GUIDE ON SECURITY CONTROLS IN OT SYSTEMS

MINISTRY OF INTERIOR

SECRETARIAT OF STATE FOR SECURITY

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

In July 2020, the collaboration of public bodies, private companies and the academic sector was requested in order to identify the security shortcomings in the operating systems, as well as to define the compensatory measures that could remedy these shortcomings.

Specifically, the entities that have collaborated with their responses are the following:

ASSOCIATIONS/FOUNDATIONS	CCI
	Borredá Foundation
	El Cano High School
	ISACA
CONSULTING	Deloitte
	EY
	GMV
	SIA-INDRA Group
	Ecix
	Capgemini
COMPANIES	Enigmedia
	Aiuken Solutions
	NextVision
	Agbar
	Ingenia
	Entelgy Innotec Security
MANUFACTURERS	Check Point Software Technologies
	Tecnalia/PESI
	Siemens
UNIVERSITIES	Comillas Pontifical University
	University of Malaga
COORDINATION	ISMS Forum
	Cybersecurity Coordination Office

CONTENTS

1. INTRODUCTION AND CURRENT CONTEXT

1.1 Introduction.

Undoubtedly, information and communication technologies (ICTs) today support the vast majority of services provided worldwide. There are still very few essential human services that do not depend on information technologies for their proper functioning.

This is taking place at a high rate of change and is a consequence of the quest for efficiency in all sectors. In recent years, these processes of change have been driven by digital transformation programs, in which practically every institution is immersed. The current scenario will make this dependence on IT even greater in the future.

The digitization of industrial processes brings with it great opportunities, some of which are perhaps much needed for mankind. Technologies and the digitization of industrial sectors will certainly help, among other things, to reduce CO2 emissions.

In addition to the opportunities offered by available technologies such as *cloud*, *big data*, *machine learning*, *artificial intelligence*, *IoT*, *5G*, etc., there are also the threats to which these technologies are subject.

Until recently, there was a false sense of security in the industrial environment due to the belief that there was no risk. This feeling was mainly based on five preconceived notions:

- The plant is isolated, not connected to the internet.
- We have a *firewall* to protect us.
- Hackers do not know about industrial systems/processes.
- My plant is nobody's target.
- Plant *safety* systems protect us from cyber-attacks.

The risk to be managed is associated with the likelihood that our assets will suffer unavailability or loss of integrity to provide service or damage (impact).

Visibility or surface exposure, which in industrial environment networks, hereinafter ***OT (Operation Technology)***, has increased in recent years and therefore increases the probability of a cyber-security incident.

Today, *OT* systems suffer from the same traditional ills as ***IT (Information Technology)*** systems due to the convergence and connectivity we are experiencing.

The consequences of a converging world, where the need to keep everything connected is growing, mean that historically isolated industrial networks are beginning to need to be connected, using protocols such as *TCP/IP*, *which are* insecure in their definition, encapsulating traditional proprietary protocol packages, such as *MODBUS*.

Even if an organization chooses to keep the *OT* system disconnected from its corporate networks or the internet, the devices used to configure and maintain these are laptops, *pen drives*, tablets and *smartphones* that have had previous contact with the internet, and with *Microsoft Windows* operating systems, so there is still a risk if security policies are not applied.

Industrial automation and control systems or ***ICS (Industrial Control Systems)***, and ***SCADA (Supervisor Control and Data Acquisition)*** systems, the latter being widely known in the sector, were isolated from the public internet network, even from the organization's private *LAN*. They had their own *OT* networks, but, little by little, their proprietary and closed protocols converged towards open network protocols, sometimes seeking to reduce costs in programming and management, which is decided to be done remotely by taking advantage of the existing *IT* infrastructure.

It is no secret that there are industrial installations, currently supported by operating systems or *hardware*, whose manufacturers stopped providing support several years ago or whose incorporation of cybersecurity profiles and, therefore, cybersecurity culture in industrial environments, is still incipient.

Whether or not we are aware of what the previous paragraph implies, the problem introduced is bigger than it seems, because we are bringing together two environments, *IT* and *OT*, with **specific knowledge needs and different life cycles**, which will complicate the establishment of **priorities** when it comes to reducing the risk of cyber-attack in the organization.

It should also be borne in mind that a cybersecurity incident in an industrial environment can have **an impact beyond the digital world**, where a traditional *IT* cyber-attack can diminish the value of the organization, damage its brand image, etc. An industrial environment is capable of automatically setting in motion actuators and mechanisms that **modify our physical world** and can provoke:

- Environmental damage.
- Impact on public health and human lives.
- Interruption of essential services for citizens.

We are therefore facing major challenges due to convergence, the adoption of *IT* in *TOs*, and the strong demand for connectivity, where traditional weaknesses in *IT* systems have come to light, now in critical facilities, and sometimes without taking into account that:

- In many cases, the staff or third parties who use these technologies are not **properly trained**.
- As a result, **the risks** involved in using certain *IT* technologies in *OT* environments are **not known**, and control measures are not applied.
- It is also the case that *IT*, *OT* and cyber security staff do not combine their efforts and knowledge to implement security measures and controls.

The most notorious case has undoubtedly been ***Stuxnet***, but more and more critical infrastructures are suffering from intrusion: power plants, gas plants, metallurgical plants, isolated *PLCs* on the internet and a long etcetera. A search on **shodan.io** or a visit to its dedicated *ICS* section is enough to see the number of devices connected to the internet without any kind of backup. Likewise, a consultation of the *MITREATT&CK for ICS1* allows us to assess the number of threats to which these systems are exposed.

Industrial automation is not new, *ICSs* have been around for a long time and work well, but integration with *TCP/IP* networks has brought them into the spotlight, and they can no longer be considered isolated environments. Criminal Organizations or

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

State-sponsored groups have the capabilities and knowledge to gain access to the controls of an industrial system/facility via specialized *malware* and other techniques.

Therefore, those who have the responsibility to provide essential services, to maintain sustainable businesses, to ensure the successful development of national R&D, or who have the responsibility to ensure the security of citizens, have the great challenge to do so by accompanying businesses in a way that is competitive, but under known, accepted and manageable levels of risk.

Fortunately, the concern is there, and to a greater or lesser extent, all *stakeholders* (industrial companies, service providers, universities, regulators, associations) have plans to address these new challenges.

1.2 *Safety & Security.*

Undoubtedly, those who have designed or are designing industrial installations have always taken *safety* aspects into account, but perhaps in the past they did not take *security* aspects into account, especially *cybersecurity*. The Spanish language does not distinguish between the meanings of the words *SAFETY* and *SECURITY*. But these words do have different concepts. In a very summarized form it could be said:

"***Safety***" is usually applied to protection against more or less fortuitous risks, such as accidental, natural disasters, etc.

"***Security***" is often applied to security against acts of an intentional nature (theft, intrusion, vandalism, aggression, etc.). *Cybersecurity* is part of this concept, but is confined to the context of information and systems security.

It should be noted that cyber security in the *OT* world cannot be based on the same criteria and approaches as in the *IT* world. To sum it up, one could say that in the *IT* world cyber security is managed with ***information centric***, whereas in the *OT* world cyber security should be focused on ***process centric***. In this way, a better understanding between plant engineers and cyber security experts is achieved, which is a fundamental issue in projects to improve industrial cyber security.

1.3 Operation Technology Networks (*OT) and* Industrial Control Systems (*ICS*).

The *ICS* are based on 3 stages:

- Measurement of process data (monitoring).
- Evaluation of the information obtained in terms of standard parameters.
- Process control based on the information measured and evaluated.

These control systems can be fully manual, fully automated, or both (hybrids).

The systems known as *SCADA* allow information from multiple points in a process to be evaluated from a console and control decisions to be made.

This leads to the need to describe what are the usual components of an *OT* network:

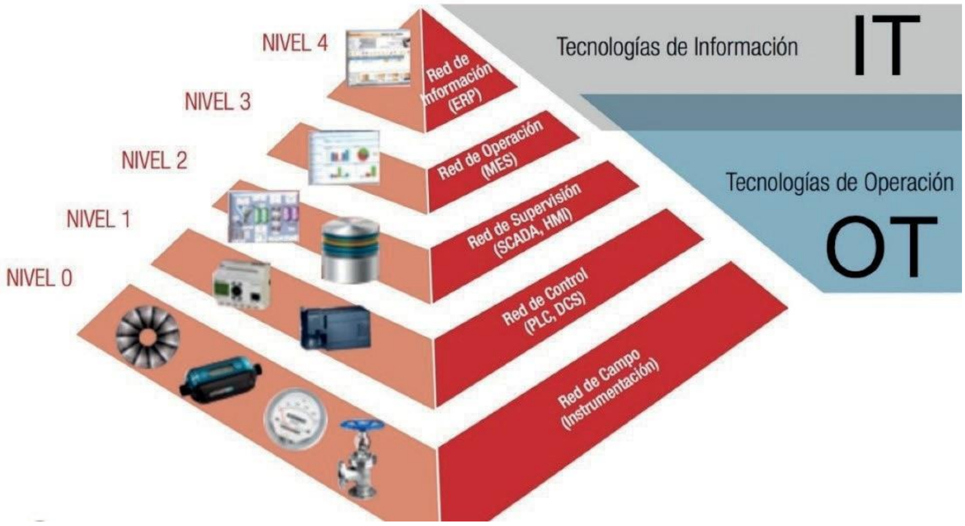

NIVEL 4
NIVEL 3
NIVEL 2
NIVEL 1
NIVEL 0
Red de Información (ERP)
Red de Operación (MES)
Red de Supervisión (SCADA, HMI)
Red de Control (PLC, DCS)
Red de Campo (Instrumentación)
Tecnologías de Información
IT
Tecnologías de Operación
OT

Illustration1 https://www.cci-es.org/Guia_Piramide

Lower layer (0). Sensor and Actuator Layer, it would be like the physical layer, where what matters is the medium or field devices and signals are transmitted, which can be either analogue or digital, with the particularities that this implies.

This would include, for example, motion sensors, temperature sensors, level sensors, magnetic sensors, actuators, etc.

Layer (1). Can be found:

- ***PLC*** (*Programmable Logic Controller)*, a device that allows the automation of an electromechanical process, controlling the operation of the machines used in production.

- ***RTU*** (*Remote Terminal Unit*) a microprocessor capable of acquiring field signals and acting accordingly based on existing programming.

- ***DCS***[2] (*Distributed Control System*), communicates with field devices and feeds data to an ***HMI*** (*Human-Machine Interface*), obtaining information from *PLCs* or *RTUs*.

Layer (2). ***HMI/SCADA*** level, which collects all the information from the *PLCs* and/or *RTUs* distributed automatically, and we start to encounter a well-known protocol: *TCP/IP*. This is the interface used, for example, by plant operators.

Layer (3). Level of the ***MES*** (*Manufacturing Execution System*) whose objective is not the evaluation of the process itself, but of its efficiency based on the information received.

Layer (4). This would include ***ERP*** (*Enterprise Resource Planning*), where it is basically decided what kind of controls will be executed, how often and with what effort, in order to have a coherent planning.

