as presented below in Table 5.1. The committees presented in Table 5.1, mainly focus on committees related to quality and safety of healthcare services provision (quality management, organisational issues etc.); medical and other devices quality (e.g. wearables, IoT etc.); Information systems (e.g. processing, healthcare-related systems etc.,); network and data security; safety and security devices (multimedia systems, audio, video, respiratory protective devices etc.; as well as buildings safety and security (e.g. ventilation, air quality, cables, plugs, sockets etc.).

Table 5.1 Committees relevant to cyber ad physical security standards in SAFECARE project

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Stds**	**Field**	**Cyber sec.**	**Physical sec.**	**SAFECARE Applicable**
CEN	CEN/CLC/ETSI/JWG eAcc	eAccessibility	eAccessibility	5	All	Yes	No	Yes
CEN	CEN/CLC/JTC 3	Quality management and corresponding general aspects for medical devices	The objective of the joint Technical Committee is to contribute to, and where necessary draft, suitable standards for "Quality management and corresponding general aspects for medical devices" that are applicable internationally and relevant to the essential requirements of EU Directives. The joint Technical Committee closely cooperates with ISO/TC 210 'Quality management and corresponding general aspects for medical devices' in the development of standards and revisions.	18	Health care	Yes	Yes	Yes
CEN	CEN/CLC/JTC 16	CEN/CENELEC Joint Technical Committee on Active Implantable Medical Devices	To standardize all active implantable medical devices and their accessories		Health care	Yes	Yes	Yes
CEN	CEN/SS F12	Information Processing Systems	Information Processing Systems	2	All	Yes	No	Yes
CEN	CEN/TC 79	Respiratory protective devices	To prepare European Standards for respiratory protective devices for use in the work place and for firefighting and for rescue purposes, where there exists a risk to health from inhaling dusts, fumes, gases, vapours or from oxygen deficiency, as well as European Standards for underwater breathing apparatus.	56	Health care	Yes	Yes	Yes
CEN	CEN/TC 156	Ventilation for buildings	Standardization of terminology, testing and rating methods, dimensioning and fitness for purpose of natural and mechanical ventilation systems and components for buildings subject to human occupancy.	76	All	No	Yes	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	Committee	Committee Title	Committee Description	Published Stds	Field	Cyber sec.	Physical sec.	SAFECARE Applicable
CEN	CEN/TC 195	Cleaning equipment for air and other gases	Standardization in the fields of terminology, classification, characteristics, and test and performance methods for air and gas cleaning equipment for general ventilation and industrial applications. Excluded: - exhaust gas cleaners for gas turbines and IC engines in mobile equipment, filters for personal protection equipment, cabin filters in mobile equipment, which are covered by other technical committees - UV-C applications	21	All	No	Yes	Yes
CEN	CEN/TC 251	Health informatics	Standardization in the field of Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems and to enable modularity. This includes requirements on health information structure to support clinical and administrative procedures, technical methods to support interoperable systems as well as requirements regarding safety, security and quality.	96	Health care	Yes	Yes	Yes
CEN	CEN/TC 264	Air quality	Standardisation of methods for air quality characterisation of emissions, ambient air, indoor air, gases in and from the ground and deposition, in particular measurement methods for air pollutants (for example particles, gases, odours, microorganisms), meteorological parameters and methods for determination of the efficiency of gas cleaning systems. Excluded are: - determination of limit values for air pollutants, - workplaces and clean rooms, - radioactive substances	123	N/A	No	Yes	Yes
CEN	CEN/TC 362	Healthcare services - Quality management systems	Healthcare services - Quality management systems	2	Health care	Yes	Yes	Yes
CEN	CEN/TC 365	Internet Filtering	Internet Filtering	1	All	Yes	Yes	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	Committee	Committee Title	Committee Description	Published Stds	Field	Cyber sec.	Physical sec.	SAFECARE Applicable
CENELEC	CLC/TC 213	Cable management systems	To prepare European standardization publications for products and systems used for the management of all types of cables, information and communication lines, electrical power distribution conductors and associated accessories. Management includes support and/or containment and/or retention and/or protection against external influences.	36	N/A	Yes	Yes	Yes
CENELEC	CLC/TC 210	Electromagnetic Compatibility (EMC)	To prepare EMC standards and guidelines with particular emphasis on the application of the EMC Directive and other EC Directives that contain EMC references and to coordinate all EMC activities in CENELEC.	165	N/A	No	Yes	Yes
CENELEC	CLC/SR 124	Wearable Electronic Devices and Technologies	Wearable Electronic Devices and Technologies		N/A	Yes	No	Yes
CENELEC	CLC/TC 100X	Audio, video and multimedia systems and equipment and related sub-systems	To monitor the adoption in CENELEC of the technical work from IEC/TC 100 standards in the field of audio, video and multimedia systems and equipment. These standards include specification of the performance, methods of measurement for consumer and professional equipment and their system application as well as interoperability with other systems and equipment. To ensure that any deviation from the IEC standards, such as common modifications, special national conditions and A-deviations, is only in response to a clear and justifiable European need, such as European and national legislative requirements. To strive towards keeping international and European requirements aligned as far as possible (applying the different mechanisms of the Dresden Agreement). To coordinate the work with other standardisation organisations on European level, taking responsibility for applicable mandates from the European Commission and developing its own standards only when necessary. Standards and other deliverables prepared by Technical Area 5 (TA5) of IEC/TC 100 do not fall under the scope of CLC/TC 100X but are	360	N/A	Yes	No	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Stds**	**Field**	**Cyber sec.**	**Physical sec.**	**SAFECARE Applicable**
			covered on European level by CLC/TC 209					
CENELEC	CLC/SR 87	Ultrasonics	Ultrasonics	31	N/A	No	Yes	Yes
CENELEC	CLC/TC 72	Automatic electrical controls	To prepare harmonized standards for rules related to inherent safety, to the operating characteristics where such are associated with application safety and to the testing of automatic electrical control devices used in appliances and other apparatus, electrical and non-electrical for household and similar purposes such as those for central heating, air conditioning etc. including the following: 1. Automatic electrical control devices mechanically, electro-mechanically, electrically or electronically operated responsive to or controlling such parameters as temperature, pressure, passage of time, humidity, light, electrostatic effect, flow or liquid level. 2. Automatic electrical control devices serving the starting of small motors that are used principally in appliances and apparatus for household and similar purposes. Such control devices may be built into or be separate from the motor. 3. Non-automatic control devices when such are associated with automatic control devices.	65	N/A	Yes	Yes	Yes
CENELEC	CLC/TC 62	Electrical equipment in medical practice	To establish harmonized standards and other publications concerning electrical equipment, electrical systems and software used in healthcare and their effects on patients, operators, other persons and the environment.	210	Health care	Yes	Yes	Yes
CENELEC	CLC/SC 46XA	Coaxial cables	To establish and maintain European Standards regarding coaxial cables for use in telecommunication, data transmission, radio frequency, video-communication and signalling equipment.	56	N/A	Yes	**Yes**	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	Committee	Committee Title	Committee Description	Published Stds	Field	Cyber sec.	Physical sec.	SAFECARE Applicable
CENELEC	CLC/TC 46X	Communication cables	To establish standards related to wires, symmetric cables, coaxial cables and waveguides with metallic conductors for use in telecommunication, data transmission, radio frequency, video communication and signalling equipment to satisfy the advances in developing technologies. Particular requirements for materials, if necessary, will be evaluated in liaison with other technical committees.	102	N/A	Yes	Yes	Yes
CENELEC	CLC/SC 31-9	Electrical apparatus for the detection and measurement of combustible gases to be used in industrial and commercial potentially explosive atmospheres	General and specific requirements for construction, safety, performance and testing of apparatus for sensing the presence of combustible gases or vapours and for measuring their concentration in industrial and commercial potentially explosive atmospheres.	11	N/A	No	Yes	Yes
CENELEC	CLC/TC 23BX	Switches, boxes and enclosures for household and similar purposes, plugs and socket outlet for D.C.	a) To prepare standards for general purpose switches including electronic switches, time-delay switches, remote control switches and isolating switches, Fireman's switches, for a.c. only, with rated voltage not exceeding 440 V, and with a maximum rated current not exceeding 125 A, intended for household and similar purposes, either indoors or outdoors. b) To prepare standards for switches and related accessories for use in Home and Building Electronic Systems (HBES), with a working voltage not exceeding 250 V a.c. and a rated current up to and including 16 A, intended for household and similar purposes, either indoors or outdoors and to associate electronic extension units.	40	N/A	No	Yes	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	Committee	Committee Title	Committee Description	Published Stds	Field	Cyber sec.	Physical sec.	SAFECARE Applicable
CENELEC	CLC/BTTF 133-1	Sound systems for emergency purposes which are not part of fire detection and alarm systems	To prepare a draft residual standard based on EN 60849:1998 that is complementary to EN 54-16 "Fire detection and fire alarm systems -- Part 16: Voice alarm control and indicating equipment"	1	N/A	No	Yes	Yes
ETSI	EP EHEALTH	ETSI PROJECT (EP) EHEALTH	Responsible for coordinating ETSI's activities in the eHealth domain, identifying gaps where further standardization activities might be required and addressing those gaps which are not the responsibility of other ETSI bodies.		Health care	Yes	No	Yes
ETSI	TC LI	TECHNICAL COMMITTEE (TC) LAWFUL INTERCEPTION (LI)	We develop standards that support the technical requirements of national and international obligations for law enforcement, including the lawful interception and retention of the communications-related data of electronic communications. Lawful Interception (LI) and Retained Data (RD) play a crucial role in helping law enforcement agencies to investigate terrorism and serious criminal activities. We have pioneered the development and maintenance of LI and RD capabilities, and our standards are being adopted around the world due to the increased efficiency and lower cost resulting from their use. Global interest in the committee's work continues to grow, with new organizations joining in the standardization process.		N/A	Yes	Yes	Yes
ETSI	TC SCP	TECHNICAL COMMITTEE (TC) SMART CARD PLATFORM (SCP)	We are responsible for the development and maintenance of specifications for Secure Elements (SEs) in a multi-application capable environment, the integration into such an environment, as well as the secure provisioning of services making use of SEs. Our work includes the development and maintenance of specifications for the SE and its interface to the outside world for use in telecommunication systems, for general telecommunication purposes as well as for Machine-to-Machine (M2M)/Internet of Things (IoT) communications. The committee's work comprises the interface,		N/A	Yes	No	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	Committee	Committee Title	Committee Description	Published Stds	Field	Cyber sec.	Physical sec.	SAFECARE Applicable
			procedures and protocol specifications between the SE and entities (remote or local) used in its management. It also includes interfaces, procedures and protocol specifications used between such entities for the secure provisioning and operation of services making use of the SE.					
ETSI	TC TCCE	TECHNICAL COMMITTEE (TC) TERRESTRIAL TRUNKED RADIO AND CRITICAL COMMUNICATIONS EVOLUTION (TCCE)	We are responsible for the design and standardization of Terrestrial Trunked RAdio (TETRA) and its evolution to critical communications mobile broadband solutions. TETRA (Terrestrial Trunked Radio) is the leading technology choice for critical communications users. With a projected 5 million terminals in use by 2020, the use of TETRA in security as well as other business-critical markets such as the transportation, military, commercial and utilities sectors continue to increase.		N/A	Yes	Yes	Yes
ETSI	ISG ETI	INDUSTRY SPECIFICATION GROUP (ISG) ENCRYPTED TRAFFIC INTEGRATION (ETI)	ISG ETI develops Group Specifications (GS) and Group Reports (GR) that define requirements and identify the use cases of Encrypted Traffic Integration techniques to mitigate against threats to networks and users arising from the deployment of encrypted traffic.		N/A	Yes	No	Yes
IEC	ISO/IEC JTC 1/SC 27	Information security, cybersecurity and privacy protection	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: Security requirements capture methodology; Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;	197	All	Yes	Yes	Yes
IEC	SC 62B	Diagnostic imaging	To prepare international publications for safety and performance for all kind of medical diagnostic imaging equipment (e.g. X-ray imaging	81	Health care	Yes	Yes	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Stds**	**Field**	**Cyber sec.**	**Physical sec.**	**SAFECARE Applicable**
		equipment	equipment, computed tomography, magnetic resonance imaging equipment) including related associated equipment and accessories as well as quality procedures (e.g. acceptance tests and constancy tests) to be applied during the life-time of imaging equipment. Included is also the development of related terminology, concepts, terms and definitions.					
ETSI	ISG SAI	INDUSTRY SPECIFICATION GROUP (ISG) SECURING ARTIFICIAL INTELLIGENCE (SAI)	The rapid expansion of Artificial Intelligence into new industries with new stakeholders, coupled with an evolving threat landscape, presents a tough challenge for security. Artificial Intelligence impacts our lives every day, from local AI systems on our mobile phones suggesting the next word in our sentences to large manufacturers using AI to improve industrial processes. AI has the potential to revolutionize our interactions with technology, improve our quality of life and enrich security – but without high quality technical standards, AI has the potential to create new attacks and worsen security.		N/A	Yes	No	Yes
IEC	ISO/IEC JTC 1/SC 25	Interconnection of information technology equipment	Standardization of microprocessor systems, interfaces, protocols, architectures and associated interconnecting media for information technology equipment and networks to support embedded and distributed computing environments, storage systems and other input/output components.	232	N/A	Yes	No	Yes
IEC	SC 62D	Electromedical equipment	To develop particular international standards and technical reports for electrical equipment used in medical practice. These documents cover the safety and/or performance of the equipment as well as related terminology, concepts, definitions and symbols.	100	Health care	Yes	Yes	Yes
IEC	TC 62	Electrical equipment in medical practice	To prepare international standards and other publications concerning electrical equipment, electrical systems and software used in healthcare and their effects on patients, operators, other persons and the environment.	1	Health care	Yes	Yes	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	Committee	Committee Title	Committee Description	Published Stds	Field	Cyber sec.	Physical sec.	SAFECARE Applicable
IEC	ISO/IEC JTC 1/SC 41	Internet of things and related technologies	Standardization in the area of Internet of Things and related technologies. Serve as the focus and proponent for JTC 1's standardization programme on the Internet of Things and related technologies, including Sensor Networks and Wearables technologies. Provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things related applications.	29	N/A	Yes	No	Yes
IEC	SC 31G	Intrinsically-safe apparatus	To prepare and maintain international standards relating to intrinsically safe electrical apparatus and systems for use where there is a hazard due to the possible presence of explosive atmospheres of gases, vapours, mists or combustible dusts.	13	N/A	No	Yes	Yes
IEC	SC 62A	Common aspects of electrical equipment used in medical practice	To prepare international standards concerning the common aspects of the manufacture, installation and application of electrical equipment used in medical practice, including systems, equipment, accessories, related terminology, concepts, terms, definitions and symbols.	81	Health care	No	Yes	Yes
IEC	SC 62C	Equipment for radiotherapy, nuclear medicine and radiation dosimetry	The preparation of standards for the safety and performance of medical equipment and systems using ionising radiation for the treatment of disease; associated equipment and software used in planning, delivering and monitoring such treatments; instruments measuring ionising radiation used in the diagnosis and treatment of disease as well as radiation conditions for testing them; and nuclear medicine equipment used for imaging the distribution of radioactive substances within the human body for both diagnostic purposes and radionuclide therapies.	40	Health care	No	Yes	Yes
ISO	ISO/TC 84	Devices for administration of medicinal products and catheters	Standardization of the performance of metered devices and supplies intended for administration of medicinal products, and standardization of syringes, needles and catheters.	35	N/A	Yes	Yes	Yes

Committees relevant to cyber ad physical security standards in SAFECARE project								
SDO	Committee	Committee Title	Committee Description	Published Stds	Field	Cyber sec.	Physical sec.	SAFECARE Applicable
ISO	ISO/TC 232	Education and learning services	Standardization in the field of education and learning services focused on, but not limited to services; management systems; facilitators; assessments; terminology; ethical conduct.	4	N/A	Yes	Yes	Yes
ISO	ISO/TC 260	Human resource management	Standardization in the field of human resource management.	13	N/A	Yes	Yes	Yes
ISO	ISO/TC 279	Innovation management	Standardization of terminology tools and methods and interactions between relevant parties to enable innovation.	4	N/A	Yes	Yes	Yes
ISO	ISO/IEC JTC 1	Information technology	Standardization in the field of information technology.	3266	All	Yes	No	Yes
ISO	ISO/TC 215	Health informatics	Standardization in the field of health informatics, to facilitate capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system.	201	Health care	Yes	Yes	Yes
ISO	ISO/TC 283	Occupational health and safety management	Standardization in the field of occupational health and safety management to enable an organization to control its OH&S risks and improve its OH&S performance.	1	Health care	Yes	Yes	Yes
ISO	ISO/TC 312	Excellence in service	Standardization in the field of excellence in service	0	N/A	Yes	Yes	Yes
ISO	ISO/TC 304	Healthcare organization management	Standardization in the field of healthcare organization management including: classification, terminology, nomenclature, management practices and metrics that comprise the non-clinical operations in healthcare entities.	1	Health care	Yes	Yes	Yes

Based on the presentation of the relevant SDOs and Committees, in the following section the cyber and physical security standards related to the healthcare sector and to SAFECARE project, are presented and analysed.

5.1.2 Cyber and physical security standards in the healthcare sector

The following paragraphs will present the aforementioned committees' work related to the healthcare sector's cyber and physical security standards based on the aim of SAFECARE and the scenarios used to test the SAFECARE platform. Due to the extensiveness of the committees' work, the list was narrowed down to follow the project's aim, with the goal to mitigate overlapping. Thereafter, we ended up with 195 standards, as presented below in Table 5.2. The standards presented in Table 5.2, mainly focused on the quality and safety of medical and other devices (22); quality and safety management in the healthcare sector (10); information systems, network and data security (21); health informatics (90); as well as buildings safety and security primarily in ventilation (15) and air quality (37).

Table 5.2 Cyber and physical security standards in the healthcare sector

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	**Standard Name**	**Standard Title**	**Field**	**Cyber security**	**Physical Security**
CEN/CLC/JTC 3	CEN ISO/TR 24971	Medical devices - Guidance on the application of ISO 14971	Healthcare	Yes	Yes
ISO/IEC JTC 1/SC 27	ISO/IEC 27000:2018	Information technology — Security techniques — Information security management systems — Overview and vocabulary	N/A	Yes	No
ISO/IEC JTC 1/SC 27	ISO/IEC 27001:2018	Information Security Management	N/A	Yes	No
ISO/IEC JTC 1/SC 27	ISO/IEC 27005:2018	Information technology — Security techniques — Information security risk management	N/A	Yes	No
ISO/IEC JTC 1/SC 27	ISO/IEC 27701:2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	N/A	Yes	No
CEN/TC 389	CEN ISO/TR 56004	Innovation Management Assessment - Guidance	N/A	Yes	Yes
CEN/TC 251	CEN ISO/TS 13972	Health informatics - Detailed clinical models, characteristics and processes	Healthcare	Yes	Yes
CEN/TC 251	CEN ISO/TS 14265	Health Informatics - Classification of purposes for processing personal health information	Healthcare	Yes	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 251	CEN ISO/TS 14441	Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment	Healthcare	Yes	Yes
CEN/TC 251	CEN ISO/TS 22756	Health Informatics - Requirements for a knowledge base for clinical decision support systems to be used in medication-related processes (ISO/TS 22756)	Healthcare	Yes	Yes
CEN/TC 251	CEN ISO/TS 82304	Health software	Healthcare	Yes	Yes
CEN/TC 251	CEN/TR 15212	Health informatics - Vocabulary - Maintenance procedure for a web-based terms and concepts database	Healthcare	Yes	Yes
CEN/TC 251	CEN/TR 15253	Health informatics - Quality of service requirements for health information interchange	Healthcare	Yes	Yes
CEN/TC 251	CEN/TR 15299	Health informatics - Safety procedures for identification of patients and related objects	Healthcare	Yes	Yes
CEN/TC 251	CEN/TR 15300	Health informatics - Framework for formal modelling of healthcare security policies	Healthcare	Yes	Yes
CEN/TC 362	CEN/TR 15592	Health services - Quality management systems - Guide for the use of EN ISO 9004	Healthcare	Yes	Yes
CEN/TC 251	CEN/TR 15872	Health informatics - Guidance on patient identification and cross-referencing of identities	Healthcare	Yes	Yes
CEN/TC 264	CEN/TR 16243	Ambient air quality - Guide for the measurement of elemental carbon (EC) and organic carbon (OC) deposited on filters	N/A	No	Yes
CEN/TC 264	CEN/TR 16269	Ambient air - Guide for the measurement of anions and cations in PM2,5	N/A	No	Yes
CEN/TC 156	CEN/TR 16798	Energy performance of buildings - Ventilation for buildings	N/A	No	Yes
CEN/TC 264	CEN/TR 16998	Ambient air - Report on nitro- and oxy-PAHs - Origin, toxicity, concentrations and measurement methods	N/A	No	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 264	CEN/TR 17078	Stationary source emissions - Guidance on the application of EN ISO 16911-1	N/A	No	Yes
CEN/TC 264	CEN/TS 15674	Air quality - Measurement of stationary source emissions - Guidelines for the elaboration of standardised methods	N/A	No	Yes
CEN/TC 264	CEN/TS 16115	Ambient air quality - Measurement of bioaerosols	N/A	No	Yes
CEN/TC 156	CEN/TS 16244	Ventilation in hospitals - Coherent hierarchic structure and common terms and definitions for a standard related to ventilation in hospitals	N/A	No	Yes
CEN/TC 389	CEN/TS 16555	Innovation management	N/A	Yes	Yes
CEN/TC 264	CEN/TS 16645	Ambient air - Method for the measurement of benz[a]anthracene, benzo[b]fluoranthene, benzo[j]fluoranthene, benzo[k]fluoranthene, dibenz[a,h]anthracene, indeno[1,2,3-cd]pyrene and benzo[ghi]perylene	N/A	No	Yes
CEN/TC 264	CEN/TS 16817	Ambient air - Monitoring the effects of genetically modified organisms (GMO) - Pollen monitoring	N/A	No	Yes
CEN/TC 264	CEN/TS 16976	Ambient air - Determination of the particle number concentration of atmospheric aerosol	N/A	No	Yes
CEN/TC 264	CEN/TS 17021	Stationary source emissions - Determination of the mass concentration of sulphur dioxide by instrumental techniques	N/A	No	Yes
CEN/TC 156	CEN/TS 17153	Ventilation for buildings - Correction of air flow rate according to ambient conditions	N/A	No	Yes
CEN/TC 264	CEN/TS 17198	Stationary source emissions - Predictive Emission Monitoring Systems (PEMS) - Applicability, execution and quality assurance	N/A	No	Yes
CEN/TC 264	CEN/TS 17286	Stationary source emissions - Mercury monitoring using sorbent traps	N/A	No	Yes
CEN/TC 251	CEN/TS 17288	Health informatics - The International Patient Summary - Guideline for European Implementation	Healthcare	Yes	Yes
CEN/TC 264	CEN/TS 17337	Stationary source emissions - Determination of mass concentration of multiple gaseous species - Fourier transform infrared spectroscopy	N/A	No	Yes
CEN/TC 264	CEN/TS 17340	Stationary source emissions - Determination of mass concentration of fluorinated compounds expressed as HF - Standard reference method	N/A	No	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 264	CEN/TS 17405	Stationary source emissions - Determination of the volume concentration of carbon dioxide - Reference method: infrared spectrometry	N/A	No	Yes
CEN/TC 264	CEN/TS 17434	Ambient air - Determination of the particle number size distribution of atmospheric aerosol using a Mobility Particle Size Spectrometer (MPSS)	N/A	No	Yes
CEN/TC 264	CEN/TS 17458	Ambient air - Methodology to assess the performance of receptor oriented source apportionment modelling applications for particulate matter	N/A	No	Yes
CEN/TC 264	CEN/TS 17638	Stationary source emissions - Manual method for the determination of the mass concentration of formaldehyde - Reference method	N/A	No	Yes
CEN/TC 264	CEN/TS 1948	Stationary source emissions - Determination of the mass concentration of PCDDs/PCDFs and dioxin-like PCBs	N/A	No	Yes
CLC/TC 210	CLC/prTS 50437	Electromagnetic emissions from access powerline communications networks	N/A	No	Yes
CLC/TC 210	CLC/TR 50481	Recommendations on filters for shielded enclosures	N/A	No	Yes
CLC/TC 210	CLC/TR 50484	Recommendations for shielded enclosures	N/A	No	Yes
CLC/TC 210	CLC/TR 50485	Electromagnetic compatibility - Emission measurements in fully anechoic chambers	N/A	No	Yes
CLC/TC 210	CLC/TS 50217	Guide for in situ measurements - In situ measurement of disturbance emission	N/A	No	Yes
CEN/CLC/JTC 3	CR 13825	Luer connectors - A report to CEN chef from the CEN forum task group "Luer fittings"	Healthcare	Yes	Yes
CEN/TC 264	CR 14377	Air quality - Approach to uncertainty estimation for ambient air reference measurement methods	N/A	No	Yes
CEN/TC 156	CR 14378	Ventilation for buildings - Experimental determination of mechanical energy loss coefficients of air handling components	N/A	No	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 251	EN 1064	Health informatics - Standard communication protocol - Computer-assisted electrocardiography	Healthcare	Yes	Yes
CEN/TC 251	EN 1068	Health informatics - Registration of coding systems	Healthcare	Yes	Yes
CEN/TC 251	EN 12251	Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords	Healthcare	Yes	Yes
CEN/TC 251	EN 12264	Health informatics - Categorial structures for systems of concepts	Healthcare	Yes	Yes
CEN/TC 264	EN 12341	Ambient air - Standard gravimetric measurement method for the determination of the PM10 or PM2,5 mass concentration of suspended particulate matter	N/A	No	Yes
CEN/TC 251	EN 12435	Health informatics - Expression of results of measurements in health sciences	Healthcare	Yes	Yes
CEN/TC 156	EN 12589	Ventilation for buildings - Air terminal units - Aerodynamic testing and rating of constant and variable rate terminal units	N/A	No	Yes
CEN/TC 156	EN 12599	Ventilation for buildings - Test procedures and measurement methods to hand over air conditioning and ventilation systems	N/A	No	Yes
CEN/TC 264	EN 12619	Stationary source emissions - Determination of the mass concentration of total gaseous organic carbon - Continuous flame ionisation detector method	N/A	No	Yes
CEN/TC 156	EN 12792	Ventilation for buildings - Symbols, terminology and graphical symbols	N/A	No	Yes
CEN/TC 251	EN 13609	Health informatics - Messages for maintenance of supporting information in healthcare systems	Healthcare	Yes	Yes
CEN/TC 79	EN 142	Respiratory protective devices - Mouthpiece assemblies - Requirements, testing, marking	Healthcare	Yes	Yes
CEN/TC 264	EN 14211	Ambient air - Standard method for the measurement of the concentration of nitrogen dioxide and nitrogen monoxide by chemiluminescence	N/A	No	Yes
CEN/TC 264	EN 14212	Ambient air - Standard method for the measurement of the concentration of sulphur dioxide by ultraviolet fluorescence	N/A	No	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 156	EN 14239	Ventilation for buildings - Ductwork - Measurement of ductwork surface area	N/A	No	Yes
CEN/TC 156	EN 14240	Ventilation for buildings - Chilled ceilings - Testing and rating	N/A	No	Yes
CEN/TC 156	EN 14277	Ventilation for buildings - Air terminal devices - Method for airflow measurement by calibrated sensors in or close to ATD/plenum boxes	N/A	No	Yes
CEN/TC 251	EN 14484	Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy	Healthcare	Yes	Yes
CEN/TC 251	EN 14485	Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive	Healthcare	Yes	Yes
CEN/TC 251	EN 14822	Health informatics - General purpose information components	Healthcare	Yes	Yes
CEN/TC 362	EN 15224	Quality management systems - EN ISO 9001	Healthcare	Yes	Yes
CEN/TC 264	EN 15259	Air quality - Measurement of stationary source emissions - Requirements for measurement sections and sites and for the measurement objective, plan and report	N/A	No	Yes
CEN/TC 264	EN 15267	Air quality - Certification of automated measuring systems	N/A	No	Yes
CEN/TC 251	EN 17269	Health informatics - The International Patient Summary	Healthcare	Yes	Yes
CEN/TC 264	EN 17346	Ambient air - Standard method for the determination of the concentration of ammonia using diffusive samplers	N/A	No	Yes
CEN/TC 264	EN 17359	Stationary source emissions - Bioaerosols and biological agents - Sampling of bioaerosols and collection in liquids - Impingement method	N/A	No	Yes
CEN/TC 264	EN 17389	Stationary source emissions - Quality assurance and quality control procedures for automated dust arrestment plant monitors	N/A	No	Yes
CEN/TC 156	EN 1751	Ventilation for buildings - Air terminal devices - Aerodynamic testing of damper and valves	N/A	No	Yes
CEN/TC 195	EN 1822	High efficiency air filters (EPA, HEPA and ULPA)	N/A	No	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 62	EN 60601	Medical electrical equipment	N/A	0	Yes
CEN/TC 62	EN 60627	Diagnostic X-ray imaging equipment - Characteristics of general purpose and mammographic anti-scatter grids	N/A	0	Yes
CEN/TC 62	EN 62304	Medical device software - Software life-cycle processes	N/A	0	Yes
CEN/TC 62	EN 80001	Application of risk management for IT-networks incorporating medical devices	N/A	0	Yes
CLC/TC 210	EN IEC 55014	Electromagnetic compatibility - Requirements for household appliances, electric tools and similar apparatus	N/A	No	Yes
CLC/TC 210	EN IEC 55015	Limits and methods of measurement of radio disturbance characteristics of electrical lighting and similar equipment	N/A	No	Yes
CLC/TC 210	EN IEC 55016	Specification for radio disturbance and immunity measuring apparatus and methods	N/A	No	Yes
CEN/TC 62	EN IEC 60522	Medical electrical equipment - Diagnostic X-rays	N/A	0	Yes
CLC/TC 210	EN IEC 61000	Electromagnetic compatibility (EMC)	N/A	No	Yes
CEN/TC 251	EN ISO 10781	Health Informatics - HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM) (ISO 10781	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 11238	Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated information on substances (ISO 11238	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 11239	Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated information on pharmaceutical dose forms, units of presentation, routes of administration and packaging (ISO 11239	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 11240	Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of units of measurement (ISO 11240	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 11615	Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated medicinal product information (ISO 11615	Healthcare	Yes	Yes

