Computers in Industry 142 (2022) 103715

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern

David G. Rosado[a,*], Antonio Santos-Olmo[a], Luis Enrique Sánchez[a], Manuel A. Serrano[b], Carlos Blanco[c], Haralambos Mouratidis[d], Eduardo Fernández-Medina[a]

[a] *GSyA Research Group, University of Castilla-La Mancha, Ciudad Real, Spain*
[b] *Alarcos Research Group, University of Castilla-La Mancha, Ciudad Real, Spain*
[c] *ISTR research group. Dept. of Computer Science and Electronics, University of Cantabria, Spain*
[d] *Institute for Analytics and Data Science, University of Essex, UK*

ARTICLE INFO

Article history:
Received 10 November 2021
Received in revised form 6 May 2022
Accepted 13 May 2022
Available online 20 June 2022

Keywords:
Risk analysis
Risk assessment
MARISMA
Cyber-physical system

ABSTRACT

Cyber-physical systems (CPSs) are smart systems that include engineered interacting networks of physical and computational components. CPSs have an increasingly presence on critical infrastructures and an impact in almost every aspect of our daily life, including transportation, healthcare, electric power, and advanced manufacturing. However, CPSs face a growing and serious security issue due to the widespread connectivity between the cyber world and the physical world. Although risk assessment methods for traditional IT systems are now very mature, these are not adequate for risk assessment of CPSs due to the different characteristics of the later. As such, there is an urgent need to define approaches that will adequately support risk assessment for CPSs. To contribute to this important challenge, we propose a novel risk analysis technique for CPSs based on MARISMA, a security management methodology, and eMARISMA, a technological environment in the cloud. Our work contributes to the state of the art through the definition of the MARISMA-CPS pattern that incorporates a set of reusable and adaptable elements that allows risks in CPSs to be managed and controlled, which is aligned with the main CPSs frameworks, such as those defined by NIST and ENISA. A case study for a smart hospital is presented, showing how the reusability and adaptability of the proposal allows the proposed MARISMA-CPS pattern to be easily adapted to any CPS environment. Such adaptability is important to ensure wide application in the domain of CPSs.

1. Introduction

CPSs are smart systems that include computing, storage, and communication features which can monitor and/or manage objects in the physical world (Orojloo and Azgomi, 2017; Alguliyev et al., 2018), and which can build a wide range of innovative applications and services that are available for citizens and businesses alike (Kozák, 2019). Research related to CPSs to date has focused on the areas of academia, industry, and governments worldwide due to the wide-ranging impact that CPS can have on society, the economy, and the environment (Griffor et al., 2017; Hofer, 2018; Tantawy et al., 2020). CPSs provide highly interconnected and integrated systems that can deliver new functionalities, improving the quality of life and allowing for technological progress in critical areas, such as customised health care (AhsanulHaque et al. 2014; Leite et al. 2018; Priyadarshini et al. 2021), emergency response (Gelenbe et al., 2012; Taylor and Sharif, 2017), traffic flow management (Xiong et al., 2015; Jindal et al., 2018), intelligent manufacturing (Lee et al., 2015; Wang et al., 2015; Khalid et al., 2018), defence and national security (Das et al., 2012; Clark and Hakim, 2017, and energy supply (Zeadally et al., 2019; Osman et al., 2021; Kumar et al., 2022).

While current research work tends to focus on achieving objectives such as stability, robustness, performance, and efficiency for physical systems (Ying et al., 2020, the issue of security in CPS has to date been widely overlooked (Ananda et al., 2019). CPSs are being increasingly and extensively being integrated into various critical infrastructures, with the result that any security breaches to these systems could have a calamitous impact. Cybersecurity plays a key role in making companies more competitive. In fact, critical

[*] Corresponding author.
E-mail addresses: david.grosado@uclm.es (D.G. Rosado), antonio.santosolmo@uclm.es (A. Santos-Olmo), luise.sanchez@uclm.es (L.E. Sánchez), manuel.serrano@uclm.es (M.A. Serrano), Carlos.Blanco@unican.es (C. Blanco), h.mouratidis@essex.ac.uk (H. Mouratidis), eduardo.fdezmedina@uclm.es (E. Fernández-Medina).

https://doi.org/10.1016/j.compind.2022.103715
0166-3615/© 2022 Published by Elsevier B.V.
CC_BY_NC_ND_4.0

industrial systems are vulnerable to a range of cyber-attacks that are capable of affecting the complete business model (Lezzi et al., 2018).

Cybersecurity is, therefore, a fundamental discipline because of its role in concincing users that CPS, their information, and the supporting communications and information infrastructures be fully protected. CPSs have many unique features which are relevant when taking decisions on matters of cybersecurity, including real-time response constraints, extremely high availability, predictability, and reliability (Brewer, 2013; Mahoney and Davis, 2017; Lu and Xu, 2019). As advances in technology permit more and more automatic control of the functions of physical systems, the risk of cyber-attacks, including the exploitation of such automation capabilities, thereby increases (Horowitz and Pierce, 2012; Deloitte, 2017; Lezzi et al., 2018). Protecting CPSs is further complicated by the fact that an ever-increasing set of CPS will in future be required to work in a wide range of operating conditions, meaning that these could be threatened by an increasing variety of cyber-attack mechanisms and processes (Griffor et al., 2017). Static assessment methods can only provide us with a rough estimate of the risk over a given period, without being able to give an accurate assessment of the risk at specific points in time (Wu et al., 2015). In order to improve the effectiveness of risk assessment, dynamic assessment methods capable of predicting future situations need to be proposed. This need is particularly acute given that the cyber-attacks that are currently occurring affect similar systems, and include attempts to adjust the RAM process by updating its variables and its safeguards. However, such dynamic assessment is extremely difficult to implement, and at present RAM approaches typically do not even address it (Jamshidi et al., 2018).

Since the traditional risk assessment method for IT systems cannot be directly applied to CPSs, these systems evidently face a major security risk. An appropriate risk assessment of CPS should provide a comprehensive understanding of the CPS security status and support the effective allocation of protected resources. Although risk assessments in traditional IT systems are mature, a distinct and novel RAM method for CPSs is needed in order to cover the growing security issues that arise due to the large differences between IT systems and CPSs (Ali et al., 2018; Ji et al., 2021). Even though there have been numerous proposals to address the IT RAM in a systematic way (Abioye et al., 2021; Bhatti et al., 2021; Aleksandrov et al., 2021), these proposals have often presented difficulties in their practical implementation when applied to highly dynamic systems like CPSs. They do not have adequate tools for processing (or if they exist, they are not very usable) because they have been designed for application in large companies and as such they are not context-sensitive, i.e., these tools do not have the capacity to adapt to special environments that require a special treatment of risks. To address these deficits, we have developed a methodology called "MARISMA" (Methodology for the Analysis of Risks on Information Systems, using Meta-Pattern and Adaptability) (Sanchez et al., 2009), supported by a technological environment called "eMARISMA" (www.emarisma.com). MARISMA is a methodology based on the reuse of knowledge for the purpose of RAM, using structures known as "patterns" that allow us to support different types of cases, while helping to significantly minimise the effort that is required in the process. In previous work (Rosado et al., 2021), the MARISMA methodology and the meta-pattern (generic structure with the main elements of a RAM process) were defined and adapted to a Big Data environment. They were also successfully applied to real cases. This paper defines a specific pattern (MARISMA-CPS) aiming to provide a complete RAM environment based on the MARISMA methodology. The proposed pattern allows risks in CPS to be managed and controlled. This pattern is based on the main CPS, IoT and risk management standards and recommendations. In particular, we have considered the ISO/IEC 27.000 and IEC 62443 standards, the baseline security recommendations for IoT, proposed by the ENISA (European Union Agency for Network and Information Security) (Ross et al., 2017), and the framework for CPSs developed by NIST (Griffor et al., 2017), which considers the inherent needs of these types of systems. It should be emphasised that this risk management and control model must be included in the company's global risk management framework.

The rest of this work is organised as follows: firstly, an introduction to the background related to the topic is made, followed by a section that introduces the main characteristics of the MARISMA framework, as well as a description of how to define the pattern. Subsequently, the MARISMA-CPS pattern is explained, with a definition of each of its elements. Then, a case study is presented and the results of the application of the MARISMA-CPS to this case study are shown. Finally, a section of conclusions and future work is included.

2. Related work

In this section we analyse the different frameworks, methodologies, recommendations, norms or standards related to RAM, as well as several proposals oriented to CPSs.

The main proposals, most widely referenced in the scientific community related to RAM are MAGERIT (Spanish Higher Council for Government, 2012), OCTAVE (Caralli et al., 2007), CRAMM (CCTA, 2005), CORAS (Lund et al., 2011), MEHARI (CLUSIF, 2010), and the different ISO/IEC standards (ISO/IEC TR 15443-1, 2012; ISO/IEC 21827, 2008; ISO/IEC 27005, 2018), plus the COBIT (De Haes et al., 2020) or NIST standards (Ross et al., 2017).

MAGERIT implements the risk management process within a governance framework to assist decision making, taking into account the risks derived from the use of information technology. Its objectives are to offer a systematic method for analysing risks, to help in describing and planning the appropriate measures for keeping the risks under control, and to prepare the organisations for the processes of evaluating, auditing, certifying, or accrediting. On the other hand, OCTAVE is a strategic planning and consulting technique, based on technological risk, that is used in security. It has three phases: the development of the initial security strategies, a technological view identifying infrastructure vulnerabilities, and a risk analysis developing security strategy and plans. Other approach is CORAS which provides a customised language for threat and risk modelling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. In the CORAS method a security risk analysis is conducted in eight steps and is supported by a tool. The proposal MEHARI has as objective to provide a set of tools specifically designed for security management, comprising a set of management actions, each of which has a specific objective. MEHARI also gives a guideline in security assessment and defines 9 steps to conduct risk assessment. Lastly, CRAMM performs its risk analysis by combining assets, threats and vulnerabilities to evaluate the risk involved and then does its risk management by suggesting a list of countermeasures. It is thus a RAM methodology that involves three phases: identifying, analysing, and managing risks.

With regards to the main standards that govern security management, we can highlight the ISO/IEC 27000 family, and particularly ISO/IEC 27005 (ISO/IEC 27005, 2018), which defines guidelines for information security risk management. The ISO/IEC 21827 standard (ISO/IEC 21827, 2008) provides a capacity and maturity model for systems security engineering and includes a risk management process within the processes which is necessary for any organisation which aspires to excellent systems security. The ISO/IEC 15443 standard (ISO/IEC TR 15443-1, 2012) assists the IT security professional to ensure security at different levels (process, product, and environment) and thus inspire confidence that a given deliverable

Table 1
Comparison between the main approaches related to RAM.

		FEATURES								
		Orientation type	Proposal type	Adaptive Catalogues	Reuse Knowledge & Learning	Dynamic and Evolving	Low Level of Subjectivity	Simplicity & Low Cost	Case Studies	Tool Supported
APROACHES	MAGERIT	Generic	Methodology	P	N	N	N	N	Y	Y
	OCTAVE	Generic	Methodology	P	N	N	N	P	Y	Y
	CRAMM	Generic	Methodology	N	N	N	N	N	Y	N
	CORAS	Generic	Methodology	N	N	N	N	N	P	Y
	MEHARI	Generic	Methodology	N	P	P	N	N	P	Y
	ISO/IEC 27000 Family	Generic	Standard	N	N	N	N	N	Y	P
	COBIT	Generic	Framework	N	N	N	N	N	Y	P
	NIST	Generic	Framework	P	N	N	N	N	Y	P
	ISO/IEC 21827/ SSE-CMM	Generic	Standard	N	N	N	N	N	Y	N
	ISO/IEC 15443	Generic	Standard	N	N	N	N	N	Y	N
	RECYPHR2015	CPS	Framework	N	N	P	N	N	N	P
	Zahid2020	CPS	Framework	N	N	N	N	P	Y	P
	Stellios2021	CPS/IoT	Model	N	N	N	N	N	N	N
	Kure2018	CPS	Model	N	N	N	N	P	Y	P
	DeSmit2017	SCADA	Model	N	N	N	N	Y	Y	N
	Vikas2019	Smart grids	Good practice	N	N	N	N	N	N	N
	MARISMA	Generic	Framework	Y	Y	Y	Y	Y	Y	Y

DESCRIPTION OF FEATURES Orientation type: It is oriented to any specific type of sector or technology. **Proposal type**: Type of RAM (framework, methodology, standard, model, etc.). **Adaptive Catalogues**: It has the capability to contain specialised taxonomies (e.g. CPS). **Reuse Knowledge & Learning**: Ability to reuse knowledge acquired during other risk analyses and to evolve **Dynamic and Evolving**: It can evolve dynamically over time. **Low Level of Subjectivity**: Includes techniques that allow greater precision in the results. **Simplicity & Low Cost**: Requires few resources for its implementation. **Case Studies**: It has been developed and refined from case studies. **Tool Supported**: It supported by tools, which allow for the automation of tasks.

will meet the security requirements. This assurance is established by incorporating security methods and techniques into the different phases of development (design, implementation, integration, maintenance, etc.). COBIT (De Haes et al., 2020) is a methodology used to ensure the control of strategic business planning by facilitating the detection of critical areas within the organisation, establishing limits and control mechanisms and mitigating the levels of exposure to the different risks. Finally, the NIST organisation has proposed a generic risk management framework that can be applied to any given information system (Ross, 2018). This framework provides guidelines on how best to manage security and privacy risks. The protection of privacy and the security of information systems and people is implemented with appropriate risk response strategies by integrating controls into the SDLC process.