[2] The terms and concepts of DCS and SCADA are very similar to each other, and are sometimes used interchangeably, depending on the sector.

1.4 Supply chain security.

OT infrastructures are closely linked to very specific services and technologies, which need to be provided by specialists, most of which are third parties and often require a significant level of interconnection with them. Likewise, many of the organizations that provide this type of services and that come from the industrial sector do not have a culture of cybersecurity, nor in many cases do they have areas with expertise in this area. This implies that the client's systems are accessed by external personnel, experts in the services they provide, but belonging to organizations where security is much less developed than in those coming from the *IT* field. This can result in insecure practices that put at risk the *OT* infrastructure, which is already more vulnerable due to the points discussed above.

An infinite number of risks can materialize through suppliers, some of the most notable being the exploitation of vulnerabilities in *OT* systems when exposed to suppliers' equipment or networks, the infection of *malware* existing in the supplier's equipment or networks, the exfiltration of information, as there is, in general, little control over the data and traffic exchanged, the unavailability of systems due to supplier actions, which could have a huge impact due to the frequent absence of backup copies in these environments, etc. In general, the same risks as in the *IT* environment, but aggravated by the very nature of the *OT* environments discussed above.

1.5 *IoT* & Privacy.

It is worth noting that many *OT* networks are currently managing industrial processes, but the digitization processes of industry, with the incursion of *IoT* solutions in industrial environments, make it necessary to take into account aspects related to privacy, the scope of which is strongly regulated by *GDPR.*

In this new scenario of industrial environments based on the interconnection of multiple intelligent devices that automate processes and generate large amounts of information, new opportunities arise that require a revision of the concept of privacy traditionally held in industrial environments.

The collection of personal data from users is inherent to the operation of these devices, irrespective of the level of awareness of the employer, technical professionals and user as to the personal information they are disclosing with the use of this new digital paradigm embedded in industrial environments.

All of the above means that those involved in this type of project must carry out a detailed analysis of the different risks and threats to be taken into account in their operating systems, and of the different processing of personal data that may be carried out with the data stored.

Therefore, privacy-oriented controls will have to be considered in industrial environments, where the application of the guiding principles of data protection law applicable in Europe, such as privacy by default and by design (*PbD*), is the best evidence to demonstrate due diligence in the exercise of the "proactive responsibility" required therein.

By including the concepts of *PbD*, privacy principles are incorporated into the design, operation and management processes of an organization’s systems to achieve a comprehensive data protection framework.

In the course of the guide, specific controls to ensure the privacy of personal data that may be stored and processed in industrial environments will be discussed.

2. REGULATORY FRAMEWORK

The National Cybersecurity Strategy.

Order PCI/487/2019 of 26 April 2019 is the regulation through which the National Cybersecurity Strategy (hereinafter ENCS) is published.

The ENCS is the reference framework for an integrated model whose bases are the involvement, coordination and harmonization of all state actors and resources, public-private collaboration, and citizen participation.

In order to achieve its objectives, the Strategy creates an organizational structure, integrated into the framework of the National Security System, which should serve to articulate the State's single action in accordance with principles shared by the actors in an appropriate institutional framework.

The objectives for cybersecurity, under the principles of unity of action, anticipation, effectiveness and resilience that govern the Strategy, dedicate a specific objective (Objective I) to the "Security and resilience of public sector information and communications networks and systems and essential services".

This objective highlights the need for these operators to actively engage in a process of continuous improvement with respect to the protection of their systems, and to become a model of good practice in cybersecurity management.

In addition, the principle of shared responsibility is included, whereby the public sector should maintain close relations with strategic companies and exchange knowledge to ensure proper coordination and cooperation in the cybersecurity environment.

Finally, the Strategy develops the strategic and institutional framework composed of the reference *CSIRTs* or incident response teams that analyse risks and, as a gateway, monitor incidents, disseminate alerts and provide solutions to mitigate their effects, sending the appropriate notifications to the competent Authorities.

Critical Infrastructure Protection Act (CIPPA)

Law 8/2011 of 28 April 2011 establishing measures for the protection of critical infrastructure ("CIP Law") transposes Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

Critical infrastructure means an element, system or part thereof whose functioning is essential for the maintenance of vital societal functions, health, safety, security, social and economic well-being, and whose disruption or destruction would have serious consequences.

The Law conceives security in the service of the citizen and the State, establishing objectives and lines of action for the protection of critical infrastructures, and aims to "establish the appropriate strategies and structures to direct and coordinate the actions of the different bodies of the Public Administrations in the protection of critical infrastructures, after identifying and designating them, to improve the prevention, preparation and response of our State to terrorist attacks or other attacks".

threats affecting critical infrastructures. To this end, the collaboration and involvement of the managing bodies and owners of these infrastructures will also be promoted, in order to optimize the degree of protection of these infrastructures against deliberate attacks of all kinds, with the aim of contributing to the protection of the population".

Derived from the Law and its implementing Regulation, the National Critical Infrastructure Protection System (PIC System) was set up in 2012, which consists of a set of public and private sector agents with competences and responsibilities in this area.

The PIC Law also provides for the creation of the National Catalogue of Strategic Infrastructures as an instrument with all the information and assessment of strategic infrastructures, and creates the National Centre for Critical Infrastructure Protection (CNPIC), which is the body responsible for the promotion, coordination and supervision of the activities entrusted to the Ministry of Interior in relation to the protection of critical infrastructures in Spain.

Finally, the PIC Act gives rise to the National Critical Infrastructure Protection Plan, with the aim of directing and coordinating actions to protect critical infrastructures, and the Strategic Sector Plans, which set out the criteria defining the measures to be adopted to deal with a risk situation based on the specific characteristics of each of the sectors.

Critical Infrastructure Protection Regulation

The CIP Law is implemented through Royal Decree 704/2011, of 20 May, which approves the Regulation on the protection of critical infrastructures.

Its purpose is to develop, specify and extend the aspects contemplated in the aforementioned Law, taking into account the necessary articulation of the bodies and entities, both from the Public Administrations and the private sector, as well as the design of planning aimed at the prevention and protection of critical infrastructures against threats or terrorist acts that may eventually use information and communications technologies as a channel.

The Regulation requires critical infrastructure operators to appoint a Security and Liaison Officer and a Security Delegate for each of the critical infrastructures identified, who will have the powers set out in the Regulation itself.

The Regulation contemplates the Operator's Security Plans as strategic documents defining the policies to guarantee the security of all the facilities or systems owned or managed by the Operator. Specific Protection Plans are also envisaged, as operational documents defining the measures adopted and those to be adopted by operators to guarantee the comprehensive security, whether physical or logical, of the infrastructures they own or manage.

Articles 23 and 26 (Approval, registration and classification) provide for the approval of Operator Security Plans and Specific Protection Plans or proposals for their improvement, for which the development of an accreditation scheme is promoted, which may be based on an international standard (*NIST*, *ISO/IEC*) or on a specific regulation (in the case of Spain, the National Security Scheme approved by Royal Decree 3/2010 of 8 January).

National Security Scheme

Royal Decree 3/2010 of 8 January 2010 regulates the National Security Scheme for e-Government (hereinafter ENS).

The purpose of the ENS is to "establish the security policy for the use of electronic media within the scope of this Law, and is made up of the basic principles and minimum requirements that adequately guarantee the security of the information processed".

The scope of application of the ENS is the Public Sector, which is made up of the institutions whose functioning is governed by articles 2 of laws 39/2015 and 40/2015, respectively, and what is indicated on the institutional public sector.

The main mandate of the ENS is set out in Article 11, according to which "all senior public administration bodies shall formally have a security policy that articulates the ongoing management of security, which shall be approved by the head of the corresponding senior body". This security policy shall be established on the basis of basic principles and shall be developed by applying the minimum requirements set out in the Scheme itself.

Since its approval, the ENS has been first modified by Royal Decree 951/2015, in order to update it to new technological needs, as well as to the international and European regulatory context.

Subsequently, by the Resolution of 13 October 2016, of the Secretary of State for Public Administrations, approving the Technical Security Instruction on compliance with the National Security Scheme, which in section VII (Solutions and services provided by the private sector) states: "When private sector operators provide services or solutions to public entities, which are required to comply with the National Security Scheme, they must be able to display the corresponding Declaration of Conformity with the National Security Scheme, in the case of BASIC category systems, or the Certification of Conformity with the National Security Scheme, in the case of MEDIUM or HIGH category systems, using the same procedures as those required in this Technical Security Instruction for public entities.”.

This last normative reference is aligned with the provisions of the first Additional Provision of the Organic Law on Data Protection and Guarantee of Digital Rights, Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights.

Network and Information Systems Security Act (NISSA)

Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems transposed into Spanish Law European Directive 2016/1148 (known as the *NIS* Directive) on measures to ensure a high common level of security of networks and information systems in the European Union.

The Royal Decree-Law aims to regulate the security of networks and information systems used for the provision of essential services and digital services, and to establish an incident notification system in our country.

It also determines the form and criteria for the identification of essential services and the operators providing them. It also lays down the strategic and institutional framework for the

The aim of the project is to develop a national strategy for the security of networks and information systems in Spain, with an emphasis on cooperation between public authorities.

It also provides for the inspection and control powers of the competent authorities and cooperation with the national authorities of other Member States, sets out a series of infringements and penalties, and lays down the safety obligations of operators.

Finally, it regulates the reporting of incidents, with special attention to incidents with cross-border impact and to information and coordination with other EU states for suggestion.

Development of the Network and Information Systems Security Law

Royal Decree-Law 12/2018 has been implemented through Royal Decree 43/2021 of 26 January, which definitively transposes Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union.

This Royal Decree develops issues such as the figure of the Information Security Officer, establishes the minimum security measures to be adopted, lists the competent sectorial Authorities, establishes a single platform for the non-classification of incidents and lists the incidents that must be reported, among other issues.

ISA 99/IEC62443, ISO 27001, ISO 27002, NIST 800-82

There are different international standards that address in some way the cyber security of industrial systems.

Among others, the *ISA 99/IEC62443* standard is an international reference framework for the cybersecurity of *OT* systems.

This standard focuses on the availability and integrity of the most important elements, establishing a life cycle for industrial cyber security consisting of three steps: assessment, development and implementation, and maintenance.

We can also consider other standards such as *ISO 27001 and 27002* for information security, or *SP NIST 800-82*, which addresses security in industrial control systems, providing an overview of *ICS* and typical system topologies, identifying threats and vulnerabilities, as well as corresponding security countermeasures.

3. RECOMMENDATION FOR BASIC SECURITY MEASURES

Before starting to develop this chapter, it is very important to point out that both the Royal Decree-Law on the security of networks and information systems and the LPIC and the ENS establish risk analysis as the starting point for the choice of safeguards.