Standards relevant to cyber ad physical security in SAFECARE project

Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 251	EN ISO 11616	Health informatics - Identification of medicinal products - Data elements and structures for the Unique Identification and Exchange of regulated Pharmaceutical Product Information (ISO 11616	Healthcare	Yes	Yes
CEN/TC 264	EN ISO 11771	Air quality - Determination of time-averaged mass emissions and emission factors - General approach (ISO 11771	N/A	No	Yes
CEN/TC 251	EN ISO 12052	Health informatics - Digital imaging and communication in medicine (DICOM) including workflow and data management (ISO 12052	Healthcare	Yes	Yes
CEN/CLC/JTC 3	EN ISO 13485	Medical devices - Quality management systems - Requirements for regulatory purposes (ISO 13485)	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 13606	Health informatics - Electronic health record communication	Healthcare	Yes	Yes
CEN/TC 264	EN ISO 13833	Stationary source emissions - Determination of the ratio of biomass (biogenic) and fossil-derived carbon dioxide - Radiocarbon sampling and determination (ISO 13833)	N/A	No	Yes
CEN/CLC/JTC 3	EN ISO 14971	Medical devices - Application of risk management to medical devices (ISO 14971)	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 17523	Health informatics - Requirements for electronic prescriptions (ISO 17523)	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 21091	Health informatics - Directory services for healthcare providers, subjects of care and other entities (ISO 21091)	Healthcare	Yes	Yes
CEN/TC 264	EN ISO 21258	Stationary source emissions - Determination of the mass concentration of dinitrogen monoxide (N2O) - Reference method: Non-dispersive infrared method (ISO 21258)	N/A	No	Yes
CEN/TC 251	EN ISO 21298	Health informatics - Functional and structural roles (ISO 21298)	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 21549	Health informatics - Patient healthcard data	Healthcare	Yes	Yes
CEN/TC 264	EN ISO 21877	Stationary source emissions - Determination of the mass concentration of ammonia - Manual method (ISO 21877)	N/A	No	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
CEN/TC 251	EN ISO 22600	Health informatics - Privilege management and access control	Healthcare	Yes	Yes
CEN/TC 264	EN ISO 23210	Stationary source emissions - Determination of PM10/PM2,5 mass concentration in flue gas - Measurement at low concentrations by use of impactors (ISO 23210)	N/A	No	Yes
CEN/TC 251	EN ISO 23903	Health Informatics - Interoperability and integration reference architecture - Model and framework (ISO 23903)	Healthcare	Yes	Yes
CEN/TC 264	EN ISO 25139	Stationary source emissions - Manual method for the determination of the methane concentration using gas chromatography (ISO 25139)	N/A	No	Yes
CEN/TC 264	EN ISO 25140	Stationary source emissions - Automatic method for the determination of the methane concentration using flame ionisation detection (FID) (ISO 25140)	N/A	No	Yes
CEN/TC 251	EN ISO 25237	Health informatics - Pseudonymization (ISO 25237)	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 27789	Health informatics - Audit trails for electronic health records (ISO 27789)	Healthcare	Yes	Yes
CEN/TC 251	EN ISO 27799	Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799)	Healthcare	Yes	Yes
eHEALTH	ETSI TR 103 477 V1.2.1 (2020)	eHEALTH; Standardization use cases for eHealth	N/A	0	Yes
CLC/TC 210	FprEN 55011	Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement - Supplement of CISPR 11 with emission requirements for Grid Connected Power Converters (GCPC)	N/A	No	Yes
CLC/TC 210	FprEN 55032	Electromagnetic compatibility of multimedia equipment - Emission requirements	N/A	No	Yes
CLC/TC 210	FprEN 55035	Electromagnetic Compatibility of Multimedia equipment - Immunity Requirements	N/A	No	Yes
CEN/TC 62	FprEN IEC 80001	Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software	N/A	0	Yes
CEN/TC 62	HD 395.1 S2	Safety of medical electrical equipment	N/A	0	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
SC 62B	IEC 60336	Medical electrical equipment - X-ray tube assemblies for medical diagnosis - Focal spot dimensions and related characteristics	Healthcare	Yes	Yes
SC 62C	IEC 60976	Medical electrical equipment - Medical electron accelerators - Functional performance characteristics	Healthcare	No	Yes
ISO/TC 215	IEC 82304	Health software	Healthcare	Yes	Yes
SC 62A	IEC TR 80001	Application of risk management for IT-networks incorporating medical devices	Healthcare	No	Yes
ISO/TC 215	IEC/TR 80001	Application of risk management for IT-networks incorporating medical devices	Healthcare	Yes	Yes
ISO/TC 215	ISO 10159	Health informatics — Messages and communication — Web access reference manifest	Healthcare	Yes	Yes
ISO/TC 215	ISO 12052	Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management	Healthcare	Yes	Yes
ISO/TC 215	ISO 12967	Health informatics — Service architecture (HISA)	Healthcare	Yes	Yes
ISO/TC 215	ISO 13119	Health informatics — Clinical knowledge resources — Metadata	Healthcare	Yes	Yes
ISO/TC 215	ISO 13120	Health informatics — Syntax to represent the content of healthcare classification systems — Classification Markup Language (ClaML)	Healthcare	Yes	Yes
ISO/TC 215	ISO 13131	Health informatics — Telehealth services — Quality planning guidelines	Healthcare	Yes	Yes
ISO/TC 215	ISO 13606	Health informatics — Electronic health record communication	Healthcare	Yes	Yes
ISO/TC 215	ISO 13940	Health informatics — System of concepts to support continuity of care	Healthcare	Yes	Yes
SC 62A	ISO 14971	Medical devices - Application of risk management to medical devices	Healthcare	No	Yes
ISO/TC 215	ISO 17090	Health informatics — Public key infrastructure	Healthcare	Yes	Yes
ISO/TC 215	ISO 17117	Health informatics — Terminological resources	Healthcare	Yes	Yes
ISO/TC 215	ISO 17523	Health informatics — Requirements for electronic prescriptions	Healthcare	Yes	Yes
ISO/TC 215	ISO 18232	Health Informatics — Messages and communication — Format of length limited globally unique string identifiers	Healthcare	Yes	Yes
ISO/TC 215	ISO 18308	Health informatics — Requirements for an electronic health record architecture	Healthcare	Yes	Yes
ISO/TC 215	ISO 21091	Health informatics — Directory services for healthcare providers, subjects of care and other entities	Healthcare	Yes	Yes
ISO/TC 215	ISO 21549	Health informatics — Patient healthcard data	Healthcare	Yes	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
ISO/TC 215	ISO 22857	Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data	Healthcare	Yes	Yes
ISO/TC 304	ISO 22886	Healthcare organization management — Vocabulary	Healthcare	Yes	Yes
ISO/TC 304	ISO 22956	Healthcare organization management — Requirements for patient-centred staffing	Healthcare	Yes	Yes
ISO/TC 215	ISO 23903	Health informatics — Interoperability and integration reference architecture — Model and framework	Healthcare	Yes	Yes
ISO/TC 215	ISO 25237	Health informatics — Pseudonymisation	Healthcare	Yes	Yes
ISO/TC 215	ISO 27269	Health informatics — International patient summary	Healthcare	Yes	Yes
ISO/TC 215	ISO 27789	Health informatics — Audit trails for electronic health records	Healthcare	Yes	Yes
ISO/TC 215	ISO 27799	Health informatics — Information security management in health using ISO/IEC 27002	Healthcare	Yes	Yes
ISO/TC 283	ISO 45001	Occupational health and safety management systems — Requirements with guidance for use	Healthcare	Yes	Yes
ISO/TC 283	ISO 45003	Occupational health and safety management — Psychological health and safety at work — Guidelines for managing psychosocial risks	Healthcare	Yes	Yes
ISO/TC 215	ISO 81001	Health software and health IT systems safety, effectiveness and security	Healthcare	Yes	Yes
SC 62A	ISO TR 17791	Health informatics -- Guidance on standards for enabling safety in health software	Healthcare	No	Yes
SC 62A	ISO TS 82304	Health software	Healthcare	No	Yes
ISO/TC 215	ISO/HL7 10781	Health Informatics — HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM)	Healthcare	Yes	Yes
ISO/TC 215	ISO/HL7 16527	Health informatics — HL7 Personal Health Record System Functional Model, Release 1 (PHRS FM)	Healthcare	Yes	Yes
ISO/TC 215	ISO/HL7 21731	Health informatics — HL7 version 3 — Reference information model — Release 4	Healthcare	Yes	Yes
ISO/TC 215	ISO/HL7 27931	Data Exchange Standards — Health Level Seven Version 2.5 — An application protocol for electronic data exchange in healthcare environments	Healthcare	Yes	Yes
ISO/TC 215	ISO/HL7 27932	Data Exchange Standards — HL7 Clinical Document Architecture, Release 2	Healthcare	Yes	Yes
ISO/TC 215	ISO/HL7 27951	Health informatics — Common terminology services, release 1	Healthcare	Yes	Yes
ISO/TC 283	ISO/PAS 45005	Occupational health and safety management — General guidelines for safe working during the COVID-19 pandemic	Healthcare	Yes	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	**Standard Name**	**Standard Title**	**Field**	**Cyber security**	**Physical Security**
ISO/TC 215	ISO/TR 11636	Health Informatics — Dynamic on-demand virtual private network for health information infrastructure	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 13054	Knowledge management of health information standards	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 14292	Health informatics — Personal health records — Definition, scope and context	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 14639	Health informatics — Capacity-based eHealth architecture roadmap	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 17791	Health informatics — Guidance on standards for enabling safety in health software	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 20514	Health informatics — Electronic health record — Definition, scope and context	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 21332	Health informatics — Cloud computing considerations for the security and privacy of health information systems	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 21548	Health informatics — Security requirements for archiving of electronic health records — Guidelines	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 21835	Health informatics — Personal health data generated on a daily basis	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 22221	Health informatics - Good principles and practices for a clinical data warehouse	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 28380	Health informatics — IHE global standards adoption	Healthcare	Yes	Yes
ISO/TC 215	ISO/TR 80001	Application of risk management for IT-networks incorporating medical devices — Application guidance	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 11633	Health informatics — Information security management for remote maintenance of medical devices and medical information systems	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 14265	Health Informatics - Classification of purposes for processing personal health information	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 14441	Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 17975	Health informatics — Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 20405	Health informatics — Framework of event data and reporting definitions for the safety of health software	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 21089	Health informatics — Trusted end-to-end information flows	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 21547	Health informatics — Security requirements for archiving of electronic health records — Principles	Healthcare	Yes	Yes

Standards relevant to cyber ad physical security in SAFECARE project					
Committee	Standard Name	Standard Title	Field	Cyber security	Physical Security
ISO/TC 215	ISO/TS 22272	Health Informatics - Methodology for analysis of business and information needs of health enterprises to support standards based architectures	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 22756	Health Informatics — Requirements for a knowledge base for clinical decision support systems to be used in medication-related processes	Healthcare	Yes	Yes
ISO/TC 215	ISO/TS 27527	Health informatics — Provider identification	Healthcare	Yes	Yes
CLC/TC 210	prEN 50082	Electromagnetic compatibility (EMC) - Generic immunity standard	N/A	No	Yes
CLC/TC 210	prEN 50093	Basic immunity standard for voltage dips, short interruptions and voltage variations	N/A	No	Yes
CLC/TC 210	prEN 50222	Standard for the evaluation of measurement results taking measurement uncertainty into account	N/A	No	Yes
CLC/TC 210	prEN 50351	Basic standard for the calculation and measurement methods relating to the influence of electric power supply and traction systems on telecommunication systems	N/A	No	Yes
CLC/TC 210	prEN 50352	Limits relating to the electromagnetic influence of electric power supply and traction systems on telecommunication systems	N/A	No	Yes
CLC/TC 210	prEN 60801	Electromagnetic compatibility for industrial-process measurement and control equipment	N/A	No	Yes
CEN/TC 62	prEN IEC 62304	Health software - Software life cycle processes	N/A	0	Yes
CEN/TC 62	prEN IEC 81001	Health Software and health IT systems safety, effectiveness and security	N/A	0	Yes
CLC/TC 210	prENV 61000	Electromagnetic compatibility (EMC)	N/A	No	Yes
ISO/TC 292	ISO 22319:2017	Security and resilience — Community resilience — Guidelines for planning the involvement of spontaneous volunteers	N/A	No	Yes
ISO/TC 292	ISO 22320:2018	Security and resilience — Emergency management — Guidelines for incident management	N/A	No	Yes
ISO/TC 292	ISO 22322:2015	Societal security — Emergency management — Guidelines for public warning	N/A	No	Yes
ISO/TC 292	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts	N/A	No	Yes
ISO/TC 292	ISO 22328 series	Security and resilience — Emergency management — Part 1: General guidelines for the implementation of a community-based disaster early warning system	N/A	Yes	Yes
ISO/TC 292	ISO 22398:2013	Societal security — Guidelines for exercises	N/A	Yes	Yes
ISO/TC 292	ISO 22300:2021	Security and resilience — Vocabulary	N/A	Yes	Yes
CEN/TC 391	EN17173:2020	European CBRNE glossary	N/A	No	Yes

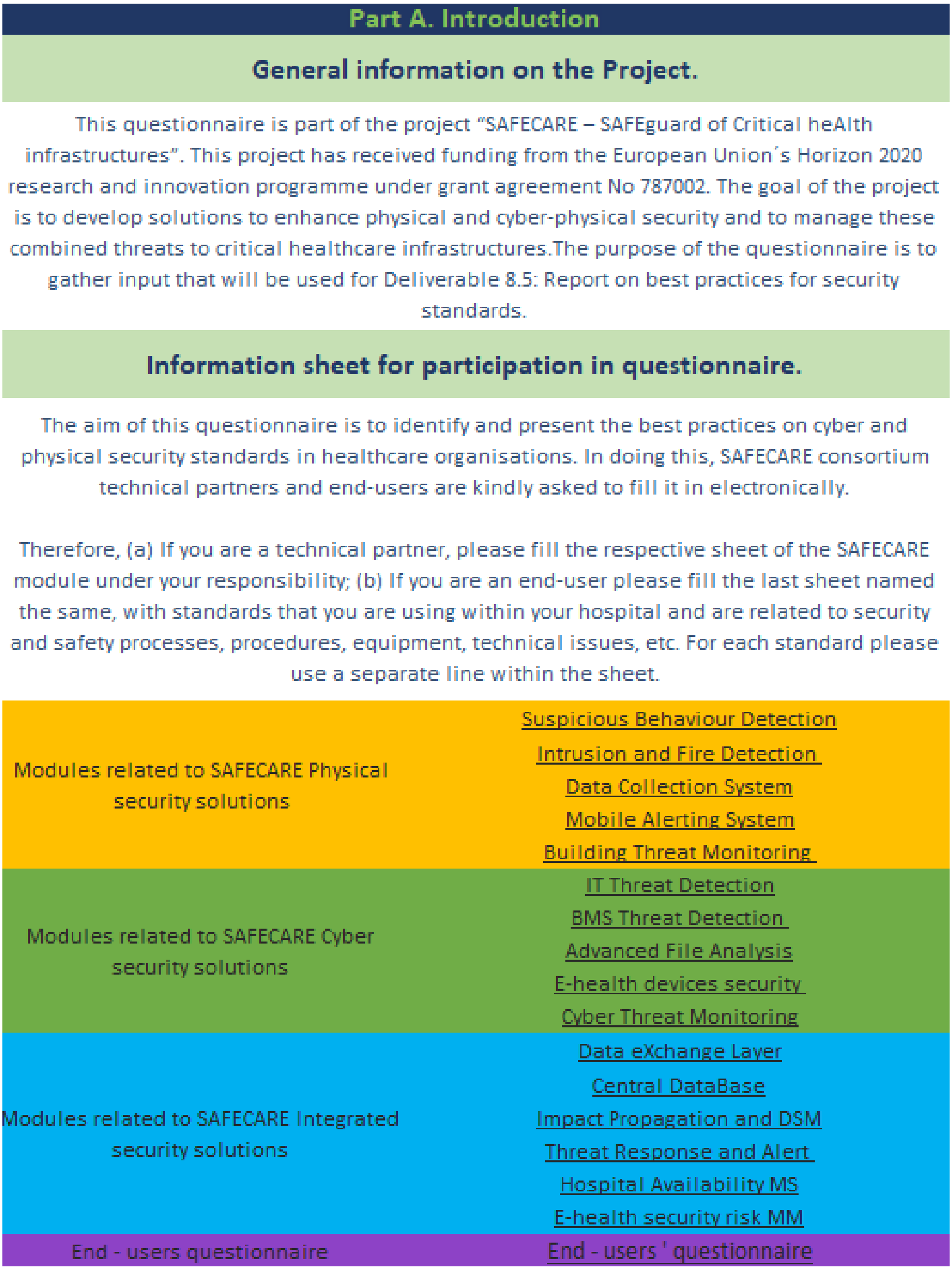
5.2 Cyber and physical security standards in SAFECARE

Complementary to the identified standards from the literature and research conducted (as presented in Table 5.2), which is quite generic and extensive, the authors decided to design a questionnaire. The aim was to identify SAFECARE technical partners' and end-users' best practices for cyber and physical security standards in the healthcare sector. Further to that we decided to conduct several interviews with external stakeholders in order to identify further standards that may be used, best practices that are followed (and are not addressed by standards) and collect gaps and lessons learned from their experience and knowledge.

5.2.1 Data collection from structured questionnaires

The authors shared a questionnaire that included general information, described the scope of the questionnaire and provided guidelines to the participating SAFECARE partners, as displayed below.

Figure 1 – Questionnaire introduction



Part A. Introduction

General information on the Project.

This questionnaire is part of the project "SAFECARE – SAFEguard of Critical heAlth infrastructures". This project has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement No 787002. The goal of the project is to develop solutions to enhance physical and cyber-physical security and to manage these combined threats to critical healthcare infrastructures.The purpose of the questionnaire is to gather input that will be used for Deliverable 8.5: Report on best practices for security standards.

Information sheet for participation in questionnaire.

The aim of this questionnaire is to identify and present the best practices on cyber and physical security standards in healthcare organisations. In doing this, SAFECARE consortium technical partners and end-users are kindly asked to fill it in electronically.

Therefore, (a) If you are a technical partner, please fill the respective sheet of the SAFECARE module under your responsibility; (b) If you are an end-user please fill the last sheet named the same, with standards that you are using within your hospital and are related to security and safety processes, procedures, equipment, technical issues, etc. For each standard please use a separate line within the sheet.

Modules related to SAFECARE Physical security solutions	Suspicious Behaviour Detection Intrusion and Fire Detection Data Collection System Mobile Alerting System Building Threat Monitoring
Modules related to SAFECARE Cyber security solutions	IT Threat Detection BMS Threat Detection Advanced File Analysis E-health devices security Cyber Threat Monitoring
Modules related to SAFECARE Integrated security solutions	Data eXchange Layer Central DataBase Impact Propagation and DSM Threat Response and Alert Hospital Availability MS E-health security risk MM
End - users questionnaire	End - users ' questionnaire

The questionnaire was mainly divided in 4 sections as depicted in the figure above. The three first sections referred to the technical partners while the last one referred to the end users. Regarding the technical partner's parts of the questionnaire, each partner has been asked to identify the cyber and physical security standards related to the module under their responsibility; select the type of the standard (process, data, technical); describe how or which part of the specific standard is used and applied to the specific sub-system; mention whether the specific standard is related to cyber or physical issues; and if it can be used in each phase of the crisis management process. In doing this, each SAFECARE module has been mapped to the different crisis management process phases (as analysed in Deliverable 8.4). The other part of the questionnaire, referred to the end-users, aiming to gather standards that they are using or being compliant with, either from the technical perspective or the procedural one.

Table 5.3 SAFECARE partners' responses

SAFECARE partners' responses												
Standard Code	**Standard Name**	**Link**	**Standard Description**	**Type of standard**	**Cyber or Physical**	**7.1 Cyber**	**7.2 Physical**	**8.1 Preparedness**	**8.2 Response**	**8.3 Recovery**	**8.4 Mitigation**	**SAFECARE Module**
DICOM PS3.15 2021c	Security and System Management Profiles	http://dicom.nema.org/medical/dicom/current/output/pdf/part15.pdf	DICOM PS3.15 2021c specifies the security requirements for the use of the DICOM medical protocol, including signatures and secure transport. The requirements were used to derive detection rules for the BMS probe.	Technical		Yes	No	Yes	No	No	No	BMS Threat Detection System, E-Health Devices Security
Emergency Data Exchange Language (EDXL) Hospital AVailability Exchange (HAVE) Version 2.0 13 January 2015	EDXL-HAVE	https://docs.oasis-open.org/emergency/edxl-have/v2.0/edxl-have-v2.0.html	EDXL-HAVE (HAVE) is an XML messaging standard primarily for exchange of information related to health facilities in the context of emergency management. HAVE supports sharing information about facility services, bed counts, operations, capacities, and resource needs so first responders, emergency managers, coordinating organizations, hospitals, care facilities, and the health community can provide each other	Technical		No	No	Yes	Yes	Yes	Yes	Hospital Availability Management System (HAMS)

SAFECARE partners' responses												
Standard Code	Standard Name	Link	Standard Description	Type of standard	Cyber or Physical	7.1 Cyber	7.2 Physical	8.1 Preparedness	8.2 Response	8.3 Recovery	8.4 Mitigation	SAFECARE Module
			with a coherent view of the health system.									
EU MDR	European Union's Medical Device Regulations	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745	Regulation (EU) 2017/745 is a regulation of the European Union on the clinical investigation and sale of medical devices for human use.	Process		Yes	Yes	Yes	Yes	Yes	Yes	E-health security risk management model
IETF RFC 5246 August 2008	TLS	https://datatracker.ietf.org/doc/html/rfc5246	The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.	Technical	Protocol	Yes	No	No	No	No	No	Hospital Availability Management System (HAMS) Mobile Alerting System (MAS)
IETF RFC 6749 October 2012	OAuth 2.0	https://datatracker.ietf.org/doc/html/rfc6749	The OAUTH 2.0 authorization framework is used to secure the access to the MAS server used by the Mobile application through the use of an authorization server (key cloak)	Process		Yes	No	No	No	No	No	Hospital Availability Management System (HAMS) Mobile Alerting System (MAS)

SAFECARE partners' responses												
Standard Code	Standard Name	Link	Standard Description	Type of standard	Cyber or Physical	7.1 Cyber	7.2 Physical	8.1 Preparedness	8.2 Response	8.3 Recovery	8.4 Mitigation	SAFECARE Module
IMDRF/CYBER WG/N60FINAL:2020	Principles and Practices for Medical Device Cybersecurity	http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf	The purpose of this IMDRF guidance document is to provide general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity.	Process		Yes	Yes	Yes	Yes	Yes	Yes	E-health devices security analytics
ISO 14971	Application of risk management to medical devices	https://www.iso.org/standard/72704.html	This document specifies terminology, principles and a process for risk management of medical devices, including software as a medical device and in vitro diagnostic medical devices. The process described in this document intends to assist manufacturers of medical devices to identify the hazards associated with the medical device, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls	Process		Yes	Yes	Yes	Yes	Yes	Yes	E-health security risk management model
ISO 31000:2018	Risk management — Guidelines	https://www.iso.org/standard/65694.html	ISO 31000:2018 provides guidelines on managing risk faced by organizations. In the context of this module, we applied the guidelines proposed to…	Process		Yes	Yes	Yes	Yes	Yes	Yes	BMS Threat Detection System
ISO 8001-2-2	Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for	https://webstore.iec.ch/publication/7484	This security report presents an informative set of common, high-level security-related capabilities useful in understanding the user needs, the type of security controls to be considered and the risks that lead to the controls.	Technical		Yes	Yes	Yes	Yes	Yes	Yes	E-health security risk management model

SAFECARE partners' responses												
Standard Code	Standard Name	Link	Standard Description	Type of standard	Cyber or Physical	7.1 Cyber	7.2 Physical	8.1 Preparedness	8.2 Response	8.3 Recovery	8.4 Mitigation	SAFECARE Module
	the disclosure and communication of medical device security needs, risks and control.											
ISO 8001-2-8	Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2security needs, risks and controls	https://webstore.iec.ch/publication/24908	Technical Report providing guidance to Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) for the application of the framework outlined in IEC TR 80001-2-2	Technical		Yes	Yes	Yes	Yes	Yes	Yes	E-health security risk management model E-health devices security analytics

SAFECARE partners’ responses												
Standard Code	Standard Name	Link	Standard Description	Type of standard	Cyber or Physical	7.1 Cyber	7.2 Physical	8.1 Preparedness	8.2 Response	8.3 Recovery	8.4 Mitigation	SAFECARE Module
ISO/IEC 31010	Risk management — Risk assessment techniques (including Bowtie)	https://www.iso.org/standard/72140.html	IEC 31010:2019 is published as a double logo standard with ISO and provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. It describes and evaluates the bowtie technique next to other risk assessment techniques.	Process		Yes	Yes	Yes	Yes	Yes	Yes	E-health security risk management model
MDCG 2019-16	Guidance on Cybersecurity for medical devices	https://ec.europa.eu/docsroom/documents/41863	The primary purpose of this document is to provide manufacturers with guidance on how to fulfil all the relevant essential requirements of Annex I to the MDR and IVDR with regard to cybersecurity.	Technical		Yes	Yes	Yes	Yes	Yes	Yes	E-health devices security analytics
MITRE ATT&CK®	MITRE ATT&CK®	https://attack.mitre.org/	MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.	Terminology		Yes	No	Yes	Yes	No	Yes	Hospital Availability Management System (HAMS)

SAFECARE partners' responses												
Standard Code	Standard Name	Link	Standard Description	Type of standard	Cyber or Physical	7.1 Cyber	7.2 Physical	8.1 Preparedness	8.2 Response	8.3 Recovery	8.4 Mitigation	SAFECARE Module
NIST 800-30	Guide for Conducting Risk Assessments.	https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final	The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.	Process		Yes	Yes	Yes	Yes	Yes	Yes	E-health security risk management model
NIST 800-53	Security and Privacy Controls for Federal Information Systems and Organizations.	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft	This publication provides a catalogue of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk.	Technical		Yes	Yes	Yes	Yes	Yes	Yes	E-health security risk management model E-health devices security analytics

SAFECARE partners’ responses												
Standard Code	**Standard Name**	**Link**	**Standard Description**	**Type of standard**	**Cyber or Physical**	**7.1 Cyber**	**7.2 Physical**	**8.1 Preparedness**	**8.2 Response**	**8.3 Recovery**	**8.4 Mitigation**	**SAFECARE Module**
NIST CSF	Framework for Improving Critical Infrastructure Cybersecurity	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf	The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.	Technical		Yes	Yes	Yes	Yes	Yes	Yes	E-health devices security analytics
NIST IR 7009	BACnet Wide Area Network Security Threat Assessment	https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7009.pdf	NISTIR7009 provides a security assessment of the most popular building automation protocol, BACnet. The results of this document were used as motivation for many of the detections implemented in the BMS probe.	Technical		Yes	No	Yes	No	No	No	BMS Threat Detection System
NIST SP 800-61	Computer Security Incident Handling Guide	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf	NISTSP800-61 provides guidelines for incident response (IR), including preparation. These guidelines were used to design the BMS probe, including the detection capabilities and the connection to other tools in the IR process.	Process		Yes	No	Yes	Yes	No	No	BMS Threat Detection System

SAFECARE partners' responses												
Standard Code	Standard Name	Link	Standard Description	Type of standard	Cyber or Physical	7.1 Cyber	7.2 Physical	8.1 Preparedness	8.2 Response	8.3 Recovery	8.4 Mitigation	SAFECARE Module
OASIS Message Queuing Telemetry Transport (MQTT) TC	MQTT	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt	Message Queuing Telemetry Transport or MQTT is a lightweight, publish-subscribe network protocol that transports messages between devices.	Technical	Protocol	Yes	No	No	No	No	No	All modules that exchange messages with dxl use MQTT
RFC 5424	The Syslog Protocol	https://datatracker.ietf.org/doc/html/rfc5424	This document describes the syslog protocol, which is used to convey event notification messages. This protocol utilizes a layered architecture, which allows the use of any number of transport protocols for transmission of syslog messages. It also provides a message format that allows vendor-specific extensions to be provided in a structured way.	Technical		Yes	Yes	No	Yes	No	No	E-health devices security analytics

According to the answers received from SAFECARE partners (presented in Table 5.3), the standards used are related to technical, process and terminology issues. Concerning technical standards, partners mentioned that they use/consider the following: DICOM PS3.15 2021c, Emergency Data Exchange Language (EDXL) Hospital Availability Exchange (HAVE) Version 2.0 13 January 2015, IETF RFC 5246 August 2008, ISO 8001-2-2, ISO 8001-2-8, MDCG 2019-16, NIST 800-53, NIST CSF, NIST IR 7009, OASIS Message Queuing Telemetry Transport (MQTT) TC, RFC 5424. These refer to message exchange, security requirements for the use of DISOM protocol, communications security, risk management for IT-networks, Security and Privacy Controls, cybersecurity etc. With regards to process standards, partners mentioned that they consider the following EU MDR, IETF RFC 6749 October 2012, IMDRF/CYBER WG/N60FINAL:2020, ISO 14971, ISO 31000:2018, ISO/IEC 31010, NIST 800-30, NIST SP 800-61, IEC 62443-4-2, IEC 62443-4-1 and IEC TR 60601-4-5:2021, which refer to medical device cybersecurity and safety, authorisation frameworks, risk management guidelines as well as guidelines for incident response (IR), including preparation. Additionally, they proposed the use of MITRE ATT&CK® that is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. Moreover, because it references to globally recognized standards for cybersecurity, this framework can serve as a model for international cooperation on strengthening cybersecurity in Cis.