As far as RAM for CPSs is concerned, there is currently a lack of proposals for real systems (Chong et al., 2019). Most of the proposals are still in their preliminary stages and are based on risk assessment only, without getting into the management of those risks (Mokalled et al., 2019). Among these preliminary proposals, the RECYPHR framework (Hessami et al., 2015), which is based on the ISO 31000 standard, is noteworthy, but it currently lacks implementation or the tools to support the framework. Furthermore, there are several generic proposals, like the security risk mitigation framework for a CPS focused on constraints proposed by Zahid (Zahid et al., 2020). A systematic mapping study on CPS security can be found in (Zahid et al., 2021), which notes the importance of this field, and which is focused on analysing risks and modelling them.

There are also some other proposals for risk assessment in CPS, like the ones shown in (Kure et al., 2018; Stellios et al., 2021), all interesting and promising works, but which are not supported by any standard and which lack methodologies and tools for supporting RAM in the context of CPSs. Among these preliminary works one can also find some interesting works dealing with different environments, like the proposals for risk assessment in IoT (Malik and Singh, 2019), SCADA systems and manufacturing (Cherdantseva et al., 2016; DeSmit et al., 2017), or smart grids (Lamba et al., 2019). In light of the foregoing, it was decided to address this need for RAM in CPS by using the MARISMA methodology. This was specifically developed to improve upon the aforementioned proposals, and has patterns as a mechanism to be extended and adapted to new dynamic contexts. As such, we believe it is appropriate and adequate for our purpose.

Table 1 shows a comparative analysis between the main RAM approaches, taking account of some of the important desirable features that any RAM process should include. In the table, 'Y′ means that the proposal includes such a feature, 'N′ means that it does not include it, and 'P′ means that it includes it in part only.

3. MARISMA framework

MARISMA is a RAM methodology that can be adapted to any type of IT environment (Santos-Olmo et al., 2016) which defines the meta-pattern, in which security controls are considered from the beginning of the risk analysis process, and which allows the reuse of artefacts and the definition of patterns for specific contexts. Moreover, as it is supported by the eMARISMA tool, the process and decision making are made agile and simple (see Fig. 1).

The meta-pattern data model is shown in Fig. 2. MARISMA's adaptability to different contexts owes principally to the definition of the pattern (details of the data model and an example of a pattern adapted to Big Data is defined in (Rosado et al., 2021). The pattern inherits the elements common to any RAM process defined in the meta-pattern, and then completes or adapts them to a specific context.

To build the pattern from the elements defined in the meta-pattern, the first thing to do is to review the literature, search for standards, recommendations, proposals and good practices in the context of RAM, trying to focus the search towards IoT and CPS environments to find domain standards and appropriate controls for CPSs, taxonomies of assets, threats and dimensions, which are the main elements of the meta-pattern. For the MARISMA-CPS pattern we have been guided by the ENISA and NIST recommendations for IoT and ISO/IEC 27.000 and IEC 62443 standards, where they establish sets of possible controls, taxonomies of assets, threats, dimensions, etc. that can serve as a first approximation for the construction of the pattern. Throughout the paper we will indicate the sources of the information that has been used to build the MARISMA-CPS

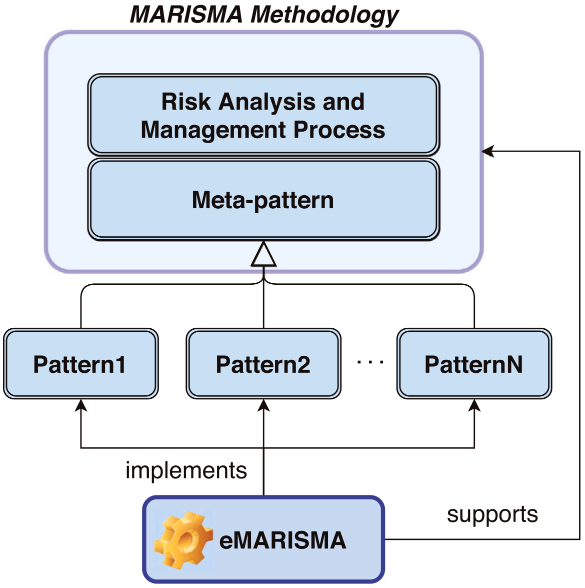


Fig. 1. General schema of MARISMA methodology.

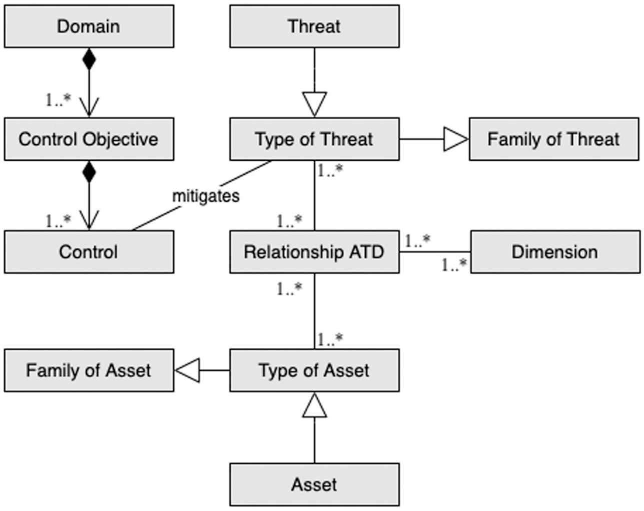


Fig. 2. Meta-pattern of MARISMA.

pattern. In addition, we have been assisted by cybersecurity and RAM experts for the complete construction of the pattern. There were 8 experts who took part in the survey from 2 consulting companies, such as Sicaman N.T and Marisma Shield organisations, with roles including senior security consultant, physical security experts, junior security consultants. Once the essential elements used to build the pattern have been analysed and selected, drawing on the expert knowledge and experience of the authors and contributors, the complex relationships between these elements are then completed, e.g., the matrices relating assets, threats and dimensions, or the relationships between domains, threats, and controls, as will be seen throughout the paper.

At this point, with the pattern already built, the next step is to apply it to real life, instantiating the pattern to a concrete case, for which we have chosen a smart hospital. In order to do so, it is necessary to study in depth the types of assets involved in the system and to analyse and identify the types of threats that may affect the system and cause damage to the assets. This application is described in detail in Section 5, where both the specific asset types and threats have been defined for a healthcare environment (shown in Table 10 and Table 11). The instantiation of the pattern to a specific context should be carried out by an expert in security and RAM issues within the company. Generally the ICT security team will be responsible for this process and for the management of the eMARISMA tool, as they are the ones qualified to manage this whole set of concepts due to their experience and knowledge in security, and to make decisions and modify the values as they deem appropriate at each moment.

4. Defining the pattern for CPSs

As noted previously, the meta-pattern is context-independent and is composed of the generic elements that cover any RAM process of any system. When a pattern is created, the elements of the meta-pattern are instantiated by adapting them to the specific context (considering both the system to be analysed and the organisation itself).

To create the MARISMA-CPS pattern, the elements of the meta-pattern required for a CPS environment are identified and selected, taking into account the characteristics of this type of environment, which must be studied by analysing the standards and recommendations for CPSs, which are discussed below. The elements that are part of the pattern employed to carry out risk analysis in CPS are shown in Fig. 3 and will also be presented below.

4.1. Standards and reference frameworks for CPSs

NIST has established the CPSs PWG (The CPSs Public Working Group), which is tasked with defining the key aspects and reference architecture of CPS and with promoting security as a basic principle in order to accelerate its development and use in many areas of our economy and society (Griffor et al., 2017. The NIST reference framework defines trustworthiness as its main aspect, including features such as safety, security, privacy, reliability, and resilience. These are the features that will also be taken into account in our MARISMA-CPS pattern.

Another important reference to consider is the report of ENISA entitled “Baseline Security Recommendations for the Internet of Things in the context of critical information infrastructures” (Ross et al., 2017). Such kinds of data-driven environments, fuelled by connected devices and network connectivity, have become a new target of cyber-attack. Consequently, ENISA has developed guidance on the steps necessary to secure IoT and CPS from cyber threats, by highlighting good security practices and proposing recommendations to operators, manufacturers, and decision makers. The identification of cyber threats is proposed in a threat taxonomy (Marinos, 2016) where a classification of threat types and threats at various levels of detail is defined. In addition, it is worth mentioning the work of (Corallo et al., 2020, 2021) where a structured classification is made of those critical assets that are to be protected against cyber-attacks in the context of Industry 4.0, and which also includes a review of the potential impacts, the appropriate assessment methods, methodological solutions and the application to a case study. A particularisation of the set of assets and threats for CPSs has been studied as part of our MARISMA-CPS pattern.

4.2. MARISMA-CPS pattern components

4.2.1. Domains, objectives and controls

We have taken the recommendations of ENISA for IoT (Ross et al., 2017) as the basis on which to define the different domains and control objectives of our pattern (the set of domains is shown in Fig. 3). These security domains classify security controls according to the control objective that is defined. Moreover, each control can be defined according to its specific nature, in which there are 3 categories: i) policy-related controls (PS); ii) organisational controls (OP) focused on the company and its employees and iii) technical controls or measures (TM), whose objective is to reduce potential risks. The

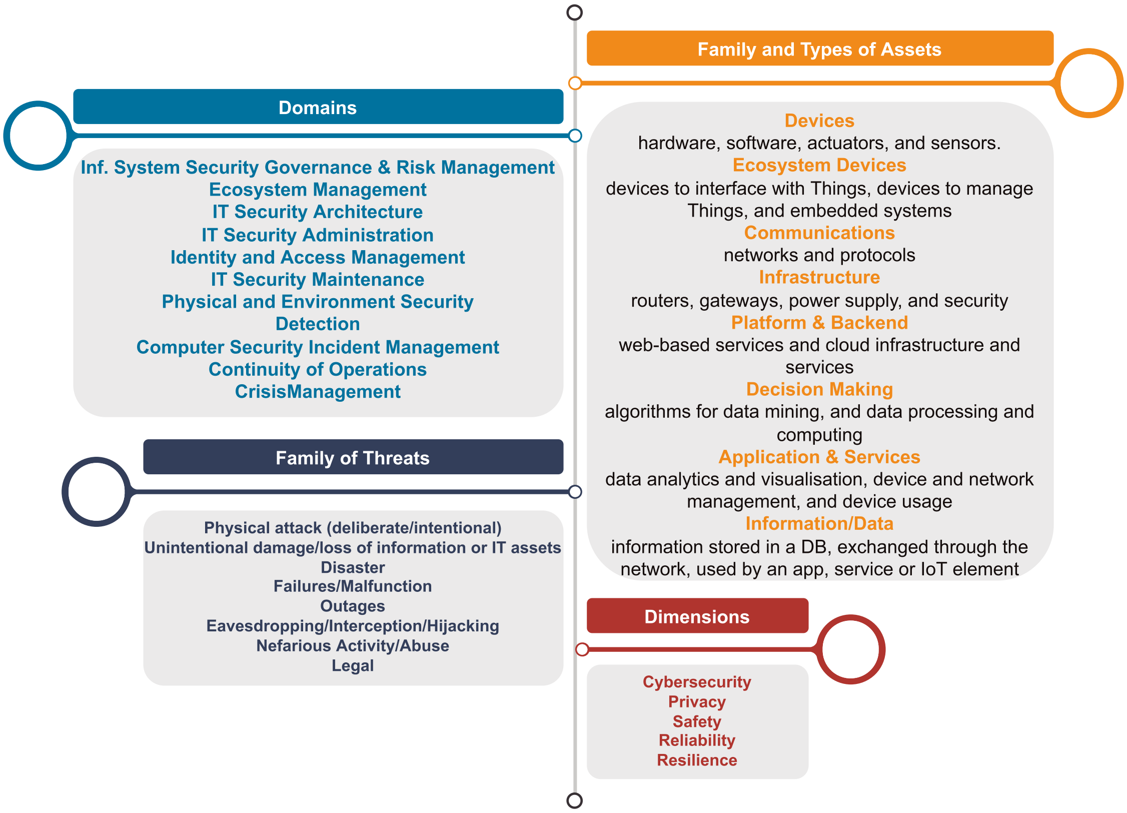

Family and Types of Assets
Devices
hardware, software, actuators, and sensors.
Ecosystem Devices
devices to interface with Things, devices to manage Things, and embedded systems
Communications
networks and protocols
Infrastructure
routers, gateways, power supply, and security
Platform & Backend
web-based services and cloud infrastructure and services
Decision Making
algorithms for data mining, and data processing and computing
Application & Services
data analytics and visualisation, device and network management, and device usage
Information/Data
information stored in a DB, exchanged through the network, used by an app, service or IoT element
Domains
Inf. System Security Governance & Risk Management
Ecosystem Management
IT Security Architecture
IT Security Administration
Identity and Access Management
IT Security Maintenance
Physical and Environment Security
Detection
Computer Security Incident Management
Continuity of Operations
CrisisManagement
Family of Threats
Physical attack (deliberate/intentional)
Unintentional damage/loss of information or IT assets
Disaster
Failures/Malfunction
Outages
Eavesdropping/Interception/Hijacking
Nefarious Activity/Abuse
Legal
Dimensions
Cybersecurity
Privacy
Safety
Reliability
Resilience

Fig. 3. Components of the MARISMA-CPS pattern.

resulting domains, objectives, and controls are shown in Table 2. Each cell indicates the control associated with each objective for each domain.