In line with this basic pillar, the aim of this section is to suggest a framework of measures as a guideline for Essential Service Operators (ESO) that provide services based on *OT* infrastructure, so as to have mechanisms in place to prevent, detect, respond to and recover from cybersecurity incidents in the operator's industrial control systems. This framework of measures will provide relevant information for the risk analysis, helping to verify that the selected controls cover at least the set of measures identified in this chapter. Finally, it aims to minimize the impacts that may affect the operation of the facilities, avoiding economic losses, physical, environmental and reputational damage.

3.1 Cybersecurity management in Industrial Control Systems (ICS).

The cyber security of SBIs' ICSs may be managed through global and/or local processes depending on the size and type of operator.

In order to establish practices with the highest level of detail possible according to the reality of each environment, it is recommended to establish or adapt these measures at different operational levels, taking as a reference the different levels of the *PERA* (*Purdue Enterprise Reference Architecture*) architecture model.

3.2 Recommended basic measures.

1- Assignment of roles and responsibilities. This is one of the most important measures, not only because of its importance, but also because it is the basis for ensuring that the following measures can be implemented and maintained in order to achieve the set objective. As far as possible, and based on the company's general governance model, a segregation of duties should be ensured, so that the responsibilities and the executive and technical capacities that each role should have can be clearly identified.

- **Cybersecurity governance in SCI**. An ICS cyber security governance role should exist and be assigned within the organizational structure of the company.

- **Installation safety officer**. This is the person ultimately responsible for the safety of the installation.

- **Owners of the ICS.** He is responsible for the industrial control system.

2- Security Strategy. Having a security strategy for *OT* networks helps to ensure compliance with the other measures listed below. This strategy should consist of at least the following points:

a. Internal security regulatory framework integrating *IT* and *OT* (policies, standards and procedures).

b. Need to apply risk management to implement appropriate security measures.

c. Need to carry out technological vulnerability management of the assets that make up *OT* networks.

d. Cybersecurity incident management.

3- Up-to-date inventory of the facility's ICSs. Having a complete inventory of ICS equipment that is kept up to date by incorporating changes is essential for ICS security management. This inventory can be used for risk and vulnerability analysis and incident response. The different ICS of each installation must be classified according to their criticality for the provision of the service. This is the basis for the system applicability document for the facility.

In relation to the inventory, have an updated ICS basing guide that includes good configuration practices. This guide will contain the general configurations of all ICSs classified by manufacturer and will be maintained by the asset owners with the support of the custodians.

4- Logical access control of ICS. Having logical access control measures to ICSs ensures that a given entity, user or process can, or cannot, access a system resource to perform a certain action. To ensure that adequate access control measures are in place in the ICS, the following should be taken into account:

a. All access is prohibited, unless expressly granted.

b. That the entity is uniquely identified.

c. That the use of resources is protected.

d. The following parameters should be defined for each entity: what needs to be accessed, with what rights and under what authorization.

e. The people who authorize, use and control the use will be different.

f. The identity of the entity is sufficiently authenticated.

g. That both local and remote access is controlled (see section "Control and monitoring of remote access" below).

5- ICS equipment shall be configured prior to their entry into operation, so that:

a. Standard accounts and passwords are withdrawn.

b. The "minimum functionality" rule applies:

1. The system must provide the functionality required for the organization to achieve its objectives and no other functionality.

2. The system will not provide operational, administrative or audit functions, thus reducing its perimeter to the minimum necessary.

3. Functions that are not of interest, not necessary, or even inappropriate for the intended purpose should be deactivated by means of configuration control.

c. The "security by default" rule is applied.

6- *OT* Network Security Architecture. The security of ICS should be the subject of a comprehensive approach detailing at least the following aspects:

a. Documentation of installations:

1. Areas.

2. Access points.

b. System documentation:

1. Equipment.

2. Internal networks and external connections.

3. System access points (workstations and administration consoles).

c. Scheme of lines of defence:

1. Interconnection points to other systems or other networks.

2. Firewall and *DMZ*.

3. Use of different technologies to prevent vulnerabilities that could simultaneously breach several lines of defence.

7- Segregation between control and corporate networks. Segregation between the ICS network and the corporate network ensures controlled and secure communication between the two, providing reciprocal protection against cyber-attacks from the other network.

From a security point of view, each of the different sub-networks can be seen as zones with different security requirements. Security is achieved by restricting information flows between these zones by means of *SW* or *HW* solutions. This prevents the propagation of attacks between these sub-networks. As an example, the *IEC-62443-1-1 and IEC-62443-3-3-3* standards provide definitions and security measures for zones and pipelines; or the *IEC-62351* standard, which addresses security measures for control systems applied to power environments, many of which can be generalized to any industrial system.

Segmentation between the ICS network and the corporate network must be segmented ensuring that there is:

a. Entry control of users arriving in each segment.

b. Output control of the information available in each segment.

c. Networks can be segmented by physical or logical devices. The point of interconnection will be particularly secured, maintained and monitored.

8- Traceability. Users' activities must be recorded in the ICS systems so that:

a. The register should indicate who performs the activity, when it is performed and on what information.

b. Logging includes the activity of users and, in particular, *OTs* and administrators as far as they can access the configuration and maintain the system.

c. Recording of successful activities and failed attempts.

9- Incident management. A security incident management procedure must be in place to ensure that security incidents are properly managed. This procedure must ensure the handling of security incidents that may have an impact on the security of the ICS, including:

a. Procedure for reporting actual or suspected incidents, detailing the escalation of notification.

b. Procedure for taking urgent action, including shutting down services, isolating the affected system, collecting evidence and protecting records, as appropriate to the case.

c. Procedure for allocating resources to investigate the causes, analyse the consequences and resolve the incident.

d. Procedures for informing internal and external stakeholders.

e. Procedures for:

1. Prevent a recurrence of the incident.
2. Include in user procedures the identification and handling of the incident.
3. Update, extend, improve or optimize incident resolution procedures.

10- Vulnerability management. In order to prevent the technological risks associated with ICSs, a vulnerability management plan for these must be carried out, which must consider the following aspects:

a. To have an updated asset map of the *OT* network.

b. Have an automatic vulnerability scanning tool.

c. Establish periodic scans of *OT* network assets prioritizing critical assets.

d. Address identified vulnerabilities.

e. Creation of metrics and indicators to enhance the monitoring of the results obtained.

11- Up-to-date *anti-malware* measures. Measures aimed at preventing ICSs from becoming infected with *malware* and preventing its spread, thus ensuring the safe and reliable operation of ICSs. These measures include procedural and technical controls aimed at detecting *malware* and preventing infection. In addition, intrusion detection or prevention tools (traffic analysis probes) must be in place.

12- Preventive and reactive measures against denial of service attacks. To this end, ICSs shall be equipped with these measures:

a. A denial of service attack detection system shall be put in place.

b. Procedures for reacting to attacks, including communication with the communications provider, shall be established.

c. The launching of attacks from within the facility to the detriment of third parties shall be prevented.

13- Security measures in relation to the use of corporate *WIFI* networks. In the event that ICSs make use of corporate *WIFI* networks, they shall have the following security measures in place:

a. Have an inventory of devices with a regular review of the inventory and potential vulnerabilities.

b. Create a dedicated management network, carrying only management and administration traffic, using secure protocols.

c. Use centralized authentication systems such as *RADIUS* servers using secure channels.

d. Perform a *DHCP* assignment of fixed *IP* address for each client/device in each of the different networks.

e. Configure clients to use *802.1X-EAP-TLS* protocol, *NAC* agent and encrypted *VPN* tunnel as recommended.

f. Limit physical access to equipment as well as logical access according to defined roles and disable the service when not in use.

g. Implement Intrusion Detection Systems (*IDS*) for the detection of possible anomalies that generate alarms.

h. Monitor network traffic and perform a periodic search for anomalies.

14- Patching procedure for applications, operating systems and *firmware*. Security patches are issued by vendors of operating systems, application *software* and hardware to address potential vulnerabilities in their products that can be exploited by potential attackers. Security patches should be applied according to internal procedures and provided that they are validated by the manufacturers for the installation in question. Contracts with *software* vendors should provide for security patching services and validation of the patches at each industrial site.

15- Laptops and mobile devices that have access to OT networks shall comply with the following security measures:

a. Have an inventory of portable equipment together with an identification of the person responsible for it and a regular check that it is positively under their control.

b. Establish a communication channel to inform the incident management service of losses or thefts.

c. Limit the information and services accessible to the minimum necessary, requiring prior authorization from those responsible for the ICS and the services concerned.

d. Avoid, as far as possible, equipment containing remote access keys to the organization. Consider remote access keys to be those that are capable of enabling access to other equipment in the organization, or others of a similar nature.

16- Secure protocols. To ensure the confidentiality of the traffic generated by ICSs, they shall use protocols considered as secure and specific solutions designed for this purpose.

17- Controls for removable devices. Removable media (e.g., *USB* sticks, external hard drives, *CD-ROM/DVD* drives) are one of the most common avenues for *malware* infection. Eliminating or at least reducing the use of removable media where technically possible, and controlling their use where this is not possible, significantly reduces the risk of *malware* infection.

18- Remote access control and monitoring. It should be implemented by secure methods. Remote access to ICSs presents potentially damaging mechanisms for *malware* and unauthorized access to ICSs, which can impact secure and reliable operation. Remote access must have a business justification and be implemented in a way that ensures its security and that only authorized persons can make use of this functionality.

It is recommended that the communications of the SCI devices with the outside be channelled through a *firewall*, preferably defining a *DMZ* where the services to which the SCI devices can connect are hosted and the services hosted in this DMZ are those that can connect to the outside. In this way, the perimeter is better limited and it is easier to protect.

It is also advisable to implement mechanisms to limit or block information flows to prevent the propagation of threats. In this sense, it is recommended to block any communication protocol that is not necessary for teleservice/remote access, in order to reduce the attack surface.

Finally, accesses to the infrastructure must be monitored and logged, so that they can be audited in the future.

19- Incident response plan. It is essential that assets/facilities are prepared for such an eventuality, in order to minimize its impact and recover the normal level of operation in the shortest possible time. Given the impossibility of foreseeing every possible type of incident, plans focus on incident management, ensuring that staff are aware of cyber security issues, trained to identify plant failures as a result of possible ICS failures and/or sabotage. Staff are actively involved in the design, development and testing of cyber incidents, establishing fluid communications and clear allocation of responsibilities. It is essential that plans are rehearsed for testing and that all staff involved are familiar with them.

20- Backup and restore capabilities. Recovery from a security incident, *hardware* or *software* failure or data corruption problem may require full or partial restoration of one or more devices or the system as a whole.

21- Strict control over administration roles and Change Management over ICSs. Administration roles have privileges to make changes to ICSs that can impact the safe and reliable operation of the ICSs and the facility controlled by them. Changes to ICS outside routine operations (e.g. *setpoint* changes, equipment start/stop, valve opening/closing) must be strictly controlled using the existing work management (e.g. work permit) and change management processes of the asset or facility to ensure that changes are implemented only after going through the relevant design, review, testing and approval process.

22- Management of log files and audit trails. Log files and audit trails are necessary both for monitoring security events and detecting anomalies and for conducting forensic analysis after any security incident.