5.2.2 Information gathering from interviews

Based on the work conducted in SAFECARE project and deliverables, as well as the analysis, reports on security management and the interviews/open discussions conducted with project partners and external stakeholders (e.g. hospitals, health regulatory authorities, insurance companies, etc.), the following gaps have been identified with regards to cyber and physical security standards in healthcare organisations:

- **Gap 1.** Some hospitals representatives underlined the importance and need of processes, products and services standards, which all affect the quality of services offered to the public. They stated that these standards create a strong health care structure that the public, providers and policy makers can rely on, assuring high quality health services. In this way, it is ensured from one hand that all patients are treated with dignity and respect, and that they receive adequate services, but also a safe and secure environment to be hospitalized in. Despite this, it was also mentioned that the plethora of existing standards in terms of physical and cyber security (this is also confirmed by the list identified through the literature conducted), causes confusion and increases variations in the quality and safety of hospitals across Europe.
- **Gap 2.** End-users also mentioned that there exist different or no security plans within each hospital and recognized that comprehensive plans for the security of a hospital are needed at a national level, in order to build a common ground.

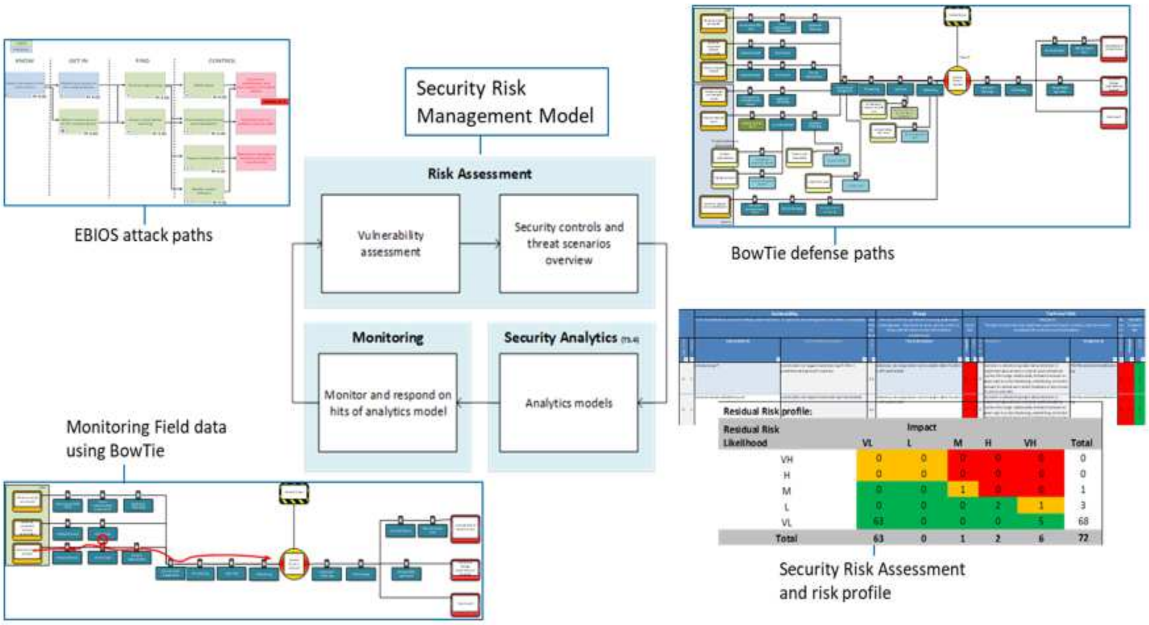
- **Gap 3.** It was also mentioned that there is a lack in crisis management process understanding and analysis (steps and stakeholders involved in healthcare setting), despite the fact that the crisis management process is well analysed in literature.
- **Gap 4.** They also stated that there exist different physical, cyber and/or cyber -physical security solutions implemented in different infrastructures: Among hospitals, there is a lack of uniformity in the adoption and implementation of solutions that can support and enhance crisis management processes.

Following the standards presented in the above sections, the gaps identified above, as well as the interviews and discussions conducted with end-users, the following recommendations/best practices for cyber and physical security standards are proposed, as they could enhance hospitals' cyber and physical safety and security as a whole:

- Several interviewees from healthcare organisations mentioned that complementary to services and products' standardisation activities, they should also get their services accredited, in order to reduce variations and enhance quality of services, as well as security and safety. The majority of EU countries have national programmes with varying degrees of stakeholder governance, of compulsion and of national uptake (28). Sub-national programmes, such as in Spain and Italy, are mostly run by regional government. Some hospitals in Europe have been accredited by Joint Commission International (JCI) that provides among others hospitals' accreditation and certification and works to improve patient safety and quality of health care (29). It also offers education, publications, advisory services etc. In more than 100 countries, JCI partners with hospitals, clinics, and academic medical centres, health systems and agencies, government ministries, academia, and international advocates to promote rigorous standards of care and to provide solutions for achieving peak performance. Combining expertise, tools, and documented insights, JCI helps as an organization seeks to provide the highest quality of care while focusing on continuous improvements. The accreditation program has been developed by international experts and sets uniform expectations for structures, processes, and outcomes for health care organizations. Each new edition of standards reflects the most current thinking in patient safety practices and concepts to help accredited and non-accredited organizations uncover their most pressing safety risks and advance their goals for continuous quality improvement (**related to Gap 1**).
- It has been also mentioned that hospitals should have a series of standardized plans (risk and vulnerability assessment, security operations, crisis management, business continuity) related to preventive planning, day-to-day operations and business continuity management (**related to Gap 2**). Complementary, within the SAFECARE project, an e-Health security Risk Management Model was developed to support the risk assessment process by quantifying security risks. The model can be used (and probably standardised) by health system manufactures and hospitals to identify risk sources, security events, vulnerabilities, threats and the related security controls. The E-Health security Risk Management Model provides a stepwise iterative approach to calculate the Risk level and define risk mitigations. By combining three methodologies/tools (EBIOS, BowTie and Security Risk assessment template), different complimentary views on a health system in scope of an assessment are visualized. EBIOS shows the underpinning

of the likelihood of an event, the BowTie diagrams show the possible impact and related security controls with their vulnerabilities. In the Security Risk Assessment template, the risk levels are quantified by combining the likelihood and impact. This results in a security profile of the assessed health system. The Health system and the related security profile needs to be validated based on field data. The E-Health Device Security Analytics and Monitoring processes are used to measure and optimize the effectiveness of the security controls of the system, identify the gaps and plan future investments and mitigation measures so that resilience and robustness of the hospital is elevated.

Figure 2 - Security Risk Management Model and the supporting elements


Security Risk Management Model
Risk Assessment
Vulnerability assessment
Security controls and threat scenarios overview
Monitoring
Monitor and respond on hits of analytics model
Security Analytics
Analytics models
EBIOS attack paths
BowTie defense paths
Monitoring Field data using BowTie
Security Risk Assessment and risk profile

Residual Risk profile:

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

- A common cyber-physical crisis management process should be established and followed within hospitals and at Member States level **(related to Gap3)**. Within SAFECARE, a global cyber-physical security management approach that maps crisis management phases with specific internal and external stakeholders, as well as the SAFECARE modules, has been proposed (as analysed in D8.4) and could be probably standardised. The proposed approach will facilitate the communication and cooperation between the different hospitals and stakeholders, in case of an incident, and enhance security and safety.
- SAFECARE solution can tackle the issue of different cyber-physical security solutions implemented in healthcare infrastructures, by providing standardised messages. Moreover, from the interviews conducted it was proposed that hospitals should integrate in their organisational structure a Holistic Security Operation Centre (HSOC) to detect, analyse, and manage cyber and physical incidents (either natural, man-made or technological) and to efficiently coordinate processes, people and technologies. Thus, a common operational picture will be achieved, and efficient information sharing will be facilitated, in order to alert other hospitals' or interconnected/interdependent CIs'

operators and involved stakeholders for any potential threats or incidents (**related to Gap 4**).

5.3 Best practices for cyber and physical security issues in the healthcare sector

To sum up and based on the standards identified from the literature review conducted and the questionnaire filled in by SAFEACARE, as well as on the interviews and discussions conducted with end-users, the best practices for cyber and physical security standards in the healthcare sector are related to quality and safety of medical and other devices (EN ISO 14971, EN ISO 13485, EN 60601, EN IEC 60522, IEC 62443-4-2, IEC 62443-4-1 and IEC TR 60601-4-5:2021,) that are also mentioned to MDCG 2019-16 Guidance on cybersecurity for medical devices (30); quality, security and safety management in the healthcare sector (ISO 22956, ISO 22300:2021, ISO 22956, ISO 22319:2017, ISO 22320:2018, ISO 22322:2015, ISO 22324:2015, ISO 22328 series, ISO 22398:2013); information systems, network and data security (21); health informatics (standards from CEN/TC 215 and ISO/TC 215 committees, ETSI TR 103 477 V1.2.1 (2020), ISO/IEC 27000:2018, ISO/IEC 27001:2018, ISO/IEC 27005:2018, ISO/IEC 27701:2019, prEN IEC 81001, ISO TR 17791).

In addition, the following standards, namely ISO 14971, ISO 31000:2018, ISO 8001-2-2, ISO 8001-2-8, and ISO/IEC 31010 have been identified from the literature and have been proposed by SAFECARE partners as well. The proposed by SAFECARE partners' technical and process standards are the following: DICOM PS3.15 2021c, Emergency Data Exchange Language (EDXL) Hospital Availability Exchange (HAVE) Version 2.0 13 January 2015, IETF RFC 5246 August 2008, MDCG 2019-16, NIST 800-53, NIST CSF, NIST IR 7009, OASIS Message Queuing Telemetry Transport (MQTT) TC, RFC 5424, EU MDR, IETF RFC 6749 October 2012, IMDRF/CYBER WG/N60FINAL:2020, NIST 800-30, NIST SP 800-61and MITRE ATT&CK.

In addition, from the interviews conducted with internal and external stakeholders, the following best practices are proposed, as they could enhance hospitals' cyber and physical safety and security as a whole:

- Hospitals should get their services accredited, in order to reduce variations and enhance quality of services (e.g. by Joint Commission International (JCI) or similar organisations).
- To facilitate the establishment of a security management framework, compliance or ISO 27001 certification could be carried out, it will allow better integration of risk management and crisis management with an organization of the resources necessary for these processes.
- Moreover, the e-Health security Risk Management Model that was developed in SAFECARE project could support the risk assessment process by quantifying security risks. The model could be used (and probably standardised) by health system manufactures and hospitals to identify risk sources, security events, vulnerabilities, threats and the related security controls.
- In addition, as proposed in the previous section, a common cyber-physical crisis management process should be established and followed within hospitals and at Member States level. The global cyber-physical security management approach (as

proposed in SAFECARE) that maps crisis management phases with specific internal and external stakeholders, as well as the SAFECARE modules, could be probably standardised. The proposed approach will facilitate the communication and cooperation between the different hospitals and stakeholders, in case of an incident, and enhance security and safety.

6 Cyber and physical security certification mechanisms

It appears from previous chapters that there exist several standards which could potentially be used for cyber and/or physical security in healthcare sector – published by different Standard Developing Organisations. In this Chapter, cyber and physical security certification related issues are presented.

6.1 Certification mechanism

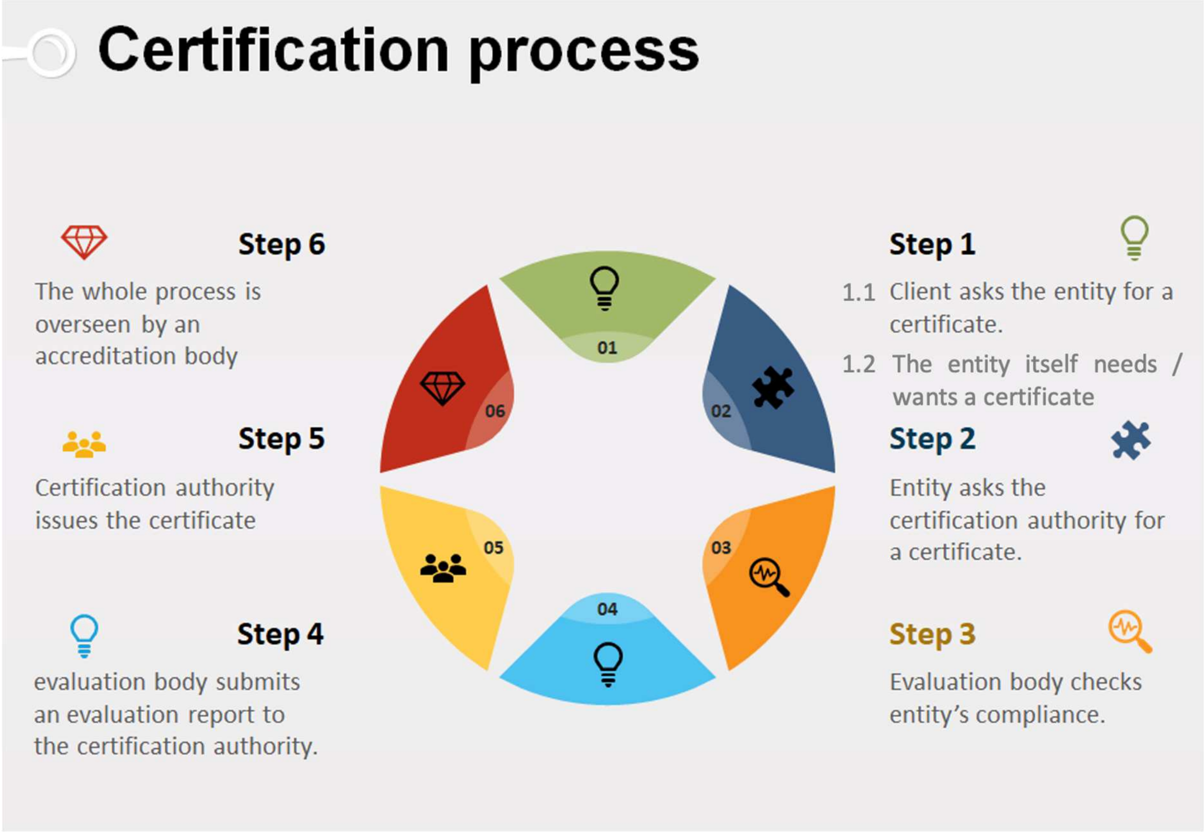
SDOs do not certify any entities, as their role is the development and agreement on standards. It is third parties (entities) that always conduct certification processes, give written assurance that a product, process or service is in conformity with certain standards and issue the final certificates (30). Certification has been defined as "the successful conclusion of a procedure to evaluate whether or not a professional activity actually meets a set of requirements" (31). A certificate is the effective conclusion of the evaluation of a professional certification activity against a set of requirements and can provide information to the potential client on e.g. the level of security attached to a product or service. These requirements can be those defining a standard or might not be mapped to any standard (28). It proves that an entity complies with certain standards, which might be more convincing than if the entity itself provided the assurance.

The key players involved in the certification process are the following:

- **Entity:** Organisation seeking certification to standards.
- **Certification Authority:** Organization accredited by a recognized accrediting body for its competence to audit and issue certification confirming that an organization meets the requirements of a standard (32).
- **Evaluation body:** An evaluator that checks whether the entity complies with a standard or with a certain set of rules and submits an evaluation report to the certification authority.
- **Accreditation body:** Organization that provides accreditation services, which is a formal, third party recognition of competence to perform specific tasks. In other words, it means that organizations seeking accreditation (certification authorities) can demonstrate to organisations seeking certification to the standards that they have been successful at meeting the requirements of international accreditation standards (32).

In order for a certificate to be issued, an entity should ask for it by a certification authority (Step 2), and this request could be triggered either by a public or private client/supplier of the entity (Step 1.1), or by the entity itself (Step 1.2). In order to obtain a certificate, an entity has to go through an evaluation (people, process and product) by an evaluation body. The evaluation body checks whether the entity complies with a standard or with a certain set of rules (Step 3) and submits an evaluation report to the certification authority (Step 4). If the candidate certificate holder passes this check, the certification authority issues the certificate (Step 5). This process is overseen by an accreditation body, which itself was created with a government mandate (Step 6). Entities' compliance with a certification scheme can be evaluated in various ways, e.g. an examination/test/checklist, a peer review or a formal analysis. For products and organisations, an analysis by an independent third party is required, which often focuses on development or operational processes.

Figure 3 - Certification process



Certification process

Step 1

1.1 Client asks the entity for a certificate.

1.2 The entity itself needs / wants a certificate

Step 2

Entity asks the certification authority for a certificate.

Step 3

Evaluation body checks entity's compliance.

Step 4

evaluation body submits an evaluation report to the certification authority.

Step 5

Certification authority issues the certificate

Step 6

The whole process is overseen by an accreditation body

The system of rules, procedures and management for performing a certification process, including the standards against which it is being certified, is called the certification programme. One certification authority may execute different certification programmes. To ensure that the certification authorities have the capacity to carry out certification programmes, they are evaluated and accredited by an accreditation body. Certification bodies may have to be accredited by a governmental or parastatal institute, which evaluates compliance with guidelines set by e.g. ISO, the European Union or some other entity for the operation of certification and inspection bodies. Through this process, entities could get guidance on the certification process and could also document their capabilities and evaluate their weaknesses, based on information from the certification scheme. Entities could even follow the principles of a certification scheme without actually achieving the certificate, as through this they could also improve security because they are a stimulus for improvement, as companies and individuals aspire to the reputation attached to the certificate.

The most common certification process, in most EU countries, is that of safety sector, as national legislation are in place within each Member State, requiring safety certifications in specific sectors, such as healthcare. For example, in France, since 2004, quality certification has been a major external quality evaluation procedure that is obligatory for all public and private healthcare facilities and is conducted every four or six years (33). Certification evaluation strategies rely on standards and benchmarking and must therefore encompass best clinical practices and care process audits, and be well supported by quality and safety indicators (Indicateur de Qualite et Securite des Soins, IQSS). Thus, the approach has implemented several care pathways, protocols, and checklist models to manage quality and reduce risk. For example, quality and risk management items include - as outlined in the French National Health Authority (Haute Autorite de Sante, HAS) certification manual - a comprehensive criteria list comprising policies governing quality and care safety improvements, professional practice evaluation (Evaluation des Pratiques Profesionnels, EPP), document management, and adverse event management (33).

6.2 Validation framework for certifications

As indicated above, in step 3 and 4, an entity has to go through an evaluation (people, process and product) by an evaluation body, which in its turn checks whether the entity complies with a standard or with a certain set of rules.

Nevertheless, there are several validation measures that are or can be used by hospital, for internal purposes, in order to track and monitor the effectiveness and efficiency of standards/certification compliance. The following is a non-exhaustive list of such monitoring systems, means and respective indicators:

- Systems
    - Patients' satisfaction measurement system, which can be applied in hospital's outpatient clinics
    - Satisfaction measurement of patients' relatives
    - Reporting system regarding hospital's malfunctions and medical mistakes
    - Complains submission system
- Means
    - Questionnaire (structured and open questions)
    - Interviews
    - Information sheets and leaflets
    - Online apps
    - Log files
    - Incident response reports
- Indicators
    - Percentage of trained employees
    - Average training days per employee
    - Number of public awareness campaigns
    - Number of patients hospitalized / year
    - Number of outpatients / year
    - Number of outpatients in Emergency Department / year
    - Average duration of hospitalization
    - Average coverage (fullness) of beds per year
    - Number of incidents occurred / year
    - Average duration of an incident to be solved
    - Reduction of response time
    - Recovery time after an incident

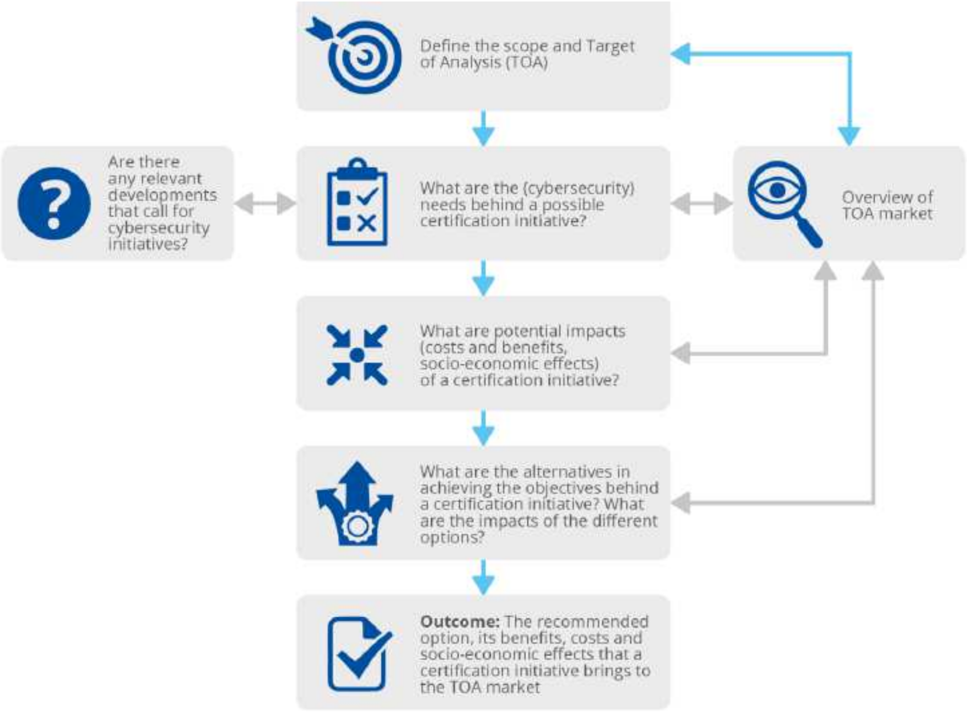
- Human casualties after an incident
- Impact of incidents in monetary terms

6.3 ENISA and the cybersecurity certification framework

In terms of cybersecurity certification, regulation (EU) 2019/881 (established under the Cybersecurity Act), establishes a European cybersecurity certification framework for ICT products, services and processes. ENISA has participated in this framework, by preparing candidate certification schemes on the request of the European Commission or the European Cybersecurity Coordination Group (representation of Member States).

EU cybersecurity certification schemes will primarily address the level of cybersecurity required for ICT products, services or processes. From an economic perspective, they could address imbalances in the market that lead to suboptimal outcomes and could also touch upon socio-economic aspects such as user trust, the duty of care of a manufacturer or provider and prevention of cybersecurity failure to protect market reputation. Therefore, the drivers for cybersecurity certification in the EU go beyond cybersecurity requirements. This broader understanding and oversight would be beneficial to the policy and regulatory certification activities of the European Commission. Towards this, ENISA conducted a study on identifying a set of methodological steps to allow for a market analysis on cybersecurity certification of ICT products, ICT services and ICT processes, which are presented below.

Figure 4 - Workflow for how to conduct assessment of the Target of Analysis (TOA) (34)


Define the scope and Target of Analysis (TOA)
Are there any relevant developments that call for cybersecurity initiatives?
What are the (cybersecurity) needs behind a possible certification initiative?
Overview of TOA market
What are potential impacts (costs and benefits, socio-economic effects) of a certification initiative?
What are the alternatives in achieving the objectives behind a certification initiative? What are the impacts of the different options?
Outcome: The recommended option, its benefits, costs and socio-economic effects that a certification initiative brings to the TOA market

In the figure presented above, the workflow on how to conduct an assessment of the Target of Analysis is presented (34). ENISA proposes two main types of analysis:

- Market assessment: A market analysis will be conducted in a market segment where there is currently no EU cybersecurity certification initiative, in order to identify if there is a justification for EU to consider new initiatives to be developed (34).

- Impact assessment: A market analysis could support the activities of the EU cybersecurity certification framework on reviewing the effects of EU cybersecurity certification. In this case, the scope of the TOA should be easier to determine, because it will be determined by the effects a scheme has on the market, given its scope that is the focus of the analysis (34).

The goal is to identify gaps in the market - from a cybersecurity certification perspective - without relying solely on input of stakeholders, but to provide evidence both from the supply and demand sides while considering societal and economic aspects. ENISA has currently transmitted the candidate EUCC scheme v.1.1.1 to the Commission in line with the provisions of Article 49 (6, 7) of Regulation (EU) 2019/881 (Cybersecurity Act). The Commission will initiate a Commission Implementing Regulation that may be adopted. ENISA has advanced in the development of a second candidate scheme, related to cloud services and is about to launch the call for an AHWG for the preparation of an EU cybersecurity certification scheme on 5G soon.

7 Security standards as part of insurance contracts in healthcare organisations

Healthcare has been reported as one of the most targeted sectors; 81% of 223 organizations surveyed, and >110 million patients in the US had their data compromised in 2015 alone, with only 50% of providers thinking that they could protect themselves from cyberattacks (35). Moreover, it has been reported that between 2009 and 2018 there have been 2.546 healthcare data breaches involving more than 500 records and resulting in theft/exposure of 189.945.874 records (36). It faces unprecedented risks and compounding regulatory compliance requirements. In addition to cyber-threats, physical threats are increasingly growing and even healthcare facilities are not immune to them. For example, in 2018, at Mercy Hospital in Chicago, four people were killed in a shooting (37). The man was able to make his way from the parking lot where the shooting started, and proceeded inside the facility. Inadequate physical security leaves both employees vulnerable and patients at risk. In fact, a study shows that hospitals are twice more likely to experience a physical attack than a cyber-attack or breach (37). Any physical or cyber incident leading to loss of assets or services, or massive patient surge, such as natural disasters or terrorist acts (including CBRNe) could affect the health care services provision and could cause overwhelming pressure to the affected health systems.

Physical and cyber attacks are not the only issue that hospitals and Critical Infrastructures in general, need to face. The proliferation of data privacy laws and industry specific cyber regulations forced many organizations to rethink the way they had been working, as these laws get even tougher by expanding: (i) the definition of "personal information" (ii) the definition of a data breach, (iii) data breach notification requirements, e.g., timing and methods of notice, and who must be notified etc.

In fact, the importance of physical and cyber security in healthcare has never been more pronounced. Now more than ever, healthcare organizations must be vigilant in establishing safeguards against physical and cyber threats. They can take practical steps to protect themselves and reduce the effects of an attack, such as strengthening resilience, as resilient organizations are less likely to be attacked and suffer less harm when attacks occur.

With regards to cyber security measures, it has been reported that healthcare organizations should adopt and implement different practices that will enhance data, systems, devices, and networks security, such as (according to ISO (2018) and NIST (2019a)) authentication, access control (authorization), availability, reliability, non-reputation, data confidentiality and integrity, backup and tracing; combined with communication, medical devises and network security mechanisms. Finally, a security-by-design approach would complete the above countermeasures, focusing on the cybersecurity concerns with respect to new devices or systems that need to be planned and implemented from the beginning of the procurement, design, development, and maintenance phases.

In addition to cyber protection measures, hospitals should also focus on physical protection and they should introduce new technologies and upgrade existing ones in order to ensure the security of their most valuable assets such as people, infrastructure, and property. Typical systems include among others the following: (a) Fences/Walls, (b) Guards, (c) Building control, (d) Intrusion detection and access control, (e) Video surveillance, (f) Audio surveillance, (g) CBRN and explosive sensors and (h) Physical Security Information Management (PSIM) systems. It is also crucial that healthcare personnel (including researchers, administrators, front desk workers, medics, transcriptionists, handlers of medical claims to IT, and technical staff) should be properly trained on physical and cybersecurity issues (38). Complementary to the aforementioned cyber and physical measures, laws and regulations, and in order to improve safety and security measures, healthcare organisations create high demands for cyber and physical security standards adoption.

Considering the aforesaid, as well as the fact that healthcare organisations need to navigate in a plethora of changing requirements for laws and regulations, they have started looking into insurance (related also to cyber and physical security) policies that cover expenses of legal counsel, regulatory action defence that also covers fines and penalties, credit monitoring for victims of a data breach, attacks, crisis management and public relations, consequential damages, business interruption loss and data recovery, cyber extortion, and more.

7.1 Insurance in the healthcare organisations

The healthcare industry must confront an evolving landscape of risk that includes changing business models, technological innovations and regulatory reforms. These challenges can impact productivity, customer relationships and financial goals. Customized healthcare facility insurance solutions can help hospitals, clinics and other healthcare facilities, assess and mitigate these risks, allowing them to meet their primary goal: delivering high-quality medical care to patients and citizens.