The ENISA report defines the set of controls and categorises them by control objectives, hence a domain must be assigned to its respective set of controls in order to complete the Table 2. For example, the objective "Security by design" has been related to a series of controls classified within the domains D2 "Ecosystem management", D3 "IT security architecture", D6 "IT security maintenance", and D7 "Physical and environmental security". For each of these domains, the control related to that objective is identified. Thus, in domain D2, controls PS-01 (consider the security of the whole IoT system) and PS-02 (ensure the ability to integrate different security policies and techniques) appear. The list of controls is shown in the Appendix.

4.2.2. *Types of assets*

The ENISA agency report (Ross et al., 2017) indicates a set of asset families and types that are typical in IoT systems and which are an essential component for CPSs. These can change in accordance with the relevant domains or business sectors (energy, industry, manufacturing, health, smart city, etc.). Fig. 3 shows the different types of assets to be incorporated in our pattern MARISMA-CPS, grouped by family of assets. The family and types of assets to be incorporated in our pattern are shown in Table 3.

These families of assets are the basis for CPSs because they cover all the elements of any given CPS. For example, for a health environment or a smart hospital, the relevant assets that form part of the asset family, such as information/data, may include patients' medical records or test results, as well as personal data. Other examples of assets could include glucose measurement devices, patient monitoring systems, record consultation systems, medication management systems, implantable devices, or even the hospital heating system, etc. to name but a few.

4.2.3. *Dimensions*

Figure 3 sets out the security dimensions of the MARISMA-CPS pattern that we have considered in light of Trustworthiness (a concept explained above and which is defined in the framework for CPSs published by the NIST (Griffor et al., 2017). The description of the dimensions is shown in Table 4.

4.2.4. *Family of threats and types of threats*

To define the different families and types of threats that can affect CPSs, the threat taxonomy given by the ENISA has been followed. This, in (Marinos, 2016), classifies threat families and threat types at various levels of detail (see Fig. 3). The description of the families of threats is shown in Table 5.

The above categorisation of threats can be used by any information system since it gives a general overview. The different threats therein are used to describe the specific features for a CPS, where the type of threats which can inflict harm in this kind of systems should be indicated, rejecting all other threats. The types of threats relevant for a CPS together with the families of threats, are shown in Table 6.

4.2.5. *Objective-domain-threats matrix*

In order to complete the pattern, it is necessary to define the objectives, domains and threats matrix (Table 7). For this purpose, we extract the detailed description from Annex A of the ENISA report for IoT (Ross et al., 2017), which defines a set of security controls grouped by security objectives, and for each security measure identifies the security domains that are involved and related. This allows us to see how different threat types are categorised by objective, and how for each of them, depending on the domain involved for that objective, the threats can be different. This occurs because a threat can attack an objective but not in all of its domains. This matrix is essential for MARISMA because it establishes the dependency relationship not only among controls (at the control objective level) but also among threats.

Table 2
Domains, objectives and controls of the MARISMA-CPS pattern.

		DOMAINS										
		D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11
OBJECTIVES	Security by design		PS-01,02	PS-01,04,05			PS-06, 07	PS-03				
	Privacy by design	PS-08,09										
	Asset Management			PS-10								
	Risks&Threats Identif.& Assessment	PS-11,12		PS-12								
	End-of-life support						OP-01,02,03					
	Proven solutions			OP-04			OP-05,06,07, 08					
	Mngnt of security			OP-06						OP-07,08		
	Human Resource Security Training	OP-09,10, 11										
	3rd-Party relationships	OP-12,13, 14										
	Hardware Security			TM-01,02				TM-01,02				
	Trust and Integrity Management		TM-07	TM-03,04		TM-05				TM-06	TM-06	TM-06
	Strong default security and privacy	TM-08		TM-08		TM-09						
	Data protection and compliance	TM-10,11, 12,13										
	System safety and reliability							TM-15		TM-16	TM-16,17	
	Secure Software/Firmware updates			TM-18,19, 20	TM-18	TM-18	TM-18					
	Authentication				TM-25	TM-21 22,23,24,25, 26						
	Authorisation			TM-28		TM-27						
	Access Control	TM-29,30				TM-27		TM-31,32, 33				
	Cryptography			TM-34,35, 36,37								
	Secure and trusted communications		TM-42,43	TM-38,39,40,41,42,43,44,45,46		TM-40						
	Secure Interfaces and network services	TM-47	TM-48,49	TM-48,49,50,51,52	TM-53	TM-49						
	Secure input and output handling			TM-54	TM-54							
	Logging								TM-55			
	Monitoring & Auditing	TM57					TM-57		TM-56			

DOMAINS D1: Information System Security Governance & Risk Management D2: Ecosystem Management D3: IT Security Architecture D4: IT Security Administration D5: Identity and access management D6: IT security maintenance D7: Physical and environmental security D8: Detection D9: Computer security incident management D10: Continuity of Operations D11: Crisis Management **CONTROLS** PS: policy-related controls; OP: organisational controls; TM: technical controls or measures

Table 3
Families and types of assets for CPSs.

Family of Assets	Type of Assets
Devices	Hardware, software, actuators, and sensors
Ecosystem Devices	Devices to interface with Things, devices to manage Things, and embedded systems
Communications	Networks and protocols
Infrastructure	Routers, gateways, power supply, and security
Platform & Backend	Web-based services and cloud infrastructure and services
Decision Making	Algorithms for data mining, and data processing and computing
Applications & Services	Data analytics and visualisation, device and network management, and device usage
Information/Data	Information stored in a database (at rest) Information sent or exchanged through the network (in transit) Information used by an application, service, or IoT element (in use)

Table 4
Description of dimensions for MARISMA-CPS pattern based on NIST framework for CPS (Griffor et al., 2017).

Dimensions	Description
Cybersecurity	To protect, detect, prevent and recover a system from attacks by ensuring its availability, integrity and confidentiality.
Privacy	To secure and protect individuals from potential risks arising from the use of and access to their personal information within systems or from the manipulation of physical environments.
Safety	The absence of catastrophic consequences for the user(s) and the absence of unacceptable risks of physical injury or damage that could cause death, injury, occupational diseases, damage or loss of equipment or property, or damage to the environment.
Reliability	The ability of a system or component to function under stated conditions for a specified period of time.
Resilience	The ability to adapt to changing conditions and to withstand and recover quickly from deliberate attacks, accidents or natural hazards or incidents.

4.2.6. *T-assets/T-threats/dimensions matrix*

Another matrix that needs to be defined for MARISMA is the matrix of type of assets, type of threats and dimensions (relationship ATD in Fig. 2), which can be found in Table 8. For the completion of this task, the authors' knowledge and extensive experience in security and RAM was of considerable use in extracting detailed information on the relationships between the threat, the affected assets, and the security controls within the security domains in Annex A of the ENISA IoT report (Ross et al., 2017), and on the relationship with the threats in Annex B of the ENISA IoT report. This matrix establishes the existing relationships among the types of threats and dimensions that for each type of asset are those most likely to be attacked. In this table we can see the type of asset and the type of threats that can attack the given type of assets. Note that not all assets are attacked by all threats. It should be stated that when a threat attacks an asset it is with the aim of damaging the asset by reducing its value. But the value of a type of asset is defined by its dimensions, e.g., where a threat attacks only the privacy (dimension) of an asset type, it does not attack the other dimensions for this asset type. Alternatively, it can attack (the dimensions of) privacy, reliability and confidentiality of a type of asset but not integrity, availability or safety of the same asset type.

5. Case study: smart hospital

A "smart hospital" is a hospital that seeks to improve existing patient care procedures, and create more sustainable, more secure

Table 5
Description of families of threats for MARISMA-CPS pattern based on ENISA threats taxonomy (Marinos, 2016).

Family of Threats	Description
Damage loss (IT assets)	Refers to destruction, harm, or injury to property or persons, and results in an accidental failure or reduction in usefulness, or events focusing on IT assets, and which imply intention.
Disaster	A disaster is a serious disruption of the functioning of a society and is divided into natural disasters and environmental disasters (man-made).
Failures/Malfunction	It is the non-functioning or under-functioning condition of any asset, e.g. device or network system failures or interruptions, software errors or configuration errors.
Outages	Outages are unexpected failures of the service or application that make it unavailable, inoperative or diminish its quality.
Eavesdropping/Interception/Hijacking	These are actions aimed at listening in on, interrupting or taking control of a third party communication without consent.
Nefarious Activity/Abuse	These are intentional actions and malicious acts intended to steal, alter or destroy ICT systems, infrastructure and/or networks.
Legal	These are planned, intended or ongoing legal actions by third parties seeking to enjoin actions or obtain compensation for losses based on the applicable law.

Table 6
Families of threats and types of threats for the MARISMA-CPS pattern.

Family of Threats	Type of Threats
Physical attack	Device modification; Device destruction (sabotage)
Damage loss (IT assets)	Data/Sensitive information leakage
Disaster	Disaster natural; Environment Disaster
Failures/Malfunction	Software vulnerabilities; Third parties failures
Outages	Failures of devices; Failure of system; Loss of support services; Network outage
Eavesdropping/Interception/Hijacking	Communication protocol hijacking; Network reconnaissance; Interception of information; Session hijacking; Information gathering; Replay of messages; Man-in-the-middle
Nefarious Activity/Abuse	Malware; Exploit Kits; Targeted attacks; DDoS; Counterfeit by malicious devices; Attacks on privacy; Modification of information
Legal	Violation of rules and regulations/Breach of legislation; Failure to meet contractual requirements; Abuse of personal data

Table 7
Matrix objective-domain-family of threats of MARISMA-CPS pattern.

		FAMILY OF THREATS							
		Physical attack	Damage loss	Disaster	Failures	Outages	Eavesdropping	Nefarious	Legal
OBJECTIVES	Security by design	ALL							
	Privacy by design		D1					D1	D1
	Asset Management		D3				D3	D3	
	Risks&Threats Identif.& Assessment				D1,D3	D1	D1,D3	D1,D3	D1
	End-of-life support				D6				
	Proven solutions		D3					D3	
	Management of security		D3,D6,D9		D3, D6	D3, D6	D3, D6	D3,D6	
	Human Resource Security Training							D1	
	Third-Party relationships		D1		D1	D1	D1	D1	
	Hardware Security	ALL		ALL		ALL			
	Trust and Integrity Management				D3	D3,D5,D9,D10,D11	D2,D3,D5,D9, D10,D11	D2,D3,D5,D9,D10, D11	
	Strong default security and privacy				ALL	ALL		ALL	
	Data protection and compliance		D1					D1	D1
	System safety and reliability			D7	D7,D9,D10	D7,D9,D10			
	Secure Software/Firmware updates				ALL	ALL	ALL	ALL	
	Authentication				ALL		ALL	ALL	
	Authorisation				ALL		ALL	ALL	
	Access Control	D1,D5,D7	D1		D1,D5,D7		D1,D5,D7	D1,D5	
	Cryptography				D3		D3	D3	
	Secure and trusted communications		D3, D5		D2,D3		D2,D3,D5	D2,D3	
	Secure Interfaces & network services				D3		D1,D2,D3	D4	
	Secure input and output handling				ALL			ALL	
	Logging		D8						
	Monitoring and Auditing		D1,D6,D8					D1,D6	

DOMAINS D1: Information System Security Governance & Risk Management D2: Ecosystem Management D3: IT Security Architecture D4: IT Security Administration D5: Identity and access management D6: IT security maintenance D7: Physical and environmental security D8: Detection D9: Computer security incident management D10: Continuity of Operations D11: Crisis Management

Table 8
Matrix of T-Assets/T-Threats/Dimensions for MARISMA-CPS pattern.

	Family of Assets							
Family of Threats	Devices	Ecosystem devices	Communications	Infrastructure	Platform/ Backend	Decision making	App & Services	Info/ Data
Type of Threats								
Physical attack								
Device modification	C P R1 R2		C R1 R2					
Device destruction	C	R1 R2		R1 R2	R1 R2			
Damage loss								
Data/Sensitive info leakage	C P S	C P S			C S			C P S
Disaster								
Disaster natural	S R1 R2	S R1 R2		S R1 R2	S R1 R2			
Environment Disaster		S R1 R2		S R1 R2	S R1 R2			
Failures/Malfunction								
Software vulnerabilities	C P S	C P S		R1 R2	R1 R2		C P R1 R2	
Third parties failures	C P S	C S		S R1 R2	R1 R2		S R1	
Outages								
Failures of devices	S R1 R2							
Failure of system	R1 R2	R1 R2			R1 R2			
Loss of support services	R1 S	C P S R1	C	C R1 R2	S R1 R2	C P S	R1	S R1 R2
Network outage			C S R1 R2	C S R1 R2				
Eavesdropping/ Interception/ Hijacking								
Commun. protocol hijacking	C		C			C		C
Network reconnaissance	C		C	C				C
Interception of information	C P		C P					C P
Session hijacking	C		C					C
Information gathering	C P		C P					C P
Replay of messages	C					C		C
Man-in-the-middle	C P		C P					C P
Nefarious Activity/Abuse								
Malware	C P S R1 R2	C P S R1 R2			C P S R1 R2			
Exploit Kits	C P S	C P S		C R1 R2				
Targeted attacks				R1 R2	R1 R2			C P S
DDoS	C P R1 R2	C P R1 R2		C P R1 R2	C P R1 R2			
Counterfeit malicious devices	C P S	C P S		C P S				
Attacks on privacy	P	P		P	P			
Modification of information	C P	C P		C	C			
Legal								
Violation rules & regulations	C P	C P	C P	C P	C P	C P	C P	C P
Failure contractual requirem.	C P S							C P
Abuse of personal data	C P		C P					C P

DIMENSIONS C: Cybersecurity; **P**: Privacy; **S**: Safety; **R1**: Reliability; **R2**: Resilience

and more intelligent healthcare facilities by introducing new capabilities that are achieved through optimised and automated processes built in an ICT environment of interconnected assets, mostly IoT assets (ENISA, 2016).