23- Supply chain security. In order to establish a secure supply chain mechanism, the following recommendations are listed:

- Establish a framework for managing the lifecycle of the industrial control system, focusing on security by design, to minimize vulnerabilities and thus reduce the attack surface (see cyber security risk management).

- Establish lasting partnerships in the field of cyber security with all partners. Draft contracts with specific contractual agreements on cyber security. Unify policies, standards and procedures.

- Raise the level of training and awareness in cybersecurity, both for internal *IT* and *OT* staff, as well as external staff (suppliers, partners, etc.), who are involved in the operation of industrial control systems. Create cross-cutting *IT/OT* working groups so that the cybersecurity culture defined by the company is disseminated at all levels. Periodically check that personnel have the required level of competence and skills (tests, briefing pills, etc.).

- Analysis and sharing of cyber threat intelligence within the sector, as well as with technology providers. Special attention to ICS manufacturers. Establish mandatory reporting of vulnerabilities as soon as they become known (special due diligence within the sector itself).

- Conduct regular reviews of the technology risk management strategy including supply chain partners. Joint assessment of vulnerabilities, ensuring that risk arising from weaknesses is addressed with appropriate comprehensive remediation management.

- **Training and awareness of *OT* personnel.** *OT* technical and operational staff will be regularly trained in those subjects they require for the performance of their duties, in particular with regard to:

  a. System configuration.

  b. Incident detection and response.

  c. Management of information on whatever medium it is held. At least the following activities shall be covered: storage, transfer, copying, distribution and destruction.

Actions shall be taken to regularly raise the awareness of *OT* technical and operational staff of their role and responsibility in bringing the security of the system up to the required levels.

In particular, it will be regularly recalled:

  a. Safety regulations relating to the proper use of the systems.

  b. The identification of suspicious incidents, activities or behaviour that need to be reported for handling by specialized personnel.

  c. The procedure for reporting security incidents, whether real or false alarms.

- **Physical Security.** The facilities where the ICS are located shall have adequate elements for the effective operation of the equipment installed there. And, in particular:

  a. Temperature and humidity conditions.

  b. Protection of cabling against accidental or deliberate incidents.

  c. Fire protection measures.

  d. Flood protection measures.

4. RESULTS OBTAINED

The 116 shortcomings detected and the compensatory measures proposed to remedy them by the collaborating entities are attached in **ANNEX I** of this document, grouped into 15 areas for a better understanding and ease of analysis.

On this point it should be noted that many of the measures in this Annex I could also be applied to subcontractors/suppliers.

In addition, **ANNEX II** includes the statistical study on the security breaches detected, as well as the origin of the information.

ANNEX III is an adaptation of the threat catalogue proposed in the MAGERIT methodology, which is initially intended for information systems. This annex provides some details that must be taken into account when dealing with networks in *OT* environments.

Finally, a glossary of terms is included in **ANNEX IV.**

ANNEX I - RESULTS OF THE CONSULTATION

	LOCAL LOGICAL ACCESSES	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Need for open session permanence in monitoring systems impedes traceability and auditing.	Increase physical and network level control measures. Parallel operator registration system. Additional networked devices allowing for the establishment of control mechanisms for the sessions and blocking.
2	Session control and blocking if necessary.	Increase physical and network level control measures. Parallel operator logging system. Additional network devices that allow session control and blocking mechanisms to be set up. Integration of session attempts, both successful as well as unsuccessful, in *SIEM*.
3	*Hardcoded* passwords. In many industrial systems there are *hardcoded* administration passwords, which are also published on internet forums.	Establish network-level controls on who connects to the equipment. These controls can be done with an industrial *NGFW* by forcing the user, before connecting to the affected equipment, to perform an initial validation against the *FW* and by securing the connection between the *FW* and the fine device in case the *FW* is equipped with this technology.
4	Existence of a single user for all operators. Administration permissions for all users. Weak, non-existent password policy or the inability of *OT* software to conform to a strong password policy.	Creation of a credentials and user administration policy that includes, at least: Creation of personalized users. *RBAC (Role Based Access Control)* profiling. Strong password policies. Register and identify persons using the generic shared user in case a specific one cannot be defined. Enable access and activity logs on the systems to be managed. Ensure hourly identification of users who have accessed the operating console. This can be with fingerprint identification, video surveillance of the operating room, central account control console.

ANNEX I - RESULTS OF THE CONSULTATION

5	User lifecycle	Implementation of privilege management policies associated with the user lifecycle (e.g. assignment and revocation of access).
6	Users with elevated privileges with access to systems.	Creation of nominal accounts with minimum functional permissions.
7	Sharing of local administrator accounts.	Monitoring of the use of shared accounts by means of an independent log in and log out of the system.
8	Plain text embedded passwords for applications.	Rotation of passwords embedded in applications to avoid knowledge of them.
9	Absence of double authentication factor.	Integration of two-factor authentication for access to systems.
10	Absence of approval workflows for critical accounts.	Creation of approval flows for criticality accounts.
11	Absence of monitoring and access control systems.	Integration of audit systems for account and access control. Session recording.
12	Absence of password policy control.	Integration of efficient, controlled and supervised counterpart rotation policies.
13	Lack of control of user registrations in the operating console.	Implement an authorization process with segregation of duties.
14	Secure federation in certain *OT* scenarios such as *Smart Grid* systems, where it is necessary to apply standardised authentication and authorization procedures and following distributed or decentralised models.	Standardisation of federated *OT* environments, and following standardised authentication and authorization models, e.g. *RBAC* (IEC-62351-8), and under network constructions following standard interconnection models. These points of interconnection normally must/may fall on *gateways, proxies* or *Cloud, Fog or Edge*.

ANNEX I - RESULTS OF THE CONSULTATION

	REMOTE ACCESS (USER, MAINTENANCE, ETC.)	
	LACK OF SECURITY	**COMPENSATORY MEASURES**
1	Unsafe tele-maintenance	Use of *VPN*. Creation of maintenance policies. Logging of all administration and maintenance actions carried out remotely. This can be reinforced by the use of a virtualized jump server that allows the recording of keyboard entries and the sessions themselves. Special mention should be made of remote access software.
2	Interconnection of *OT* to the cloud in the outsourcing of services.	Evaluate the possibility of centralizing information in a single management point for *OT* and *IT/Cloud*, simplifying the work of security administrators.
3	Use of mobile devices in the *OT* world.	Secure these new connectivity mechanisms with an access control solution that can be installed on the production line. It is desirable, in order to avoid introducing different elements into the line, that the solution has the ability to facilitate access to the mobile network. In the case of corporate mobile devices, they should be enrolled in *MDM* solutions. Definition of a whitelist of devices and/or implementation of solutions that allow for control or restrictions of mobile devices accessing the *OT* network.
4	Excessive delegation of maintenance work to third parties.	More customer-friendly contract renegotiation and closer monitoring of contracts.
5	Remote access by third parties or subcontractors of parts of the installations (part *OT*) that are uncontrolled or cannot be audited.	Secure remote access management to plant and from a single centralized point via both *NGFWs* performing *IT/OT* segregation.
6	Management/administration of industrial systems from a *PC* with internet access.	*Whitelisting* of equipment allowing access to *OT* systems.

ANNEX I - RESULTS OF THE CONSULTATION

	PROTECTION AGAINST ATTACKS	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Lack of proactive security. There are no pro-active security mechanisms in industrial networks. Lack of advanced attack detection systems.	Have in place reactive protection systems such as firewalls, *IPS* systems, behavioural analysis systems, etc. Which block attempts to exploit vulnerabilities in industrial systems. These systems must also have anti-virus, *anti-bot*, file control and at least *IPS* capabilities for *Virtual Patching* of known vulnerabilities. Establish formal processes and tools for malware / antivirus management. Include *EDR* functionalities for behavioural monitoring in devices that allow it.
2	Denial of Service attacks.	Implementation of *DOS* and *DDOS* attack detection capabilities. Implementation of capabilities for blocking and/or limiting the source of the attack. Definition of business continuity plans and minimization of associated risks.
3	Protection against complex attacks.	Progress in anomaly-based intrusion detection systems (and therefore AI and *machine-learning*), and research in distributed detection supported by auto-learning techniques, *Big Data*, *NDR*, etc..
4	Lack of resilience in *OT* systems	Research on corrective measures based on restoration methods or mechanisms working at optimal times (if possible in approximately real time). If unable to return to an operational state similar to that prior to the manifestation of the failure, systems shall remain in a safe state. where they do not affect other devices employees or services.

ANNEX I - RESULTS OF THE CONSULTATION

	INVENTORY	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Non-existence of inventories.	Real-time inventory tools are needed. Of particular interest are the *ADBs* described in NISTIR 800-82r2 and included in the NIST1800-23 reference model since, by using passive mechanisms, i.e. non-intrusive to productive traffic, they are able to perform automatic, real-time asset inventorying. These systems are also capable of identifying manufacturer, *firmware*, serial number, vulnerabilities associated with the *firmware* version and operating systems. Implementation of automated or semi-automated auditing tools that are also integrated with inventory tools. In this way, an up-to-date inventory of all existing assets will always be available. It is recommended that, as far as possible, the inventorying mechanism can be obtained by from the existing network traffic in the installation. Perform audits, in order to know the assets (manufacturer, operating system, hardware version, *firmware* version, *IP* address, protocol used for communication, etc.). All this data could be obtained by means of market *software* called *Industrial Anomaly Detec- tion*. You cannot protect what you do not know you have.
2	Lack of control over the installation of *IoT* devices.	Establish a procedure for searching for devices through the exhaustive inventory of *IP* addresses. Implement control procedures for the installation of new devices. Monitor communication patterns and secure channels.

ANNEX I - RESULTS OF THE CONSULTATION

	NETWORK ARCHITECTURE	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Lack of definition of a network security architecture design for *OT* environments.	Definition and implementation of a procedure to define and regulate a base architecture model including the *OT* network and its relationship with IT/corporate environments. Increase physical and network access control measures. Reduce as far as possible the connections of equipment to more than one network. Incorporate network monitoring systems that can detect improper access attempts and firewalls where possible. Raise awareness and train operators, engineers, developers and maintenance personnel. Establishment of procedures for secure access and use of dispositives. If applicable/set up access in the *DMZ*.
2	Lack of segmentation.	Segmentation, as far as possible taking into account the standard of security zones and ducts proposed in the ISA99/IEC62443 standard, with separation with firewalls from different manufacturers and respecting Purdue levels. In addition, an *IT/OT* barrier must be created including several *DMZs* where the *OT* security system signature update servers and patch servers for the existing generalist operating systems on the *OT* network will be located. A second *DMZ will* be used to create jump machines to provide secure access to telemaintainers. Use of tools: Data Diode, Firewall, Network Access Control (*NAC*), *IDS/IPS* supporting industrial protocols. Strictly necessary use of wireless networks and only if they are secure. Use of mechanisms for the identification of devices deployed in the environment to prevent the connection of unauthorized elements to the network. Implement the segmentation of each of the automation cells based on industrial *switches* and *firewalls*, as this equipment is located in the factory cabinets, with their corresponding electro-magnetic interference, dust, dirt, etc.