There is a plethora of insurance products that can cover the healthcare facility (depending on the nature of the hospital and the services it offers) indicatively the following (39):

- **General liability insurance:** This healthcare facilities insurance covers property damage, accidents related to occurrences in outpatient facilities, and damage to rental property.
- **Building coverage:** Covers an organisation's physical contents against natural hazards (e.g. fire, storm, etc.), accidental damage or theft.
- **Property coverage:** Everything that a healthcare facility owns, rents, or leases from others, including items such as business equipment, medical equipment, fixtures, furniture, and inventory, should be protected under an extensive property coverage policy.
- **Flood insurance:** Hospitals should ensure purchasing a flooding policy to ensure that flooding is covered.
- **Equipment replacement coverage:** Refers to medical diagnostic equipment that a hospital rents, leases or owns.
- **Commercial auto insurance:** Any vehicles used for business purposes should be covered under this type of policy.

- **Management liability insurance:** The management in any healthcare facility are often targeted for lawsuits. This includes directors and officers.
- **Decontamination coverage:** If a healthcare facility is required to clean up pollutants after an event, this coverage pays for things like testing, removal, clean-up, replacement of affected items and restoration.
- **Employees' compensation:** This often state required coverage pays injured or ill employees for health-related wage loss and medical costs.
- **Coverage for patients:** If property is stolen from a patient, this coverage protects you from liability.
- **Business interruption:** Coverage for costs incurred due to business interruption, such as an inability to provide services for a period of time.
- **Public relations expenses:** This insurance covers the costs associated with hiring a public relations firm to protect company's reputation following am attack/disaster.

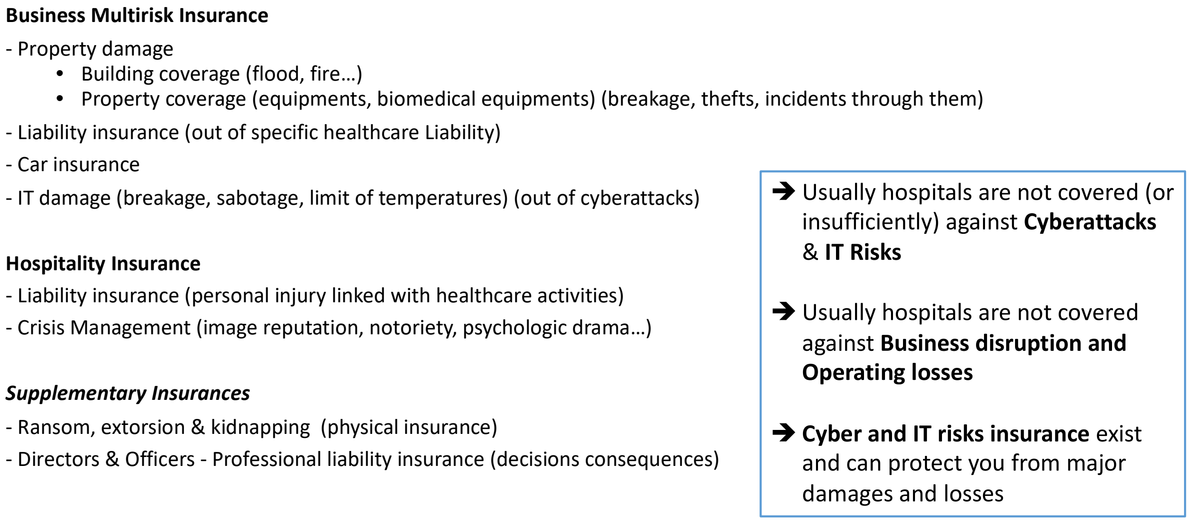
Additionally to the aforementioned, cyber insurance can be critical for healthcare organizations, as efforts to recover quickly from security incidents are a must in order to avoid severe impacts on the ability to diagnose and treat patients. Cyber insurance provides the impacted organizations with the necessary resources to recover to normal operations, or to an accepted level, quickly. The cyber insurance market is still relatively new and evolving and remains underdeveloped relative to other commercial insurance products on the market. It has been reported that the European cyber insurance industry is growing rapidly, although still small in size, with insurers reporting for 2018 an increase of 72% in gross written premiums, 3 amounting to EUR 295 million in 2018 (40). While the cyber insurance market has reached a significant size since its inception, in comparison to the overall insurance market, cyber remains a small component.

Several insurance products exist that provide cyber insurance, and cover indicatively the following (41):

- **Liability and defence Costs:** Liability and defence costs include coverage for losses and the cost of defence for lawsuits related to network security liability, such as negligent security failures or weaknesses that enable malware to spread; as well as electronic media liability, such as copyright or trademark infringement.
- **Network security:** Coverage for network security costs, including hardware and software, as well as network security liability and network security defence.
- **Incident response:** Coverage for the costs incurred for incident response in the wake of a data breach.
- **Insurance for lost or stolen laptops and mobile devices:** Coverage for the cost of replacing lost or stolen laptops or mobile devices.
- **Business interruption:** Coverage for costs incurred due to business interruption as a result of a cyber event, such as an inability to provide services for a period of time.
- **Forensic expenses:** Forensic expenses include costs incurred for investigating, isolating, and eliminating a threat.
- **Legal expenses:** Legal expenses may include defence and settlement costs for defending against a lawsuit because of a data breach.

- **Notification expenses:** Notification expenses include the costs associated with notifying consumers that their data may have been compromised.
- **Regulatory fines and penalties:** It can cover the cost of regulatory fines if regulators determine that the organisation failed to adequately protect sensitive consumer data.
- **Public relations expenses:** This insurance covers the costs associated with hiring a public relations firm to protect company's reputation following a data breach.

Figure 5 - Hospitals - most common insurance products



Business Multirisk Insurance

- Property damage
  - Building coverage (flood, fire…)
  - Property coverage (equipments, biomedical equipments) (breakage, thefts, incidents through them)
- Liability insurance (out of specific healthcare Liability)
- Car insurance
- IT damage (breakage, sabotage, limit of temperatures) (out of cyberattacks)

Hospitality Insurance

- Liability insurance (personal injury linked with healthcare activities)
- Crisis Management (image reputation, notoriety, psychologic drama…)

Supplementary Insurances

- Ransom, extorsion & kidnapping (physical insurance)
- Directors & Officers - Professional liability insurance (decisions consequences)

➔ Usually hospitals are not covered (or insufficiently) against **Cyberattacks & IT Risks**

➔ Usually hospitals are not covered against **Business disruption and Operating losses**

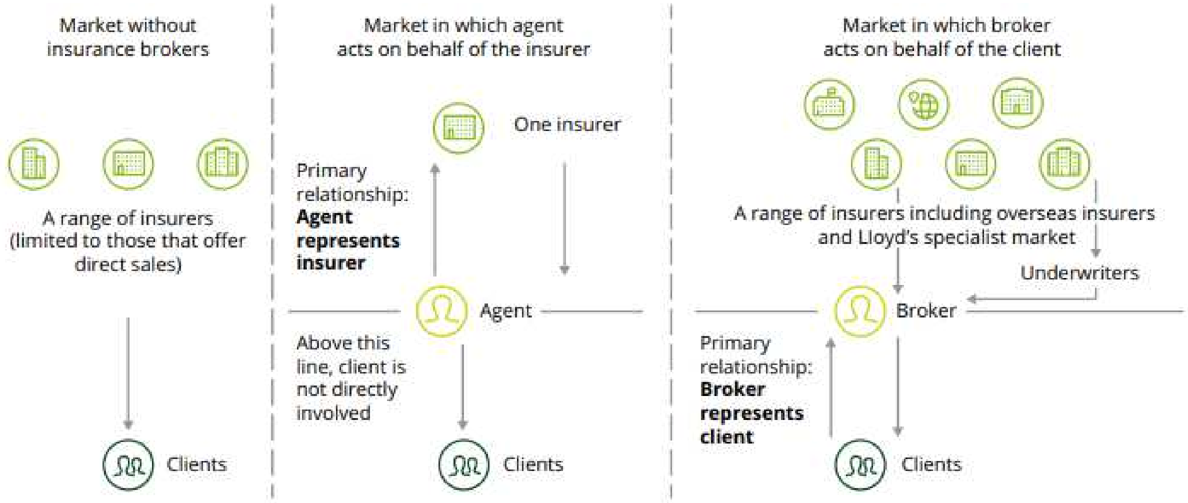
➔ **Cyber and IT risks insurance** exist and can protect you from major damages and losses

In the insurance market, there exist several insurance products distribution channels (as displayed in the following Figure) and key players. Insurers supply insurance across different policy lines, under many different brand names and through multiple channels. These distribution channels include (42):

- **Direct sales to customers:** In this process, clients negotiate with insurers to arrange coverage and buy products. The client will need to assess their risk levels and coverage needs them and will be limited to the products offered by the insurer through the direct channel.
- **Sales through an insurer agent or distributor:** In this process, insurers distribute their products through agents (brand representatives), and the clients work directly with the agent to arrange coverage that fits their needs (insurers engage with one agent, for each insurer). This may provide greater opportunity for products to be customised.
- **Sales through an insurance broker:** In this process, insurers distribute their products through brokers. The clients communicate with the broker, who will negotiate with insurer(s) to arrange the coverage. The broker has access to a range of insurers' offerings and may compare and aggregate different insurers' products for the client (to meet needs and price). Brokers are contracted with multiple insurance companies to efficiently negotiate and place coverage for their clients. It is important to mention that brokers represent their clients' interests in the market, rather than the insurer. They provide to clients personalised services and ongoing policy review and claims support. Insurance companies employ and use insurance underwriters to manage the insurance underwriting process. Underwriters are companies, individuals, or insurance companies

that carry on this critical activity for their own account or for that of others. The underwriters represent the insurer, not the customer, in the purchase transaction.

Figure 6 – Insurance products distribution channels (42)


Market without insurance brokers
A range of insurers (limited to those that offer direct sales)
Clients
Market in which agent acts on behalf of the insurer
One insurer
Primary relationship: Agent represents insurer
Agent
Above this line, client is not directly involved
Clients
Market in which broker acts on behalf of the client
A range of insurers including overseas insurers and Lloyd's specialist market
Underwriters
Broker
Primary relationship: Broker represents client
Clients

The list below represents indicative information that would shape the insurer's profile of an organisation looking for cyber or physical insurance coverage:

- **General business information:** This is related to the specification of organisation's size, type, sector, level of digitalisation, turnover, geolocation, weather, etc.
- **Buildings, properties and equipment safety and security measures:** A description of buildings, properties and equipment (incl. medical devices) that a hospital rents, leases or owns, as well as the safety and security measures used and the policies, standards and procedures followed to prevent unauthorized access, damage and interference to the organization's facilities.
- **Information Systems security:** Description of standards, policies, measures and procedures applied to support Information Systems security (e.g. authentication, availability, reliability, non-reputation, data storage and use, backup and tracing, update processes etc.).
- **Data security:** Description of standards, policies and procedures applied to support confidentiality, integrity, availability and consistency of all data stored in different forms. These guidelines are applicable to all information/records/data created, received or maintained by all permanent and temporary employees and consultants, third party vendors of the organization and business distributors who have access to the organization's data, wherever these data records are and whatever form they are in, in the course of carrying out their designated duties and functions.
- **Network security:** Physical and cyber security measures adopted to protect the network.

- **Incident management:** Policy, procedures and guidelines for safety and security incident management shall be prepared and implemented to detect, monitor, record, response, escalate and prevent events and weaknesses effectively.
- **Risk management:** Identify and assess key risks and vulnerabilities, as well as determine the controls required to keep those risks within acceptable limits.

Having collected this information, an organization can apply for insurance. The application process is usually managed by an underwriter and involves collecting information via self-assessed questionnaires (proposal forms), telephone interviews and client presentations. As mentioned above, insurance underwriters evaluate the risk and exposures of potential clients and decide what coverage the client should receive, the amount they should pay for it, or whether even to accept the risk and insure them. Their aim is to protect the insurance company from risks that they feel will make a loss and issue insurance policies at a premium that is commensurate with the exposure presented by a risk. Each insurance company has its own set of underwriting guidelines to help the underwriter determine whether or not the company should accept the risk.

To figure out the level of risk that represents an organisation, underwriters draw on a range of tools that collect information from a number of different data sources, such as vulnerability scans, threat intelligence, research etc. Another recent underwriting requirement introduced by cyber insurers is the use of supplementary application forms specifically addressing ransomware controls. As with other application forms, some questions represent absolute cybersecurity requirements while others fall into the preferred category. The "must have" controls typically include the following: (a) multi-factor authentication, (b) backups and protected backup storage, (c) disabled or protected Remote Desktop Protocol (RDP). Based on the analysis of each client, the underwriters may decline the risk, or may provide a quotation in which the premiums have been loaded or in which various exclusions have been stipulated, which restrict the circumstances under which a claim would be paid.

In terms of physical security policies, insurance market is quite experienced and risks well understood and managed, while cyber security policies still lag behind with several obstacles hindering its adoption. Some of these obstacles are the following among other: (a) the limited availability of historical data does not allow accurate pricing of insurance premiums. To tackle this, many insurance companies have entered into partnerships with information technology security firms to improve their access to incidents information, although, so far, few have reported that these partnerships have provided sufficient data and expertise to quantify cyber risk (43); (b) even if more data were available - that data may become quickly out-of-date as a result of the constantly evolving complexity and vectors of cyber attacks (43); (c) the need to create more intelligent and sophisticated underwriting process in order to support insurers' risk assessment, coverage limits and costs (44); (d) lack of harmonisation across policy offerings (e.g. definitions, terminology, exclusions etc.) leads to difficulty in offers comparison and therefore reduces the attractiveness of such products; (e) misunderstandings about cyber insurance coverage, as some insurers are expanding the stand-alone cyber insurance and some others are expanding the scope of traditional coverage to include cyber risk (43) .

It appears that further developments of the cyber insurance market should be made, that will likely require evolving product design that can cope with the dynamic nature of cyber risks. To tackle the aforementioned obstacles, leaders in the cyber insurance market have created partnerships with Information Technology leaders, e.g. AIG with RSA, IBM, K2 (45). Additionally, efforts have been made to increase historical data collection and analysis, enhance harmonisation, improve risk management etc. In support of this, insurance companies have recognised the value of accredited standards to support risk management. And as insurance companies are already recognizing the value of accredited standards to support risk management, as every sector, including the healthcare sector relies on certification, inspection, testing or measurement services to promote its proficiency on a wide range of issues such as quality, security and safety. Accreditation is internationally recognized as a robust and independent declaration of an organization's competence, the validity and suitability of its methods, the appropriateness of its equipment and facilities, and ongoing assurance through its internal quality control.

In some sectors, the value of standards in the overwriting process has been clearly identified. For example, in Italy, the Italian Workers' Compensation Authority (INAIL) reported how the roll-out of occupational health and safety standard OHSAS 18001 had reduced the severity and frequency of accidents by as much as 40 % in some sectors amongst organizations certified to the standard. This, in turn, led to lower insurance costs among participating companies (46). Moreover, in Japan, the Development Bank of Japan (DBJ) provided more attractive loan rates and discounted insurance premiums to commercial businesses that have accredited certification of their business continuity management system to ISO 22301 and ISO 22313. This helped the bank to manage its risk exposure as it encouraged firms to build resilience and be more in control of their risks. Security consultancy Counterpane Internet Security, for example, was offering customers of its managed security monitoring service the savings of 20 % - 40 % on insurance against the risk of losing revenue or critical information through network security breaches (45). In another example from early 2001, J.S. Wurzler Underwriters, one of the first cyber insurance brokers/underwriters, was offering 20% discount to organization that followed their defined security standards.

In addition to the aforementioned examples and with regards to cyber insurance, from the interviews conducted with SAFECARE partners, external hospitals and insurance companies, it appeared that factors affecting the cost of the insurance contract are the years of the contract, the risk profile of the insured company, the implementation of safety and security measures as well as the adoption of standards could reduce the cost of the contract. With regards to cyber-physical security standards adoption, it was mentioned that: (a) physical security standards adoption is a perquisite for traditional healthcare organisations coverage (physical security), and (b) in terms of cyber insurance, cyber security standards adoption is not a factor affecting the cost formula, but it is a good-to-have and could potentially reduce the contract by 10-15%. It was also mentioned that standards' adoption provides mutual benefits to insurers and insurance companies, as it can be a proof of an organization's competence and quality as well it can support risk management during the overwriting process.

8 Conclusion

The aim of the Deliverable is to extract and present best practices on cyber and physical security standards in healthcare organisations. In meeting this aim, initially (Chapter 0) the standardization landscape was described, with a focus given to the relative legal framework, the Standards Developing Organisations (SDOs), as well as the relative standardisation process. In Chapter 5 the cyber and physical security standards in the healthcare sector, as well as the gaps, recommendations, and best practices, were identified and presented (based on the normative literature, SAFECARE partners' and external stakeholders' knowledge and experience). In Chapter 6, cyber and physical security certification related issues are presented. Finally, in Chapter 7 the importance of cyber and physical standards is identified and highlighted and the adoption and consideration of these standards in the insurance process (overwriting, cost etc.) is analysed.

In doing this, it appears that if healthcare organisations should adopt cyber-physical security solutions, such as SAFECARE that are based on process and technical standards, they could benefit by (a) better managing risks, threats, impacts and attacks; (b) enhancing the communication and coordination of internal and external stakeholders; (c) supporting them in getting certified on process and technical standards and (d) assisting them in insurance overwriting process and insurance cost reduction. In doing this, the quality of services offered to the public will be enhanced and a strong health care structure that the public, providers and policy makers can rely on will be created. In this way, it is ensured from one hand that all patients will be treated with dignity and respect, and that they will receive adequate services, in a safe and secure environment.

9 References

1. **K.M., Stine, K, Quill and GA, Witte.** Framework for Improving Critical Infrastructure Cybersecurity. *Framework for Improving Critical Infrastructure Cybersecurity.* [Online] 2014. [Cited: 10 04 2021.]

2. **EU.** Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. [Online] 2016. https://eur-lex.europa.eu/legal-content/EN/TXT.

3. —. Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). [Online] 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

4. **European Commission.** Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation. [Online] 2012. [Cited: 12 05 2021.]

5. —. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''). [Online] 2013. [Cited: 20 05 2020.] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN.

6. —. REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU . [Online] 2017. [Cited: 12 05 2021.] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0746&from=EN.

7. —. European standards. *European standards.* [Online] European Commission, 2021. [Cited: 12 05 2021.] https://ec.europa.eu/growth/single-market/european-standards_en.

8. —. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation. [Online] 2012. [Cited: 19 06 2021.]

9. —. *Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.* [Online] 2012. [Cited: 19 06 2021.] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025.

10. **European Committee for Standardization (CEN).** European Committee for Standardization (CEN). [Online] 2021. [Cited: 19 06 2021.] https://www.cen.eu/Pages/default.aspx.

11. **European Committee for Electrotechnical Standardization (CENELEC).** *European Committee for Electrotechnical Standardization (CENELEC).* [Online] European Committee for Electrotechnical Standardization (CENELEC), 2021. [Cited: 19 05 2021.] https://www.cenelec.eu/aboutcenelec/whoweare/index.html.

12. **European Telecommunications Standards Institute (ETSI) .** European Telecommunications Standards Institute (ETSI) . *European Telecommunications Standards Institute (ETSI) .* [Online] 2021. [Cited: 19 06 2021.] https://www.etsi.org/.

13. **CEN-CENELEC.** CEN-CENELEC. *CEN-CENELEC.* [Online] 2021. [Cited: 19 05 2021.] https://www.cencenelec.eu/Pages/default.aspx.

14. **INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO).** AGREEMENT ON TECHNICAL CO-OPERATION BETWEEN ISO AND CEN (Vienna Agreement) . [Online] 2001. [Cited: 19 06 2021.] https://isotc.iso.org/livelink/livelink/fetch/2000/2122/3146825/4229629/4230450/4230458/01__Agreement_on_Technical_Cooperation_between_ISO_and_CEN_(Vienna_Agreement).pdf?nodeid=4230688&vernum=-2.

15. **CENELEC.** IEC - CENELEC Agreement on Common planning of new work and parallel voting. [Online] 2016. [Cited: 19 06 2021.] https://ftp.cencenelec.eu/CENELEC/Guides/CLC/13_CENELECGuide13.pdf.

16. **Internation Standardisation Organisation.** Internation Standardisation Organisation. *Internation Standardisation Organisation.* [Online] 2021. [Cited: 19 06 2021.] https://www.iso.org/home.html.

17. **International Electrotechnical Committee (IEC) .** International Electrotechnical Committee (IEC) . *International Electrotechnical Committee (IEC) .* [Online] 2021. [Cited: 19 06 2021.] https://www.iec.ch/homepage.

18. **International Telecommunication Union (ITU) .** International Telecommunication Union (ITU) . *International Telecommunication Union (ITU) .* [Online] 2021. [Cited: 19 06 2021.] https://www.itu.int/en/Pages/default.aspx.

19. **Internet Engineering Task Force (IETF) .** Internet Engineering Task Force (IETF) . *Internet Engineering Task Force (IETF) .* [Online] 2021. [Cited: 19 06 2021.] https://www.ietf.org/.

20. **World Wide Web Consortium (W3C).** World Wide Web Consortium (W3C). *World Wide Web Consortium (W3C).* [Online] 2021. [Cited: 19 06 2021.] www.w3.org.

21. **DG for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW).** DG for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). *DG for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW).* [Online] 2021. [Cited: 19 6 2021.] https://ec.europa.eu/growth/.

22. **DG for Communications Networks, Content and Technology (DG CNECT).** DG for Communications Networks, Content and Technology (DG CNECT). *DG for Communications Networks, Content and Technology (DG CNECT).* [Online] 2021. [Cited: 19 06 2021.] https://ec.europa.eu/digital-single-market/.

23. **DG for Migration and Home Affairs (DG Home).** DG for Migration and Home Affairs (DG Home). *DG for Migration and Home Affairs (DG Home).* [Online] 2021. [Cited: 19 06 2021.] https://ec.europa.eu/home-affairs/index_en.

24. **CEN-CENELEC.** CEN-CENELEC. *European Standardisation.* [Online] 2021. [Cited: 02 07 2021.] https://www.cencenelec.eu/european-standardization/.

25. **Poustourli, A.** European and International Workshop Agreements: A Brief Example in Security Research Areas. *13th INTERNATIONAL CONFERENCE "STANDARDIZATION, PROTYPES AND QUALITY: A MEANS OF BALKAN COUNTRIES' COLLABORATION".* 2016.

26. **ISO.** ISO/IEC GUIDE 2:2004 - Standardization and related activities — General vocabulary. [Online] 2016. [Cited: 01 09 2021.] https://www.iso.org/standard/39976.html.

27. —. ISO. [Online] 2021. [Cited: 01 09 2021.] https://www.iso.org/deliverables-all.html.

28. **Shaw, Charles, et al., et al.** Towards hospital standardization in Europe. *International Journal for Quality in Health Care Advance.* 2010.

29. **Joint Commission International (JCI).** Joint Commission International (JCI). *Joint Commission International (JCI).* [Online] 2021. [Cited: 02 08 2021.] https://www.jointcommissioninternational.org/about-jci/who-we-are/.

30. **European Commission.** MDCG 2019-16 - Guidance on Cybersecurity for medical devices . *MDCG 2019-16 - Guidance on Cybersecurity for medical devices .* [Online] 2020. [Cited: 20 10 2021.] https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native.

31. **Dankers, C.** Environmental and Social Standards, Certification and Labelling for Cash Crops. *FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS.* [Online] 2003. [Cited: 02 09 2021.] http://www.fao.org/3/Y5136E/y5136e00.htm#Contents.

32. **ENISA.** Security certification practice in the EU. [Online] 2013. [Cited: 05 07 2021.] https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study/at_download/fullReport.

33. **Certification Answers.** Certification Answers. [Online] 2021. [Cited: 15 08 2021.] https://www.certification-answers.com.au/keyplayers.

34. **Salma, Israa and Waeli, Mathias.** A framework for the implementation of certification procedures in nurse level: a mixed approach study. *BMC Health Services Research .* 2021, Vol. 21, 932.

35. **ENISA.** CYBERSECURITY CERTIFICATION MARKET STUDY. [Online] 2021. [Cited: 02 09 2021.] https://www.enisa.europa.eu/publications/cybersecurity-certification-market-study.

36. **KPMG.** Health care and cyber security: increasing threats require increased capabilities. [Online] 2015. https://assets.kpmg/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf.

37. **HIPAA.** HIPAA Journal. *Healthcare Data Breach Statistics.* [Online] 2018. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

38. **Adelafa, L.** Healthcare experiences twice the number of cyber attacks as other industries. [Online] 2018. https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.

39. **Martin G., Martin P., Hankin C., Darzi A., Kinross J.** Cybersecurity and healthcare: how safe are we? *BMJ.* 2017, Vol. 358, j3179.

40. **General Liability.** Healthcare Facilities Insurance Policy Information. [Online] 2021. [Cited: 01 09 2021.] https://generalliabilityinsure.com/small-business/healthcare-facilities-insurance.html.

41. **European Insurance and Occupational Pensions Authority (EIOPA).** THE CYBER INSURANCE MARKET WORKING GROUP - February 2020 Summary Report. [Online] 2020. [Cited: 02 09 2021.] • Encourage the use of solid quantitative models in addition to qualitative information for effective risk-based premiums calculation; and.

42. **Zeguro.** Cyber Insurance Checklist: What You Should Keep in Mind When Buying Cyber Insurance. [Online] 2021. [Cited: 02 09 2021.] https://www.zeguro.com/blog/cyber-insurance-checklist-what-you-should-keep-in-mind-when-buying-cyber-insurance.

43. **Deloitte.** The economic value of insurance broking - National Insurance Brokers Association. [Online] 2020. [Cited: 01 09 2021.] https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-dae-niba-economic-value-of-insurance-brokers-151020.pdf.

44. **OECD.** *Enhancing the Role of Insurance in Cyber Risk Management.* s.l. : OECD, 2017.

45. **Romansky, Sasha, et al., et al.** Content Analysis of Cyber Insurance Policies:How do carriers write policies and price cyber risk? *Journal of Cybersecurity.* 2019, Vol. 5, 1.

46. **Bogomolniy, Oleg.** Cyber Insurance Conundrum:Using CIS Critical Security Controls for Underwriting Cyber Risk. [Online] 2021. [Cited: 10 09 2021.] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiqk_vE4NjzAhWGq6QKHS4qAZ8QFnoECAgQAQ&url=https%3A%2F%2Fwww.sans.org%2Freading-room%2Fwhitepapers%2Flegal%2Fcyber-insurance-conundrum-cis-critical-security-controls-un.

47. **Istituto Nazionale Assicurazione contro gli Infortuni sul Lavoro (INAIL).** Promozione e cultura della prevenzione . [Online] 2021. [Cited: 02 07 2021.] https://www.inail.it/cs/internet/attivita/prevenzione-e-sicurezza/promozione-e-cultura-della-prevenzione/sgsl.html.

48. **British Standard Institute (BSI).** *BS11200: Crisis Management – guidance and good practice* . s.l. : BSI, 2014.