5.1. Defining the dimensions for the case study

In order to be able to perform the risk analysis, MARISMA first defines a set of dimensions (shown in the pattern in Fig. 3) that must be established for the case study and which are shown in Table 9.

5.2. Defining assets for the case study

Hospitals have a large set of assets that are essential to their operation and, therefore, need to be protected. Many of these assets are common to both smart and traditional hospitals, but there are many others that are specific to smart hospitals because, since they are intelligently connected, they can make decisions in an autonomous manner. These assets include, for example, patient and employee mobile devices, identification systems or clinical information that interconnects with many systems (ENISA, 2016) (see Table 10).

Once the assets have been identified and classified, incorporating them into the eMARISMA tool is simple because the tool facilitates their definition and classification by following a hierarchical structure between families, types of assets and assets defined in the pattern (a sample of some of them is provided in Fig. 4). As shown, the tool makes it possible to define more asset-related information, such as the asset value, which is a numeric element indicating the value of the asset to the company or the organisation. This value will

Table 9
Description of dimensions for case study.

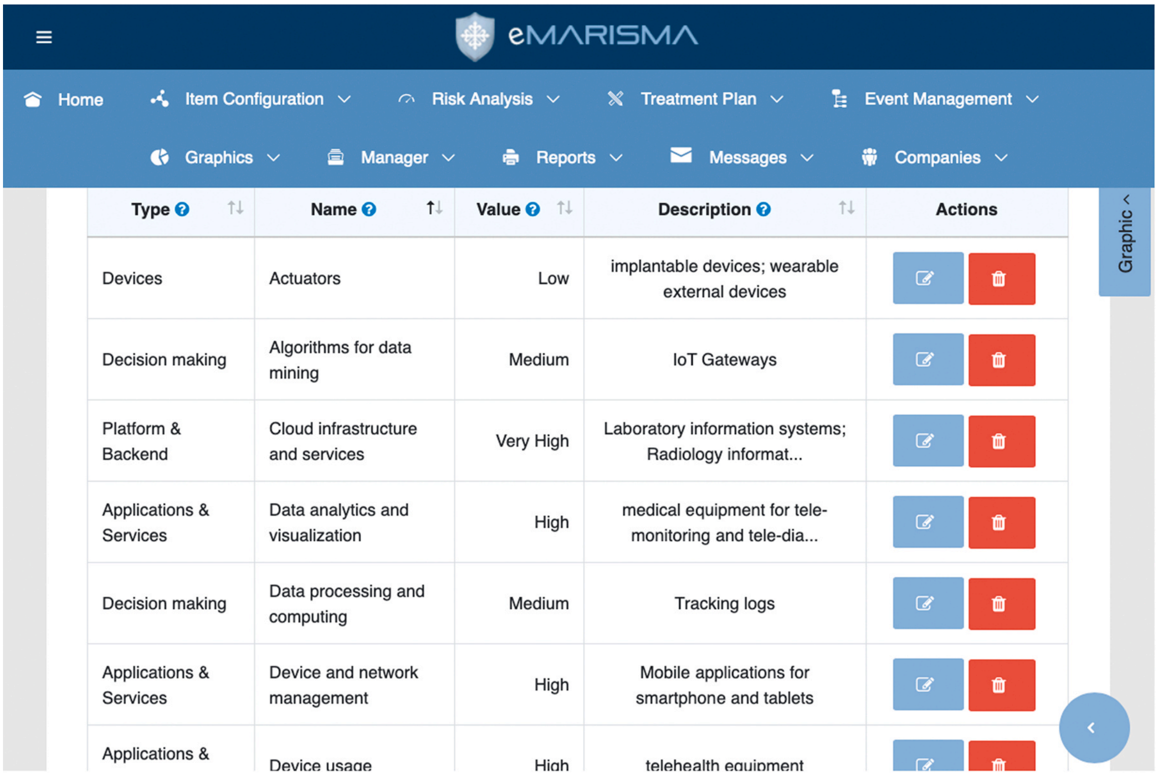
Dimensions	Description
Cybersecurity	Systems, devices and sensitive information must be protected with techniques and tools to ensure confidentiality, integrity, and availability.
Privacy	A large amount of personal health data is managed, stored and transmitted, so the privacy of such data is an essential element that must be guaranteed.
Safety	This is required to assure that the system will not misbehave in a manner that could lead it into hazardous states, thus rendering it susceptible to causing losses in general and accidents in particular for the hospital patients and the healthcare personnel.
Reliability	It must be ensured in both software and hardware. Software ensures device functionality and proper coordination between medical devices and patients. Hardware enables the operation of services and the transmission of sensitive information to medical equipments.
Resilience	The hospital must ensure cyber resilience by guaranteeing the availability and continuity of services that depend on ICT assets.

Table 10
Assets of the case study for the assets types defined in MARISMA-CPS pattern.

MARISMA-BiDa PATTERN		PATTERN INSTANTIATED
Family of Asset	Type of Asset	Assets for the Case Study
Devices	Software	RFID systems with location services
	Hardware	medical equipment for distribution of drugs or to administer treatment; stationary devices.
	Actuators	implantable devices; wearable external devices
	Sensors	mobile devices; wearable external devices; Temperature sensors
Ecosystem Devices	Devices to interface with Things	Identification systems; Smart patient room operation and management systems
	Devices to manage Things	Mobile clients
	Embedded systems	supportive devices
Communications	Networks	Transmission media
	Protocols	Network interface cards; Alarm and emergency communication applications for mobile devices
Infrastructure	Routers	Backbone network devices
	Gateways	IoT Gateways
	Power supply	Power and climate regulation systems; Medical gas supply;
	Security	Biometric scanners; CCTV; Automated door lock system
Platform & Backend	Web-based services	Hospital and Research information systems
	Cloud infrastructure and services	Laboratory information systems; Radiology information systems; Pharmacy information system; Pathology information system; Blood bank system; Picture archiving and communication systems
Decision making	Algorithms for data mining	IoT Gateways
	Data processing and computing	Tracking logs
Applications & Services	Data analytics and visualization	medical equipment for tele-monitoring and tele-diagnosis
	Device and network management	Mobile applications for smartphone and tablets
	Device usage	telehealth equipment
Information/Data	Information stored in a database (at rest)	Clinical/administrative patient data; Financial, organisational & hospital data; Staff data; Vendor details
	Information sent or exchanged through the network (in transit)	Electronic medical record
	Information used by an application, service, or IoT element (in use)	Patient data

be used to enable the tool to prioritise and improve the accuracy in assessing the risk level of the assets.

When using the MARISMA-CPS pattern to perform the risk analysis, as soon as the assets have been added to the tool, the relationships established in the pattern among assets, threats and dimensions will serve to allow the tool to start executing the risk analysis with the assets in the case study. The tool will show the results of the current risk for this set of assets in real-time. A list of the appropriate controls with which to protect this set of assets is also shown.



Type	Name	Value	Description	Actions
Devices	Actuators	Low	implantable devices; wearable external devices	
Decision making	Algorithms for data mining	Medium	IoT Gateways	
Platform & Backend	Cloud infrastructure and services	Very High	Laboratory information systems; Radiology informat...	
Applications & Services	Data analytics and visualization	High	medical equipment for tele-monitoring and tele-dia...	
Decision making	Data processing and computing	Medium	Tracking logs	
Applications & Services	Device and network management	High	Mobile applications for smartphone and tablets	
Applications &	Device usage	High	telehealth equipment	

Fig. 4. Some types of assets for the case study added to the eMARISMA tool.

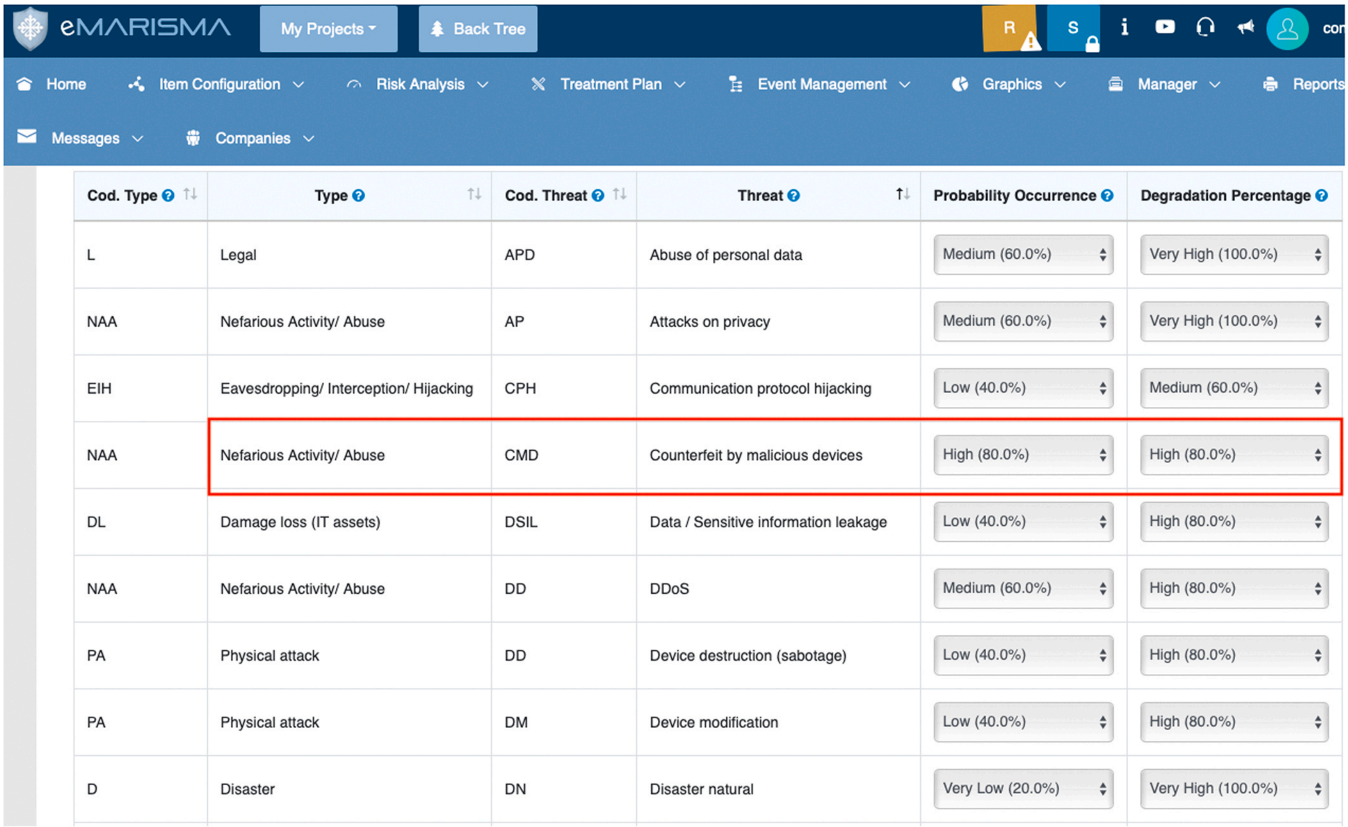
Table 11
List of threats for the case study.