ANNEX I - RESULTS OF THE CONSULTATION

3	No *IT/OT DMZ* In the *OT* architecture there is no *IT/OT DMZ* in the plants.	This *DMZ* is essential as it fulfils two functions: *1)* Hosting OS and *firmware* update systems of industrial systems. 2) Secure remote access network, where jump machines will be located for secure tele maintenance.
4	Convergence between *IT* and *OT* systems Increasingly, direct relations and communication are being established between the *IT* world and the *OT* world. The difference in cyber security maturity between the two worlds is abysmal.	*IT* systems must be equipped with solutions to protect against advanced attacks such as *ransomware, anti-phishing, zero-days*, both at the workstation and network level, and unified and simple management of these is desirable. Security Governance: Structure, Roles, Functions, Responsibilities and common or integrated management processes for the *IT* and *OT* world. Installation of separate *IT/OT* domain managers to prevent the other domain from being compromised in case of a vulnerability of one of them. Address the integration of security components at perimeter and network level, such as *firewalls, IDS/IPS, VPN* and diode communication. Establish *VLANs* on layer 3 *switches* and set up *ACLs* between different network segments. Isolate *OT* checkpoints from outgoing internet and email access.
5	Lack of implementation of zones and ducts in *OT* network.	Definition and implementation of *OT* network segmentation.
6	Weaknesses in the ducts between network layers.	Develop an access policy that limits and controls the conduits enabled between layers. Be particularly vigilant of conduits that publish status information on variables and set points.
7	Control deficiencies of active elements of the operational network.	Remove external administrators from *routers, switches* and *hubs* in the operational network. Disable all unnecessary network protocols in the system and limit their use to a minimum (*hardening*).
8	Weaknesses in the control of network elements, for corporate use.	Access control and video surveillance subsystems, which exist in virtually all industrial installations, often use network accesses that can compromise network security, and therefore *VLANs* should be established on layer 3 *switches* and *ACLs* should be established between the network segment of these access control and video surveillance subsystems with the rest of the networks.

9	Deficiencies in the control of elements of communications wireless.	Digital wireless subsystems (*VHF*, satellite, *WIFI*, etc.) must have the same control schemes and architecture as the rest of the network, so that they cannot compromise the security of the network.
10	Lack of documentation on the network's topology and protocols.	Perform an audit to know each of the network components installed in the factory and make a detailed network configuration not only with the network components that exist, but also their IPs and the different protocols that are executed between each of the components of the installation. All this data could be obtained by means of commercially available software called *Industrial Anomaly Detection*.
11	Shared use of corporate *WIFI*.	Segregation of *WIFI* for corporate, production and personal use. Implementation of network access control measures *WIFI*, etc.

ANNEX I - RESULTS OF THE CONSULTATION

	NETWORK ANALYSIS	
	LACK OF SECURITY	COMPENSATORY MEASURES
1.	Detection of traffic anomalies.	The inclusion of behavioural analysis and anomaly detection *(BAD)* systems at critical times is recommended, as per NIST 1800-23. These systems are responsible for, by receiving a copy of the network traffic, taking a "snapshot" of the plant status including, protocols, *SSOOs*, manufacturers, Purdue model, asset inventory, vulnerability discovery. In addition, once the equipment is switched to operational mode, it generates alarms based on: traffic deviations, protocol change, instruction change, *PLC firmware* upgrade, *firmware down-grade, configuration* download, configuration upload, a new asset is discovered on the network.
2.	Absence of vulnerability analysis.	Establish greater control over settings, connections and *software* updates. Include action plans for remediation.
3.	Absence of event management systems.	*SIEM* integration for the control of events and system *logs* of those systems that allow it.
4.	Existing vulnerabilities are unknown.	Application of vulnerability diagnostics.
5.	Lack of effective methods to prevent information leakage.	Use of *DLP* tools in related *OT* systems for service with *IT* systems. Control / restriction of information on portable devices. Use of *IRM (Information Right Management)* tools. Secure disposal of information on obsolete devices. Restrictions on external access from the industrial network (use of internet, *e-mail*, etc.). Media use regulations.

ANNEX I - RESULTS OF THE CONSULTATION

6.	Detection and handling of incomplete cyber security incidents.	Establish processes for monitoring events and detecting, notifying and responding to cybersecurity incidents (*SIEM*, *SOAR*, etc.).
7.	Absence of network monitoring	In addition to the identification of non-inventoried assets, network monitoring allows us to detect anomalies (*BAD*) through the analysis of industrial products in use. The use of *IDS/IPS* and *DPI* can be completed with the integration of *honeypots*, *deceptions hosts*, etc.
8.	No automatic vulnerability scanning.	Configuration control, segmentation with *DMZ*, indirect connectivity control, key in booths, facility and room access control system, network monitoring and *SIEM*.
9.	Automation of responses. To date, responses are based on manual procedures without yet relying on *ICT* systems to lead new actions and responses to failures, incidents or attacks.	Research into automatic or semi-automatic response mechanisms to provide prevention.
10.	Model and Tools for the identification of Critical Infrastructure Elements, sensitive to cascading effects leading to serious disruption of essential performance or service.	Based on the Resilience and Integrated Risk Management Committee. Possible sensitive categories: 1. *SCADA* control centres, monitoring. 2. *IT* and *OT* technological infrastructure. 3. Essential personnel - crisis committee, security, emergency, *O&M*, systems and cyber... - including subcontractors. 4. Critical processes of the installation (operation, safety systems, logistics, etc.). 5. Security systems *security*. 6. Essential equipment and machinery (power station/electrical panels, water and gas systems, etc.). 7. Physical infrastructures (buildings and geophysical environment, communication network: road, rail, etc., nearby towns and natural environments). 8. External services and basic supplies. 9. Other sector-specific areas.

ANNEX I - RESULTS OF THE CONSULTATION

	NETWORK PROTOCOLS	
	LACK OF SECURITY	**COMPENSATORY MEASURES**
1	Industrial protocols in communications between logic controllers and supervisory systems without the capability of control mechanisms and/or encryption.	Increase physical and network level control measures. Raise awareness and train operators, engineers, developers and maintenance personnel. Additional arrangements to establish control and monitoring mechanisms and to encryption.
2	Insecure industrial communications protocols.	The ideal measure, but the most complicated and the one that takes the longest time to implement, is for manufacturers of Industrial Systems to incorporate secure protocols in their solutions, including encryption for example. Include *HW* encryptors in point-to-point communications. These ciphers should not introduce significant latencies. Include measures to control traffic behaviour, so that, although it is not capable of blocking, it does allow alerting of anomalous behaviour in network traffic.
3	Absence of specific control policies and procedures for *OT* networks in place.	Definition of a control *framework* for effective management of the *OT* environment.
4	Lack of security in the multiple communication protocols used by *OT* devices.	Use of *OPC UA-based* architectures for the homogenisation of communications and the establishment of security measures within the protocols used. Ensure that communication traffic between the devices and their controllers/ is executed on an encrypted channel/ or in a protected micro network segment.

ANNEX I - RESULTS OF THE CONSULTATION

5	Lack of knowledge of *OT* protocols used for possible protection.	Since *OT* protocols are not encrypted, it is advisable to avoid "*man in the middle*" problems. To do so, it is necessary to implement solutions such as: use of *VPNs* for communications through public networks, use of specific security *hardware* to protect the local network, use of encryption systems in communications, use of two-factor authentication, etc.
6	Lack of general standardisation of *IT/OT* systems integration in a secure way. There are several standards that focus on *IT* integration in *OT* environments, such as *IEC* 62351 (for power environments), and even if all integrated technologies follow specific standards.	National and international standardisation of the integration of *IT* technologies in complex *OT* environments.

ANNEX I - RESULTS OF THE CONSULTATION

	CONFIGURATION	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Lack of certified *OT* products in the *IT* environment. Equipment not certified for cybersecurity at the facility.	Definition of protocols and certification standards / Certification of industrial devices. Use of equipment designed under the premise of cybersecurity and with guarantees of its maintenance during the life cycle of the product and, if possible, certified, although as we all know, what ultimately needs to be certified is 100% of the installation.
2	Use of general purpose operating system.	Implementation of a patching policy for general purpose operating systems. Installation of reactive security systems to enable virtual patching techniques.
3	Shortcomings in backups and their management. Policy for the management of devices which are likely to connect to the *OT* network. Absence or mismanagement of centralized *backups* (resilience).	Development and implementation of measures covering aspects such as planning, remote copying and recovery testing. Develop and implement a backup process, off-site as far as possible, that ensures the existence of copies for configuration, for activity *logs* and for administration logs. In the event of a cyber-attack and *ransomware*, being able to restore systems from a centralized point and with guaranteed versioning.

4	Existence of default configurations (ports, passwords, etc.). Network equipment not configured correctly. Existence of very sensitive points. *Software* control deficiencies in the operating console. Weaknesses in *SW* version control and operating console configuration.	Development and implementation of technical policies/procedures for configuration and deployment of needs-based technologies to replace default configurations. Modification of network structure to avoid the use of *dual home* equipment. Establish basing guidelines for network devices. Periodic configuration reviews. Identification of these points and creation of *DMZs*. Develop a procedure to monitor and prevent the installation of unauthorized applications, in particular office applications (*Offi- ce*, *Chat*, etc.). Apart from backup control, establish a test environment and a production release authorization mechanism with segregation of duties.
5	Unnecessary services in *OT* devices. Default *ICS* device configurations. Lack of equipment bastioning (e.g. disabling *USB*).	Disable protocols: *Snmp; Telnet; UPnP, RDP*, *FTP*, etc., as well as connections that are not strictly necessary for the operation of the system. Port blocking. Delete/block/change accounts and default passwords. Blocking unused or insecure services/ports, *plugins*, etc. Use of configuration management tools. Disable resources/processes that are not required and apply basing measures.
6	Absence of *Blac- klist* or *Whitelist* systems. Lack of protection at the *end-point*.	Configuration of *Blacklists* or *Whitelists* to deny or allow the execution of certain commands on systems. *Whitelisting* coupled with various basing of the installation.
7	Absence of self-service workflow management.	Configure and design the flow system for self-service in the different applications.
8	Deficiencies in the control of the continuity of the operation.	Establish a risk assessment system, similar to the *BIAs*, to identify continuity weaknesses in the event of unforeseen equipment, console configuration and *SW* failures.