10 Appendix 1- SDOs committees relevant to cyber and physical security

Table 10.1 Committees relevant to cyber security

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/CLC/ETSI/JWG eAcc	eAccessibility	eAccessibility	5	All
CEN	CEN/CLC/JTC 3	Quality management and corresponding general aspects for medical devices	The objective of the joint Technical Committee is to contribute to, and where necessary draft, suitable standards for "Quality management and corresponding general aspects for medical devices" that are applicable internationally and relevant to the essential requirements of EU Directives. The joint Technical Committee closely cooperates with ISO/TC 210 'Quality management and corresponding general aspects for medical devices' in the development of standards and revisions. The objective of the joint Technical Committee is to contribute to a further global harmonization of standards in close co-operation with ISO/TC 210. In principle the standards are drafted by ISO/TC 210 under the Vienna agreement with ISO-lead, including the joint work programme with IEC/SC 62. The joint Technical Committee will liaise with other Technical Committees - to achieve a coherent set of horizontal and product standards; - to minimize the necessity for additional European requirements; - to advise on aspects concerning quality management and risk management to ensure an optimal use of EN ISO 13485 and EN ISO	18	Healthcare

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			14971.		
CEN	CEN/CLC/JTC 13	Cybersecurity and Data Protection	Development of standards for cybersecurity and data protection covering all aspects of the evolving information society including but not limited to: - Management systems, frameworks, methodologies - Data protection and privacy - Services and products evaluation standards suitable for security assessment for large companies and small and medium enterprises (SMEs) - Competence requirements for cybersecurity and data protection - Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices Included in the scope is the identification and possible adoption of documents already published or under development by ISO/IEC JTC 1and other SDOs and international bodies such as ISO, IEC, ITU-T, and industrial fora. Where not being developed by other SDO's, the development of cybersecurity and data protection CEN/CENELEC publications for safeguarding information such as organizational frameworks, management systems, techniques, guidelines, and products and services, including those in support of the EU Digital Single Market.	21	All
CEN	CEN/CLC/JTC 16	CEN/CENELEC Joint Technical Committee on	To standardize all active implantable medical devices and their accessories		Healthcare

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
		Active Implantable Medical Devices			
CEN	CEN/SS F12	Information Processing Systems	Information Processing Systems	2	All
CEN	CEN/TC 79	Respiratory protective devices	To prepare European Standards for respiratory protective devices for use in the work place and for fire fighting and for rescue purposes, where there exists a risk to health from inhaling dusts, fumes, gases, vapours or from oxygen deficiency, as well as European Standards for underwater breathing apparatus.	56	Healthcare
CEN	CEN/TC 215	Respiratory and anaesthetic equipment	Standardization in the field of anaesthetic and respiratory equipment in particular: - anaesthetic machines; - lung ventilators; - medical gas supply systems and related components; - medical breathing systems; - anaesthetic gas scavenging systems; - related monitoring equipment; - tracheal tubes and related equipment. Excludes equipment currently within the scopes of other CEN/TC, but includes (with appropriate liaison with CENELEC) electrically powered equipment.	71	Healthcare

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 224	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	The development of standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations and privacy in a multi sectorial environment. It covers: - Operations such as applications and services like electronic identification, electronic signature, payment and charging, access and border control; - Personal devices with secure elements independently of their form factor, such as cards, mobile devices, and their related interfaces; - Security services including authentication, confidentiality, integrity, biometrics, protection of personal and sensitive data; - System components such as accepting devices, servers, cryptographic modules; CEN/TC 224 multi-sectorial environment involves sectors such as Government/Citizen, Transport, Banking, e-Health, as well as Consumers and providers from the supply side such as card manufacturers, security technology, conformity assessment body, software manufacturers.	32	All
CEN	CEN/TC 225	AIDC technologies	Standardization of data carriers for automatic identification and data capture, of the data element architecture therefore, of the necessary test specifications and of technical features for the harmonization of cross-sector applications. Establishment of an appropriate system of registration authorities, and of means to ensure the necessary maintenance of standards.	21	All

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 239	Rescue systems	To define standards for emergency for emergency medical vehicles and the equipment thereof as well as for first aid equipment, in the interests of providing safe and comfortable transport and preclinical treatment for patients.	9	Healthcare
CEN	CEN/TC 251	Health informatics	Standardization in the field of Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems and to enable modularity. This includes requirements on health information structure to support clinical and administrative procedures, technical methods to support interoperable systems as well as requirements regarding safety, security and quality.	96	Healthcare
CEN	CEN/TC 310	Advanced automation technologies and their applications	Standardization in the field of automation systems and technologies and their application and integration to ensure the availability of the standards required by industry for design, sourcing, manufacturing and delivery, support, maintenance and disposal of products and their associated services. Areas of standardisation may include enterprise modelling and system architecture, information and its supporting systems, robotics for fixed and mobile robots in industrial and specific non-industrial environments, automation and control equipment and software, human and mechanical aspects, integration technologies and system operational aspects. These standards may utilise other standards and technologies beyond the scope of TC310, such as machines,	6	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
			equipment, information technologies, multi-media capabilities, and multi-modal communications networks.		
CEN	CEN/TC 319	Maintenance	Standardization in the field of maintenance as far as generic standards which are generally applicable are concerned	7	N/A
CEN	CEN/TC 353	Information and Communication Technologies for Learning, Education and Training	Produce standards in the field of information and communication technologies relating to learning, education and training. The European Standards (EN), Technical Specifications (TS) and Technical Reports (TR) that are developed will have a well-defined European scope. These may include: - Development of CWAs and other specifications into standards, if appropriate - Developments of national standards into European Standards	10	All
CEN	CEN/TC 362	Healthcare services - Quality management systems	Healthcare services - Quality management systems	2	Healthcare
CEN	CEN/TC 365	Internet Filtering	Internet Filtering	1	All
CEN	CEN/TC 389	Innovation Management	Standardization of tools that allow companies and organizations to improve their innovation management, including all kinds of innovation	7	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
			and all the related aspects, as well as the relations with R&D activities.		
CEN	CEN/TC 419	Forensic Science Processes	To ensure the integrity of the forensic process (as a single process), the Project Committee should develop European Standards which lay down the provisions for forensic science processes, which start at the scene of crime, through the recognition, recording, recovery, transportation and storage of material followed by the examination, analysis of material, interpretation of results, reporting and data exchange	2	N/A
CEN	CEN/TC 445	Digital information Interchange in the Insurance Industry	Standardization in the field of digital information interchange in the European insurance industry. This applies to aspects of policy administration (quotation, offer, application, transfer of contract and premium data, premium and commission statement, party and contract changes, search and information services for party and contract) and of claims handling (notification, verification, assessment, authorization, settlement and reimbursement, recovery, status information). Standardization will focus on the digital information interchange among insurance companies, intermediaries, sales organizations, portals, service providers and customers. All lines of business in the insurance industry may be considered, such as life, health, property and casualty.	1	Healthcare

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/WS 099	CEN Workshop on the Semantic and Syntactical Interoperability for Crisis and Disaster Management	CEN Workshop on the Semantic and Syntactical Interoperability for Crisis and Disaster Management	1	All
CEN	CEN/WS 100	CEN Workshop Trial Guidance Methodology (TGM)	CEN Workshop Trial Guidance Methodology (TGM)	1	N/A
CEN	CEN/WS 101	CEN WS Crisis management - Building a Common Simulation Space	CEN WS Crisis management - Building a Common Simulation Space	1	All
CEN	CEN/WS 102	CEN Workshop on guidelines for introducing tele-medical and pervasive monitoring technologies	This Workshop will develop a CEN Workshop Agreement (CWA), which will define guidelines for introducing, implementing and operating sensor monitoring technologies into the private homes of citizens who are in need of care and for the purpose of detecting critical events and trends. The guidelines will describe and exemplify the processes and procedures to support an ethically responsible balance between, on the one hand, respect for the autonomy and privacy of the citizens in need of care and,	1	Healthcare

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
		balancing privacy protection against the need for oversight and care	on the other, the obligation to provide quality care of typically frail citizens. The guidelines will not include issues of security or technical requirements for availability of information to relevant parties. The guidelines will not include management of or procedures for handling monitoring data. The primary target groups of the workshop are care organizations (public or private) that are responsible for delivering social care and health care to citizens		
CEN	CEN/WS 104	Societal and Social Impact Assessment Framework to Support Adoption of New Capabilities in Crisis Management	Societal and Social Impact Assessment Framework to Support Adoption of New Capabilities in Crisis Management		All
CEN	CEN/WS 111	Guidelines for Micro-SMEs on GDPR Compliance	Guidelines for Micro-SMEs on GDPR Compliance		All
CEN	CEN/WS ICT	ICT/SKILLS Workshop (IT profiles and curricula)	ICT/SKILLS Workshop (IT profiles and curricula)	9	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/WS JXF	XFS for the Java Platform	XFS for the Java Platform	35	All
CEN	CEN/WS TER-CDM	Terminologies in Crisis and Disaster Management	Terminologies in Crisis and Disaster Management	1	All
CEN	CEN/WS ZDMTerm	Zero Defects in Digital Manufacturing Terminology	Establish the terminology and definition of concepts associated with digital manufacturing in the context of Industry 4.0, especially including concepts of zero defects manufacturing, and to explain how these concepts relate to quality management initiatives.		All
CEN	CEN/WS EXOSK	Integration process of new technologies of physical assistance such as exoskeletons	Integration process of new technologies of physical assistance such as exoskeletons		All
CENELEC	CEN/CLC/WS ZONeSEC	Interoperability of security systems for the surveillance of widezones	Interoperability of security systems for the surveillance of widezones	1	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CEN/CLC/WS SEP-IoT	Workshop on Best Practices and a Code of Conduct for Licensing Industry Standard Essential Patents in 5G and the Internet of Things (IoT), including the Industrial Internet	The scope of the workshop will be primarily to define a set of recommended best practices for licensing SEPs relating to the IoT to be followed by both good faith licensors and good faith licensees. A further objective of the workshop will be developing a workable industry Code of Conduct based on the best practices identified by workshop participants and considering ways to improve and ideally streamline or standardise the licensing process. Together these would form a concept that has been proposed called the "IoT SEP Licensing Portal".	1	All
CENELEC	CEN/CLC/JTC 19	Blockchain and Distributed Ledger Technologies	preliminary scope: To prepare, develop and/or adopt standards for Blockchain and Distributed Ledger technologies covering the following aspects: - Organizational frameworks and methodologies, including IT management systems - Processes and products evaluation schemes - Blockchain and distributed ledger guidelines - Smart technology, objects, distributed computing devices, data services The JTC will focus on European requirements, especially in the legislative and policy context, and will proceed with the identification and possible adoption of standards already available or under development in other SDOs, which could support the EU Digital Single Market and/or EC Directives/Regulations.		All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CEN/CLC/JTC 13	Cybersecurity and Data Protection	Development of standards for cybersecurity and data protection covering all aspects of the evolving information society including but not limited to: - Management systems, frameworks, methodologies - Data protection and privacy - Services and products evaluation standards suitable for security assessment for large companies and small and medium enterprises (SMEs) - Competence requirements for cybersecurity and data protection - Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices Included in the scope is the identification and possible adoption of documents already published or under development by ISO/IEC JTC 1and other SDOs and international bodies such as ISO, IEC, ITU-T, and industrial fora.	21	All
CENELEC	CEN/CLC/JTC 12	Design for All	To develop the deliverable requested in 4.1 of M/473: 'A new standard (or other deliverable as appropriate to be proposed by the ESOs and accepted by the European Commission), should be developed that describes how the goods manufacturing industry as well as public and private service entities in their processes can consider accessibility following Design for all approach with due consideration for assistive technologies and services that could help bridging the usage gap of the product or service'.	1	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CEN/CLC/ETSI/SEG-CG	CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids	CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids		N/A
CENELEC	CEN/CLC/ETSI/JWG eAcc	eAccessibility	eAccessibility	5	All
CENELEC	CEN/CLC/ETSI/SMCG	CEN-CENELEC-ETSI Coordination Group on Smart Meters	CEN-CENELEC-ETSI Coordination Group on Smart Meters	1	N/A
CENELEC	CLC/TC 215	Electrotechnical aspects of telecommunication equipment	To address standardization in the field of electrotechnical aspects of telecommunication equipment and associated infrastructures and liaise with other standardization bodies as appropriate. - To prepare harmonized standards (EN, TS or TR) covering all aspects of generic and application-specific telecommunications cabling (e.g. ISDN, LAN and others) within all types of premises. - These documents also cover the requirements and recommendations for building infrastructures related to the effective installation and operation of associated telecommunication equipment by reference to the existing or forthcoming standards provided by the relevant committees or using technical inputs from them	71	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 213	Cable management systems	To prepare European standardization publications for products and systems used for the management of all types of cables, information and communication lines, electrical power distribution conductors and associated accessories. Management includes support and/or containment and/or retention and/or protection against external influences.	36	N/A
CENELEC	CLC/SR 124	Wearable Electronic Devices and Technologies	Wearable Electronic Devices and Technologies		N/A
CENELEC	CLC/SR 123	Management of network assets in power systems	Management of network assets in power systems		N/A
CENELEC	CLC/SR 122	UHV AC transmission systems	UHV AC transmission systems		N/A
CENELEC	CLC/TC 108X	Safety of electronic equipment within the fields of Audio/Video,	To deal with the adoption in CENELEC of technical work of IEC/TC 108 and to coordinate the work with other technical bodies at European level e.g. ETSI. To make own standards where a particular need arises. NOTE The field of application of IEC/TC 108 is as follows: Standardization in the	34	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
		Information Technology and Communication Technology	field of safety for audio/video and similar technology, information technology and communication technology equipment. - To ensure that any deviation from the IEC standards, such as common modifications, special national conditions and A-deviations, is only in response to a clear and justifiable European need, such as European and national legislative needs. - To resolve application questions e.g. raised by CCA Operational Staff Meetings relative to standards within the responsibility of CLC/TC 108X. -To keep IEC/TC 108 informed of European requirements so that they may be considered for inclusion in IEC standards within the responsibility of IEC/TC 108.		
CENELEC	CLC/SR 103	Transmitting equipment for radiocommunication	Transmitting equipment for radiocommunication	22	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 100X	Audio, video and multimedia systems and equipment and related sub-systems	To monitor the adoption in CENELEC of the technical work from IEC/TC 100 standards in the field of audio, video and multimedia systems and equipment. These standards include specification of the performance, methods of measurement for consumer and professional equipment and their system application as well as interoperability with other systems and equipment. To ensure that any deviation from the IEC standards, such as common modifications, special national conditions and A-deviations, is only in response to a clear and justifiable European need, such as European and national legislative requirements. To strive towards keeping international and European requirements aligned as far as possible (applying the different mechanisms of the Dresden Agreement). To coordinate the work with other standardisation organisations on European level, taking responsibility for applicable mandates from the European Commission and developing its own standards only when necessary. Standards and other deliverables prepared by Technical Area 5 (TA5) of IEC/TC 100 do not fall under the scope of CLC/TC 100X but are covered on European level by CLC/TC 209	360	N/A
CENELEC	CLC/SR 86C	Fibre optic systems and active devices	Fibre optic systems and active devices	113	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 86BXA	Fibre optic interconnect, passive and connectorised components	To prepare and maintain European Standards and specifications for fibre optic interconnecting devices, passive and/or connectorised components, fibre optic protective housings, fibre management systems, fusion splice protectors, mechanical splices, unprotected microduct tubes and microduct tube connectors.	314	N/A
CENELEC	CLC/SR 86B	Fibre optic interconnecting devices and passive components	Fibre optic interconnecting devices and passive components		N/A
CENELEC	CLC/TC 86A	Optical fibres and optical fibre cables	To prepare and maintain specifications for optical fibres and optical fibre cables, excluding image transmission types	108	N/A
CENELEC	CLC/SR 86	Fibre optics	Fibre optics	25	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 72	Automatic electrical controls	To prepare harmonized standards for rules related to inherent safety, to the operating characteristics where such are associated with applicational safety and to the testing of automatic electrical control devices used in appliances and other apparatus, electrical and non-electrical for household and similar purposes such as those for central heating, air conditioning etc. including the following: 1. Automatic electrical control devices mechanically, electro-mechanically, electrically or electronically operated responsive to or controlling such parameters as temperature, pressure, passage of time, humidity, light, electrostatic effect, flow or liquid level. 2. Automatic electrical control devices serving the starting of small motors that are used principally in appliances and apparatus for household and similar purposes. Such control devices may be built into or be separate from the motor. 3. Non-automatic control devices when such are associated with automatic control devices.	65	N/A
CENELEC	CLC/TC 62	Electrical equipment in medical practice	To establish harmonized standards and other publications concerning electrical equipment, electrical systems and software used in healthcare and their effects on patients, operators, other persons and the environment.	210	Healthcare

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 57	Power systems management and associated information exchange	To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centres, substations and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems and databases, which may be outside the scope of TC 57. The special conditions in a high voltage environment have to be taken into consideration.	115	All
CENELEC	CLC/SC 46XC	Multicore, multipair and quad data communication cables	To produce European Cable Specifications for multicore and symmetrical pair/quad cables used in digital and analogue communication systems such as ISDN, LAN and data communication systems. According to the installation considerations, five categories of cables are to be considered: 1. equipment cables, 2. work area cables, 3. horizontal floor wiring cables, 4. riser cables, 5. campus cables.	36	N/A
CENELEC	CLC/SC 46XA	Coaxial cables	To establish and maintain European Standards regarding coaxial cables for use in telecommunication, data transmission, radio frequency, video-communication and signalling equipment.	56	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 46X	Communication cables	To establish standards related to wires, symmetric cables, coaxial cables and waveguides with metallic conductors for use in telecommunication, data transmission, radio frequency, video communication and signalling equipment to satisfy the advances in developing technologies. Particular requirements for materials, if necessary, will be evaluated in liaison with other technical committees.	102	N/A
CENELEC	CLC/SR 46F	RF and microwave passive components	RF and microwave passive components	76	N/A
CENELEC	CLC/BTWG 154-1	EMC standardization in the EU regulatory framework	To develop the necessary alignment elements between EMC standardisation activities and the regulatory framework		N/A
ETSI	EP EHEALTH	ETSI PROJECT (EP) EHEALTH	Responsible for coordinating ETSI's activities in the eHealth domain, identifying gaps where further standardization activities might be required and addressing those gaps which are not the responsibility of other ETSI bodies.		Healthcare
ETSI	TC CYBERSECURITY	TECHNICAL COMMITTEE (TC) CYBER	The rapid evolution and growth in the complexity of new systems and networks, coupled with the sophistication of changing threats, present demanding challenges for maintaining the security of Information and		All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
		(CYBERSECURITY)	Communications Technologies (ICT) systems and networks. Security solutions must include a reliable and secure network infrastructure, but they must also protect the privacy of individuals and organizations. Security standardization, sometimes in support of legislative actions, has a key role to play in protecting the Internet and the communications and business it carries. We offer market-driven cybersecurity standardization solutions, along with advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. See also the TC CYBER Roadmap.		
ETSI	TC LI	TECHNICAL COMMITTEE (TC) LAWFUL INTERCEPTION (LI)	We develop standards that support the technical requirements of national and international obligations for law enforcement, including the lawful interception and retention of the communications-related data of electronic communications. Lawful Interception (LI) and Retained Data (RD) play a crucial role in helping law enforcement agencies to investigate terrorism and serious criminal activities. We have pioneered the development and maintenance of LI and RD capabilities, and our standards are being adopted around the world due to the increased efficiency and lower cost resulting from their use. Global interest in the committee's work continues to grow, with new organizations joining in the standardization process.		N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ETSI	SC EMTEL	SPECIAL COMMITTEE (SC) EMERGENCY TELECOMMUNICATIONS (EMTEL)	The EMTEL Special Committee is responsible for the capture of European requirements concerning emergency communication services, covering typically the four scenarios in case of an emergency e.g. communication of citizens with authorities, from authorities to citizens, between authorities and amongst citizens. In addition, EMTEL deals with topics like location (e.g. Advanced Mobile Location), NG112 opening emergency services communications to data, video and text, communications involving IoT devices in emergency situations and alerting.		All
ETSI	TC INT	TECHNICAL COMMITTEE (TC) CORE NETWORK AND INTEROPERABILITY TESTING (INT)	We develop test specifications to test interoperability, conformance, performance and security. The methodology used is end-to-end (e2e) and includes verification of both the control and user plane. The test specifications are based on 3GPP specifications which enable network operators to test their network for services for both fixed and mobile customers. We produce test purposes, test descriptions, and TTCN-3 test cases to enable interoperability testing of the core network elements and covering the single-network, interconnect and roaming scenarios. Use Cases and requirements specified by ETSI for Automated and Autonomic Management and Control (self- management) of Networks and Services are tested via “industry standards-anchored” Proof of Concepts (PoC) events. Specifically, within 5G Network Slice Service Assurance space along with SDN, NFV, E2E Orchestration. As all those paradigms are		All

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			targeting a common objective they can be considered as key Enablers for 5G.		
ETSI	TC SCP	TECHNICAL COMMITTEE (TC) SMART CARD PLATFORM (SCP)	We are responsible for the development and maintenance of specifications for Secure Elements (SEs) in a multi-application capable environment, the integration into such an environment, as well as the secure provisioning of services making use of SEs. Our work includes the development and maintenance of specifications for the SE and its interface to the outside world for use in telecommunication systems, for general telecommunication purposes as well as for Machine-to-Machine (M2M)/Internet of Things (IoT) communications. The committee's work comprises the interface, procedures and protocol specifications between the SE and entities (remote or local) used in its management. It also includes interfaces, procedures and protocol specifications used between such entities for the secure provisioning and operation of services making use of the SE.		N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ETSI	TC TCCE	TECHNICAL COMMITTEE (TC) TERRESTRIAL TRUNKED RADIO AND CRITICAL COMMUNICATIONS EVOLUTION (TCCE)	We are responsible for the design and standardization of TErrestrial Trunked RAdio (TETRA) and its evolution to critical communications mobile broadband solutions. TETRA (Terrestrial Trunked Radio) is the leading technology choice for critical communications users. With a projected 5 million terminals in use by 2020, the use of TETRA in security as well as other business-critical markets such as the transportation, military, commercial and utilities sectors continue to increase. TETRA is designed to address a specific set of communication requirements. These include high reliability, single and group calling capabilities, PTT (Push-To-Talk), and the possibility for direct peer-to-peer communications in situations such as natural disasters and emergencies when the supporting network is unavailable. Accordingly, much of our work of is driven by the requirements of Public Protection and Disaster Relief and other mission-critical services.		N/A
ETSI	TC NTECH	TECHNICAL COMMITTEE (TC) NETWORK TECHNOLOGIES (NTECH)	We are the ETSI competence centre on network technologies in current and future networks, with special focus on network interconnection. This includes maintaining and evolving the specifications of the architectures and protocols deployed in fixed networks or used in support of network interconnection, as well as monitoring relevant work on future networks technologies performed outside ETSI and provide guidelines on their applicability to ETSI compliant networks. The committee is also the ETSI's		All

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			technical contact point for CEPT/ECC WG NaN (Numbering and Networks).		
ETSI	ISG ETI	INDUSTRY SPECIFICATION GROUP (ISG) ENCRYPTED TRAFFIC INTEGRATION (ETI)	ISG ETI develops Group Specifications (GS) and Group Reports (GR) that define requirements and identify the use cases of Encrypted Traffic Integration techniques to mitigate against threats to networks and users arising from the deployment of encrypted traffic. The group defines detailed specifications of mitigation measures with a view to their further development in ETSI Technical Committees that are identified as appropriate for their adoption. As a pre-standardization activity, the ISG ETI intends to frame the security concerns arising from widespread adoption of encryption by default in networks and to build the foundation of a longer-term response to the threats from encrypted.		N/A
IEC	ISO/IEC JTC 1/SC 27	Information security, cybersecurity and privacy protection	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: Security requirements capture methodology; Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services; Cryptographic and other security mechanisms, including but not limited	197	All

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; Security aspects of identity management, biometrics and privacy; Conformance assessment, accreditation and auditing requirements in the area of information security; Security evaluation criteria and methodology. SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.		
IEC	SC 62B	Diagnostic imaging equipment	To prepare international publications for safety and performance for all kind of medical diagnostic imaging equipment (e.g. X-ray imaging equipment, computed tomography, magnetic resonance imaging equipment) including related associated equipment and accessories as well as quality procedures (e.g. acceptance tests and constancy tests) to be applied during the life-time of imaging equipment. Included is also the development of related terminology, concepts, terms and definitions.	81	Healthcare

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ISO	ISO/TC 272	Forensic sciences	Standardization and guidance in the field of Forensic Science. This includes the development of standards that pertain to laboratory and field based forensic science techniques and methodology in broad general areas such as the detection and collection of physical evidence, the subsequent analysis and interpretation of the evidence, and the reporting of results and findings.	3	N/A
ETSI	ISG SAI	INDUSTRY SPECIFICATION GROUP (ISG) SECURING ARTIFICIAL INTELLIGENCE (SAI)	The rapid expansion of Artificial Intelligence into new industries with new stakeholders, coupled with an evolving threat landscape, presents a tough challenge for security. Artificial Intelligence impacts our lives every day, from local AI systems on our mobile phones suggesting the next word in our sentences to large manufacturers using AI to improve industrial processes. AI has the potential to revolutionize our interactions with technology, improve our quality of life and enrich security – but without high quality technical standards, AI has the potential to create new attacks and worsen security. The ETSI Industry Specification Group on Securing Artificial Intelligence (ISG SAI) focuses on three key areas: using AI to enhance security, mitigating against attacks that leverage AI, and securing AI itself from attack. The ETSI ISG SAI works alongside a landscape of huge growth in AI, creating standards to preserve and improve the security of Artificial Intelligence.		N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 25	Interconnection of information technology equipment	Standardization of microprocessor systems, interfaces, protocols, architectures and associated interconnecting media for information technology equipment and networks to support embedded and distributed computing environments, storage systems and other input/output components. Standards for home and building electronic systems in residential and commercial environments to support interworking devices (IoT-related) and applications such as energy management, environmental control, lighting, and security. Cabling system standards for information and communication technology (ICT), in all types of residential, commercial and industrial environments for the design, planning and installation, test procedures, automated infrastructure management systems and remote powering.	232	N/A
IEC	SC 62D	Electromedical equipment	To develop particular international standards and technical reports for electrical equipment used in medical practice. These documents cover the safety and/or performance of the equipment as well as related terminology, concepts, definitions and symbols. Note. Examples of the types of equipment covered by the scope of SC 62D include equipment used to diagnose patients, equipment used to monitor patients, and equipment used to treat or as an aid in the treatment of patients. Exclusions: Medical diagnostic imaging and related equipment	100	Healthcare

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
			(see scope of SC 62B) and medical equipment using high-energy ionizing radiation in therapy (see scope of SC 62C) are excluded.		
ISO	ISO/TC 295	Audit data services	Standardization in the field of audit data services covers the content specification as well as the collection, pre-processing, management and analysis techniques for the identification, communication, receipt, preparation and use of audit data.	1	N/A
IEC	TC 62	Electrical equipment in medical practice	To prepare international standards and other publications concerning electrical equipment, electrical systems and software used in healthcare and their effects on patients, operators, other persons and the environment.	1	Healthcare
IEC	ISO/IEC JTC 1/SC 41	Internet of things and related technologies	Standardization in the area of Internet of Things and related technologies. Serve as the focus and proponent for JTC 1's standardization programme on the Internet of Things and related technologies, including Sensor Networks and Wearables technologies. Provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things related applications.	29	N/A
IEC	ISO/IEC JTC 1	Information technology	International standardization in the field of Information Technology	494	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ETSI	TC ATTM	TECHNICAL COMMITTEE (TC) ACCESS, TERMINALS, TRANSMISSION AND MULTIPLEXING (ATTM)	We are responsible for the standardization of access, terminals, transmission and multiplexing. This includes cabling, radio links, installations, signal transmission and other forms of signal treatment up to digitalization, in the private and public domains, focusing on the specific technology, equipment, installations and regulatory aspects of the physical layer. We are developing tools for ICT users to monitor deployment of sustainable smart cities and the sustainable efficiency, including eco-efficiency and energy management, of their sites and networks. This also offers the means of implementing the most efficient broadband systems and physical networks.		N/A
IEC	ISO/IEC JTC 1/SC 17	Cards and security devices for personal identification	Standardization in the area of: Identification and related documents Cards Security devices and tokens and interface associated with their use in inter-industry applications and international interchange	104	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 32	Data management and interchange	Standards for data management within and among local and distributed information systems environments. SC 32 provides enabling technologies to promote harmonization of data management facilities across sector-specific areas. Specifically, SC 32 standards include: • reference models and frameworks for the coordination of existing and emerging standards; • definition of data domains, data types, and data structures, and their associated semantics; • languages, services, and protocols for persistent storage, concurrent access, concurrent update, and interchange of data; • methods, languages, services, and protocols to structure, organize, and register metadata and other information resources associated with sharing and interoperability, including electronic commerce.	95	All
IEC	ISO/IEC JTC 1/SC 40	IT Service Management and IT Governance	Standardization of IT Service Management and IT Governance. Develop standards, tools, frameworks, best practices and related documents for IT Service Management and IT Governance, including areas of IT activity such as audit, digital forensics, governance, risk management, outsourcing, service operations and service maintenance, but excluding subject matter covered under the scope and existing work programs of JTC 1/SC 27 and JTC 1/SC 38.	27	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	TC 123	Management of network assets in power systems	Standardisation to deliver, in co-operation with other TC/SCs and international organizations, common methods and guidelines for coordinated lifetime management of network assets in power systems to support good asset management. In addition this may include the development of new methods and guidelines. Excluded: Generation business assets; The scopes of other IEC Technical Committees, such as TC 8, TC 56 and TC 57.	0	All
IEC	TC 79	Alarm and electronic security systems	To prepare international standards for the protection of buildings, persons, areas and properties against fraudulent actions having the purpose to enter in a place or to take or to use something without permission and other threat related to persons. The scope includes, but is not limited to equipment and systems, either used by ordinary persons or by trained people in the following residential and non residential applications: - Access control systems; - Alarm transmission systems; - Video surveillance systems; - Combined and/or integrated systems even including fire alarm systems*; - Fire detection and fire alarm systems*; - Intruder and hold-up alarm systems; - Remote receiving and/or surveillance centres;	55	All

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			- Social alarm systems. These systems can be used for providing a local or remote alarm; they can be used for calling private guards, social assistance, fire brigade or police force. They can be used for recording and transmission of dated or undated information, sounds, pictures of places and people for surveillance purposes.		
ETSI	TC STQ	TECHNICAL COMMITTEE (TC) SPEECH AND MULTIMEDIA TRANSMISSION QUALITY (STQ)	We are responsible for standardization relating to terminals and networks for speech and media quality, end-to-end single media and multimedia transmission performance, Quality of Service (QoS) parameters for networks and services and Quality of Experience (QoE) descriptors and methods. New specifications published recently cover methods for objective assessment of listening effort, and characterization methodology and requirements for the LC3plus speech codec. With our Working Group STQ Mobile we work closely with the Third Generation Partnership Project (3GPP™) and collaborate with other Standard Developing Organizations. The Committee regularly organizes Workshops, successfully bringing together key stakeholders, promoting ETSI work and attracting participation in TC STQ. The next workshop will focus on Emerging Services for Speech and Audio, and will take place in Bratislava, Slovakia, on 27-28 October 2020.		N/A