Family of Threats	Type of Threats	Threats for the Case Study
Physical attack	Device modification; Device destruction (sabotage)	Theft Device and Data
Damage loss (IT assets)	Data/Sensitive information leakage	Medical system configuration error; Physician and/or patient errors; Noncompliance
Disaster	Disaster natural; Environment Disaster	Fire, Flood, Earthquake
Failures/Malfunction	Software vulnerabilities; Third parties failures	Cloud service providers; Medical device manufacturer; Network providers; Power suppliers; Software failures; Inadequate firmware; Device failure; Network components failure; Insufficient maintenance; Overload; Absence of audit logs
Outages	Failures of devices; Failure of system; Loss of support services; Network outage	Communication between IoT and non- IoT
Eavesdropping/ Interception/Hijacking	Communication protocol hijacking; Network reconnaissance; Interception of information; Session hijacking; Information gathering; Replay of messages; Man-in-the-middle	Hijacking to Networks/sesion and Medical devices; Skimming
Nefarious Activity/Abuse	Malware; Exploit Kits; Targeted attacks; DDoS; Counterfeit by malicious devices; Attacks on privacy; Modification of information	Denial of Service; Social Engineering: Phishing, Baiting and Device cloning (RFID); Malware: Virus and Ransonware; Unauthorised access control; Medical device tampering;
Legal	Violation of rules and regulations/Breach of legislation; Failure to meet contractual requirements; Abuse of personal data	Theft or exposure Clinical patient data

5.3. *Defining threats for the case study*

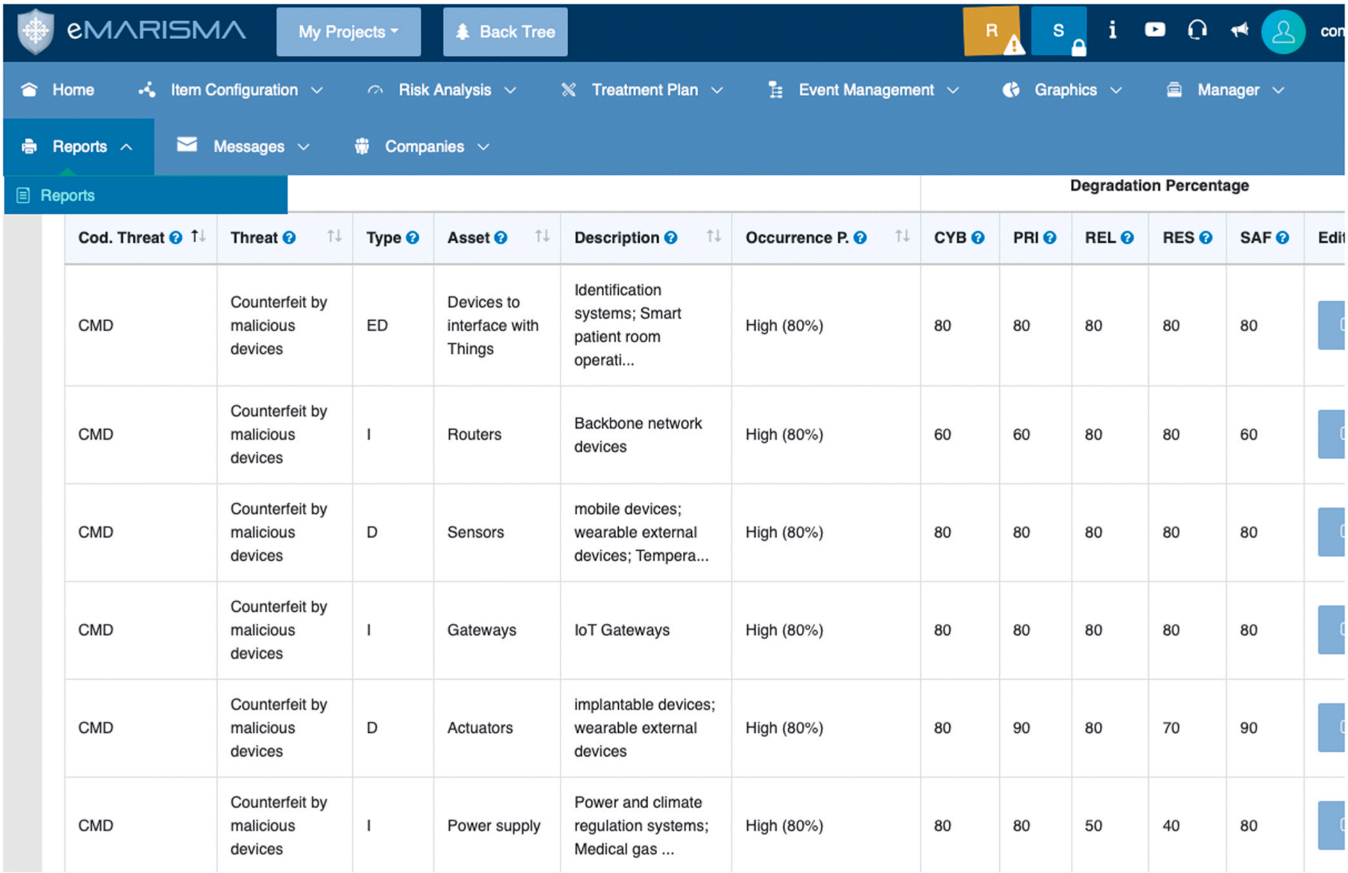
In order to continue with the risk analysis process, the set of threats that may affect the system under analysis must first be identified. Taking all the threats of the MARISMA-CPS pattern as the basis, those threats that will affect the system are identified, taking into account also the set of assets to be protected (see Table 11). As all the threats to CPS are already defined in the preloaded pattern of the eMARISMA tool, those threats that affect the case study are selected by indicating the values in the percentages of degradation of the value of the asset (the damage caused to the asset) and of the probability of occurrence (i.e., the probability that an attack will occur). These values range from 0 to 100, taken from 10 to 10 (see Fig. 5). The tool initially loads default values for degradation and occurrence rates, which are assigned values based on experience from previous analyses and from the tool's own learning. The eMARISMA tool facilitates the modification of the default values carried out by the security experts in RAM, who employ their judgement and knowledge about the possible threats that may affect the system, the damage they can cause and the likelihood of their occurrence. In order to eliminate threats that do not affect the system, a low value or even 0 % is, valid.

Taking as an example the case study of the threat of "tampering with medical devices" (see Table 11), (which belongs to the threat type "Counterfeit by malicious devices" and the threat family "Nefarious Activity/Abuse"), Fig. 5 shows that one can update the values



Cod. Type	Type	Cod. Threat	Threat	Probability Occurrence	Degradation Percentage
L	Legal	APD	Abuse of personal data	Medium (60.0%)	Very High (100.0%)
NAA	Nefarious Activity/ Abuse	AP	Attacks on privacy	Medium (60.0%)	Very High (100.0%)
EIH	Eavesdropping/ Interception/ Hijacking	CPH	Communication protocol hijacking	Low (40.0%)	Medium (60.0%)
NAA	Nefarious Activity/ Abuse	CMD	Counterfeit by malicious devices	High (80.0%)	High (80.0%)
DL	Damage loss (IT assets)	DSIL	Data / Sensitive information leakage	Low (40.0%)	High (80.0%)
NAA	Nefarious Activity/ Abuse	DD	DDoS	Medium (60.0%)	High (80.0%)
PA	Physical attack	DD	Device destruction (sabotage)	Low (40.0%)	High (80.0%)
PA	Physical attack	DM	Device modification	Low (40.0%)	High (80.0%)
D	Disaster	DN	Disaster natural	Very Low (20.0%)	Very High (100.0%)

Fig. 5. Occurrence and degradation for threats types with eMARISMA for the case study.



						Degradation Percentage					
Cod. Threat	Threat	Type	Asset	Description	Occurrence P.	CYB	PRI	REL	RES	SAF	Edi
CMD	Counterfeit by malicious devices	ED	Devices to interface with Things	Identification systems; Smart patient room operati...	High (80%)	80	80	80	80	80	
CMD	Counterfeit by malicious devices	I	Routers	Backbone network devices	High (80%)	60	60	80	80	60	
CMD	Counterfeit by malicious devices	D	Sensors	mobile devices; wearable external devices; Tempera...	High (80%)	80	80	80	80	80	
CMD	Counterfeit by malicious devices	I	Gateways	IoT Gateways	High (80%)	80	80	80	80	80	
CMD	Counterfeit by malicious devices	D	Actuators	implantable devices; wearable external devices	High (80%)	80	90	80	70	90	
CMD	Counterfeit by malicious devices	I	Power supply	Power and climate regulation systems; Medical gas ...	High (80%)	80	80	50	40	80	

Fig. 6. Degradation percentage x dimensions x assets x threats on the eMARISMA tool.

of occurrence probability and the degradation percentage up to 80 % based upon the expert's experience. Experts consider that the manipulation of medical devices can threaten both the safety of the patients (for example, a device implanted in a patient could be deactivated), their privacy, and the operation of the hospital in general, since the device could be modified to serve as a back door through which to carry out any other type of attack. These are, therefore, highly critical attacks and urgent attention must be paid to them. In this context, it is of the utmost importance to realise that medical devices have become a key pivot point for attacks in the healthcare context, as they are considered an easy and particularly vulnerable entry point. The indicated values of both probability and degradation are created for one particular type of threat, signifying that they will influence all the relationships with the asset types that are affected by that threat (as defined in Table 8).

5.4. Risk analysis for the case study

The next step in the risk analysis is to indicate the impact of the threats on each of the affected assets, taking into account the dimensions. This allows one to calculate the total damage or degradation caused to the asset when the threat attacks the system (calculated from the damage per dimension).

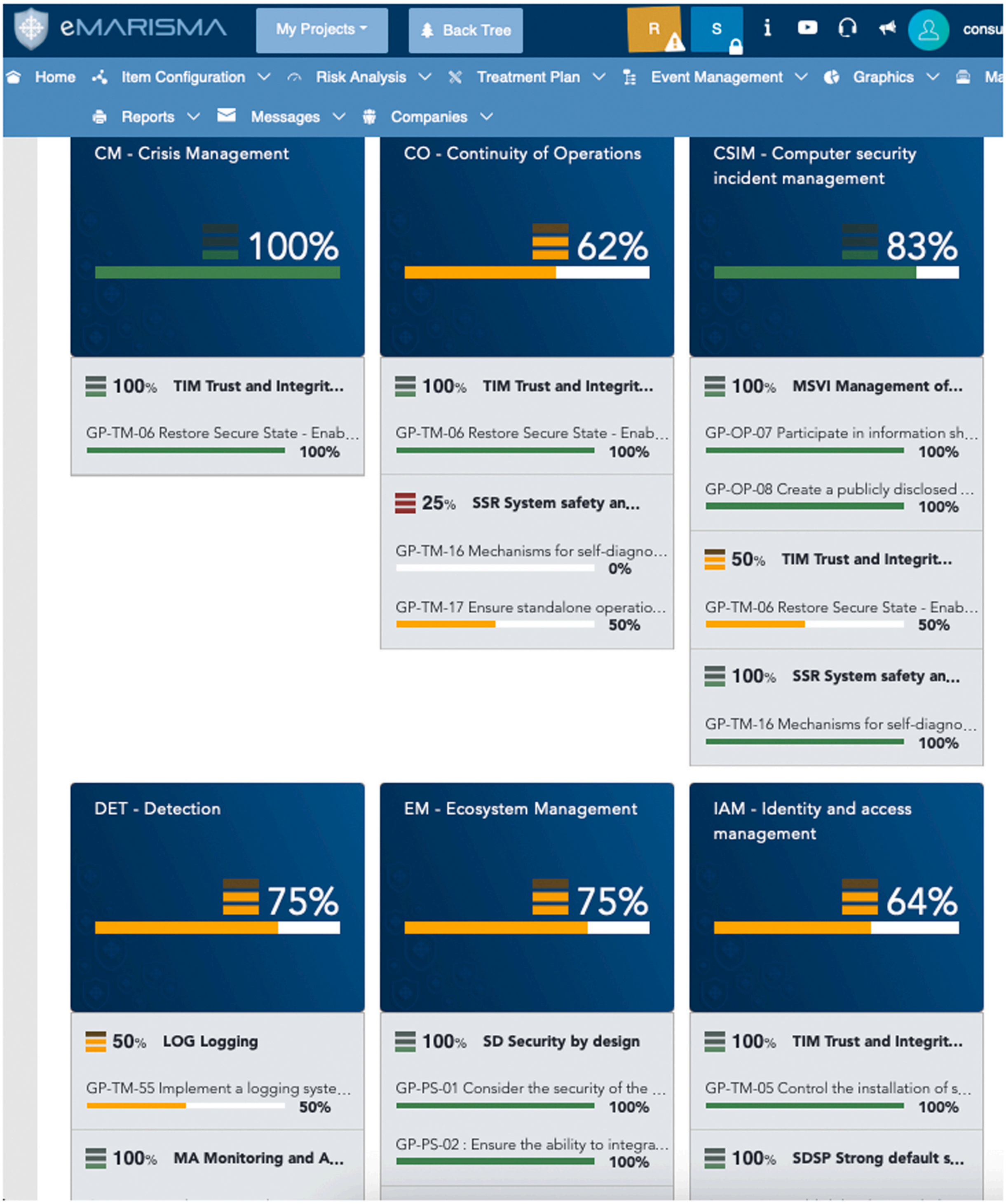
To this end, the tool displays the relationship established by the pattern among threats, assets and dimensions (as defined in Table 8) with the assigned values obtained in the previous step (see Fig. 6). The default values assigned to the dimensions are selected from the value defined in the degradation percentage from the previous step (see Fig. 5). These values can be the default values that the tool automatically assigns based on its knowledge and experience in previous projects, or the values that security experts have assigned on the basis of their own criteria. At this point, the experts can also use their judgement to modify the values at for each of the dimensions concerned.

Following on from the example in the previous section of the case study on the threat "medical device tampering" (which is of the threat type "counterfeit by malicious devices" and has a probability of occurrence of 80 % (as defined previously)), it can be seen how the percentage of degradation depends on the dimensions and on the type of asset - which for this type of threat involves the asset families "Devices", "Ecosystem devices", "Communications" and "Infrastructure".