9	The false automation of processes. Automated *IT/OT* asset management and following specific dynamic identity management models.	There are many processes that are mistakenly considered to be automated, as they require proper administration, control and management. Procedures associated with critical automated processes should be adequately documented and the roles that oversee them identified. Design and implementation of management models for identity and *tracking* of existing or new assets.
10	Lack of security integration at all stages of development and implementation of new systems and changes. Security measures not integrated in *ICS*, especially in low-end ICS.	Establish security requirements for new *ICS*. Integrate these requirements in the different phases of development and implementation, as well as in the changes. Establish a process for change management in the *ICS*. Conduct security assessments of new systems prior to procurement and production deployment. Use of the security paradigms *'Security by Design*', '*Privacy By Design*' and '*Security By Default*'.
11	Mismanagement of trust and integrity.	Trust must be established in the *bootstrapping* environment (*secure bootstrapping*) so that the integrity of the device can be verified from the outset. Cryptographically sign the code to ensure that it has not been tampered with at a later stage and monitor the execution of the code to ensure that it has not been overwritten. Allow a system to revert to a state that was known to be secure.
12	Use of *IT* equipment on the *OT* side, which is not designed to withstand industrial environments.	Replace these with equipment with suitable hardware or relocate to suitable and physically secure spaces to achieve system availability. if possible 24/7, being able to guarantee as far as possible business continuity as far as possible.
13	*HW/SW* protection and "from" design, known as "*security by design*", affects the vast majority of *OT* devices, which present high computational constraints to manage cryptographic resources (e.g. *RTUs/PLCs*). This must be considered during the design of these components.	Consider protection measures at *HW* level such as *TPM (Trusted Platform Module)* and *TEE (Trusted Execution Environment)* to create a "root of trust" environment, secure boot and integrated protection of operating systems. To this end, it is also essential to address the current *HW/SW* restrictions of most drivers.

ANNEX I - RESULTS OF THE CONSULTATION

	UPGRADES AND OBSOLESCENCE	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	*Legacy* devices without the capability to handle IDs and/or authorisations in logic controllers (*PLCs*, *RTUs*, *DCS*).	Increase physical and network level control measures. Raise awareness and train operators, engineers, developers and maintenance staff. Establish procedures for access and use of legacy devices with safe conditions of use. Location of legacy devices in isolated network segments. Additional devices to handle IDs and/or authorisations.
2	*Software* or *firmware* not upgraded	As a compensatory measure, the use of virtual patching mechanisms at network level is proposed (given that it is very complex to install agents by the manufacturer's support for industrial assets). These mechanisms protect the assets affected by the different vulnerabilities at network level, making their exploitation impossible. It is advisable for this mechanism to include not only proprietary *IT* signatures but also protection signatures specific to the industrial systems and that signatures in known formats such as *SNORT* or *YARA* can be added. Agree with the vendor on a patch deployment strategy and schedule. Establish a mitigation plan to cover the absence of critical patches. It is also advisable to create *test-beds* or pre-production systems on which to test the impact of system updates associated with industrial processes. These *test-beds* can be either physical or virtual. Encapsulation of obsolete operating systems such as *Windows XP* or *Windows 7* by virtualising these operating systems. Use of cryptography in devices for validation of new software versions through digital signature in update processes and to prevent code tampering. Establish a centralized patch management system (*WSUS*) if one exists.

ANNEX I - RESULTS OF THE CONSULTATION

3	Lack of support for installation of security endpoints on *HMI* systems	General purpose systems should be fitted with *endpoints* certified by the manufacturer of industrial systems to protect against advanced attacks. These systems shall be capable of blocking not only against known threats but also against *zero days* or unknown threats.
4	Existence of *WIFI* connections with obsolete *hardware* that does not allow for the deployment of security mechanisms (encryption/authentication, etc.).	Replacement of access points with devices that allow a higher level of security. Implementation of *RADIUS/MAC* filtering systems. Use of wired connection as far as possible.
5	Deficiencies in anti-virus updates.	Agree with the vendor on an anti-virus implementation strategy and schedule. Establish a mitigation plan to cover upgrade delays. Protect the outermost layer of the network with surveillance elements, *firewalls*, *IDEs* and the like.

ANNEX I - RESULTS OF THE CONSULTATION

	TRACEABILITY, MONITORING	
	LACK OF SECURITY	**COMPENSATORY MEASURES**
1	Absence of activity logs in logic controllers (*PLCs*, *RTUs*, *DCS*).	Incorporate systems for monitoring and recording network activity. Incorporate monitoring and activity logging systems where possible. Raise awareness and train operators, engineers, developers and maintenance personnel.
2	There is no control over *reporting*.	Integration of a *reporting* system for all metrics and volumetrics.
3	A system scanning system is not available.	Configuration in integration of periodical scanners to keep the integration of accounts on the systems up to date.
4	Absence of record keeping in the management of system changes.	Establishment of repositories for change logging and change history.
5	No security logging system (access, external connections, etc.).	Implementation of decentralised automatic detection and logging of security changes and their management.
6	Lack of visibility of *OT* network traffic.	Installation of probes. Control of insecure and/or unnecessary open *TCP/IP* ports and services, such as ports 23, 21 or 80, as well as the use of *UDP* ports for critical control transactions. Establish rigorous security policies, and maintenance and maintenance plans, and frequent follow-up.

ANNEX I - RESULTS OF THE CONSULTATION

7	Routine control of web services, which are set up for remote monitoring tasks or for administrative management. Many web applications may have security weaknesses that can lead to security vulnerabilities. to multiple types of remote attacks.	Establish security policies to verify the applied *web* code, establish tracking and monitoring plans for web applications, and harden access to the control plant from remote locations (including from the corporate network). Consider *WAF* implementation (*Web Application Firewall*)
8	Audit, *accountability* and traceability of actions, especially in those *OT* scenarios where there is a federation of entities, such as *Smart Grids*.	Adaptation of new technologies such as *Distributed Ledger Technologies (DLT)*, which offer data immutability, security and provenance.

ANNEX I - RESULTS OF THE CONSULTATION

	USE OF MOBILE DEVICES	
	LACK OF SECURITY	**COMPENSATORY MEASURES**
1	Control weaknesses of portable equipment	Policy for managing devices that may be connected to the *OT* network. Limit the possibility of portable equipment connecting to *OT* networks. Monitor each wired connection. Implement a policy to prevent simultaneous access to the wired network and the *WIFI* network. Robustness of the guest *WIFI* network. Devices do not always have a unique identifier to facilitate tracking, monitoring and asset management. Staff monitoring hosts on the network do not necessarily consider *IoT* devices as just another *host.* You must have tracking systems that include all assets, however simple they may be, such as thermostats.
2	Use of low-performance *IoT* equipment without appropriate cyber security measures.	Use *IoT* components where possible and designed with cybersecurity in mind and throughout the product lifecycle. Where this is not possible, detection and control measures in the acquisition environment and in communication infrastructures and information systems for analysing the acquired data should be maximised.
3	Apply *BYOD* policies without considering preventive measures and security policies. In fact, there are risks of *USB* and autorun.inf infections.	Define *BYOD-specific* security policies and review the current status of devices, regularly run *anti-malware* or anti-virus tools (e.g. at the start of the day), and install intrusion detection mechanisms (mainly based on in anomalies). Also, it is essential to The Commission should address awareness-raising and training plans in this area.

ANNEX I - RESULTS OF THE CONSULTATION

	AWARENESS, STAFF, TRAINING	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Lack of security culture in the *OT* world.	Establish company training and awareness-raising policies.
2	Specific training for employees and users.	Regular and targeted training with attendance records for employees/operators of the infrastructure/systems.
3	Training of *OT* technical operation profiles in *IT* skills.	Specific training on identified gaps.
4	Training of technical *IT* operation profiles in *OT* skills.	Specific training on identified gaps.
5	Not having a dedicated *OT* cyber security manager and staff trained to meet the needs of the area.	Assign such responsibility.
6	No advanced intrusion drills (*Red Team*) combining physical, digital and social engineering vectors.	Conduct periodic penetration testing and crisis response coordination exercises.
7	Inexperience in responding to cybersecurity incidents.	Have an on-demand cyber security incident response support service.

ANNEX I - RESULTS OF THE CONSULTATION

	PHYSICAL SECURITY	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Insufficient isolation of control systems.	Implementation of control measures, both physical and logical, to restrict access (e.g. "caged" servers).
2	Insecure access control systems.	Ensure that cabling and access to critical equipment is protected and secure. Establish access controls (password/key/ or biometric access) to critical systems. Logging of physical access history to the control centre of the systems (access logs/video surveillance recordings). Visual identification of access restriction to critical areas.
3	Lack of control of the administration console.	Locate the administration console in the Control Room. Implement a *SIEM* type log system.
4	Deficiencies in physical access to the operational network.	Implement separation and distance between the control networks and the corporate network to make it difficult to connect erroneously or maliciously between networks.
5	Weaknesses in the control of physical access to the facilities.	Access to places where there are active devices (control room, *PLC*, actuator and sensor rooms, control rooms, actuator and sensor rooms, control rooms, etc.) is not allowed. The use of communication towers, communication towers and *shelters*, etc.) must be adequately restricted and controlled.
6	Absence of security measures on particularly sensitive devices.	Cataloguing of sensitive devices. Isolation, access control, cabin alarms and possible rounds in exceptional cases.
7	Lack of control in systems *CCTV*	Periodic review of *CCTV* systems. Establish a procedure for data protection.

ANNEX I - RESULTS OF THE CONSULTATION

	SUPPLIER MANAGEMENT	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	Sole or single-source providers.	Identify single suppliers and require additional measures from them. Diversify suppliers.
2	Products without factory safety measures.	Policies for testing and implementing security in purchased products. Safety testing of purchased products. Establish network security measures at detection and protection level.
3	Lack of procedure in the procurement of products and services with special attention to the supply chain.	Robust contractual procedures that are regularly reviewed by the client.

ANNEX I - RESULTS OF THE CONSULTATION

	STRATEGIES	
	LACK OF SECURITY	COMPENSATORY MEASURES
1	*OT* labs to test the vulnerability of *OT* equipment in *IT* networks.	Design and implementation of own or third-party laboratories.
2	Security requirements in the procurement of devices.	Establishment and application of a *baseline* of safety requirements according to standards such as *IEC-62443-33* as part of technology procurement processes.
3	Not having a business continuity plan in place.	Have conducted the *BIA* and implemented some essential contingency measure.
4	Lack of regular and frequent ethical hacking reviews of the entire infrastructure.	Conduct at least an annual vulnerability scan of the most critical infrastructures.
5	Crisis management and associated communication.	Crisis management is one of the most important aspects in dealing with complex scenarios related to security breaches. Its associated communication plan is vital. Developing a proper Crisis Plan and integrating it throughout the organization and all critical systems is vital. In its development, the communication plan and the decision tree are critical.
6	Business Impact Analysis of Systems.	In many cases, large investments are made in information protection and the safeguarding of their assets. However, these investments are not supported by a rigorous business impact analysis. Systems that may be considered as non-critical a priori, after an analysis can actually cause a very important impact to the organization. An impact analysis is essential.
7	Appropriate documentation of systems and their configuration.	The systems and their associated configuration must be adequately documented. The *security guidelines* applied and their compliance must be properly described. Strict requirements must be established in this area, especially for the most critical systems.