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
ISO	ISO/TC 46	Information and documentation	Standardization of practices relating to libraries, documentation and information centres, publishing, archives, records management, museum documentation, indexing and abstracting services, and information science.	126	All
ETSI	ISG F5G	INDUSTRY SPECIFICATION GROUP (ISG) FIFTH GENERATION FIXED NETWORK (F5G)	We aim at studying the evolution of the fixed network needed to match and further enhance the benefits that 5G has brought to mobile networks and to communications, defining improvements with respect to previous solutions and the new characteristics of what represents the 5th generation fixed network. Our starting point is the identification of the overall characteristics of the 5th generation fixed network and the exploration of relevant scenarios and related use cases for home, business and multiple vertical industries. This will allow us performing a gap analysis to identify both enhancements to existing standards and development of new specifications where required, and further outlining the complete F5G technology landscape.		N/A
ISO	ISO/TC 171	Document management applications	Standardization of technologies and processes involving capture, indexing, storage, retrieval, distribution and communication, presentation, migration, exchange, preservation, integrity maintenance and disposal in the field of document management applications. Documents may be managed in micrographic or electronic form.	99	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ETSI	ISG ZSM	INDUSTRY SPECIFICATION GROUP (ISG) ZERO TOUCH NETWORK AND SERVICE MANAGEMENT (ZSM)	The pivotal deployment of 5G and network slicing has triggered the need for a radical change in the way networks and services are managed and orchestrated. Full end-to-end automation of network and service management has become an urgent necessity for delivering services with agility and speed and ensuring the economic sustainability of the very diverse set of services offered by Digital Service Providers. The ultimate automation target is to enable largely autonomous networks which will be driven by high-level policies and rules; these networks will be capable of self-configuration, self-monitoring, self-healing and self-optimization without further human intervention. All this requires a new horizontal and vertical end-to-end architecture framework designed for closed-loop automation and optimized for data-driven machine learning and artificial intelligence algorithms.		N/A
ISO	ISO/TC 184	Automation systems and integration	Standardization in the field of automation systems and their integration for design, sourcing, manufacturing, production and delivery, support, maintenance and disposal of products and their associated services. Areas of standardization include information systems, automation and control systems and integration technologies.	861	All
ISO	ISO/TC 251	Asset management	Standardization in the field of asset management.	4	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 24	Computer graphics, image processing and environmental data representation	The current area of work for JTC 1/SC 24 consists of: standardization of interfaces for information technology based applications relating to computer graphics and virtual reality, image processing, environmental data representation, support for Mixed and Augmented Reality (MAR), and interaction with, and visual presentation of, information	85	N/A
ISO	ISO/TC 262	Risk management	Standardization in the field of risk management	5	All
ISO	ISO/TC 84	Devices for administration of medicinal products and catheters	Standardization of the performance of metered devices and supplies intended for administration of medicinal products, and standardization of syringes, needles and catheters.	35	N/A
ISO	ISO/TC 267	Facility management	Standardization in the field of facility management	5	All
IEC	ISO/IEC JTC 1/SC 35	User interfaces	Standardization in the field of user-system interfaces in information and communication technology (ICT) environments and support for these interfaces to serve all users, including people having accessibility or other specific needs, with a priority of meeting the JTC 1 requirements for cultural and linguistic adaptability.	81	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 36	Information technology for learning, education and training	Standardization in the field of information technologies for learning, education, and training to support individuals, groups, or organizations, and to enable interoperability and reusability of resources and tool. Excluded from this scope are: • standards or technical reports that define educational standards (competencies), cultural conventions, learning objectives, or specific learning content. • work done by other ISO or IEC TCs, SCs, or WGs with respect to their component, specialty, or domain. Instead, when appropriate, normative or informative references to other standards shall be included. Examples include documents on special topics such as multimedia, web content, cultural adaptation, and security.	53	N/A

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
IEC	ISO/IEC JTC 1/SC 37	Biometrics	Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects. Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification. Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protections techniques, biometric security testing, evaluations and evaluations methodologies.	131	N/A
ISO	ISO/TC 292	Security and resilience	Standardization in the field of security to enhance the safety and resilience of society.	39	All
ISO	ISO/PC 317	Consumer protection: privacy by design for consumer goods and services	Standardization in the field of consumer protection: privacy by design for consumer goods and services	0	All

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 42	Artificial Intelligence	Standardization in the area of Artificial Intelligence •Serve as the focus and proponent for JTC 1's standardization program on Artificial Intelligence •Provide guidance to JTC 1, IEC, and ISO committees developing Artificial Intelligence applications	6	N/A
ISO	ISO/TC 232	Education and learning services	Standardization in the field of education and learning services focused on, but not limited to services; management systems; facilitators; assessments; terminology; ethical conduct.	4	N/A
ISO	ISO/TC 260	Human resource management	Standardization in the field of human resource management.	13	N/A
ISO	ISO/TC 279	Innovation management	Standardization of terminology tools and methods and interactions between relevant parties to enable innovation.	4	N/A
ISO	ISO/IEC JTC 1	Information technology	Standardization in the field of information technology.	3266	All
ISO	ISO/TC 215	Health informatics	Standardization in the field of health informatics, to facilitate capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system.	201	Healthcare

Committees relevant to cyber security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
IEC	SC 65C	Industrial networks	To prepare international standards on wired, optical and wireless industrial networks for industrial-process measurement, control and manufacturing automation, as well as for instrumentation systems used for research, development and testing purposes. The scope includes cabling, interoperability, co-existence and performance evaluation.	163	N/A
IEC	SC 65E	Devices and integration in enterprise systems	To prepare international standards specifying: (1) Device integration with industrial automation systems. The models developed in these standards address device properties, classification, selection, configuration, commissioning, monitoring and basic diagnostics. (2) Industrial automation systems integration with enterprise systems. This includes transactions between business and manufacturing activities which may be jointly developed with ISO TC184.	120	N/A
ISO	ISO/TC 283	Occupational health and safety management	Standardization in the field of occupational health and safety management to enable an organization to control its OH&S risks and improve its OH&S performance.	1	Healthcare
ISO	ISO/TC 312	Excellence in service	Standardization in the field of excellence in service	0	N/A

Committees relevant to cyber security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ISO	ISO/TC 304	Healthcare organization management	Standardization in the field of healthcare organization management including: classification, terminology, nomenclature, management practices and metrics that comprise the non-clinical operations in healthcare entities.	1	Healthcare

Table 10.2 Committees relevant to physical security

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/CLC/JTC 3	Quality management and corresponding general aspects for medical devices	The objective of the joint Technical Committee is to contribute to, and where necessary draft, suitable standards for "Quality management and corresponding general aspects for medical devices" that are applicable internationally and relevant to the essential requirements of EU Directives. The joint Technical Committee closely cooperates with ISO/TC 210 'Quality management and corresponding general aspects for medical devices' in the development of standards and revisions. The objective of the joint Technical Committee is to contribute to a further global harmonization of standards in close co-operation with ISO/TC 210. In principle the standards are drafted by ISO/TC 210 under the Vienna agreement with ISO-lead, including the joint work programme with IEC/SC 62. The joint Technical Committee will liaise with other Technical Committees - to achieve a coherent set of horizontal and product standards; - to minimize the necessity for additional European requirements; - to advise on aspects concerning quality management and risk management to ensure an optimal use of EN ISO 13485 and EN ISO 14971.	18	Healthcare

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/CLC/JTC 4	Services for fire safety and security systems	The Technical Committee should develop standards for services for fire safety and security systems. The standards specify the requirements for quality of services supplied by companies and the competencies of their involved staff charged with the planning and design, engineering, installation and hand over, maintenance and repair of fire safety and/or security systems*. * Examples of fire safety and/or security systems, are fire detection-, fire extinguishing -, voice alarm-, intruder alarm-, hold up-, access control , social alarm-, smoke and heat exhaust ventilation-, CCTV systems, control equipment for escape and evacuation route, and combination of such systems as mentioned before.	1	All
CEN	CEN/CLC/JTC 16	CEN/CENELEC Joint Technical Committee on Active Implantable Medical Devices	To standardize all active implantable medical devices and their accessories		Healthcare
CEN	CEN/CLC/WS HECTOS	CEN-CENELEC Workshop on Guidelines on evaluation systems and schemes for physical security	CEN-CENELEC Workshop on Guidelines on evaluation systems and schemes for physical security products	1	All

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
		products			
CEN	CEN/CLC/WS ZONeSEC	Interoperability of security systems for the surveillance of widezones	Interoperability of security systems for the surveillance of widezones	1	All
CEN	CEN/SS A11	Security services	Security services		All
CEN	CEN/SS B02	Structures	Structures	16	N/A
CEN	CEN/SS B99	Building and construction - Undetermined	Building and construction - Undetermined		N/A
CEN	CEN/SS F01	Technical drawings	Technical drawings	63	N/A
CEN	μία	Graphical symbols	Graphical symbols	8	All
CE	CEN/SS	Waste -	Waste - Characterization, treatment and streams		N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
N	S27	Characterization, treatment and streams			
CEN	CEN/TC 10	Lifts, escalators and moving walks	Establishment of safety rules for the construction and installation: - of lifts and service lifts; - of escalators and passenger conveyors.	38	All
CEN	CEN/TC 33	Doors, windows, shutters, building hardware and curtain walling	Definition of functions of doors, windows, shutters, building hardware, and curtain walls and performance levels and classification associated with these functions which characterize the usage including the ability to meet the essential requirements (of the Construction Products Directive), tests requirements and, if necessary, the essential dimensions, terminology, symbols, packaging, marking and labelling.	111	N/A
CEN	CEN/TC 38	Durability of wood and wood-based products	Standardization of natural or conferred durability of wood and wood-based products against biological agents and their characteristics associated with exposure	48	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 44	Commercial and Professional Refrigerating Appliances and Systems, Performance and Energy Consumption	Standardization of Appliances and Systems for refrigeration for preparation, catering retail and wholesale of food and beverage related products such as: - refrigerated & frozen food display cabinets with or without incorporate condensing unit; - refrigerators & frozen food storage cabinets, Walk In Cold Room, ice maker and ice cream machines; - refrigeration systems composed of remote elements with respect to: - performance requirements and related test methods; - requirements and test methods for determination of energy consumption; Industrial scale production plants are excluded. Condensing Units and Chillers appliances are excluded. Safety and Environmental matters are excluded.	13	N/A
CEN	CEN/TC 50	Lighting columns and spigots	Harmonisation of existing standards in the field of lighting poles up to 20 m for pedestrian, roads and open space applications. In addition to luminaries, lighting columns could support minor attachments like cameras, flowers boxes, small signs etc. Flags and cables are excluded.	10	N/A
CEN	CEN/TC 53	Temporary works equipment	Standardization of temporary works equipment used for maintenance, building, construction work and for temporary structures made of the same equipment. The products and systems are normally intended for repeated use. Standardization of machinery is excluded.	21	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 57	Central heating boilers	To establish European Standards with regard to constructional and performance requirements as well as efficiency tests for liquid and solid fuel-fired central heating boilers as well as boiler bodies of gas-fired central heating boilers to be equipped with a forced draught burner, oil fired air-heaters, heat storage units and hot water performance requirements (regarding efficiency) of storage tanks as part of a hot water storage system	12	N/A
CEN	CEN/TC 58	Safety and control devices for burners and appliances burning gaseous or liquid fuels	Safety and control devices for equipment burning gaseous or liquid fuels, ranging from small domestic appliances to large industrial burners, excluding the following: - mechanical controls other than gas controls - devices for transmission and distribution equipment	15	N/A
CEN	CEN/TC 69	Industrial valves	The standardization of valves for all industrial applications and for all types of fluids, including : - steam traps; - valve actuator interface; - safety devices against excessive pressure (safety valves and bursting disks); - control valves (excluding the actuator element and their interface); but excluding: - sanitary valves (as defined by CEN/TC 164/WG 8).	76	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 70	Manual means of fire fighting equipment	a) The design, manufacture and maintenance of portable fire extinguishers for the protection of buildings and any other possible applications; b) The design, manufacture and maintenance of mobile fire extinguishers for the protection of buildings and any other possible applications; c) The design, and manufacture of fire blankets for all possible applications; d) The design, manufacture and maintenance of all manual means for fire fighting for all possible applications with the exception of manual means used by the fire brigades which are covered by the work of TC 192 and means for fire fighting covered by TC 191.	16	All
CEN	CEN/TC 72	Fire detection and fire alarm systems	To prepare standards, harmonised where necessary to meet the essential requirement 'Safety in case of fire' of the Construction Products Directive, in the field of fire detection and fire alarm systems in and around buildings, covering test methods, requirements and recommendations for: - components; - the combination of components into systems; - the planning, design and installation of systems for use in and around buildings; - usage, maintenance and servicing; - the connections to and control of other fire protection systems; - the combination with other systems to form integrated systems; - the combination with fixed firefighting systems; - the contribution of fire detection and fire alarm systems to fire safety engineering.	39	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 74	Flanges and their joints	Standardization of flanges and their joints in pipelines and piping systems, for all applications excluding hydraulic and pneumatic load transmission. Definition of "nominal pressure" and "nominal size"; - flanges: dimensions and tolerances, selection of materials, technical conditions of delivery; - bolts, screws and nuts: selection of required bolts, screws and nuts, dimensions, technical conditions of delivery, materials; - gaskets: dimensions and tolerances, materials, technical conditions of delivery; - calculation method for flanges design; - determination of P/T ratings.	36	N/A
CEN	CEN/TC 79	Respiratory protective devices	To prepare European Standards for respiratory protective devices for use in the work place and for fire fighting and for rescue purposes, where there exists a risk to health from inhaling dusts, fumes, gases, vapours or from oxygen deficiency, as well as European Standards for underwater breathing apparatus.	56	Healthcare
CEN	CEN/TC 85	Eye protective equipment	Establishment of specifications and test methods relevant to eye and face protectors.	20	N/A
CEN	CEN/TC 88	Thermal insulating materials and products	Standardisation in the field of thermal insulating materials and products for application in buildings, including insulation for installed equipment and for industrial insulation, covering: terminology and definitions, list of required properties with regard to different applications, methods for the determination of these properties, sampling procedures, conformity criteria, specifications for insulating materials and products, marking and labelling of insulating materials and products.	69	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 89	Thermal performance of buildings and building components	Standardization in the field of energy performance of buildings, including particularly energy transfer through building components and thermal insulation of installed equipment in buildings, covering: - rules for expressing relevant thermal properties and requirements; - calculation and test methods; - input data, including climatic data; - effects of moisture.	75	N/A
CEN	CEN/TC 93	Ladders	Standardization of portable ladders designed for general professional and non-professional use, attic stairs/loft ladders and ladders designed for specific professional use which are not covered by the scope of other Technical Committees	8	N/A
CEN	CEN/TC 98	Lifting platforms	This standard specifies the safety requirements of Suspended Access Equipment (SAE). SAE comprises a working platform suspended by wire ropes from a roof rig. The working platform is lifted and lowered by one or more hoists and may also be traversed and rotated. The system may be powered or hand operated.	6	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 104	Concrete and related products	CEN/TC 104 deals with the standardisation of provisions for concrete and related products, in particular with respect to properties and requirements for: - fresh and hardened concrete; - production and delivery of fresh concrete; - constituent materials of concrete, e.g. mixing water, additions and admixtures; - sheaths for prestressing tendons; grout for prestressing tendons; - fibres for use in concrete; - execution of concrete structures; - production and execution of sprayed concrete; - products for the protection and repair of concrete structures. Additionally relevant test methods and provisions for the assessment of conformity for the products and procedures mentioned above are standardized. Not covered by the scope of TC 104 are: - the constituent materials; aggregate (see CEN/TC 154), Pigments (see CEN/TC 298) and Cement (see CEN/TC 51); - the design of concrete structures and components (see CEN/TC 250/SC 2); - precast concrete products (see CEN/TC 229); - prefabricated autoclave aerated and no-fines light weight concrete components (see CEN/TC 177).	119	N/A
CEN	CEN/TC 106	Large kitchen appliances using gaseous fuels	To define and to supply the checking procedures of the essential characteristics of the appliances, fed by gas, as shown below: - open burners and wok burners, ovens and steaming ovens, boiling pans, fryers, hot cupboards and bain-marie, hot water heaters for beverage, salamanders and rotisseries, brat pans and paëlla, solid tops, warming plates and griddles, barbecues, charcoals and grills.	12	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 109	Central heating boilers using gaseous fuels	All the gas-fired central heating boilers, including the boilers of the condensing type, with or without integrated domestic hot water production, of all types and all nominal inputs, i.e. : - the boilers fitted with atmospheric burners or premixed burners (fan-assisted or not), - the units composed of a boiler body and its fan-assisted burner, constituting an indissociable entity, - the assemblings of a boiler body (according to the requirements prescribed by the CEN/TC 57) and a fan-assisted burner (according to the requirements prescribed by the CEN/TC 131), but only for the specific characteristics suited to the utilisation of gaseous fuels.	14	N/A
CEN	CEN/TC 121	Welding and allied processes	Standardization of welding by all processes, as well as allied processes; these standards include terminology, definitions and the symbolic representation of welds on drawings, apparatus and equipment for welding, raw materials (gas, parent and filler metals) welding processes and rules, methods of test and control, design of welded joints, qualification and/or education of welding personnel, as well as safety and health. Excluded are electrical arc welding equipment and electrical safety matters related to welding which are the responsibility of CENELEC/TC 26.	325	N/A
CEN	CEN/TC 122	Ergonomics	Standardisation in the field of ergonomics principles and requirements for the design of work systems and work environments, including machinery and personal protective equipment, to promote the health, safety and well-being of the human operator and the effectiveness of the work systems.	126	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 125	Masonry	Standardization in the field of masonry units of clay, calcium silicate, dense aggregate concrete, lightweight aggregate concrete, autoclaved aerated concrete, natural stone, manufactured stone, mortar for masonry, ancillary components for masonry and associated test methods.	67	N/A
CEN	CEN/TC 127	Fire safety in buildings	1) To develop standards utilizing relevant existing work where available e.g. in ISO, IEC, CENELEC, CEC and EFTA assessing the fire behaviour of building products, components and elements of construction, 2) To develop standards for classification of products, components and elements of construction, appropriate to the fire risks related to their application, 3) To develop standards for assessing fire hazard and for providing fire safety in buildings.	81	All
CEN	CEN/TC 128	Roof covering products for discontinuous laying and products for wall cladding	Standardization in the area of general and specific requirements and test methods for roof covering products for discontinuous laying and products for wall cladding, including anchor devices intended to prevent persons from falling and/or to arrest falls, used in and on buildings and civil engineering works	37	N/A
CEN	CEN/TC 129	Glass in building	Standardization in the field of glass used in building including: - definitions of all types of glass products, basic and processed; - definition of characteristics; - test methods for measurement of characteristics; - calculation methods for characteristics; - requirements e.g. durability; - classifications e.g. anti-bandit glazing; - glazing methods.	48	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 130	Space heating and/or cooling appliances without integral thermal sources	- to prepare product standards defining the characteristics of space heating and/or cooling appliances without integral heat source (e.g. radiators, panels, convectors with or without a fan) - to prepare test standards for determining the nominal thermal output of above mentioned appliances in order to provide a common basis for their evaluation as well as to determine the thermal output in different operating conditions to be used as a basis for designing heating and/or cooling systems, insuring the reproducibility and repeatability of test data within stated tolerances - to prepare product standards defining the characteristics of radiators valves and fittings operated automatically or manually with or without presetting to control the thermal exchange - to specify methods and procedures to evaluate all the characteristics included in product standards - to define criteria and procedures to provide factory product controls to maintain the product characteristics within stated tolerances.	17	N/A
CEN	CEN/TC 131	Gas burners using fans	Preparation of European standards for independent gas burners using fans. NOTE: It is recommended that the standards should also be applied as appropriate togas burners using fans integrated in appliances.	1	N/A
CEN	CEN/TC 132	Aluminium and aluminium alloys	Standardization in the field of unwrought, wrought and cast products made from aluminium and aluminium alloys, particularly: - designations; - terms and definitions; - material specifications; - technical conditions of delivery; - dimensions and tolerances; - methods of testing specific to aluminium.	116	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 133	Copper and copper alloys	Standardization in the field of unwrought, wrought and cast products made from copper and copper alloys, including: - designations, terminology; - material specifications; - conditions of delivery; - dimensions and tolerances; - methods of testing peculiar to copper alloys.	94	N/A
CEN	CEN/TC 135	Execution of steel structures and aluminium structures	Standardization of rules for execution of steel and aluminium structures for building and civil engineering works including rules for inspection and control.	6	N/A
CEN	CEN/TC 137	Assessment of workplace exposure to chemical and biological agents	Standardization in the field of assessment of exposure to agents at the workplace including the planning and performing of measurement but excluding the establishment of limit values.	41	All
CEN	CEN/TC 138	Non-destructive testing	Standardization of the terminology, equipment and general principles of all recognised methods for non-destructive testing including: - radiographic testing; - ultrasonic testing; - eddy current testing; - penetrant testing; - magnetic particle testing; - acoustic emission testing; - visual testing; - thermographic testing; - leak testing; - X-ray diffraction methods; as well as standardization of the principles of qualification and certification of non-destructive testing personnel and methodology for qualification of non-destructive testing.	114	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 140	In vitro diagnostic medical devices	Standardization in the field of in vitro diagnostic medical devices which are reagents, reagent product, calibrators, control materials, kits, instruments, apparatus, equipment, or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information: - concerning a physiological or pathological state or; - concerning a congenital abnormality or; - to determine the safety and compatibility with potential recipients, or; - to monitor therapeutic measures. Specimen receptacles are considered to be in vitro diagnostic medical devices. 'Specimen receptacles' are those devices, whether vacuum-type or not, specifically intended by their manufacturers for the primary containment and preservation of specimens derived from the human body for the purpose of in vitro diagnostic examination. Products for general laboratory use are not in vitro diagnostic medical devices unless such products, in view of their characteristics, are specifically intended by their manufacturer to be used for in vitro diagnostic examination.	44	Healthcare

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 142	Woodworking machines - Safety	Standardization of design and manufacture in the field of safety of machines and tools for the processing of wood and similar materials, destined for processing by the machines and tools, taking account of the European Machinery Directive, and of the purpose for which the machine is intended for use. By extension it also applies to facilities and equipment for conditioning of wood. Similar materials are wood materials (chip board, fibre board, plywood etc) cork, cane, shell, amber, ivory, horn and wood substitutes. Conditioning means e.g. drying, steaming, impregnation.	37	N/A
CEN	CEN/TC 143	Machine tools - Safety	Standardization in the field of safety of machine tools, their accessories and tools designed to form and to machine cold metal both with and without the removal of metal.	19	N/A
CEN	CEN/TC 149	Power-operated warehouse equipment	Standardization in the field of safety of power-operated warehouse equipment. These are all types of storage and retrieval machines which are restricted to the rails on which they travel in- and outside the aisles and which store and retrieve as well as take into commission unit loads and/or long goods such as bar materials. Also included are the transfer equipment used to change between aisles, the horizontal or vertical carousels and the mobile storage racks	2	N/A
CEN	CEN/TC 156	Ventilation for buildings	Standardization of terminology, testing and rating methods, dimensioning and fitness for purpose of natural and mechanical ventilation systems and components for buildings subject to human occupancy.	76	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 158	Head protection	To prepare European standards for all types of protective helmets.	13	N/A
CEN	CEN/TC 159	Hearing protectors	To prepare European standards related to personal hearing protective equipment to be used when sound exposure is expected to be hazardous to the ear including fit testing systems for determination of the individual hearing protection performance.	14	N/A
CEN	CEN/TC 162	Protective clothing including hand and arm protection and lifejackets	To prepare European Standards (requirements and testing) in the field of clothing to protect against physical and chemical hazards. Hand and arm protectors are included as well as high visibility clothing and clothing against drowning (e.g. lifejackets).	138	N/A
CEN	CEN/TC 164	Water supply	To establish standards for the installation and performance requirements of systems, constructions of components used for the water supply from the production facility, including the treatment of the water, to the taps attached or unattached to a sanitary appliance with the view of maintaining the quality of water as stated in Directive 80/778.	201	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 165	Waste water engineering	Functional standards, standards for performance and installation in the field of wastewater engineering for systems and components. Where there is no existing material related TC, product standards for all components of discharge pipes, drain and sewer pipes, pipelines, separators etc. according to the resolutions of BT (for the organization of work in the field of metallic tubes see resolution BT 160/1989). Standards for design, calculation, construction, commissioning, operation and maintenance in the field of wastewater engineering, from the point of origin (with the exception of the product standards for sanitary appliances*) up to the point of disposal, including treatment plants and use of treated wastewater for purposes other than agricultural irrigation. *) flushing cisterns, urinals, kitchen sinks, basins bidets, baths, (including whirlpool baths) and shower trays, see TC 163 Resolution 2 (London), WG 3 and 4.	107	N/A
CEN	CEN/TC 167	Structural bearings	Standardization of structural bearing device used for bridges, stadiums, industrial buildings etc. describing the various types and giving the recommendations for design, specifications for materials, manufacture and installation, criteria for acceptance and testing. Excluded, for example, are: connections between piers and columns obtained by reinforced concrete, welded or bolted connections.	12	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 186	Industrial thermo-processing - Safety	Standardization in the field of safety of equipment for industrial thermoprocessing equipment (for example industrial furnaces or kilns and industrial heating equipment) in the field such as: -Metallurgical and metal working plant; in the fields of: 1. Thermal Production; 2. Melting, Pouring; 3. Heating; 4. Heat treatment; 5. Surface treatment; 6. Coating; 7. Joining; 8. Surface treatment. - Glass making plant; - Ceramic manufacturing plant; - Chemical plant; - Waste incineration equipment. And heated by: - Gaseous fuels; - Liquid fuels; - Mixed fuels; - Electricity. Blast furnaces, converters (in steel plants) , boilers, welding machines and food processing equipment are excluded.	3	N/A
CEN	CEN/TC 191	Fixed firefighting systems	Standardization in the field of: - components for fixed firefighting systems;- the design, construction and maintenance of fixed firefighting systems primarily for installation in buildings and other construction works with recommendations for other possible applications and; - components for fixed smoke and heat ventilation systems; - the design, construction and maintenance of fixed smoke and heat ventilation systems for installation in buildings; - fire extinguishing media for use in fixed systems and other firefighting equipment.	67	All
CEN	CEN/TC 192	Fire and Rescue Service Equipment	Standardization of equipment and vehicles for rescue and firefighting, excluding personal protective equipment and that covered by CEN/TC 191.	24	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 194	Utensils in contact with food	Standardization in the field of kitchen, table and household utensils, used in the preparation, cooking, serving and consumption of food and beverage, domestically and in catering establishments. Standardization of conditions of storage and transportation of catering containers containing prepared foodstuffs.	95	N/A
CEN	CEN/TC 195	Cleaning equipment for air and other gases	Standardization in the fields of terminology, classification, characteristics, and test and performance methods for air and gas cleaning equipment for general ventilation and industrial applications. Excluded: - exhaust gas cleaners for gas turbines and IC engines in mobile equipment, filters for personal protection equipment, cabin filters in mobile equipment, which are covered by other technical committees - UV-C applications	21	All
CEN	CEN/TC 204	Sterilization of medical devices	Standardization in the field of validation and monitoring of sterilization processes as used in manufacturing of medical devices.	26	Healthcare
CEN	CEN/TC 206	Biological and clinical evaluation of medical devices	Standardization of the approach to biological and clinical evaluation of medical and dental materials and devices together with standardization of biological test methods applicable to those materials and devices as well as good clinical practice principles to clinical investigations in humans of those devices.	23	Healthcare

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 207	Furniture	Standardization in the field of all furniture (including mattresses, mechanical aspects of the electrically operated furniture; excluding transport furniture), considering, where appropriate: - terminology; - safety and health; - product environmental sustainability and sector-specific applications of circular economy principles; - test methods and requirements for end products, parts, components, surfaces, surface finishes and furniture hardware; -dimensions. Standards for raw materials are excluded.	73	N/A
CEN	CEN/TC 215	Respiratory and anaesthetic equipment	Standardization in the field of anaesthetic and respiratory equipment in particular: - anaesthetic machines; - lung ventilators; - medical gas supply systems and related components; - medical breathing systems; - anaesthetic gas scavenging systems; - related monitoring equipment; - tracheal tubes and related equipment. Excludes equipment currently within the scopes of other CEN/TC, but includes (with appropriate liaison with CENELEC) electrically powered equipment.	71	Healthcare