The type of threat "counterfeit by malicious devices" was found to have a probability of degradation of 80 % affecting their five dimensions but, depending on the affected asset, these degradation values per dimension can however be changed. For example, for the asset type "Actuators", a 90 % degradation is considered for the dimensions "Privacy" and "Safety" due to the damage it may produce in the privacy of patients' devices and in patients' safety if the threat materialises. In that case, a higher percentage of degradation is then assigned.

5.5. Risk analysis: results

To conclude the risk analysis, an internal verification (using a security checklist) must be carried out to discover the real security level of our system. This verification is carried out based on the defined pattern, since the pattern has defined a set of domains, control objectives, and controls, which are the three levels into which the checklist is divided. This check is performed in order to discover the current security coverage, i.e., which controls are already implemented in the system or company, which still have to be



CM - Crisis Management 100%
100% TIM Trust and Integrit...
GP-TM-06 Restore Secure State - Enab... 100%

CO - Continuity of Operations 62%
100% TIM Trust and Integrit...
GP-TM-06 Restore Secure State - Enab... 100%
25% SSR System safety an...
GP-TM-16 Mechanisms for self-diagno... 0%
GP-TM-17 Ensure standalone operatio... 50%

CSIM - Computer security incident management 83%
100% MSVI Management of...
GP-OP-07 Participate in information sh... 100%
GP-OP-08 Create a publicly disclosed ... 100%
50% TIM Trust and Integrit...
GP-TM-06 Restore Secure State - Enab... 50%
100% SSR System safety an...
GP-TM-16 Mechanisms for self-diagno... 100%

DET - Detection 75%
50% LOG Logging
GP-TM-55 Implement a logging syste... 50%
100% MA Monitoring and A...

EM - Ecosystem Management 75%
100% SD Security by design
GP-PS-01 Consider the security of the ... 100%
GP-PS-02 : Ensure the ability to integra... 100%

IAM - Identity and access management 64%
100% TIM Trust and Integrit...
GP-TM-05 Control the installation of s... 100%
100% SDSP Strong default s...

Fig. 7. Dashboard shows levels of coverage of the controls for the case study.

implemented, those which can be applied, and those which should be discarded, and thus to learn what the current security level is in real time. The result of the checklist makes it possible to provide an overview of the security level of the system, identifying at a glance the main strengths and weaknesses, and so providing important tools for decision making. It also serves to identify, via recommendations, the controls to be implemented in order to improve security, protect the assets, and reduce the risk.

The tool provides a dashboard that shows the real-time coverage levels of the controls for all grouping levels (domains, objectives and controls) in real-time, allowing them to be tracked graphically and visually, as shown in Fig. 7. It also allows a visualisation of the current level by means of kiviat diagrams in three categories: (i) by overall audit (see top of Fig. 8); (ii) by domain (see foot of Fig. 8); and (iii) by control objectives. Once the risk has been calculated with all the elements added, the tool also displays a large amount of information in both text and visual form that allows the security expert to always know the level of risk to which the system under analysis is currently subjected. The tool, among many other possibilities, shows the level of risk per asset (see Fig. 9), the level of risk

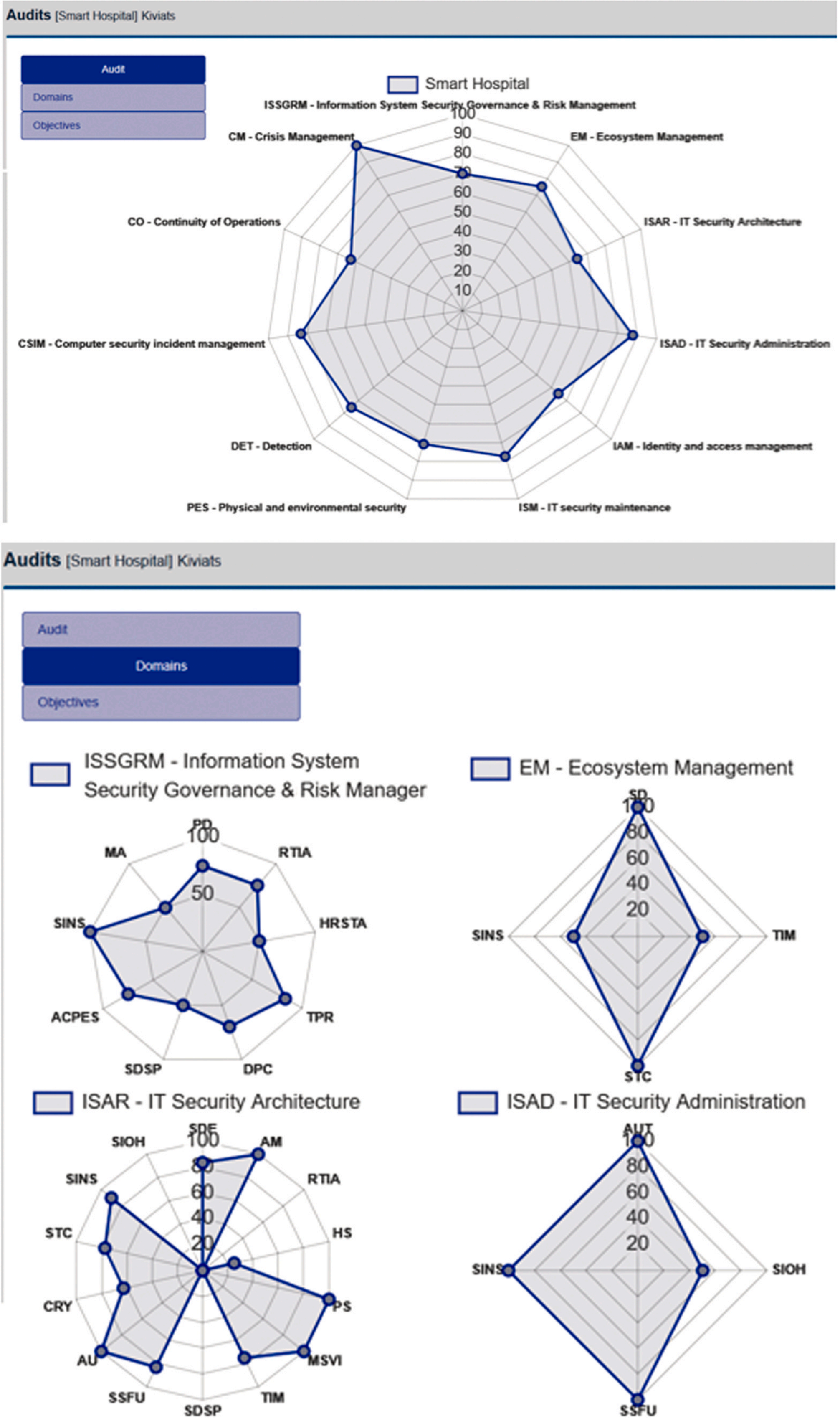

Audits [Smart Hospital] Kiviats
Audit
Domains
Objectives
Smart Hospital
ISSGRM - Information System Security Governance & Risk Management
EM - Ecosystem Management
ISAR - IT Security Architecture
ISAD - IT Security Administration
IAM - Identity and access management
ISM - IT security maintenance
PES - Physical and environmental security
DET - Detection
CSIM - Computer security incident management
CO - Continuity of Operations
CM - Crisis Management
100
90
80
70
60
50
40
30
20
10
Audits [Smart Hospital] Kiviats
Audit
Domains
Objectives
ISSGRM - Information System Security Governance & Risk Manager
PD
100
50
RTIA
HRSTA
TPR
DPC
SDSP
ACPES
SINS
MA
EM - Ecosystem Management
SD
100
80
60
40
20
TIM
STC
SINS
ISAR - IT Security Architecture
SDE
100
80
60
40
20
AM
RTIA
HS
PS
MSVI
TIM
SDSP
SSFU
AU
CRY
STC
SINS
SIOH
ISAD - IT Security Administration
AUT
100
80
60
40
20
SIOH
SSFU
SINS

Fig. 8. Levels of coverage with Kiviat diagrams for the case study.

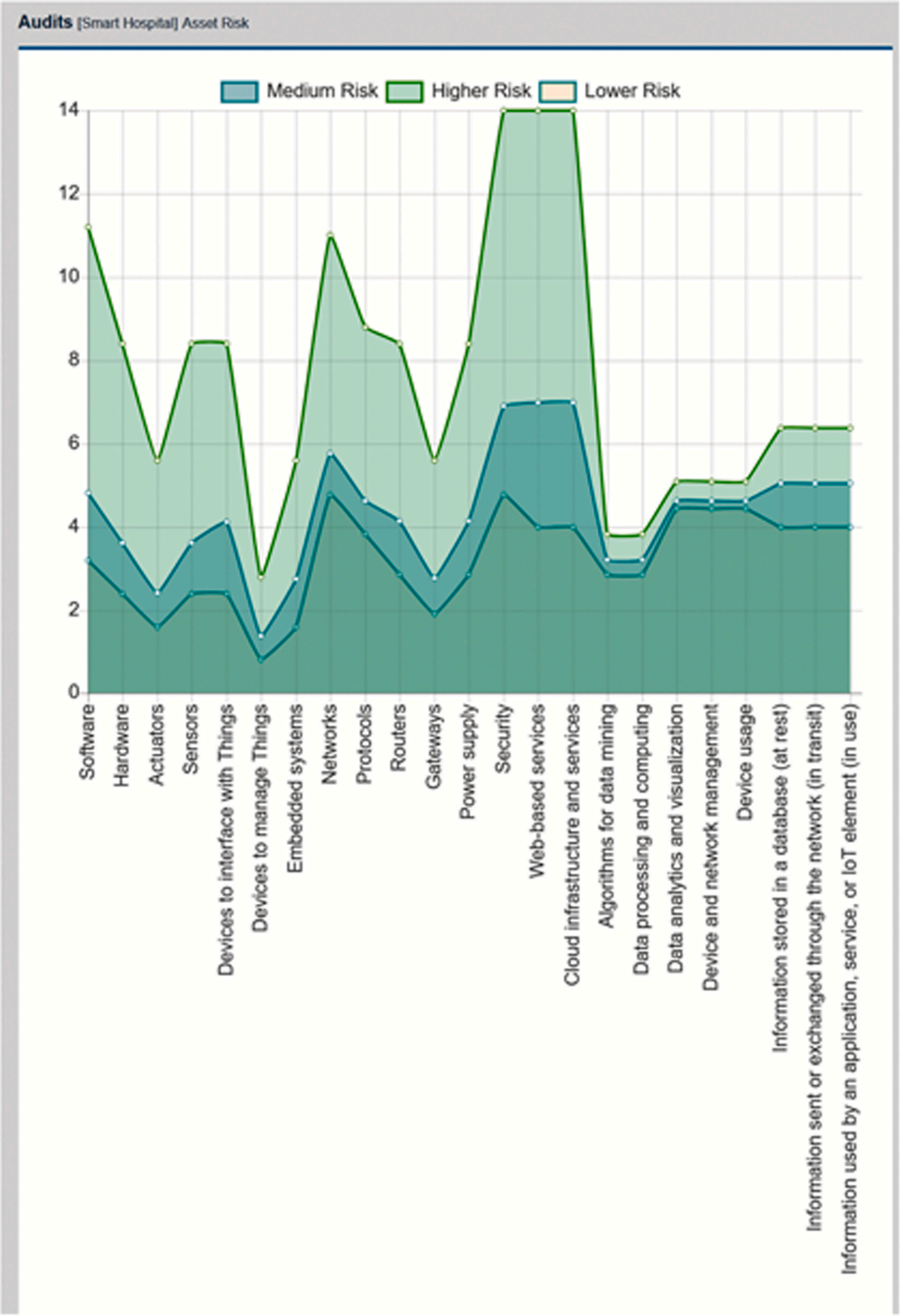


Fig. 9. Risk calculated per asset type using the MARISMA tool for the case study.

per threat (see Fig. 10), plus a lot of other information on the result of the risk analysis performed.