ANNEX I - RESULTS OF THE CONSULTATION

8	Data is not the critical aspect of the systems.	In many cases, information security is not built on the basis of the criticality of the data associated with the systems. Many investments are made in security, but they are not always focused on the protection of data in storage or in transit. It is essential to protect both parts of the systems: the repositories and the communications.
9	Lack of defined or unclear security responsibilities in the *OT* world.	Creation of specific security roles and responsibilities for *OTs* (*OT Security Managers*), dependent on a common role integrating *IT/OT* security (*CSO*, *CISO*, etc.).
10	Absence of established safety objectives.	Establish safety improvement targets on a regular basis. Plan and allocate resources to achieve the objectives set. Establish indicators for the evolution of the achievement of these objectives.
11	Lack of internal safety standards or lack of staff awareness of them.	Identification of applicable regulations. Establish an Internal Security Policy Framework integrating *IT* and *OT* (policies, standards and procedures). Consider the general Framework for *TOs*, and the specific one for each sector (leads to several vertical and horizontal modules). Dissemination of the Regulatory Framework to the public The Commission has also been involved.
12	Lack of a formal classification and critique of information and *CSI* and the measures to be applied.	Establish a standard and procedures for the classification and criticality of information and *ICS*.
13	Absence of Risk Management	Conduct periodic (annual) *AARRs* or when relevant changes occur. Establishment of risk acceptance criteria. Realisation of Risk Treatment Plan (RTP)/ Safety Master Plan (SSP).

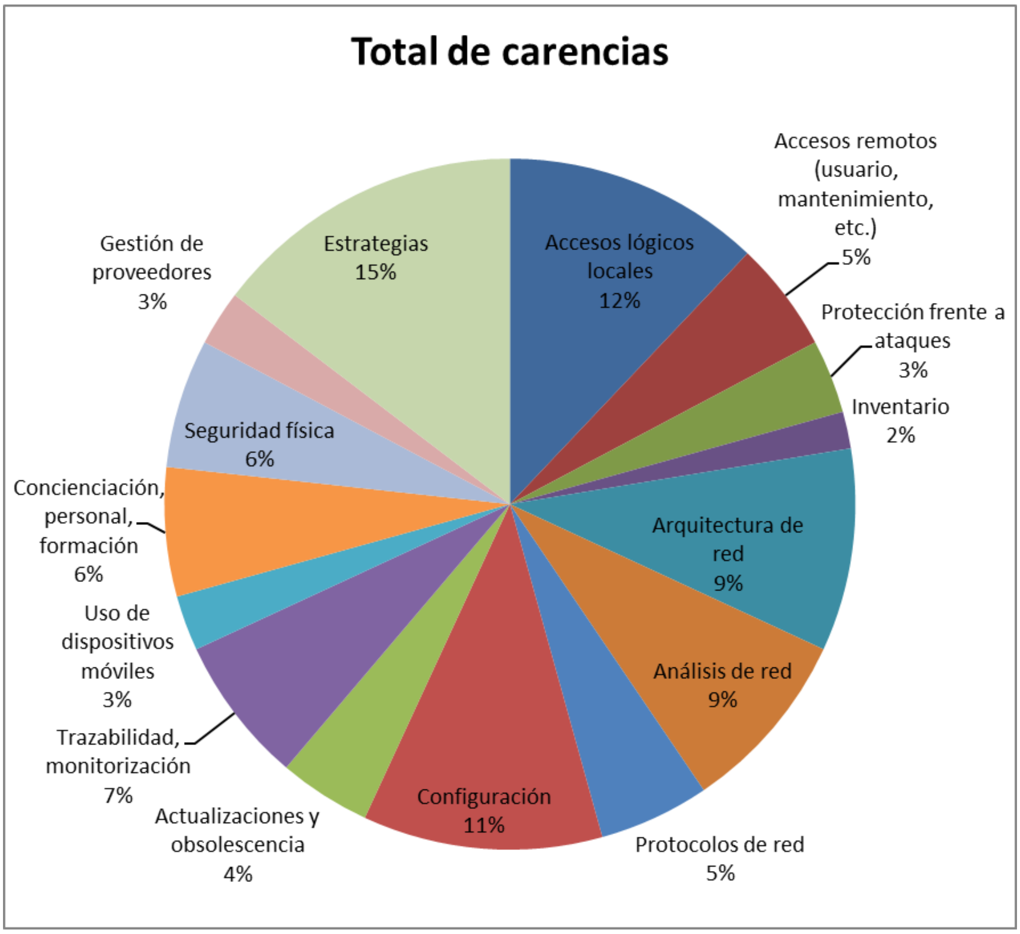
14	Lack of control of the entire supply chain and complexity of the supply chain.	Establishment of a Supplier Identification, Evaluation and Management process. Identification of interdependencies. Carrying out *AARR* in the supply chain. Supply Chain Management System. Agreement with suppliers including security (logical, physical and personal). Service Level Agreements (SLAs). Establish the minimum security requirements to be met by providers.
15	Lack of State knowledge and control of security and compliance.	Establishing a Framework of Con-troles. Compliance management process (implementation and review). Integrated Security Dashboard. Establish a plan for regular Compliance and Vulnerability Scanning audits and plans for the correction of weaknesses found. Use of passive vulnerability detection tools. Establish threat intelligence processes: detection of internal and external threats. Use of *GRC-IRM* tools for Integrated Security Governance and Management.
16	Absence of formal Business Continuity Plans.	Absence of formal Business Continuity Plans. Conducting a Business Impact Analysis *(BIA)* to identify critical processes. Business Continuity Plans. Crisis Management Plans. Standards and Procedures for Copying and information retrieval.
17	Lack of business case for systems and services related to cybersecurity.	Conduct an audit to find out where we are, where we want to get to and a plan of how to get to the end point, so that we can make a budget and discuss and approve it with the company management.

ANNEXII-STATISTICS

In summary, the following shortcomings were identified from the entities consulted:

FIELD	NO. LACKS
Local logical access	14
Remote accesses (user, maintenance, etc.)	6
Protection against attacks	4
Inventory	2
Network architecture	11
Network analysis	10
Network protocols	6
Configuration	13
Upgrades and obsolescence	5
Traceability, monitoring	8
Use of mobile devices	3
Awareness, staff, training	7
Physical security	7
Supplier management	3

ANNEXII-STATISTICS



ANNEXII-STATISTICS

Number of entities that have identified gaps for each area:

	PARTICIPATION BY ENTITY			
FIELD	CONSULTING	ASSOCIATION	UNIVERSITY	MANUFACTURER
Local logical access	2	2	0	3
Remote access (user, maintenance, etc.)	1	0	0	4
Protection against attacks	0	1	1	3
Inventory	1	1	0	4
Network architecture	2	2	1	5
Network analysis	1	0	2	5
Network protocols	2	1	1	3
Configuration	2	2	1	4
Upgrades and obsolescence	1	2	2	5
Traceability, monitoring	1	2	1	2
Use of devices mobiles	0	1	1	2
Awareness-raising, staff, training	1	2	1	1
Physical security	2	1	0	2
Supplier management	2	1	0	5
Strategies	1	1	1	5

ANNEX II - STATISTICS

Representation as a percentage of the entities that have identified gaps for each area, in relation to the total number of partners in each group:

	REPRESENTATION BY ENTITY			
FIELD	**CONSULTING**	**ASSOCIATION**	**UNIVERSITY**	**MANUFACTURER**
Local logical access	100%	50%	0%	50%
Remote access (user, maintenance, etc.)	50%	0%	0%	67%
Protection against attacks	0%	25%	50%	50%
Inventory	50%	25%	0%	67%
Network architecture	100%	50%	50%	83%
Network analysis	50%	0%	100%	83%
Network protocols	100%	25%	50%	50%
Configuration	100%	50%	50%	67%
Updates and obsolescence	50%	50%	100%	83%
Traceability, monitoring	50%	50%	50%	33%
Use of devices mobiles	0%	25%	50%	33%
Awareness-raising, staff, training	50%	50%	50%	17%
Physical security	100%	25%	0%	33%
Supplier management	100%	25%	0%	83%
Strategies	50%	25%	50%	83%

ANNEX III - ADAPTATION OF THE THREATS TO THE

Based on the categorisation made in the MAGERIT threat catalogue - version 3.0, there are four typologies of origin:

- Intentional attacks.
- Natural disasters.
- Unintentional errors and mistakes.
- Of industrial origin.

The hazards identified below could be duplicated, if necessary, in order to establish different impacts depending on the area where the hazards are likely to occur.

A.3	**Manipulation of activity logs**	The records created in the background by *OT* applications cannot guarantee their integrity for established technical or organizational reasons, making it impossible to establish accountability.
A.4	**Manipulation of the configuration**	Virtually all assets depend on their configuration, which depends on the diligence of the administrator: access privileges, activity flows, activity logging, routing, etc.
A.5	**Impersonation of the user's identity**	When an attacker manages to impersonate an authorized user, he enjoys the privileges of the authorized user for his own purposes. It is important to analyse the type of privileges implied by the impersonated identity and whether the impersonation has occurred locally or remotely.
A.6	**Abuse of access privileges**	Privilege is a special authorization granted to a particular user to perform relevant operations. Abuse of a privileged account occurs when the privileges associated with the user are used inappropriately or fraudulently, either intentionally, acci- dentally or through ignorance of procedures.
A.7	**Unintended use**	Use of system resources for unintended purposes, typically of personal interest: games, personal internet queries, personal databases, personal software, storage of personal data, etc.
A.8	**Dissemination of harmful *software***	Intentional spread of viruses, *spyware*, worms, Trojans, *DDOS* attacks or *ramsomware* are among the main categories of malware. Special mention should be made of the cloud environment, where an attack can significantly affect business activity. In addition to the *cloud* environment, attacks originating in the supply chain should also be mentioned.
A.9	**Message re-routing**	Sending information to an incorrect destination through a system or network, which takes the information where or where it is not supposed to go. This can be person-to-person, process-to-process or process-to-process messages. An attacker can force a message to pass through a particular network node where it can be intercepted. Particularly noteworthy is the case where the attacker's attack leads to fraudulent delivery, ending up with the information in the wrong hands.

ANNEX III - ADAPTATION OF THE THREATS TO THE

A.10	**Alteration of sequency**	Alteration of the order of the messages transmitted. With the intention that the new order alters the meaning of the set of messages, damaging the integrity of the data affected or the actions carried out.
A.11	**Unauthorised access**	The attacker gains unauthorized access to system resources, typically by exploiting a flaw in the authorization process or access control system.
A.12	**Traffic analysis**	The attacker is able to draw conclusions from the origin, destination, metadata, volume and frequency of exchanges without having to analyse the content of the communications.
A.13	**Repudiation**	A posteriori denial of actions or commitments acquired in the past. Repudiation of origin: Denial of being the sender or origin of a message or communication. Repudiation of receipt: Denial of having received a message or communication. Repudiation of delivery: Denial of having received a message for delivery to another.
A.14	**Interception of information (eavesdropping)**	The attacker gets passive access to information that does not belong to him, without the information itself being altered.
A.15	**Modification of information**	Intentional alteration of information, with intent to profit or cause damage.
A.18	**Destruction of information**	Intentional deletion of information, with the intention of making a profit or causing damage. Point out the increasing migration of information to *cloud* environments, with what this means compared to traditional media.
A.19	**Dissemination of information**	Deliberate disclosure of material information.
A.22	**Programme manipulation**	Intentional alteration of the functioning of programs and *firmware*, pursuing an indirect benefit when used.
A.23	**Equipment handling**	Intentional alteration of the functioning of equipment, aiming at an indirect benefit when used.
A.24	**Denial of service**	Lack of sufficient resources causes the system to crash when the workload is excessive.
A.25	**Theft**	The theft of equipment directly results in the lack of a means to provide services, unavailability. Theft can affect all types of equipment, with equipment theft and theft of data carriers being the most common.
A.26	**Destructive attack**	Sabotage, vandalism, terrorism, military action, etc.
A.27	**Occupation ene- miga**	When premises have been invaded and there is a lack of control over one's own means of work.