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 224	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	The development of standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations and privacy in a multi sectorial environment. It covers: - Operations such as applications and services like electronic identification, electronic signature, payment and charging, access and border control; - Personal devices with secure elements independently of their form factor, such as cards, mobile devices, and their related interfaces; - Security services including authentication, confidentiality, integrity, biometrics, protection of personal and sensitive data; - System components such as accepting devices, servers, cryptographic modules; CEN/TC 224 multi-sectorial environment involves sectors such as Government/Citizen, Transport, Banking, e-Health, as well as Consumers and providers from the supply side such as card manufacturers, security technology, conformity assessment body, software manufacturers.	32	All
CEN	CEN/TC 225	AIDC technologies	Standardization of data carriers for automatic identification and data capture, of the data element architecture therefore, of the necessary test specifications and of technical features for the harmonization of cross-sector applications. Establishment of an appropriate system of registration authorities, and of means to ensure the necessary maintenance of standards.	21	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 228	Heating systems and water based cooling systems in buildings	Standardisation of functional requirements for all types of heating systems, including domestic hot water production, water based cooling emission and distribution systems in buildings and powe generation systems in the direct environment of the building. Furthermore standardisation in relation to energy performance of buildings. The work includes: - General performance requirements for heating systems, - General requirements for design of heating systems, water based cooling systems and power generation systems; - Requirements for installation and commissioning, including system tests on the heating and water based cooling system as a whole; - Requirements for preparation of instructions for operation, maintenance and use of heating and water based cooling systems; - Requirements for inspection of heating systems; - Methods for calculation of design heat loads, as basis for sizing of heating equipment; - Methods for calculation of energy use of heating systems, water based cooling systems and power generation systems in the direct environment of the building (e.g. wind power, thermo solar and photovoltaic), including energy economy and environmental impact, as basis for supporting energy performance criteria and/or energy certification of heating systems, water based cooling systems and power generation systems on building or building unit level; - Assessment of energy performance of district heating and cooling systems.	43	N/A
CEN	CEN/TC 230	Water analysis	Standardization in the area of water analysis including: - definition of terms; - sampling of water; - measurement; - reporting. Excluded are the limits of acceptability for water quality.	189	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 239	Rescue systems	To define standards for emergency for emergency medical vehicles and the equipment thereof as well as for first aid equipment, in the interests of providing safe and comfortable transport and preclinical treatment for patients.	9	Healthcare
CEN	CEN/TC 251	Health informatics	Standardization in the field of Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems and to enable modularity. This includes requirements on health information structure to support clinical and administrative procedures, technical methods to support interoperable systems as well as requirements regarding safety, security and quality.	96	Healthcare
CEN	CEN/TC 255	Hand-held, non-electric power tools - Safety	1) Standardization in the field of safety of non-electric hand-held power tools (including their use when mounted in fixtures) which can be both in one generic standard for aspects common to several types of tools, and standards for specific types of tools; 2) Coordination with CLC/TC 61F, CEN/TCs 65, 142, 144, 213, 151, 196 etc. for the purpose of ensuring the highest possible consistency in common safety measures; 3) Utilization of the work carried out in PNEUROP and other European Sector Committees or organizations; 4) Consideration of how B1-Standards for eg. the measurement of noise and vibration, and dust suppression, should be achieved in the field of responsability and with the aid of the CEN committees established for the purpose; 5) Standardization of vocabulary, symbols, and pictograms related to safety of hand-held tools.	14	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 263	Secure storage of cash, valuables and data media	Standardization in the field of physical security of products which provide secure storage of cash, valuables and data media in terms of resistance to fire and also including high security locks.	7	N/A
CEN	CEN/TC 264	Air quality	Standardisation of methods for air quality characterisation of emissions, ambient air, indoor air, gases in and from the ground and deposition, in particular measurement methods for air pollutants (for example particles, gases, odours, microorganisms), meteorological parameters and methods for determination of the efficiency of gas cleaning systems. Excluded are: - determination of limit values for air pollutants, - workplaces and clean rooms, - radioactive substances	123	N/A
CEN	CEN/TC 268	Cryogenic vessels and specific hydrogen technologies applications	Standardization in the field of insulated vessels (vacuum or non- vacuum) for the storage and the transport of refrigerated liquefied gases, as defined in Class 2 of "Recommendations on the Transport of dangerous goods - Model regulation", in particular concerning the design of the vessels and their safety accessories, gas/materials compatibility, insulation performance, the operational requirements of the equipment and accessories. The preparation of standards for hydrogen refuelling points	40	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 282	Installation and equipment for LNG	Developing and maintaining standards in the field of installations, equipment and procedures used for production, transportation, transfer, storage, regasification and use of LNG, taking into account the programme of work of other CEN technical committees dealing with LNG. Standardization covers the supply chain from the inlet to the outlet of the relevant natural gas/LNG facilities, and comprises both onshore and offshore siting options for them. Standardization involves contribution to and adoption of ISO standards (under Vienna Agreement) as well of development of homegrown European standards. CEN/TC 282 further coordinates questions concerning LNG in the technical work of technical committees dealing with cryogenic equipment	12	N/A
CEN	CEN/TC 285	Non-active surgical implants	To standardize non-active surgical implants, including implant materials but not including dental implants and ophthalmic implants and, where appropriate, associated instrumentation to satisfy at least the essential requirements of the European Directive on Medical Devices, taking into account the work of CEN, CENELEC and ISO Technical Committees.	25	Healthcare
CEN	CEN/TC 296	Tanks for the transport of dangerous goods	Standardization of design, construction, inspection and testing of metallic tanks intended for transport of dangerous goods of a capacity of more than 450 l. It shall cover tanks of road tankers, tanks of rail-tank-wagons and tanks intended for multimodal transport. "Tank" means the shell and all relevant equipments.	26	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 301	Road vehicles	Preparation of road vehicle European Standards answering essentially to European mandates. Since the automotive industry is acting globally, the international level (ISO/TC 22 Road vehicles) shall have top priority for any other standardization projects.	25	N/A
CEN	CEN/TC 305	Potentially explosive atmospheres - Explosion prevention and protection	To develop standards where necessary in the fields of: – test methods for determining the flammability characteristics (ignition, propagation, explosion effects, etc.) of substances; – equipment and protective systems for use in potentially explosive atmospheres and equipment and systems for explosion prevention and protection. NOTE: The requirements for electrical parts and electrical hazards are covered by references to electrical standards.	36	All
CEN	CEN/TC 309	Footwear	Preparation of European Standards on: Test methods, terminology and minimum performance requirements for components for footwear, - Test methods and terminology for whole shoes, - Environmental aspects of footwear, excluding those items already covered by other CEN Technical Committees, in particular footwear for professional use	83	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 310	Advanced automation technologies and their applications	Standardization in the field of automation systems and technologies and their application and integration to ensure the availability of the standards required by industry for design, sourcing, manufacturing and delivery, support, maintenance and disposal of products and their associated services. Areas of standardisation may include enterprise modelling and system architecture, information and its supporting systems, robotics for fixed and mobile robots in industrial and specific non-industrial environments, automation and control equipment and software, human and mechanical aspects, integration technologies and system operational aspects. These standards may utilise other standards and technologies beyond the scope of TC310, such as machines, equipment, information technologies, multi-media capabilities, and multi-modal communications networks.	6	N/A
CEN	CEN/TC 319	Maintenance	Standardization in the field of maintenance as far as generic standards which are generally applicable are concerned	7	N/A
CEN	CEN/TC 320	Transport - Logistics and services	Development of standards for activities and services undertaken in support of the transport of passengers, freight and personal effects.	12	N/A
CEN	CEN/TC 322	Equipments for making and shaping of metals - Safety requirements	Standardization in the field of safety of equipment for making of iron, steel and non-ferrous metals and their shaping by rolling, forging and extruding as semi-finished or finished products; excluding - equipments for coal and ore preparation, - industrial thermoprocessing equipment (covered by CEN/TC 186) - foundry machinery (covered by CEN/TC 202) - Surface treatment equipment (covered by CEN/TC 271), - Wire	6	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			drawing machinery.		
CEN	CEN/TC 325	Crime prevention through building, facility and area design	Development of European standards for the prevention of crime at industrial facilities, educational institutions, hospitals, residential building areas, department stores, squares and public meeting places through building, facility and area design. The standards will include their area of application, the corresponding strategy, security levels, building and area layout, application of construction elements, roads and pavements. The standards may be applied to new and significantly refurbished buildings, facilities and areas. The standards will not deal with building products and security systems components.	7	All
CEN	CEN/TC 332	Laboratory equipment	Standardization of laboratory equipment except the following exclusions: - Electrical safety and electromagnetic compatibility; - Basic laboratory furniture; - Apparatus and equipment exclusively intended for biotechnological or in vivo and in vitro diagnostic use for medical applications.	59	Healthcare
CEN	CEN/TC 339	Slip resistance of pedestrian surfaces - Methods of evaluation	Standardization of a single test method for the evaluation of slip resistance applicable to all pedestrian surfaces, excluding road surfaces (skid resistance) and excluding sport surfaces.	1	N/A
CEN	CEN/TC 340	Anti-seismic devices	Standardization of the design, manufacture, testing, installation and maintenance of antiseismic devices for use in structures erected in seismic areas and designed in	1	All

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			accordance with Eurocode 8.		
CEN	CEN/TC 344	Steel static storage systems	Steel static storage systems	6	N/A
CEN	CEN/TC 347	Methods for analysis of allergens	To develop CEN documents for analytical methods applicable to know allergens in materials and products. Allergens in food, medicinal products, natural latex proteins or other proteins, identification of new allergens, testing of sensitizing potential of allergens are excluded from scope of the TC.	4	Healthcare
CEN	CEN/TC 353	Information and Communication Technologies for Learning, Education and Training	Produce standards in the field of information and communication technologies relating to learning, education and training. The European Standards (EN), Technical Specifications (TS) and Technical Reports (TR) that are developed will have a well-defined European scope. These may include: - Development of CWAs and other specifications into standards, if appropriate - Developments of national standards into European Standards	10	All
CEN	CEN/TC 362	Healthcare services - Quality management systems	Healthcare services - Quality management systems	2	Healthcare
CE	CEN/T	High Chairs	High Chairs	1	N/A

Committees relevant to physical security

SDO	Committee	Committee Title	Committee Description	Published Standards	Field
N	C 364				
CEN	CEN/TC 365	Internet Filtering	Internet Filtering	1	All
CEN	CEN/TC 389	Innovation Management	Standardization of tools that allow companies and organizations to improve their innovation management, including all kinds of innovation and all the related aspects, as well as the relations with R&D activities.	7	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 391	Societal and Citizen Security	The main objective of CEN/TC 391 is to elaborate a family of European standards, standard-like documents (e.g. procedures, guidelines, best practices, minimal codes of practice and similar recommendations) in the Societal and Citizen Security sector including aspects of prevention, response, mitigation, continuity and recovery before, during and after a destabilising or disruptive event. Verification and training will also be considered. CEN/TC 391 will not deal with issues already dealt in other TCs. Concerning technology, CEN/TC 391 may identify needs in product standardisation, but this will not lead to direct action by this CEN/TC. These issues shall be communicated to those CEN, ISO or other TCs working within the framework of these specific products. Where other TCs do not address the identified areas, then CEN/TC 391 will develop the standard(s) or proposed deliverables where appropriate. The standardisation activities will consider the following main issues related to Societal and Citizen Security: - Products and services (equipment, communication, information, goods, transport, energy, cultural inheritance and properties); - Infrastructures (roads, ports, airports, rail stations, bridges, factories...); - Stakeholder needs and requirements, potential conflicts; - Relationship (cultural and geographical diversity); - Citizen requirements and vulnerabilities, including privacy.	10	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 393	Equipment for storage tanks and for filling stations	Standardization of equipment for all kinds of storage tanks and for filling stations. The general interest of CEN/TC 393 is for equipment relating to the storage of fuels, that are liquids under atmospheric conditions, but the equipment may be used for other purposes. The standardization may include performance requirements and product descriptions together with the necessary test methods and the requirements concerning the evaluation of conformity.	19	N/A
CEN	CEN/TC 398	Child Protective Products	Child Protective Products	3	N/A
CEN	CEN/TC 413	Insulated means of transport for temperature sensitive goods with or without cooling and/or heating device	Standardization in the field of definitions, requirements, test methodologies, classification, dimensioning and marking for equipment and devices for insulated means of transport for temperature sensitive goods. Equipment includes tanks, mobile containers, truck or trailer bodies, road and train swap bodies, rail wagons, vans and car derived vans for temperature sensitive goods. Device includes mechanical refrigeration systems, eutectic systems, direct and indirect gas refrigerating systems, dry ice systems, heating systems and special requirements for multi-temperature systems	1	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 419	Forensic Science Processes	To ensure the integrity of the forensic process (as a single process), the Project Committee should develop European Standards which lay down the provisions for forensic science processes, which start at the scene of crime, through the recognition, recording, recovery, transportation and storage of material followed by the examination, analysis of material, interpretation of results, reporting and data exchange	2	N/A
CEN	CEN/TC 439	Private security services	The scope of the CEN/TC 439 is to be responsible for the standardization in all civilian security services. Excluded from the scope are: − Standardization of the product related requirements; − The Societal and citizen sector including aspects of prevention, response, mitigation and recovery before, during and after a destabilizing or disruptive event, which falls under the responsibility of CEN/TC 391 'Societal and citizen security', − CEN-CENELEC/TC 4 'Services for fire safety and security systems' − Cash-in-transit (CIT), cash processing and cash management activities.	3	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 445	Digital information Interchange in the Insurance Industry	Standardization in the field of digital information interchange in the European insurance industry. This applies to aspects of policy administration (quotation, offer, application, transfer of contract and premium data, premium and commission statement, party and contract changes, search and information services for party and contract) and of claims handling (notification, verification, assessment, authorization, settlement and reimbursement, recovery, status information). Standardization will focus on the digital information interchange among insurance companies, intermediaries, sales organizations, portals, service providers and customers. All lines of business in the insurance industry may be considered, such as life, health, property and casualty.	1	Healthcare

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CEN	CEN/TC 449	Quality of care for older people	The development of standards for care that is provided for older people regardless of where they live, based on the older person's individual needs and choices. The focus is to promote secure and safe old age care with self-determination and participation for the older person and his/her family and close friends. Focus is also to provide support to the staff in creating an accessible and supportive physical and psychosocial environment that provides the opportunity for maintaining function and meaningful activities for older people as well as ensuring a good work environment for the staff. Old age care is a complex activity that requires a common understanding and cooperation between all the contributory actors to promote and develop the quality of the services. The standard(s) covers services however they are financed. The term care is a comprehensive notion that includes social and nursing care, rehabilitation, service and other related areas. The scope does not include standardization of products (medical devices and associated software), clinical and professional knowledge and the built environment.		Healthcare
CEN	CEN/TC 459/SC 3	Structural steels other than reinforcements	Standardization of technical delivery conditions for hot-rolled steels for structural applications as well as dimensions and tolerances of structural steel sections and hot rolled steel bars for engineering use and tolerances on dimensions, shape and mass for hot-rolled flat products of non-alloy and alloy steels with a rolled width >- 600 mm (including steels for pressure purposes). Note: Reinforcing and prestressing steels are not covered by the scope of this Technical Committee.	46	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CEN	CEN/TC 459/SC 4	Concrete reinforcing and prestressing steels	Standardization of technical delivery conditions appropriate to: -steel products (bars, coils, welded fabric, lattice girders) for the reinforcement of concrete; -prestressing steels. Standardization of any test methods specific to reinforcing and prestressing steel products not already covered by other ECISS, CEN or ISO Technical Committees.	5	N/A
CEN	CEN/WS 099	CEN Workshop on the Semantic and Syntactical Interoperability for Crisis and Disaster Management	CEN Workshop on the Semantic and Syntactical Interoperability for Crisis and Disaster Management	1	All
CEN	CEN/WS 100	CEN Workshop Trial Guidance Methodology (TGM)	CEN Workshop Trial Guidance Methodology (TGM)	1	N/A
CEN	CEN/WS 101	CEN WS Crisis management - Building a Common Simulation Space	CEN WS Crisis management - Building a Common Simulation Space	1	All
CEN	CEN/WS 102	CEN Workshop on guidelines for	This Workshop will develop a CEN Workshop Agreement (CWA), which will define guidelines for introducing, implementing and operating sensor monitoring	1	Healthcare

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
		introducing tele-medical and pervasive monitoring technologies balancing privacy protection against the need for oversight and care	technologies into the private homes of citizens who are in need of care and for the purpose of detecting critical events and trends. The guidelines will describe and exemplify the processes and procedures to support an ethically responsible balance between, on the one hand, respect for the autonomy and privacy of the citizens in need of care and, on the other, the obligation to provide quality care of typically frail citizens. The guidelines will not include issues of security or technical requirements for availability of information to relevant parties. The guidelines will not include management of or procedures for handling monitoring data. The primary target groups of the workshop are care organizations (public or private) that are responsible for delivering social care and health care to citizens		
CEN	CEN/WS 104	Societal and Social Impact Assessment Framework to Support Adoption of New Capabilities in Crisis Management	Societal and Social Impact Assessment Framework to Support Adoption of New Capabilities in Crisis Management		All
CEN	CEN/WS 105	Guidelines to develop long-term strategies (roadmaps) to innovate responsibly	Responsible Research and Innovation (RRI) provides a way to address the needs and concerns of people and society in order to develop processes, products and services aiming to positive societal impacts, guiding innovation towards sustainable development goals. Based on the outcomes of the H2020 PRISMA project (www.rri-prisma.eu), this Workshop aims to develop guidelines to develop long-term strategies		N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
			to innovate responsibly		
CEN	CEN/WS TER-CDM	Terminologies in Crisis and Disaster Management	Terminologies in Crisis and Disaster Management	1	All
CEN	CEN/WS EXOSK	Integration process of new technologies of physical assistance such as exoskeletons	Integration process of new technologies of physical assistance such as exoskeletons		All
CENELEC	CLC/WS SGRM	CENELEC workshop on Specifications for Graphene Related Material	The workshop intents to disseminate research results achieved within the Graphene Flagship. Even though IEC/TC 113 deals with the characterization or specification of GRM we see the necessity for this workshop due to the fact that the participants of the Graphene Flagship rather try to avoid formal standardization due to complexity and time-consuming processes. Accordingly, the Graphene Flagship is aware of the general benefits of standardization but struggle with the technical aspects. However, the intention of the workshop is to propose the development of formal standards at IEC based on the CWAs published.		N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CEN/CLC/WS ZONeSEC	Interoperability of security systems for the surveillance of widezones	Interoperability of security systems for the surveillance of widezones	1	All
CENELEC	CEN/CLC/WS HECTOS	CEN-CENELEC Workshop on Guidelines on evaluation systems and schemes for physical security products	CEN-CENELEC Workshop on Guidelines on evaluation systems and schemes for physical security products	1	All
CENELEC	CEN/CLC/JTC 12	Design for All	To develop the deliverable requested in 4.1 of M/473: 'A new standard (or other deliverable as appropriate to be proposed by the ESOs and accepted by the European Commission), should be developed that describes how the goods manufacturing industry as well as public and private service entities in their processes can consider accessibility following Design for all approach with due consideration for assistive technologies and services that could help bridging the usage gap of the product or service'.	1	All

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CENELEC	CEN/CLC/JTC 4	Services for fire safety and security systems	The Technical Committee should develop standards for services for fire safety and security systems. The standards specify the requirements for quality of services supplied by companies and the competencies of their involved staff charged with the planning and design, engineering, installation and hand over, maintenance and repair of fire safety and/or security systems*. * Examples of fire safety and/or security systems, are fire detection-, fire extinguishing -, voice alarm-, intruder alarm-, hold up-, access control , social alarm-, smoke and heat exhaust ventilation-, CCTV systems, control equipment for escape and evacuation route, and combination of such systems as mentioned before.	1	All
CENELEC	CEN/CLC/ETSI/SEG-CG	CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids	CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids		N/A
CENELEC	CEN/CLC/ETSI/SMCG	CEN-CENELEC-ETSI Coordination Group on Smart Meters	CEN-CENELEC-ETSI Coordination Group on Smart Meters	1	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 213	Cable management systems	To prepare European standardization publications for products and systems used for the management of all types of cables, information and communication lines, electrical power distribution conductors and associated accessories. Management includes support and/or containment and/or retention and/or protection against external influences.	36	N/A
CENELEC	CLC/TC 210	Electromagnetic Compatibility (EMC)	To prepare EMC standards and guidelines with particular emphasis on the application of the EMC Directive and other EC Directives that contain EMC references and to coordinate all EMC activities in CENELEC.	165	N/A
CENELEC	CLC/SR 122	UHV AC transmission systems	UHV AC transmission systems		N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CENELEC	CLC/TC 108X	Safety of electronic equipment within the fields of Audio/Video, Information Technology and Communication Technology	To deal with the adoption in CENELEC of technical work of IEC/TC 108 and to coordinate the work with other technical bodies at European level e.g. ETSI. To make own standards where a particular need arises. NOTE The field of application of IEC/TC 108 is as follows: Standardization in the field of safety for audio/video and similar technology, information technology and communication technology equipment. - To ensure that any deviation from the IEC standards, such as common modifications, special national conditions and A-deviations, is only in response to a clear and justifiable European need, such as European and national legislative needs. - To resolve application questions e.g. raised by CCA Operational Staff Meetings relative to standards within the responsibility of CLC/TC 108X. -To keep IEC/TC 108 informed of European requirements so that they may be considered for inclusion in IEC standards within the responsibility of IEC/TC 108.	34	All
CENELEC	CLC/TC 99X	Power installations exceeding 1 kV a.c. (1,5 kV d.c.)	To prepare harmonized standards for high voltage power installations (exceeding 1 kV a.c. or 1,5 kV d.c.) located indoors or outdoors, including earthing. The standards will specify the design requirements of the installations, and the selection and erection of electrical equipment in order to ensure the safety of persons and the proper operation of the installations. The standards will not be applicable to factory built and type tested equipment, but will be relevant to the installation of this equipment. The standards will not be applicable to overhead and underground lines between separate installations.	5	N/A
CE	CLC/SR	Fire hazard testing	Fire hazard testing	36	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
NELEC	89				
CENELEC	CLC/SR 87	Ultrasonics	Ultrasonics	31	N/A
CENELEC	CLC/TC 86BXA	Fibre optic interconnect, passive and connectorised components	To prepare and maintain European Standards and specifications for fibre optic interconnecting devices, passive and/or connectorised components, fibre optic protective housings, fibre management systems, fusion splice protectors, mechanical splices, unprotected microduct tubes and microduct tube connectors.	314	N/A
CENELEC	CLC/TC 81X	Lightning protection	To prepare European Standards or, where not possible, guides for lightning protection for structures and buildings as well as for persons, services and contents.	25	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 79	Alarm systems	To prepare harmonized standards for detection, alarm and monitoring systems for protection of persons and property, and for elements used in these systems. The scope includes in particular intruder and hold-up alarm systems, access control systems, periphery protection systems, combined alarm - fire alarm systems, social alarm systems, CCTV-systems, other monitoring and surveillance systems related to security applications, as well as associated and dedicated transmission and communication systems. The standards shall specify conformity tests.	103	All
CENELEC	CLC/TC 78	Equipment and tools for live working	To prepare CENELEC standards for work equipment, devices and tools, including personal protective equipment used for work on or near live electrical systems or installations.	67	N/A
CENELEC	CLC/TC 76	Optical radiation safety and laser equipment	To prepare harmonized standards in the field of equipment incorporating lasers (and light emitting diodes) or intended only for use with lasers. Also covered are those factors introduced by the use of lasers which are needed to characterize the equipment and/or which are essential to safe use. The scope includes the preparation of standards defining limits for human exposure to optical radiation (100 nm to 1 mm) from artificial sources.	18	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CENELEC	CLC/TC 72	Automatic electrical controls	To prepare harmonized standards for rules related to inherent safety, to the operating characteristics where such are associated with applicational safety and to the testing of automatic electrical control devices used in appliances and other apparatus, electrical and non-electrical for household and similar purposes such as those for central heating, air conditioning etc. including the following: 1. Automatic electrical control devices mechanically, electro-mechanically, electrically or electronically operated responsive to or controlling such parameters as temperature, pressure, passage of time, humidity, light, electrostatic effect, flow or liquid level. 2. Automatic electrical control devices serving the starting of small motors that are used principally in appliances and apparatus for household and similar purposes. Such control devices may be built into or be separate from the motor. 3. Non-automatic control devices when such are associated with automatic control devices.	65	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CENELEC	CLC/TC 66X	Safety of measuring, control, and laboratory equipment	To prepare harmonised safety standards for test and measurement equipment, industrial- process control equipment, and laboratory equipment wherever they are used. Such equipment includes:a) equipment and systems to measure, test, generate, and analyse, simple and complex electromagnetic quantities and equipment that by electromagnetic means measure physical quantities.Note: Aspects of this equipment other than safety are covered by other technical committees.b) equipment and systems for industrial-process measurement and control.Note: Aspects of this equipment other than safety are covered by TC 65 except that SC 65A has a Horizontal Safety Function relating to the functional safety of electrical/electronic/ programmable electronic systems and SC 65B is responsible for the functional safety of programmable controllers.c) laboratory equipment for analysis, handling and preparation of materials.Note: This equipment includes measuring instruments, systems and their accessories, for preparation, treatment and analysis of materials in the fields of research, medicine, industry and education, and for environmental monitoring.	23	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 64	Electrical installations and protection against electric shock	To prepare International standards - concerning protection against electric shock arising from equipment, from installations and from systems without limit of voltage, - for the design, erection foreseeable correct use and verification of all kind of electrical installations at supply voltage up to 1 kV a.c or 1,5 kV d.c., except those installations covered by the following IEC committees: TC 9X, TC 18X, TC 44X, TC 97, TC 99X, - in co-ordination with TC 99X, concerning requirements additional to those of TC 99X for the design, erection and verification of electrical installations of buildings above 1 kV up to 35 kV. The object of the standards shall be: - to lay down requirements for installation and co-ordination of electrical equipment, - to lay down basic safety requirements for protection against electric shock for use by technical committees, - to lay down safety requirements for protection against other hazards arising from the use of electricity, - to give general guidance to IEC member countries that may have need of such requirements, and - to facilitate international exchanges that may be hampered by differences in national regulations. The standards will not cover individual items of electrical equipment other than their selection for use.	105	N/A
CENELEC	CLC/TC 62	Electrical equipment in medical practice	To establish harmonized standards and other publications concerning electrical equipment, electrical systems and software used in healthcare and their effects on patients, operators, other persons and the environment.	210	Healthcare

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CENELEC	CLC/TC 57	Power systems management and associated information exchange	To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centres, substations and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems and databases, which may be outside the scope of TC 57. The special conditions in a high voltage environment have to be taken into consideration.	115	All
CENELEC	CLC/SC 46XC	Multicore, multipair and quad data communication cables	To produce European Cable Specifications for multicore and symmetrical pair/quad cables used in digital and analogue communication systems such as ISDN, LAN and data communication systems. According to the installation considerations, five categories of cables are to be considered: 1. equipment cables, 2. work area cables, 3. horizontal floor wiring cables, 4. riser cables, 5. campus cables.	36	N/A
CENELEC	CLC/SC 46XA	Coaxial cables	To establish and maintain European Standards regarding coaxial cables for use in telecommunication, data transmission, radio frequency, video-communication and signalling equipment.	56	N/A

Committees relevant to physical security

SDO	Committee	Committee Title	Committee Description	Published Standards	Field
CENELEC	CLC/TC 46X	Communication cables	To establish standards related to wires, symmetric cables, coaxial cables and waveguides with metallic conductors for use in telecommunication, data transmission, radio frequency, video communication and signalling equipment to satisfy the advances in developing technologies. Particular requirements for materials, if necessary, will be evaluated in liaison with other technical committees.	102	N/A
CENELEC	CLC/SR 46F	RF and microwave passive components	RF and microwave passive components	76	N/A
CENELEC	CLC/SC 31-9	Electrical apparatus for the detection and measurement of combustible gases to be used in industrial and commercial potentially explosive atmospheres	General and specific requirements for construction, safety, performance and testing of apparatus for sensing the presence of combustible gases or vapours and for measuring their concentration in industrial and commercial potentially explosive atmospheres.	11	N/A
CENELE	CLC/SC 31-3	Intrinsically safe apparatus and systems "i"	To standardize specific requirements for construction and testing of intrinsically safe electrical apparatus, type of protection "i", intended for use in potentially explosive atmospheres.	4	N/A

Committees relevant to physical security					
SDO C	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/SC 31-1	Installation rules	To standardize rules for the installation of electrical apparatus in a potentially explosive atmosphere.		N/A
CENELEC	CLC/TC 31	Electrical apparatus for potentially explosive atmospheres	To standardize the general requirements for the construction and testing of electrical apparatus for potentially explosive atmospheres and the specific requirements for the construction and testing of electrical apparatus, type of protection "o" (oil immersed) and type of protection "q" (powder filled) and types with protection for use in the presence of combustible dusts, and to co-ordinate the work of the sub-committees dealing with the standardization of specific requirements for other individual types of protection.	45	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/TC 23BX	Switches, boxes and enclosures for household and similar purposes, plugs and socket outlet for D.C.	a) To prepare standards for general purpose switches including electronic switches, time-delay switches, remote control switches and isolating switches, Fireman's switches, for a.c. only, with rated voltage not exceeding 440 V, and with a maximum rated current not exceeding 125 A, intended for household and similar purposes, either indoors or outdoors. b) To prepare standards for switches and related accessories for use in Home and Building Electronic Systems (HBES), with a working voltage not exceeding 250 V a.c. and a rated current up to and including 16 A, intended for household and similar purposes, either indoors or outdoors and to associate electronic extension units. c) To prepare standards for general purpose plugs and fixed and portable socketoutlets, with a rated voltage not exceeding 440 V d.c. and a rated current not exceeding 10A, intended to be used in restricted access areas where only skilled or instructed people have access. d) To prepare standards for general purpose boxes and enclosures for household devices, boxes and enclosures with provision for suspension means, connecting boxes and enclosures, floor boxes and enclosures, enclosures for housing protective devices and similar power consuming devices with a rated voltage not exceeding 440 V, intended for household and similar purposes, either indoors or outdoors. e) To prepare standards for ancillary products which relate to/incorporate products covered by a), b), c), e.g. luminaire couplers, adaptors/cable reels, indicator light units, etc.	40	N/A
CENELE	CLC/SR 3C	Graphical symbols for use on equipment	Graphical symbols for use on equipment	4	N/A

Committees relevant to physical security

SDO	Committee	Committee Title	Committee Description	Published Standards	Field
C					
CENELEC	CLC/SR 3	Information structures, documentation and graphical symbols	Information structures, documentation and graphical symbols	28	N/A
CENELEC	CLC/BT WG 154-1	EMC standardization in the EU regulatory framework	To develop the necessary alignment elements between EMC standardisation activities and the regulatory framework		N/A
CENELEC	CLC/BT WG 143-1	LVD standardization in the EU regulatory framework	The objective of the CLC/BTWG 143-1 'LVD standardization in the EU regulatory framework' is - To address horizontal issues in relation to standardization surrounding LVD Directive 2014/35/EU and its possible review; - To offer a platform to prepare and/or mirror the LVD working party and LVD ADCO; - Coordinate on matters related to LVD work programme and sectoral agreements re. its assessment and acceptance for citation in the OJEU, including any revision to document templates; - Maintain the CENELEC Guide 32 Guidelines for Safety Related Risk Assessment and Risk Reduction for Low Voltage Equipment.		N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
CENELEC	CLC/BTTF 133-1	Sound systems for emergency purposes which are not part of fire detection and alarm systems	To prepare a draft residual standard based on EN 60849:1998 that is complementary to EN 54-16 "Fire detection and fire alarm systems -- Part 16: Voice alarm control and indicating equipment"	1	N/A
ISO	ISO/TC 21	Equipment for fire protection and fire fighting	Standardization in the field of all fire protection and fire fighting apparatus and equipment including extinguishing media as well as the personal equipment of the fire fighter, and related work on terminology, classification and symbols.	101	All
ISO	ISO/TC 76	Transfusion, infusion and injection, and blood processing equipment for medical and pharmaceutical use	Standardization of containers (such as infusion bottles and bags, injection vials, ampoules, glass cylinders, cartridges, prefillable syringes, etc.) application systems (such as giving sets, non-electrically driven portable infusion devices, blood collection systems, etc.) and accessories for infusion, transfusion, injection and blood processing in blood banks, terms, definitions, requirements and test methods for these devices, specifications and test methods for quality and performance of their materials and components (such as elastomeric closures, caps and ports, pipettes, etc.) and quality management systems for primary packaging materials.	76	Healthcare

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ETSI	TC LI	TECHNICAL COMMITTEE (TC) LAWFUL INTERCEPTION (LI)	We develop standards that support the technical requirements of national and international obligations for law enforcement, including the lawful interception and retention of the communications-related data of electronic communications. Lawful Interception (LI) and Retained Data (RD) play a crucial role in helping law enforcement agencies to investigate terrorism and serious criminal activities. We have pioneered the development and maintenance of LI and RD capabilities, and our standards are being adopted around the world due to the increased efficiency and lower cost resulting from their use. Global interest in the committee's work continues to grow, with new organizations joining in the standardization process.		N/A
ISO	ISO/TC 92	Fire safety	Standardization of the methods of assessing fire hazards and fire risk to life and to property; the contribution of design, materials, building materials, products and components to fire safety and methods of mitigating the fire hazards and fire risks by determining the performance and behaviour of these materials, products and components, as well as of buildings and structures. Excluded: materials and equipments already covered by other technical committees; fields covered by other ISO and IEC committees.	144	All
ISO	ISO/TC 94	Personal safety -- Personal protective equipment	Standardization of the performance of personal protective equipment designed to safeguard wearers against all known possible hazards.	179	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ISO	ISO/TC 96	Cranes	Standardization in the field of cranes and related equipment which suspend loads by means of a load-handling device, particularly in respect of terminology, load rating, testing, safety, general design principles, maintenance, operation and load lifting attachments.	108	All
ISO	ISO/TC 121	Anaesthetic and respiratory equipment	Standardization of anaesthetic and respiratory equipment and supplies, related devices and supply systems.	101	Healthcare
ISO	ISO/TC 150	Implants for surgery	Standardization in the field of implants for surgery 1) and their required instrumentation, covering terminology, specifications and methods of tests for all types of implants, and for the materials both basic and composite used in their manufacture and application.	165	Healthcare
ETSI	SC EMTEL	SPECIAL COMMITTEE (SC) EMERGENCY TELECOMMUNICATIONS (EMTEL)	The EMTEL Special Committee is responsible for the capture of European requirements concerning emergency communication services, covering typically the four scenarios in case of an emergency e.g. communication of citizens with authorities, from authorities to citizens, between authorities and amongst citizens. In addition, EMTEL deals with topics like location (e.g. Advanced Mobile Location), NG112 opening emergency services communications to data, video and text, communications involving IoT devices in emergency situations and alerting.		All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ISO	ISO/TC 211	Geographic information/Geomatics	Standardization in the field of digital geographic information. Note: This work aims to establish a structured set of standards for information concerning objects or phenomena that are directly or indirectly associated with a location relative to the Earth.	81	All
ISO	ISO/TC 212	Clinical laboratory testing and in vitro diagnostic test systems	Standardization and guidance in the field of laboratory medicine and in vitro diagnostic test systems. This includes, for example, quality management, pre- and post-analytical procedures, analytical performance, laboratory safety, reference systems and quality assurance.	40	Healthcare
ETSI	TC TCCE	TECHNICAL COMMITTEE (TC) TERRESTRIAL TRUNKED RADIO AND CRITICAL COMMUNICATIONS EVOLUTION (TCCE)	We are responsible for the design and standardization of TErrestrial Trunked RAdio (TETRA) and its evolution to critical communications mobile broadband solutions. TETRA (Terrestrial Trunked Radio) is the leading technology choice for critical communications users. With a projected 5 million terminals in use by 2020, the use of TETRA in security as well as other business-critical markets such as the transportation, military, commercial and utilities sectors continue to increase. TETRA is designed to address a specific set of communication requirements. These include high reliability, single and group calling capabilities, PTT (Push-To-Talk), and the possibility for direct peer-to-peer communications in situations such as natural disasters and emergencies when the supporting network is unavailable. Accordingly, much of our work of is driven by the requirements of Public Protection and Disaster Relief and other mission-critical services.		N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 27	Information security, cybersecurity and privacy protection	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: Security requirements capture methodology; Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services; Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; Security aspects of identity management, biometrics and privacy; Conformance assessment, accreditation and auditing requirements in the area of information security; Security evaluation criteria and methodology. SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.	197	All
IEC	SC 62B	Diagnostic imaging equipment	To prepare international publications for safety and performance for all kind of medical diagnostic imaging equipment (e.g. X-ray imaging equipment, computed tomography, magnetic resonance imaging equipment) including related associated equipment and accessories as well as quality procedures (e.g. acceptance tests and	81	Healthcare

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
			constancy tests) to be applied during the life-time of imaging equipment. Included is also the development of related terminology, concepts, terms and definitions.		
ISO	ISO/TC 272	Forensic sciences	Standardization and guidance in the field of Forensic Science. This includes the development of standards that pertain to laboratory and field based forensic science techniques and methodology in broad general areas such as the detection and collection of physical evidence, the subsequent analysis and interpretation of the evidence, and the reporting of results and findings.	3	N/A
IEC	SC 62D	Electromedical equipment	To develop particular international standards and technical reports for electrical equipment used in medical practice. These documents cover the safety and/or performance of the equipment as well as related terminology, concepts, definitions and symbols. Note. Examples of the types of equipment covered by the scope of SC 62D include equipment used to diagnose patients, equipment used to monitor patients, and equipment used to treat or as an aid in the treatment of patients. Exclusions: Medical diagnostic imaging and related equipment (see scope of SC 62B) and medical equipment using high-energy ionizing radiation in therapy (see scope of SC 62C) are excluded.	100	Healthcare
IEC	TC 62	Electrical equipment in medical practice	To prepare international standards and other publications concerning electrical equipment, electrical systems and software used in healthcare and their effects on patients, operators, other persons and the environment.	1	Healthcare

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 17	Cards and security devices for personal identification	Standardization in the area of: Identification and related documents Cards Security devices and tokens and interface associated with their use in inter-industry applications and international interchange	104	All
IEC	SC 31G	Intrinsically-safe apparatus	To prepare and maintain international standards relating to intrinsically safe electrical apparatus and systems for use where there is a hazard due to the possible presence of explosive atmospheres of gases, vapours, mists or combustible dusts.	13	N/A

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
IEC	ISO/IEC JTC 1/SC 40	IT Service Management and IT Governance	Standardization of IT Service Management and IT Governance. Develop standards, tools, frameworks, best practices and related documents for IT Service Management and IT Governance, including areas of IT activity such as audit, digital forensics, governance, risk management, outsourcing, service operations and service maintenance, but excluding subject matter covered under the scope and existing work programs of JTC 1/SC 27 and JTC 1/SC 38. The work will initially cover: •Governance of IT, including the development of the ISO/IEC 38500 series standards and related documents. •Operational aspects of Governance of IT, including ISO/IEC 30121 Information Technology — Governance of digital forensic risk framework, and interfaces with the management of IT as well as the role of governance in the area of business innovation. •All aspects relating to IT service management, including the development of the ISO/IEC 20000 series standards and related documents. •All aspects relating to IT-Enabled Services — Business Process Outsourcing, including the development of the ISO/IEC 30105 series standards and related documents.	27	All
IEC	SC 62A	Common aspects of electrical equipment used in medical practice	To prepare international standards concerning the common aspects of the manufacture, installation and application of electrical equipment used in medical practice, including systems, equipment, accessories, related terminology, concepts, terms, definitions and symbols.	81	Healthcare

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
IEC	TC 79	Alarm and electronic security systems	To prepare international standards for the protection of buildings, persons, areas and properties against fraudulent actions having the purpose to enter in a place or to take or to use something without permission and other threat related to persons.	55	All
IEC	SC 62C	Equipment for radiotherapy, nuclear medicine and radiation dosimetry	The preparation of standards for the safety and performance of medical equipment and systems using ionising radiation for the treatment of disease; associated equipment and software used in planning, delivering and monitoring such treatments; instruments measuring ionising radiation used in the diagnosis and treatment of disease as well as radiation conditions for testing them; and nuclear medicine equipment used for imaging the distribution of radioactive substances within the human body for both diagnostic purposes and radionuclide therapies.	40	Healthcare
ISO	ISO/TC 46	Information and documentation	Standardization of practices relating to libraries, documentation and information centres, publishing, archives, records management, museum documentation, indexing and abstracting services, and information science.	126	All
ISO	ISO/TC 251	Asset management	Standardization in the field of asset management.	4	All

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
IEC	ISO/IEC JTC 1/SC 23	Digitally Recorded Media for Information Interchange and Storage	Standardization in the field of removable digital storage media utilizing optical, holographic and magnetic recording technologies, and flash memory technologies for digital information interchange.	135	N/A
ISO	ISO/TC 262	Risk management	Standardization in the field of risk management	5	All
ISO	ISO/TC 84	Devices for administration of medicinal products and catheters	Standardization of the performance of metered devices and supplies intended for administration of medicinal products, and standardization of syringes, needles and catheters.	35	N/A
ISO	ISO/TC 267	Facility management	Standardization in the field of facility management	5	All
IEC	ISO/IEC JTC 1/SC 35	User interfaces	Standardization in the field of user-system interfaces in information and communication technology (ICT) environments and support for these interfaces to serve all users, including people having accessibility or other specific needs, with a priority of meeting the JTC 1 requirements for cultural and linguistic adaptability.	81	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	ISO/IEC JTC 1/SC 36	Information technology for learning, education and training	Standardization in the field of information technologies for learning, education, and training to support individuals, groups, or organizations, and to enable interoperability and reusability of resources and tool. Excluded from this scope are: • standards or technical reports that define educational standards (competencies), cultural conventions, learning objectives, or specific learning content. • work done by other ISO or IEC TCs, SCs, or WGs with respect to their component, specialty, or domain. Instead, when appropriate, normative or informative references to other standards shall be included. Examples include documents on special topics such as multimedia, web content, cultural adaptation, and security.	53	N/A
IEC	ISO/IEC JTC 1/SC 37	Biometrics	Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common f ile frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects. Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification. Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protections techniques, biometric security testing, evaluations and evaluations methodologies.	131	N/A

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
ISO	ISO/TC 292	Security and resilience	Standardization in the field of security to enhance the safety and resilience of society.	39	All
ISO	ISO/PC 317	Consumer protection: privacy by design for consumer goods and services	Standardization in the field of consumer protection: privacy by design for consumer goods and services	0	All
ISO	ISO/TC 232	Education and learning services	Standardization in the field of education and learning services focused on, but not limited to services; management systems; facilitators; assessments; terminology; ethical conduct.	4	N/A
IEC	SC 31J	Classification of hazardous areas and installation requirements	To prepare and maintain international standards relating to the use of equipment including area classification, the selection and installation, inspection and maintenance, repair, overhaul and reclamation of equipment where there is a hazard due to the possible presence of explosive atmospheres of gases, vapours, mists or combustible dusts.	11	All

Committees relevant to physical security					
SDO	Committee	Committee Title	Committee Description	Published Standards	Field
IEC	SC 31M	Non-electrical equipment and protective systems for explosive atmospheres	To prepare and maintain international standards relating to non-electrical equipment and protective systems for use where there is a hazard due to the possible presence of explosive atmospheres of gases, vapours, mists or combustible dusts.	9	All
IEC	SC 45B	Radiation protection instrumentation	To prepare standards that address instrumentation used for: - the measurement of ionizing radiation in the workplace, to the public, and in the environment for radiation protection purposes; - illicit trafficking detection and identification of radionuclides; - radiation-based security screening.	62	All
ISO	ISO/TC 260	Human resource management	Standardization in the field of human resource management.	13	N/A
ISO	ISO/TC 279	Innovation management	Standardization of terminology tools and methods and interactions between relevant parties to enable innovation.	4	N/A
ISO	ISO/TC 215	Health informatics	Standardization in the field of health informatics, to facilitate capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system.	201	Healthcare

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
IEC	TC 106	Methods for the assessment of electric, magnetic and electromagnetic fields associated with human exposure	To prepare international standards on measurement and calculation methods to assess human exposure to electric, magnetic and electromagnetic fields.	28	N/A
ISO	ISO/TC 283	Occupational health and safety management	Standardization in the field of occupational health and safety management to enable an organization to control its OH&S risks and improve its OH&S performance.	1	Healthcare
IEC	TC 31	Equipment for explosive atmospheres	To prepare and maintain international standards relating to equipment for use where there is a hazard due to the possible presence of explosive atmospheres of gases, vapours, mists or combustible dusts	63	N/A
IEC	TC 34	Lighting	To map and maintain the standardization structure and to prepare, review and maintain international standards and related IEC deliverables regarding safety, performance and compatibility specifications for: a) Electric lamps and electric light sources b) Caps and holders c) Controlgear and control devices for electric lamps, electric light sources, and electronic lighting equipment d) Luminaires e) Lighting systems	54	All

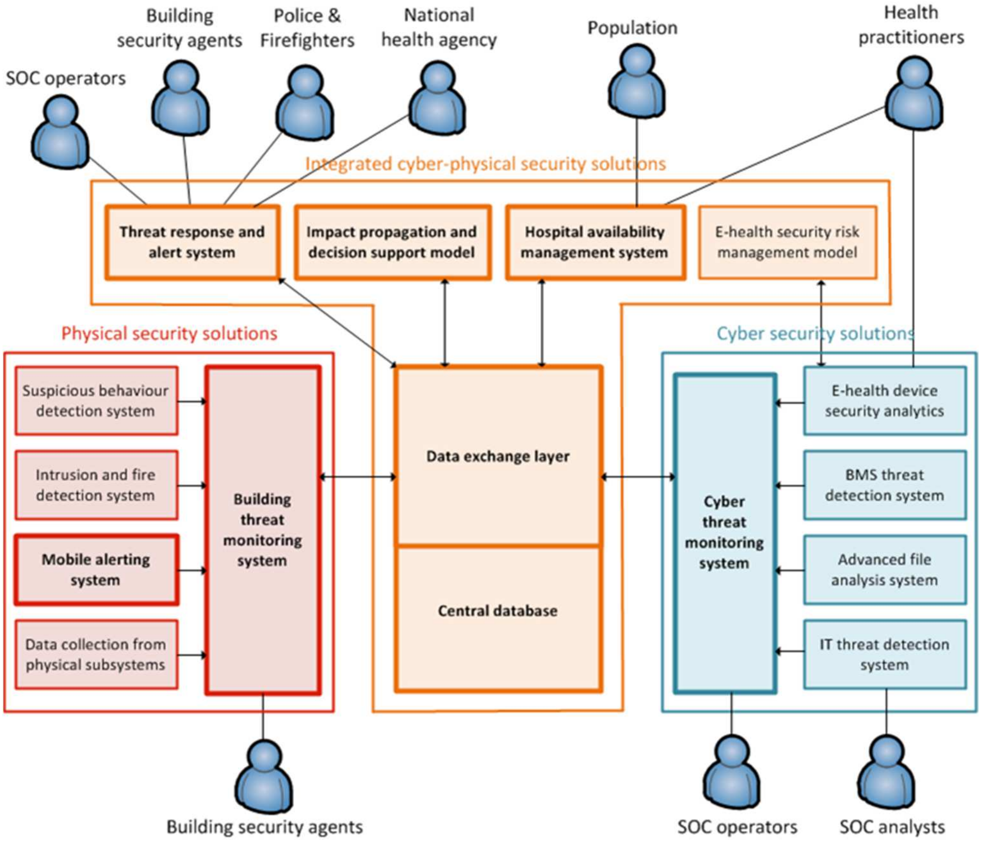
Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
			f) Miscellaneous equipment related to items a), b), c), d) and e)		
ISO	ISO/TC 312	Excellence in service	Standardization in the field of excellence in service	0	N/A
IEC	TC 72	Automatic electrical controls	To prepare standards related to inherent safety, to the operating characteristics where such are associated with applicational safety, and to the testing of automatic electrical control devices used in appliances and other apparatus, electrical and non-electrical, for household and similar purposes, but also extended to industrial purposes when no dedicated product standards exist, such as that for central heating, air conditioning, process heating building automation, etc.,	34	All
ISO	ISO/TC 304	Healthcare organization management	Standardization in the field of healthcare organization management including: classification, terminology, nomenclature, management practices and metrics that comprise the non-clinical operations in healthcare entities.	1	Healthcare
IEC	TC 81	Lightning protection	To prepare international standards and guides for lightning protection for structures, as well for persons, installations, services and contents. The objective of the standards will be: • To develop requirements for design and installation of Lightning Protection Systems for structures, • To develop requirements for design and installation of Surge Protection Measures for structures as they relate to protection from lightning effects, • To develop basic requirements for protection against electromagnetic effects due to	19	All

Committees relevant to physical security					
SDO	**Committee**	**Committee Title**	**Committee Description**	**Published Standards**	**Field**
			lightning, • To give general guidance to IEC member countries that may have need of such requirements and • To facilitate international exchanges that may be hampered by differences in national regulations.		
IEC	TC 89	Fire hazard testing	To prepare international standards, technical specifications and technical reports in the areas of: Fire hazard assessment, fire safety engineering and terminology as related to electrotechnical products. Measurement of fire effluent (e.g. smoke, corrosivity, toxic gases and abnormal heat), and reviews of the state of the art of current test methods as related to electrotechnical products. Widely applicable small scale test methods for use in product standards and by manufacturers and regulators. Horizontal safety function: Guidance and test methods for assessing fire hazards of electrotechnical equipment, their parts (including components) and electrical insulating materials.	49	All

11 Appendix 2 - SAFECARE modules throughout the crisis-management cycle

<u>The SAFECARE global architecture</u>

The SAFECARE global architecture can be broken down into 3 parts, as shown in Figure 1, namely: physical security solutions; cyber security solutions; and integrated cyber-physical security solutions. The physical security solutions and the cyber security solutions consist of smart modules and efficient integrated technologies to respectively improve physical security and cyber security. More specifically, physical security solutions embed integrated intelligent video monitoring and interconnect building monitoring systems as well as management systems. Meanwhile, cyber security solutions correspond to cyber monitoring systems as well as threat detection systems related to information technology (IT), building management system (BMS) and e-health systems. Both physical security solutions and cyber security solutions are interconnected thanks to the integrated cyber-physical security solutions. The integrated cyber-physical security solutions consist of intelligent modules whose role is to integrate different data sources and better take into account the combination of physical and cyber security threats.



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

Figure 7 - SAFECARE global architecture

The physical security solutions rely on:

- Suspicious Behaviour Detection System (SBDS);
- Intrusion and Fire Detection System (IFDS);
- Data Collection System;
- Mobile Alerting System (MAS);
- And the building threat monitoring system (BTMS).

The cyber security solutions rely on:

- IT Threat Detection System;
- The BMS Threat Detection System;
- The Advanced File Analysis System (AFAS);
- E-health devices security analytics;
- Cyber Threat Monitoring System (CTMS).

The integrated cyber-physical security solutions rely on:

- The Data eXchange Layer (DXL);
- Central DataBase (CDB);
- Impact Propagation and Decision Support Model (IPDSM);
- Threat Response and Alert System (TRAS);
- Hospital Availability Management System (HAMS);
- E-health security risk management model.

In the following paragraphs the crisis management phases and the mapping of the SAFECARE modules (as presented in D8.4) to each phase are presented.

The SAFECARE modules throughout the crisis-management cycle

Crisis management has been defined as "the developed capability of an organization to prepare for, anticipate, respond to and recover from crises (47). It consists of four phases, namely Preparedeness, Response, Recovery and Mitigation. The concept of the cycle implies an ongoing process which tries to eliminate disruptions, to provide immediate assistance to affected ontologies, to reduce disaster losses and to improve the conditions of the affected communities. Usually, the crisis management cycle is triggered by an event and begins with the response to that event. As the main aim is to respond to the specific threat, crisis management programs often prioritize the preparedness and response phases, leaving limited resources to address recovery and mitigation. A systems approach to crisis management suggests a different understanding of the crisis cycle that balances resources among the four phases. In this section the four phases of the crisis management process will be described and the SAFECARE modules will be mapped to each phase.

Preparedness phase

Preparedness is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective actions that internal and external stakeholders should cooperate closely to ensure organization readiness. Risk assessment constitutes the fundamental first step in preparedness and this means the identification and analysis of major threats, hazards and related vulnerabilities. This procedure helps organizations make decisions on equipment supply, maintenance and improvement, identification protective measures and to take quick decisions during the crisis. Having determined the risks that could impact airports and how, actions that support response process should be identified. More specifically, appropriate institutional structures, clear mandates supported by comprehensive policies, plans and legislation and the allocation of resources for all these capacities through regular budgets are also instrumental for thorough preparedness to crisis.

In this phase of the crisis management process, the following SAFECARE modules are related:

- The **Impact Propagation and Decision Support Model** is the cornerstone of the SAFECARE tool. Thanks to the knowledge of the internal context of the hospital capitalized on by the ontology it embeds, it has an indisputable role to play in the **preparedness** step.
- The **BMS threat detection system** can be used during the preparedness, to help in risk assessment by highlighting existing vulnerabilities in network devices or by reviewing previous security alerts related to specific devices. It can also be used for training purposes, when taking as input pre-recorded network traffic that can be replayed for simulation.
- **E-health device security analytics module** can be used in Preparedness, as analytics can provide statistics on security configuration, posture, threats, vulnerabilities related to medical devices to support risk management.
- The **IT threat detection system** can be used in Preparedness, as it can provide statistics and trends of security threats based on past security alerts and exploitation of vulnerabilities. This can be useful for training and risk assessment.
- The **E-health security risk management model** can be used in Preparedness, as it can perform and structure the risk assessment required as part of this step. Results are documented and decisions can be made based on risk estimations.
- The **cyber threat monitoring system** can be used in Preparedness phase to provide statistics and details on past security incidents. This can be useful for training and risk assessment.
- The **DXL** can be used in Preparedness, as it provides the service of distribution of messages among the various SAFECARE modules and allows other modules to be involved for the preparedness purpose.
- The **Threat Response and Alert System** is used in Preparedness, for training purposes, as it allows stakeholder to practice different simulation scenario, as part of training and continuous improvement. Moreover, its fast alerting capability combined with the potential risk anticipation by the Impact Propagation Module is aimed at reducing and avoiding risk, by taking early and swift action and reaction plan.
- The **CDB** can be used in Preparedness, as the statistics generated on the basis of assets characteristics included in CDB and details on past security incidents could support the whole SAFECARE solution risk management. This can be useful also for training and risk assessment.
- The **Mobile Alerting System** can be used in Preparedness, as it provides access to previous security incidents and impacts.

- The **BTMS** can be used in Preparedness, as the Milestone XProtect®, as a part of the Building Threat Monitoring System, manages the setup of security devices and placing of critical assets graphically. It helps highlight existing physical security vulnerabilities and improve the security by optimizing the setup.
- The HAMS provides a training interface to allow users learn how HAMS works and what type of information it can visualize.

Response

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

In this phase of the crisis management process, the following SAFECARE modules are related:

- **IPDSM** can be used at the time of the crisis **in the response** step to determine the propagation of the impacts of an incident on the assets (as well as their evaluations) to better react. This assumes that its ontology is correctly maintained in order to reflect the real context of the hospital.
- The **BMS threat detection system** can be used during response, by detecting security-relevant events when they happen and providing information about source and destination hosts, protocols, type of event and other data, which allow the crisis management team to investigate and respond to an attack. The module can be both for real-time crisis management, when gathering information and detecting security events from live network traffic.
- **E-health device security analytics module** can be used in Response, to generate alerts on security misconfigurations, threats or vulnerabilities related to medical devices with root cause and recommended action to support remediation.
- The **IT threat detection system** can be used in Response, as it can support the detection of potential threats and raise security alerts related to the IT infrastructure, providing information about the targeted hosts. The information is useful for the initial assessment of the incident during the crisis management.
- **The E-health security risk management** model can be used in Response phase, to define the EDSA models used for detecting & handling security incidents. Secondary response is that incidents will gathered and analyzed to update the model as such.

- **The advanced file analysis system** can be used in Response phase, to detect malware and raise security alerts, providing a security risk level with an analysis report for each file. The report is useful for the initial assessment of the incident during the crisis management.
- The **cyber threat monitoring system** can be used in Response phase to manage security alerts to respond quickly to incidents. The tool is useful for information gathering and assessment. It can also help the crisis management team by providing relevant response plans related to the incident.
- The **DXL** can be used in Response, as it provides the service of distribution of messages among the various SAFECARE modules, it allows other modules to respond to risk management events.
- The **Suspicious behaviour detection** system can be used in Response phase, as it processes videos streams from surveillance cameras in near real-time. It will trigger security alerts in case of suspicious behaviours, such as crowding, loitering in restricted areas, weapon carrying and covered faces, and report to the Buiding Threat Monitoring System.
- The **Intrusion and Fire Detection System** can be used in Response phase, as it detects in near real-time intrusion behaviours, such as tailgating, and fire, based on video streams from surveillance cameras and other digital sensors, such as door access controls and smoke/fire alarms. It triggers security alerts and reports to the Building Threat Monitoring System.
- The **CDB** can be used in Response, to store and manage security alerts to respond quickly to incidents. The tool is useful for information storing and assessment of all real events happened.
- The **Mobile Alerting System** can be used in Response, as it (a) enables the communication between the BTMS and the security guards to quickly verify dubious physical security threats detected by the security operators; (b) provides the security guards with the ability to report incidents; (c) sends potential impacts to supervisors in charge (hospital general manager, security chief) and (d) sends notifications to users with response plans to instruct personnel on the actions to take to respond to an incident.
- The **BTMS** can be used in Response, as it centralises security events from the Suspicious Behaviour Detection System, Intrusion and Fire Detection System and Data Collection System and communicates with the Mobile Alerting System. It allows the user to acknowledge or reject an alert, forward an incident to the Central Database and show the impacts.
- The HAMS main role is about providing relevant information to security managers during the Response phase. Visualizing in near-realtime incidents and impacts through graph based interfaces helps users to manage emergencies and incidents.

Recovery

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

In this phase of the crisis management process, the following SAFECARE modules are related:

- To be efficient, **IPDSM** can receive feedbacks in terms of (1) new incidents detected, (2) new mitigation solutions adopted and (3) changes about the appreciation of the value of assets. These feedbacks come from the response, recovery and mitigation steps.
- The **IT threat detection system** can be used in Recovery, as it can support the collection of security events that allow triggering alerts and responding to the threat. The collected security events can be useful to gather evidence of the incident during the crisis management.
- The **E-health security risk management model** can be used in Recovery phase, to define a recovery after incident has been detected by ESDA.
- The **advanced file analysis system** can be used in Recovery phase, to keep files corresponding to malware and can provide the footprint of malware. This is useful to gather evidence of the incident during the crisis management.
- The **cyber threat monitoring system** can be used in Recovery phase, as it can provide a list of compromised assets related to an incident, which is useful when compiling the evidence report.
- The **BTMS** can be used in Recovery, as the video and related metadata for each incident is saved by the Milestone XProtect®. The videos are used as evidence by the stakeholders. They are also used as training data for future system improvements.

Mitigation

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

In this phase of the crisis management process, the following SAFECARE modules are related:

- To be efficient, **IPDSM** can receive feedbacks in terms of (1) new incidents detected, (2) new mitigation solutions adopted and (3) changes about the appreciation of the value of assets. These feedbacks come from the response, recovery and mitigation steps.
- The **E-health security risk management** model can be used in Mitigation phase, to create and implement comprehensive set of measures, mitigating security risks.
- The **advanced file analysis system** can be used in Preparedness phase, to provide statistics and trends of security threats based on past malware detected. This can be useful for training and risk assessment.

- The **cyber threat monitoring system** can be used in Mitigation phase, as it can create and implement comprehensive set of reaction plan, mitigating security risks.
- The **DXL** can be used in Mitigation, as it provides the service of distribution of messages among the various SAFECARE modules, it permits mitigating security risks.
- The **Threat Response and Alert System** is used in Mitigation phase, as it could support risk arise and ensure that stakeholders implement the reaction plan as soon as possible. The rest of SAFECARE module provides all the information needed to help quickly mitigate any risk. The alerting module role is to make sure stakeholder are alerted and on the bridge as quickly and as efficiently as possible. In short, the alerting system's role is to focus stakeholder's attention on the reaction plan to put in place, using a wide range of medias and providing as many useful information as possible. Since the alerting system is directly connected to the global architecture, it reduces delay and allows the push of relevant information to the right stakeholders.
- The **CDB** can be used in Mitigation, as the experience of past events duly stored and registered is a useful tool for mitigating security risks.
- The HAMS provides an overview of the past messages received during the Response phase. Users can analyse potential impacts on assets status and availability after an incident as well as visualize reports of the alerting campaign, in order to improve the management of mitigation phase.