Thus, for example, for the domain “Computer Security incident management” there is a coverage of 83 %, which coincides with the average percentage of the control objectives defined for this domain, which are: ‘Management of security’ with a coverage of 100 %; ‘Trust and integrity management’ with a coverage of 50 %;, and ‘System safety and reliability’ with a coverage of 100 %. The results are

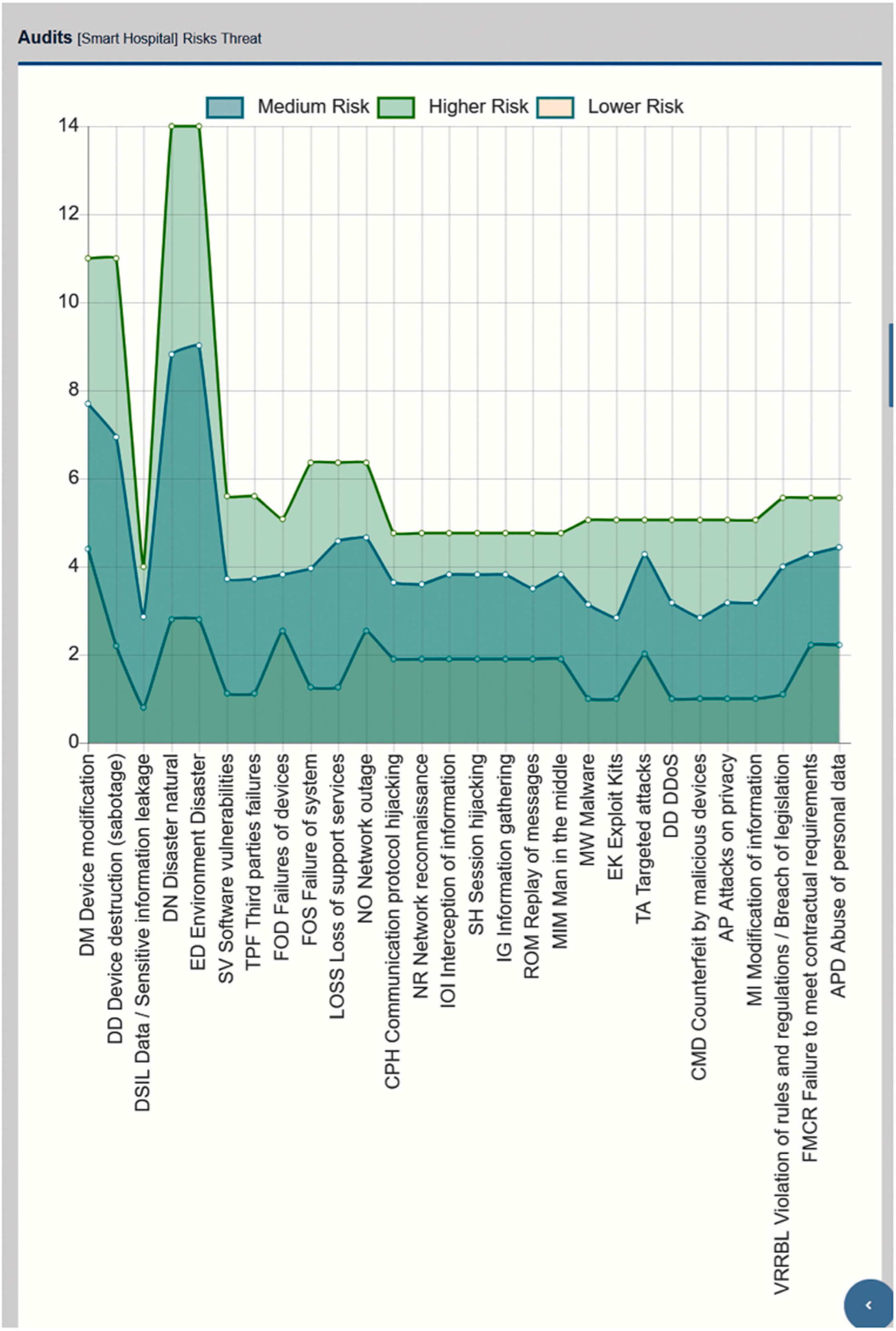

Audits [Smart Hospital] Risks Threat
Medium Risk
Higher Risk
Lower Risk
14
12
10
8
6
4
2
0
DM Device modification
DD Device destruction (sabotage)
DSIL Data / Sensitive information leakage
DN Disaster natural
ED Environment Disaster
SV Software vulnerabilities
TPF Third parties failures
FOD Failures of devices
FOS Failure of system
LOSS Loss of support services
NO Network outage
CPH Communication protocol hijacking
NR Network reconnaissance
IOI Interception of information
SH Session hijacking
IG Information gathering
ROM Replay of messages
MIM Man in the middle
MW Malware
EK Exploit Kits
TA Targeted attacks
DD DDoS
CMD Counterfeit by malicious devices
AP Attacks on privacy
MI Modification of information
VRRBL Violation of rules and regulations / Breach of legislation
FMCR Failure to meet contractual requirements
APD Abuse of personal data
‹

Fig. 10. Risk calculated per threat type using the MARISMA tool for the case study.

obtained by calculating the average value across all control coverage levels for each control target.

6. Conclusions and future work

The research carried out in this work has allowed us to develop a pattern totally oriented towards CPS, using as a basis to the meta-pattern of the MARISMA methodology. This pattern is made up of three taxonomic catalogues (controls, assets and threats) evolved from international standards and recommendations and oriented towards CPS. The dependency matrices between the elements of the pattern have also been obtained, which allows it to obtain the necessary properties for the reuse of knowledge and its subsequent adaptation over time. Its integration within the MARISMA framework, and the tool that supports it, has allowed its validation in practical cases.

Among the lessons learned, we can also highlight that the construction of the pattern and its subsequent validation has allowed us to see the possibility of defining patterns with a higher specialisation level, which would allow us to obtain more precise risk analyses, thereby investing fewer resources but obtaining a greater learning capacity as the knowledge acquired is more focused on a specific sector. To obtain these new patterns, the inheritance capabilities of the MARISMA meta-pattern can be used, as well as its capabilities for knowledge acquisition and reuse.

Consequently, our future work will be focused on the application of new real-life cases in more business domains, such as a smart cities or smart grids. With the experience of these new real-life cases, the MARISMA-CPS pattern will be further refined and validated, and thanks to the eMARISMA tool, the use of this pattern will help to automatically create sub-patterns. These new sub-patterns share the same structure as MARISMA-CPS pattern but are specialised in particular sectors that are closely related to CPS, such as those of health, manufacturing, energy, smart cities, etc. On a secondary level, and as a future work in the medium term, the aim is to develop a learning system in eMARISMA that one can learn from the security events or incidents that occur in an organisation so as to calibrate the pattern with more appropriate values and to improve the level of security in any future risk analyses that are carried out. Furthermore, the intention is to enable this knowledge to be extended to the rest of the systems that may be involved in the control of eMARISMA by using the same MARISMA-CPS pattern.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

Acknowledgements

This work has been developed within the AETHER-UCLM (PID2020-112540RB-C42) funded by MCIN/AEI/10.13039/501100011033, Spain, ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521) and ALBA-UC (TED2021-130355B-C33, id.3611130630-130630-28-521) funded by “Ministerio de Ciencia e Innovacion”, Spain, and supported by the European Union’s Horizon 2020 Project “CyberSANE” under Grant Agreement No. 833683.

Appendix A. Security controls for CPSs by ENISA

Tables A.1, A.2, A.3.

Table A.1
Description of policy-related security controls (Ross et al., 2017.

	Cod	Description of policy-related security controls
POLICY-RELATED CONTROLS	PS01	Consider the security of the whole IoT system from a consistent and holistic approach.
	PS02	Ensure the ability to integrate different security policies and techniques.
	PS03	Security must consider the risk posed to human safety.
	PS04	Designing for power conservation should not compromise security.
	PS05	Design architecture by compartments to encapsulate elements in case of attacks.
	PS06	It is necessary to implement test plans to verify whether the product performs as it is expected.
	PS07	it is important to conduct code review during implementation.
	PS08	Make privacy an integral part of the system.
	PS09	Perform privacy impact assessments before any new applications are launched.
	PS10	Establish and maintain asset management procedures and configuration controls.
	PS11	Identify significant risks using a defence-in-depth approach.
	PS12	Identify the intended use and environment of a given IoT device.

Table A.2
Description of organisational security controls (Ross et al., 2017).

	Cod	Description of organizational security controls
ORGANISATIONAL CONTROLS	OP01	Develop an end-of-life strategy for IoT products.
	OP02	Disclose the duration and end-of-life security and patch support.
	OP03	Monitor the performance and patch known vulnerabilities up until the “end-of-support”
	OP04	Use proven solutions,
	OP05	Establish procedures for analysing and handling security incidents.
	OP06	Coordinated disclosure of vulnerabilities.
	OP07	Participate in information-sharing platforms to report vulnerabilities.
	OP08	Create a publicly disclosed mechanism for vulnerability reports.
	OP09	Ensure the personnel practices promote privacy and security.
	OP10	Document and monitor the privacy and security training activities.
	OP11	Ensure that cybersecurity roles and responsibilities for all workforce are established.
	OP12	Data processed by a third-party must be protected by a data processing agreement.
	OP13	Only share consumers’ personal data with third parties with express consent of the consumers.
	OP14	Adopt cyber supply chain risk management policies.

Table A.3
Description of technical security controls (Ross et al., 2017).

	Cod	Description of technical security controls
THECNICAL CONTROLS	TM01	Employ a hardware-based immutable root of trust.
	TM02	Use hardware that incorporates security features.
	TM03	Trust must be established in the boot environment
	TM04	Sign code cryptographically to ensure it has not been tampered.
	TM05	Control the installation of software in operating systems.
	TM06	Enable a system to return to a state that was known to be secure.
	TM07	Use protocols and mechanisms able to manage trust.
	TM08	Any applicable security features should be enabled by default.
	TM09	Establish hard to crack, device-individual default passwords.
	TM10	Personal data must be collected and processed fairly and lawfully.
	TM11	Make sure that personal data is used for the specified purposes.
	TM12	Minimise the data collected and retained.
	TM13	IoT stakeholders must be compliant with the GDPR.
	TM14	Users must be able to exercise their rights.
	TM15	Design with system and operational disruption in mind.
	TM16	Mechanisms for self-diagnosis and self-repair/healing.
	TM17	Ensure standalone operation.
	TM18	Ensure that the device has the ability to update Over-The-Air (OTA).
	TM19	Offer an automatic firmware update mechanism.
	TM20	Backward compatibility of firmware updates.
	TM21	Design the authentication and authorisation schemes.
	TM22	Ensure that default passwords/usernames are changed.
	TM23	Authentication mechanisms must use strong passwords or PINs, 2FA.
	TM24	Authentication credentials shall be salted, hashed and/or encrypted.
	TM25	Protect against ‘brute force’ and/or other abusive login attempts.
	TM26	Ensure password recovery or reset mechanism is robust.
	TM27	Limit the actions allowed for a given system.
	TM28	Device firmware should be designed to isolate privileged code.
	TM29	Data integrity and confidentiality must be enforced.
	TM30	Ensure a context-based security and privacy reflecting different levels of importance.
	TM31	Measures for tamper protection and detection.
	TM32	Ensure that the device cannot be easily disassembled.
	TM33	Ensure that devices only feature the essential physical external ports.
	TM34	Ensure an effective use of cryptography to protect the CIA of data.
	TM35	Cryptographic keys must be securely managed.
	TM36	Build devices to be compatible with lightweight encryption and security techniques.
	TM37	Support scalable key management schemes.
	TM38	Guarantee the different security of the information.
	TM39	Ensure that communication security is provided.
	TM40	Ensure credentials are not exposed in internal or external network traffic.
	TM41	Guarantee data authenticity to enable reliable exchanges from data.
	TM42	Do not trust data received and always verify any interconnections.
	TM43	IoT devices should be restrictive rather than permissive in communicating.
	TM44	Make intentional connections.
	TM45	Disable specific ports and/or network connections for selective connectivity.
	TM46	Controlling the traffic sent or received by a network.
	TM47	Risk Segmentation. Splitting network elements into separate components.
	TM48	Protocols to ensure if a device is compromised, it does not affect the whole set.
	TM49	Avoid provisioning the same secret key in an entire product family.
	TM50	Ensure only necessary ports are exposed and available.
	TM51	Implement a DDoS-resistant and Load-Balancing infrastructure.
	TM52	Ensure web interfaces fully encrypt the user session.
	TM53	Avoid security issues when designing error messages.
	TM54	Data input validation and output filtering.
	TM55	Implement a logging system that records events.
	TM56	Implement regular monitoring to verify the device behaviour.
	TM57	Conduct periodic audits and reviews of security controls.

References

Abioye, T.E., Arogundade, O.T., Misra, S., Adesemowo, K., Damaševičius, R., 2021. Cloud-based business process security risk management: a systematic review, taxonomy, and future directions. Computers 10https://doi.org/10.3390/computers10120160. 〈https://www.mdpi.com/2073-431X/10/12/160〉.

AhsanulHaque, S., MahfuzulAziz, S., Rahman, M., 2014. Review of cyber-physical system in healthcare. Int. J. Distrib. Sens. Netw. 1–20 10.0.4.131/2014/217415.

Alguliyev, R., Imamverdiyev, Y., Sukhostat, L., 2018. Cyber-physical systems and their security issues. Comput. Ind. 100, 212–223. https://doi.org/10.1016/j.compind.2018.04.017

ENISA, 2016. Security and resilience for smart health service and infrastructures. Eur. Union Agency Netw. Inf. Secur. 〈https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals〉.

ISO/IEC TR 15443-1, 2012. Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts. URL: https://www.iso.org/standard/59138.html.

Brewer, T. ,2013. Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop, April 23–24, 2012.Technical Report National Institute of Standards and Technology Gaithersburg, MD.10.6028/NIST.IR.7916.

CCTA, U.K. ,2005. CCTA Risk Analysis and Management Method CRAMM.〈http://www.cramm.com〉.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27. https://doi.org/10.1016/j.cose.2015.09.009. arXiv:42.

Clark, R.M., Hakim, S., 2017. Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security (pp.). Cyber-Physical Security. Springer International Publishing, Cham, pp. 1–17. https://doi.org/10.1007/978-3-319-32824-9_1. (pp.).

Corallo, A., Lazoi, M., Lezzi, M., 2020. Cybersecurity in the context of industry 4.0: a structured classification of critical assets and business impacts. Comput. Ind. 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

Corallo, A., Lazoi, M., Lezzi, M., Pontrandolfo, P., 2021. Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level. IEEE Trans. Eng. Manag. 1–21. https://doi.org/10.1109/TEM.2021.3084687

De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., 2020. Cobit as a framework for enterprise governance of it. In: Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations. Springer International Publishing, Cham, pp. 125–162. https://doi.org/10.1007/978-3-030-25918-1_5. 978-3-030-25918-1.

Deloitte, 2017. Industry 4.0 and cybersecurity: Managing risk in an age of connected production. Deloitte Univ. Press 1, 1–22.〈https://www2.deloitte.com/us/en/insights/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html〉.

Aleksandrov, M.N., Vasiliev, V.A., Aleksandrova, S.V. ,2021. Implementation of the risk-based approach methodology in information security management systems.In 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT QM IS) (pp. 137–139).10.1109/ITQMIS53292.2021.9642767.

Ali, S., AlBalushi, T., Nadir, Z., Hussain, O.K., 2018. Risk management for cps security (pp.). Cyber Security for Cyber Physical Systems. Springer International Publishing,, Cham, pp. 11–33. https://doi.org/10.1007/978-3-319-75880-0_2. (pp.).

Ananda, T.K., Simran T G., Sukumara, T., Sasikala, D., Kumar P, R. ,2019. Robustness evaluation of cyber physical systems through network protocol fuzzing.In 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 1–6). 10.1109/ICACCE46606.2019.9079995.

Spanish Higher Council for Government, 2012. PAe - MAGERIT v.3: Methodology of analysis and risk management information systems. Ministry of Public Administration of Spain.〈https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YqjkzS0lPA4.〉.

Bhatti, B.M., Mubarak, S., Nagalingam, S., 2021. Information security risk management in it outsourcing – a quarter-century systematic literature review. J. Glob. Inf. Technol. Manag. 24, 259–298. https://doi.org/10.1080/1097198X.2021.1993725

Ross, R., 2018. Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. doi: https://doi.org/10.6028/NIST.SP.800-37r2.

Caralli, R., Stevens, J., Young, L.,Wilson, W. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.Technical Report CMU/SEI-2007-TR-012 Software Engineering Institute, Carnegie Mellon University Pittsburgh, PA.〈http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419〉.

Chong, M.S., Sandberg, H., and Teixeira, A.M. (2019). A tutorial introduction to security and privacy for cyber-physical systems.In 2019 18th European Control Conference (ECC) (pp. 968–978). 10.23919/ECC.2019.8795652.

CLUSIF, M., 2010. Processing guide for risk analysis and management. Club De La Securite De LInformation Francias, Second ed.

Das, S.K., Kant, K., Zhang, N., 2012. Securing Cyber-Physical Infrastructure: Perspectives and Overview of the Handbook. Handbook on Securing Cyber-Physical Critical Infrastructure. Elsevier, Boston. https://doi.org/10.1016/B978-0-12-415815-3.00053-4

DeSmit, Z., Elhabashy, A.E., Wells, L.J., Camelio, J.A., 2017. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. J. Manuf. Syst. 43, 339–351. https://doi.org/10.1016/j.jmsy.2017.03.004

Gelenbe, E., Gorbil, G.,Wu, F.-J. , 2012. Emergency cyber-physical-human systems. In Computer Communications and Networks (ICCCN), 2012 21st International Conference on (1–7). IEEE.10.1109/ICCCN.2012.6289183.

Griffor, E., Wollman, D.,Greer, C. , 2017. Framework for Cyber-Physical Systems: Volume 1, Overview.Technical Report June National Institute of Standards and Technology Gaithersburg, MD.10.6028/NIST.SP.1500–201.

Hessami, A.G., Jahankhani, H., Nkhoma, M. ,2015. Responsive Cyber-Physical Risk Management (RECYPHR).In International Conference on Global Security, Safety, and Sustainability 263–274). Springer.10.1007/978–3-319–23276-8_24.

Hofer, F., 2018. Architecture, technologies and challenges for cyber-physical systems in industry 4.0: A systematic mapping study.In Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement ESEM '18. New York, NY, USA: Association for Computing Machinery.10.1145/3239235.3239242.

Horowitz, B.M. and Pierce, K. , 2012. System Aware Cyber Security Application of Dynamic System Models and State Estimation Technology to the Cyber Security of Physical Systems Objectives for System Aware Cyber Security Research. In NIST (Ed.).Cybersecurity in Cyber-Physical Systems Workshop(96–97). NISTIR 7916.10.6028/NIST.IR.7916.

Jamshidi, A., Ait-kadi, D., Ruiz, A., Rebaiaia, M.L., 2018. Dynamic risk assessment of complex systems using fcm. Int. J. Prod. Res. 56, 1070–1088. https://doi.org/10.1080/00207543.2017.1370148

Ji, Z., Yang, S.-H., Cao, Y., Wang, Y., Zhou, C., Yue, L., Zhang, Y., 2021. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Saf. Environ. Prot. 148, 1279–1291. https://doi.org/10.1016/j.psep.2021.03.004

Jindal, A., Aujla, G.S., Kumar, N., Chaudhary, R., Obaidat, M.S., You, I., 2018. Sedative: Sdn-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems. IEEE Netw. 32, 66–73. https://doi.org/10.1109/MNET.2018.1800101

Khalid, A., Kirisci, P., Khan, Z.H., Ghrairi, Z., Thoben, K.-D., Pannek, J., 2018. Security framework for industrial collaborative robotic cyber-physical systems. Comput. Ind. 97, 132–145. https://doi.org/10.1016/j.compind.2018.02.009. 〈https://www.sciencedirect.com/science/article/pii/S016636151730088X〉.

Kozák, S., Ruzicky`, E., Kozáková, A., Stefanovic, J., Kozák, V. , 2019. Ict for advanced manufacturing.In ICEIS (2) pp. 682–688). 10.5220/0007768506820688.

Kumar, R., Narra, B., Kela, R., Singh, S., 2022. Afmt: Maintaining the safety-security of industrial control systems. Comput. Ind. 136, 103584. https://doi.org/10.1016/j.compind.2021.103584. 〈https://www.sciencedirect.com/science/article/pii/S0166361521001913〉.

Kure, H.I., Islam, S., Razzaque, M.A., 2018. An integrated cyber security risk management approach for a cyber-physical system. Appl. Sci. 8https://doi.org/10.3390/app8060898. 〈https://www.mdpi.com/2076-3417/8/6/898〉.

Lamba, V., Šimková, N., Rossi, B., 2019. Recommendations for smart grid security risk management. Cyber-Phys. Syst. 5, 92–118. https://doi.org/10.1080/23335777.2019.1600035

Lee, J., Bagheri, B., Kao, H.A., 2015. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. Manuf. Lett. 3, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

Leite, F.L., Schneider, D., Adler, R., 2018. Dynamic Risk Management for Cooperative Autonomous Medical Cyber-physical Systems (pp.) In: Gallina, B., Skavhaug, A., Schoitsch, E., Bitsch, F. (Eds.), Computer Safety, Reliability, and Security. Springer International Publishing, Cham, pp. 126–138. https://doi.org/10.1007/978-3-319-99229-7_12. (pp.).

Lezzi, M., Lazoi, M., Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: a reference framework. Comput. Ind. 103, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Lu, Y., Xu, L.D., 2019. Internet of things (IoT) cybersecurity research: a review of current research topics. IEEE Internet Things J. 6, 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847

Lund, M.S., Solhaug, B., Stølen, K., 2011. Model-Driven Risk Analysis. Springer Berlin Heidelberghttps://doi.org/10.1007/978-3-642-12323-8

Mahoney, T.and Davis, J. ,2017. Cybersecurity for Manufacturers: Securing the Digitized and Connected Factory In MFORESIGHT, Michigan, United States of America.volume MF-TR-2017.〈http://mforesight.org/〉.

Malik, V., Singh, S., 2019. Security risk management in iot environment. J. Discret. Math. Sci. Cryptogr. 22, 697–709. https://doi.org/10.1080/09720529.2019.1642628

Marinos, L. , 2016. ENISA threat taxonomy: A tool for structuring threat information. Initial report.Technical Report January European Union Agency For Network And Information Security.〈https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view〉.

Mokalled, H., Pragliola, C., Debertol, D., Meda, E., Zunino, R., 2019. A comprehensive framework for the security risk management of cyber-physical systems (pp.) In: Flammini, F. (Ed.), Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction. Springer International Publishing, Cham, pp. 49–68. https://doi.org/10.1007/978-3-319-95597-1_3. (pp.).

Orojloo, H., Azgomi, M.A., 2017. A game-theoretic approach to model and quantify the security of cyber-physical systems. Comput. Ind. 88, 44–57. https://doi.org/10.1016/j.compind.2017.03.007. 〈https://www.sciencedirect.com/science/article/pii/S0166361516302731〉.

Osman, N.F.M., Elamin, A.A.A., Ahmed, E.S.A., Saeed, R.A., 2021. Cyber-physical system for smart grid.In Artificial Intelligence Paradigms for Smart Cyber-Physical Systems (301–323). IGI Global.10.4018/978–1-7998–5101-1.ch014.

Priyadarshini, I., Kumar, R., Tuan, L.M., Son, L.H., Long, H.V., Sharma, R., Rai, S., 2021. A new enhanced cyber security framework for medical cyber physical systems. SICS Softw. Intensive Cyber-Phys. Syst. 35, 159–183. https://doi.org/10.1007/s00450-021-00427-3

Rosado, D.G., Moreno, J., Sánchez, L.E., Santos-Olmo, A., Serrano, M.A., Fernández-Medina, E., 2021. Marisma-bida pattern: integrated risk analysis for big data. Comput. Secur. 102, 102155. https://doi.org/10.1016/j.cose.2020.102155

Ross, M., Jara, A.J., and Cosenza, A. (2017). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.Technical Report November European Union Agency For Network And Information Security.10.2824/03228.

Sanchez, L.E., Parra, A.S., Rosado, D.G., Piattini, M., 2009. Managing security and its maturity in small and medium-sized enterprises. J. Univers. Comput. Sci. 15, 3038–3058. https://doi.org/10.3217/jucs-015-15-3038

Santos-Olmo, A., Sánchez, L., Rosado, D., Fernández-Medina, E., Piattini, M., 2016. Applying the action-research method to develop a methodology to reduce the installation and maintenance times of information security management systems. Future Internet 8, 36. https://doi.org/10.3390/fi8030036

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., 2021. Risk assessment for iot-enabled cyber-physical systems (pp.) In: Tsihrintzis, G.A., Virvou, M. (Eds.), Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris. Springer International Publishing, Cham, pp. 157–173. https://doi.org/10.1007/978-3-030-41196-1_8. (pp.).

Tantawy, A., Abdelwahed, S., Erradi, A., Shaban, K., 2020. Model-based risk assessment for cyber physical systems security. Comput. Secur. 96, 101864. https://doi.org/10.1016/j.cose.2020.101864. ⟨https://www.sciencedirect.com/science/article/pii/S016740482030136X⟩.

Taylor, J.M.and Sharif, H.R. , 2017. Security challenges and methods for protecting critical infrastructure cyber-physical systems.In 2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT) (pp. 1–6). 10.1109/MoWNet.2017.8045959.

Wang, L., Törngren, M., Onori, M., 2015. Current status and advancement of cyber-physical systems in manufacturing. J. Manuf. Syst. 37, 517–5027. https://doi.org/10.1016/j.jmsy.2015.04.008

Wu, W., Kang, R., Li, Z. ,2015. Risk assessment method for cyber security of cyber physical systems.In Proceedings of 2015 the 1st International Conference on Reliability Systems Engineering, ICRSE 2015. (1–5). IEEE.10.1109/ICRSE.2015.7366430.

Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., Chen, S., Zhao, K., 2015. Cyber-physical-social system in intelligent transportation. IEEE/CAA J. Autom. Sin. 2, 320–333. https://doi.org/10.1109/JAS.2015.7152667

Ying, Z., Li, Q., Meng, S., Ni, Z., Sun, Z., 2020. A survey of information intelligent system security risk assessment models, standards and methods (pp.) In: Zhang, X., Liu, G., Qiu, M., Xiang, W., Huang, T. (Eds.), Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications. Springer International Publishing, Cham, pp. 603–611. https://doi.org/10.1007/978-3-030-48513-9_48. (pp.).

Zahid, M., Inayat, I., Daneva, M., Mehmood, Z., 2020. A security risk mitigation framework for cyber physical systems. J. Softw. Evol. Process 32, e2219. https://doi.org/10.1109/ICPS49255.2021.9468202

Zahid, M., Inayat, I., Daneva, M., Mehmood, Z., 2021. Security risks in cyber physical systems—a systematic mapping study. J. Softw. Evol. Process, e2346. https://doi.org/10.1002/smr.2346

Zeadally, S., Sanislav, T., Mois, G.D., 2019. Self-adaptation techniques in cyber-physical systems (cpss). IEEE Access 171126–171139. https://doi.org/10.1109/ACCESS.2019.2956124

ISO/IEC 21827, 2008. Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®). International Organization for Standardization ISO. ISO/IEC, pp. 132.https://www.iso.org/standard/44716.html.

ISO/IEC 27005, 2018. Information technology – Security techniques – Information security risk management. Iso/Iec. pp. 80. 9780626231675. http://link.springer.com/chapter/10.1007/978-3-8348-9870-8_3.