A.28	**Unavailability of staff**	Deliberate absence from work: Strikes, absenteeism, unexcused absences, blocking of access, etc.
A.29	**Extortion**	Pressure exerted on someone by means of threats in order to force them to act in a certain way.
A.30	**Social engineering**	Collection of personal information, without the use of technology.
A.31	**Unavailability of suppliers**	Deliberate absence of a supplier: Strikes, work absenteeism, unjustified absences, blocking of access, etc. This type of attack directly affects the supply chain.
A.32	**Unavailability of buildings/facilities (A)**	Unavailability of buildings/facilities due to intentional attacks from internal or external sources

NATURAL DISASTERS		
N.1	Any natural phenomenon that is dangerous to the system.	There is a great variety within the possible categories, such as atmospheric, hydrological, seismic, volcanic or fire. Specific examples would be hurricanes, storms, drought, erosion, flooding, tsunamis, faults, lava flows, subsidence or fire, cold or heat, and so on. extremes, etc.

ANNEX III - ADAPTATION OF THE THREATS TO THE

UNINTENTIONAL ERRORS AND MISTAKES		
E.1	**User errors**	Mistakes people make when using services or systems.
E.2	**Administrator errors**	Mistakes by persons responsible for installation and operation.
E.3	**Errors in monitoring**	• unmonitored equipment • unauthorised equipment • unmonitored measures • unmonitored inputs / outputs (from pdi) • *input data, output data, intermediate data*
E.4	**Configuration errors**	• authorised services • authorised flows (*routing*) • authorised protocols • authorised data [formats • unauthorized user accounts (default, absent staff,...) • system architecture (zones and ducts) • certificates (signature validation) • bastioning (fortification) configuration [security].
E.7	**Organisational weaknesses**	When it is not clear who has to do exactly what and when, including taking action on assets or reporting to the management hierarchy. Uncoordinated actions, errors of omission, etc.
E.8	***Software* dissemination harmful**	Innocent spread of viruses, *spyware*, worms, Trojans, *DDOS* attacks or *ramsomware* are among the main categories of malware. Special mention should be made of the *cloud* environment, in which an error can significantly affect the business. In addition to the *cloud* environment, errors originating in the supply chain should also be mentioned.
E.9	**Re-routing errors**	Sending information through a system or a network using, accidentally, a route incorrect routing that takes the information where or where it should not go; this may be messages between people, between processes or between processes. Particularly noteworthy is the case where the routing error leads to a delivery error, resulting in information ending up in the hands of who is not expected.
E.10	**Sequence errors**	Accidental alteration of the order of the messages transmitted.

ANNEX III - ADAPTATION OF THE THREATS TO THE

E.15	**Alteration of information**	Accidental alteration of information. This threat is only identified on data in general, i.e. when the information is on a computer medium.
E.18	**Destruction of information**	Accidental loss of information. This threat is only identified for data in general, as when the information is on a computer medium, there are specific threats. Point out the growing migration of information to *cloud* environments with what this means compared to traditional media.
E.19	**Dissemination of information**	Disclosure by indiscretion. Verbal incontinence, electronic media, paper media, etc. Information accidentally reaches people who should not be aware of it. He pointed to the increasing migration of information to *cloud* environments and what this means compared to traditional media.
E.20	**Programme vulnerabilities**	Defects in the code that result in faulty operation unintentionally by the user, but with consequences on the integrity of the data or the ability to operate.
E.21	**Maintenance/programme update errors**	Defects in equipment upgrading procedures or controls that allow software with known defects to continue to be used and repaired by the manufacturer.
E.22	**Maintenance/equipment upgrade errors**	Defects in equipment operating procedures or controls that allow equipment to continue to be used beyond the rated time of use
E.24	**System crash due to resource depletion**	Lack of sufficient resources causes the system to crash when the workload is excessive.
E.25	**Loss of equipment**	The loss of equipment directly results in the lack of a means to provide services, i.e. unavailability. All types of equipment can be lost, with the loss of equipment and data carriers being the most common. In the case of equipment that hosts data, information leakage can also occur.
E.28	**Unavailability of personnel (pandemic and others)**	Accidental absence from the workplace: Sars Covid19 pandemic, public disturbances, germ warfare, gas leak, accident, etc.
E.29	**Unavailability of Buildings/Facilities [E]**	Unavailability of buildings or facilities due to unauthorized errors and failures. Can be separated by key buildings or facilities.

ANNEX III - ADAPTATION OF THE THREATS TO THE

INDUSTRIAL ORIGIN		
I.1	**Fire**	Fire: The potential for fire to destroy resources in industrial systems. This threat can be separated by key buildings or facilities.
I.2	**Water damage**	Leakage, leakage, flooding: possibility of water draining resources from industrial systems resources.
I.3	**Mechanical pollution**	Vibrations, dust, dirt, etc.
I.4	**Electromagnetic pollution**	Radio interference, magnetic fields, ultraviolet light, etc.
I.5	**Failure of physical or logical origin**	Equipment failures and/or software failures. This may be due to a defect at source or may occur during the operation of industrial systems. In special-purpose systems, it is sometimes difficult to know whether the origin of the failure is physical or logical; but for the consequences that follow, this distinction is usually not relevant.
I.6	**Power failure**	Cessation of power supply.
I.7	**Inadequate temperature and/or humidity conditions**	Deficiencies in the acclimatisation of the premises, exceeding the working margins of the equipment: excessive heat, excessive cold, excessive humidity.
I.8	**Failure of communication services**	Cessation of the ability to transmit data from one site to another. Typically due to physical destruction of the means of transport, stoppage or simple inability to cope with the traffic present.
I.9	**Interruption of other essential services or supplies**	Other services or resources on which the operation of equipment depends, e.g. paper for printers, toner, coolant, ...
I.10	**Degradation of information storage media**	As a consequence of the passage of time or physical conditions such as temperature, humidity, pressure, etc. To point out the growing migration of information to *cloud* environments with what this means compared to traditional media.
I.11	**Electromagnetic emissions**	The act of making internal data available to third parties via radio. It is a threat where the sender is a passive victim of the attack. Virtually all electronic devices emit radiation to the outside that could be intercepted by other equipment (radio receivers) resulting in information leakage.
I.12	**Unavailability of buildings/facilities (I)**	Unavailability of buildings or installations due to accidents of industrial origin.

ANNEX IV - GLOSSARY OF TERMS

ACL:	*Access Control List*
ANS:	Service Level Agreement
BAD:	*Behavioural analytics and anomaly detection*
BIA:	*Business Impact Analysis*
BYOD:	*Bring Your Own Device*
CISO:	*Chief Information Security Officer*
CSIRT:	*Computer Security Incident Response Team*
CSO:	*Chief Security Officer*
DCS:	*Distributed Control System*
DDOS:	*Distributed Denial of Service*
DLP:	*Data Loss Prevention*
DLT:	*Distributed Ledger Technologies*
DMZ:	*Demilitarised Zone*
TWO:	*Denial of Service*
EDR:	*Endpoint Detection and Response*
ENS:	National Security Scheme
ERP:	*Enterprise Resource Planning*
FW:	*Firewall*
GDPR:	General Data Protection Regulation (2016/679)
GRC:	Governance, Risk and Compliance
HMI:	*Human-Machine Interface*
HW:	Hardware
R&D:	Research + Development
IA:	Artificial Intelligence
ICS:	*Industrial Control Systems*
IDS:	*Intrusion Detection System*
IEC:	*International Electrotechnical Commission*

ANNEX IV - GLOSSARY OF TERMS

IoT:	*Internet Of Things*
IP:	*Internet Protocol*
IPS:	*Intrusion Prevention System*
MRI:	*Information Rights Management*
ISA:	*International Society of Automation*
ISO:	*International Organization for Standardization*
IT:	*Information Technology*
LAN:	*Local Area Network*
MONTH:	*Manufacturing Execution System*
NAC:	*Network Access Control*
NGFW:	*Next-Generation Firewall*
NIS:	*Network and Information Systems*
NIST:	*National Institute of Standards and Technology*
O&M:	*Operation and Maintenance*
OPC UA:	*Open Protocol Communication Unified Architecture*
PCI Order:	Order of the Presidency Relations with the Parliament and Equality
OSE:	Essential Service Operator
OT:	*Operation Technology*
PbD:	*Privacy by Design*
PDS:	Security Master Plan
PEAR:	*Purdue Enterprise Reference Architecture*
PIC:	Critical Infrastructure Protection
PLC:	*Programmable Logic Controller*
PTR:	Risk Treatment Plan
RBAC:	*Role Based Access Control*
RD:	Royal Decree
RTU:	*Remote Terminal Unit*

ANNEX IV - GLOSSARY OF TERMS

SCADA:	*Supervisor Control and Data Acquisition*
SCI:	Industrial Control System
SIEM:	*Security Information and Event Management*
SO:	Operating System
SOAR:	*Security Orchestration, Automation and Response*
SW:	Software
TCP/IP:	*Transmission Control Protocol/Internet Protocol*
TEE:	*Trusted Execution Environment*
ICTS:	Information and Communications Technologies
TPM:	*Trusted Platform Module*
EU:	European Union
UPnP:	*Universal Plug and Play*
USB:	*Universal Serial Bus*
VHF:	*Very High Frequency*
VLAN:	*Virtual Local Area Network*
VPN:	*Virtual Private Network*
WIFI:	*Wireless Fidelity*
WSUS:	*Windows Server Update Services*

GUIDE ON SECURITY CONTROLS IN OT SYSTEMS

Agbar

Aiuken Cybersecurity

Capgemini

Check Point SOFTWARE TECHNOLOGIES LTD.

Centro de Ciberseguridad Industrial

COMILLAS UNIVERSIDAD PONTIFICIA ICAI ICADE CIHS

Deloitte.

ecix

enigmedia

Entelgy Innotec SECURITY

EY Building a better working world

FUNDACIÓN BORREDÁ al servicio de la seguridad

gmv INNOVATING SOLUTIONS

indra

Ingenia

ISACA.

NEXTVISION Ciberseguridad Inteligente

PESI PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

REAL INSTITUTO elcano ROYAL INSTITUTE

SIEMENS

tecnalia Inspiring Business

UNIVERSIDAD DE MÁLAGA

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

OCC OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD MINISTERIO DEL INTERIOR ESPAÑA

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR