The new electricity distribution:

Cybersecurity in the digital transformation

Centro de Ciberseguridad Industrial

Naturgy Foundation

The new electricity distribution:

Cybersecurity in the digital transformation

April 2023

Centro de Ciberseguridad Industrial

Naturgy Foundation

The **Industrial Cybersecurity Center (CCI)** is an independent, non-profit organisation whose mission is to promote and contribute to the improvement of Industrial Cybersecurity, in a context in which organisations within sectors such as manufacturing or the energy sector play a critical role in the construction of today's society, as pillars of the welfare state.

The CCI faces up to this challenge through the development of research and analysis activities, generation of opinion, preparation and publication of studies and tools, and exchange of information and knowledge concerning the influence of both technologies, including their processes and practices, and individuals on matters related to the risks—and their management—derived from the integration of industrial processes and infrastructures in Cyberspace.

As of today, the CCI is the ecosystem and meeting point of entities—private and public alike—and of the professionals affected by, concerned by or dealing with Industrial Cybersecurity; and it is also the Spanish-speaking reference for the exchange of experiences and the dynamisation of sectors involved in this field.

Paseo de las Delicias, 30, 2ª Planta
28045 MADRID
Tel.: +34 910 910 751
e-mail: info@cci-es.org
www.cci-es.org

Blog: blog.cci-es.org
Twitter: @info_cci
LinkedIn: www.linkedin.com/in/centroCiberseguridadindustrial

Contents

Executive summary

The **digital transformation** is altering the processes of energy production, distribution and consumption. It is currently possible, for example, to obtain real-time data from any installation to detect potential risks and anticipate damage, or provide consumers with the information they require, also in real time, as well as being able to intervene directly in certain systems.

However, this increase in connectivity and the deployment of digital technologies also increases the need to protect critical assets against threats. In the specific case of energy, the impact of a failure in supply resulting from a cyberattack could have major consequences across different sectors, in addition to affecting end users. Precisely for this reason, one of the pillars on which the digital transformation rests is cybersecurity. This document addresses the challenges associated with cybersecurity in one of the areas that is most important in terms of energy supply: the **distribution of electricity.**

> One of the pillars on which the digital transformation rests is cybersecurity.

Electricity distribution is also a sector that forms part of a market that is changing rapidly and many of the organisations involved have been adapting to the new scenario for some time, both through developing the necessary digitisation projects and by incorporating cybersecurity, as well as purchasing new technologies and assets. Nonetheless, the sector still faces **significant challenges related to this transformation:**

- The constant integration of more renewables, mostly solar and wind power.
- Distributed generation, with the emergence of the figure of the “prosumer” and a shift in the paradigm in which the flow of energy always went in the same direction.
- Grid digitalisation, including advanced metering systems (smart grids) that allow many of the new services consumers seek to be effectively managed; assets such as novel digital substations that open up networks which have traditionally been tightly closed; or the network of charging points for electric vehicles, which require digitalised transformation centres to process consumer data and manage load distribution.

Associated with the evolution in these areas, **new challenges are appearing in the field of cybersecurity:**

- Managing new supply chains. It is becoming necessary to open up to a greater number of manufacturers in order to incorporate new technologies that will allow us to meet novel challenges, and analysing risks at different levels is absolutely vital. Every aspect ranging for design to each of the phases of the implementation of new projects must be considered, as well as the necessary adaptations and renovations.
- The assigning of new roles and responsibilities. The appearance of new actors and increased dependence on both hardware and software lead to a necessary reflection on the assignment of roles and responsibilities.
- New systems of interdependencies. These include networks, data and payment systems, communications, etc.
- Device and application security levels.
- New approaches to vulnerability management. This involves considering equipment obsolescence, continuous software updating, equipment criticality, etc.
- The role of the cloud and the design of data processing centres

> Electricity distribution faces important challenges in the digital transformation: distributed generation, new services and information for consumers, electric vehicle...

The growth in the activity of cybercriminals, coupled with their increasingly evident professionalism, makes significant investments absolutely necessary. It also intensifies the need for awareness-raising and staff training strategies, improved incident response procedures and above all, the involvement of all employees in cybersecurity. Therefore, entities in the electricity sector must work on procedures, but also on the training of personnel in addition to the strictly technological side.

Organisations within the electricity sector are already implementing a series of protection mechanisms in order to reduce their exposure to the activity of cybercriminals to a minimum. These include adopting segmentation and defence in depth, tracking all changes in device configurations, controlling access and privileges, evaluating and managing vulnerabilities, monitoring all aspects related to security, and guaranteeing service continuity together with the safety of people, the environment and equipment.

Given the importance of cybersecurity, the European Union has taken the lead by approving many **regulations on cybersecurity,** security and resilience; some with a far-reaching impact on the sector. Among these, the following should be highlighted:

- The NIS2 Directive (Directive (EU) 2022/2555 of the European Parliament, which requires critical entities to take specific security measures) includes the supply chain and makes senior management responsible for safeguarding it.
- Directive (EU) 2022/2557 of the European Parliament, on a coordinated EU-wide approach to strengthen the resilience of critical infrastructures.
- The Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements

> The Europen Union has taken the lead by approving many regulations on cybersecurity.

All of this entails necessary **investment in cybersecurity** in order to strengthen the resilience of operators and of the system, including end consumers and the new ways in which they relate to the system; as well as to maintain a coherent approach and improve service capacity throughout the EU. Undoubtedly, this investment is totally justified as it will strengthen the processes of identification, protection, detection, and response and recovery from possible threats. In fact, the costs associated with managing and restoring systems after a cyberattack would far outstrip any additional burden resulting from compliance with the regulations. These costs must therefore be adequately acknowledged when considering both investment and the operating costs resulting from continuous technological evolution.

> All of this entails necessary investment in cybersecurity in order to strengthen the resilience of the system and must therefore be adequately acknowledged.

1. Introduction

The concept of digital transformation is associated with change, with the evolution that companies undergo to improve their functioning and with offering greater value to customers through taking advantage of digital technologies. It therefore concerns all the areas of a company and provides benefits for enterprises in all sectors as well as for end consumers.

Moreover, digitalisation is transforming processes of energy production, distribution and consumption. Today, it is possible to obtain real-time data from a turbine in a power plant, from a dam sluice gate or from a substation transformer and send them to a control room where potential risks can be detected and damage anticipated before it occurs, thanks to predictive maintenance.

Similarly, the application of artificial intelligence makes it possible to identify in real time not only occasional anomalies, but also activities that can improve productivity in the medium and short term.

With regard to interventions on the ground, the Internet of Things, in its variant IIoT (Industrial Internet of Things), makes tools such as drones or robots available which are capable of inspecting electricity infrastructures, and in this way it increases precision and efficiency, in addition to eliminating or greatly reducing risks to people and environmental impact.

Furthermore, there is an increasing demand on the part of end consumers to have access to information in real time as well as to be able to interact with systems.

According to a report by the Boston Consulting Group[1] (BCG), the digital technologies that are being used in industry, including the energy sector, are profoundly transforming production. They are giving rise to new ways of defining relationships between suppliers, producers and clients, as well as between people and machines.

That same document defines the nine pillars of industrial digitalisation: big data and analytics (including artificial intelligence and machine learning); autonomous and collaborative robots; digital twins and simulation; IT/OT convergence; IIoT; cloud computing; additive manufacturing (3D printing); augmented reality; and cybersecurity.

It should be noted that cybersecurity is included as one of the key elements that must be taken into account among these cornerstones of digitalisation. The increase in connectivity and the use of standard communication protocols associated with the deployment of the technologies mentioned, leads to a greater need to protect critical assets against threats.

> The digital technologies that are being used in industry, including the energy sector, are profoundly transforming production.

In addition, cybersecurity also plays an important role in competitiveness. If we consider the profitability of production systems that can be considered as critical, a cyber incident affecting such a system would cause a direct reduction in this parameter due—at the very least—to economic and productivity losses (that is, production costs would increase and the number or quality of units produced would decrease).

In the case that concerns this document, in addition to all of this it is necessary to include considerations of how a power outage as a result of a cyberattack would affect the end consumer. What consequences would it have for the population not to have heating for their homes in winter? Or hot water? How would it affect the security of a city not to have street lighting? And what about a hospital? A cyberattack would not only affect the industrial company itself, it would also affect the millions of users and end consumers.

In this CCI document, five cybersecurity professionals from the electricity sector present views of the current risk scenario in terms of cybersecurity and its consequences for the critical sectors of a country, focusing on electricity distribution. The attackers and the types of cyber incidents to be considered are wide-ranging and sophisticated, but the potential threats can be grouped into five specific types that are described and classified in the next section.

This study also indicates what the future challenges for electricity distribution are going to be and how these scenarios require cybersecurity to be given an important role. To meet the challenges, a new model based on recognised standards and existing norms is proposed.

The reader will also find in this document cybersecurity regulations and good practices, ending with a perspective on the evolution of investment in and spending on this area by the electricity sector.

2. The current situation

The activities of cybercriminals have evolved over the years, expanding and becoming more sophisticated. In addition, as a result of the dizzying pace of the evolution that the digitalisation of the whole of society is experiencing, the potential attack surface has multiplied. This is a context that inevitably affects industry.

This chapter therefore lays out the situation that the electricity distribution sector finds itself in at present. Within this context, it describes high-impact cybersecurity incidents, classifying the most important types of cybersecurity incidents and reporting the role that Europe is playing in this scenario.

2.1. Critical sectors

When we talk about cybersecurity incidents, we are no longer dealing with a rarity. In fact, they appear on the front pages of the newspapers in every country, they are almost immediately posted on social media with thousands or millions of users, and they are discussed and debated at hundreds of events related to technology, or even totally unrelated to it.

Historically, the banking and telecommunications sectors were the most affected by attacks: banks, because they housed physical and digital money long before users had digital wallets; and telecommunications companies, because they were the access platforms for the Internet.

Today, the situation has changed greatly. There are no longer any “safe” sectors. We can see, for example, how cyber incidents affecting the agri-food sector have increased by 600% in the last year and the FBI has issued its first warnings to the sector. During the worst moments of the Covid-19 pandemic, we also witnessed cases of incidents related to the health sector: despite being such a difficult time for everyone, there were hospitals that could not use their systems and patient care was affected.

The car industry, oil giants, chemical companies, the retail sector, manufacturers, etc., absolutely all enterprises, whether they are startups, SMEs or large companies, are being affected by different types of attacks.

2.2. The electricity distribution sector

Companies in the electricity sector are certainly no exception. For several years they have been suffering incidents, and this situation has worsened in the current context of Russia’s invasion of Ukraine, when they have become targets not only of physical military attacks, but also of “cyberarmies” which try to take over control of them.

Moreover, there is an additional feature of the electricity sector that makes it quite different from the vast majority of industries: if it is affected, all other sectors will also be affected. So it becomes a potential strategic target.

It is worth noting the special case of state-backed attacks on the electricity sector. This is something that has become evident since 2021, especially over the past year, both due to the war in Ukraine and because of the repeated warnings from the American Cybersecurity Agency (CISA) to reinforce the defences of the electricity sector. We may not be able to talk of literal cyberarmies, but there certainly are groups that protect states both technically and legally, and which have the means to further specialise their attacks; also at the technical and economic level.

Since 2021, various targeted attacks have been experienced, about which much has been written given their consequences. These have served to reveal continuous activity in cloud environments which have even seen some serious incidents. Among these cases, it is worth emphasising that software updating repositories have been compromised, located on servers of providers that offer cybersecurity solutions and services to the military and to energy sectors. These types of incidents were the beginning of the concept of “attack via the supply chain”.

Regarding such incidents, CISA has issued warnings about various phishing attacks launched to obtain credentials and information of specific users. Suspicious activity has also been detected in energy system networks.

Meanwhile, in Ukraine we are seeing hybrid attacks (physical and digital), with coordinated artillery strikes and cyberattacks.

2.3. Attackers

Based on this situation, knowing the different types of attackers (better known as "hackers" in the specific terminology) that can affect industrial organisations within the electricity sector is of the utmost importance if we are to understand what organisations need to do to protect themselves. To this end, it is also important to know their motivation:

- **Hacktivist groups** mainly try to damage reputations or to disrupt operations without further damaging infrastructures, motivated by some cause they support; for example, environmental and ecologist groups, political or religious reasons, social movements making a stand for a worker or client (or type of client) who has been affected in some way, etc.

- **Terrorist groups** whose objective is to sow terror or cause harm. These directly seek to disrupt operations, but try to cause as much damage as possible to the infrastructure, even trying to make it permanently non-operational.

- **Criminal groups** that seek to obtain some economic benefit from the attack.

- **Insiders** are usually disgruntled direct or subcontracted employees who try to financially damage an organisation as retribution.

- **Opportunists** usually do not target the specific organisation in the proper sense of the word, but rather they are probing with attack techniques or even malware and they came across a specific organisation almost by accident. Their intention is not to cause damage for the sake of it, but mostly they try to obtain some benefit after having caused it.

The most typical action, in the first three cases where the attackers are usually organised groups, is to carry out an attack via an Advanced Persistent Threat (APT) in such a way that the industrial organisation that is attacked is not aware of it until it is too late. The average time it takes an entity to realise that its security has been breached via an APT is between 6 and 12 months after the attack has begun.

2.4. High-impact cybersecurity incidents

The range of types of potential attack is extremely broad and includes, for example, cases that affect the supply chain. But if we focus on more specific cases that are currently affecting companies in the electricity sector, we have the following five types:

Ransomware. This is a type of malware that encrypts the contents of computers affected and demands a ransom to allow the owner to recover access. If we were to classify the long list of companies affected by cybersecurity incidents, this would be the most common cause.

Ransomware discovered in recent years has considerable capabilities. For example, exfiltrating information over a period of time prior to encrypting the content in such a way that if the victim refuses to pay to recover their files, the extortion may vary and payment can be demanded in exchange for not making the information public.

Phishing. This is, without a doubt, the most popular method that companies use in campaigns and events aimed at raising awareness, to grab the attention of users and make them better protected; but, in turn, it is the worst enemy of cybersecurity departments, since the ingenuity of the attackers to mask their techniques, impersonating identities and trying to trick their victims into providing information or access, is truly impressive.

Fileless malware. This is malware that is mostly associated with attacks related to widespread spam and identity theft that has once again made it fashionable to infect computers without the need to have a file executing malicious activity on the system. This type of malware makes use of tools and processes within the operating system itself (for example, Powershell or WMI) without downloading additional executable files to the victim and thus making it more difficult for anti-malware tools to detect.

In general, it requires the "complicity" of the system user in order to affect the computer: the user clearly would not do this knowingly. This technique has been widely used in recent years to affect engineering stations and thus compromise equipment used to configure industrial process controllers.

Incorrect configurations or default configurations. It is important to pay special attention to configurations, especially those related to using remote services.

Exploiting misconfigured remote services is something that, at least since 2012 with search engines like ShodanHQ and other similar tools, efforts are being made to prevent by demonstrating on the Internet how easy it is to detect misconfigured computers. Nonetheless, and despite there being so much information on social networks, at events and available via digital media, this continues to be a major problem in the electricity sector.

> The electricity sector forms part of a market that is changing very quickly. This makes it necessary to reorganise internally and adapt the industrial culture.

Exploiting vulnerabilities. Just as with any type of written code, industrial control devices (such as the software used by human–machine interfaces (HMIs), SCADA servers, engineering stations and all the other components that require an operating system) have security flaws, commonly known as bugs. Previously, these security flaws were not well known by the general public and represented a significant advantage for cybercriminals as very few users had information on how to protect themselves or what impact they could have on their systems. But now they are publicly reported in different media to let all those involved in a sector know when something represents a threat, the scope of that threat and measures that can be taken to mitigate the risks.

There are specialised organisations and portals where these incidents are published, such as Mitre CVEs, CISA advisors or even the manufacturers of industrial systems themselves (as in the case of Siemens).

Nowadays, there are also many industrial systems that are linked to the Internet with communication protocols that are not always robust from a cybersecurity perspective. These therefore expose systems to attacks by experts, and also the not-so-expert. This means that attacks based on these security breaches are easier to carry out against products within the world of industrial operation technologies, but at the same time they are more complex. All of this makes it easier for attackers to achieve their goals and more complex for industrial organisations to resolve incidents if they become victims and do not have sufficient knowledge or tools to mitigate certain attacks.

Of the five types of attacks described, the first three affect users directly (regardless of their job title or position). The other two are related to technological areas themselves, where poor practices in cybersecurity management, both in design or deployment/execution and in maintenance or operation, may result in a threat materialising in the installations.

The difficulty in combating these types of attacks is not only due to their sophistication, but also sometimes to the lack of maturity in terms of cybersecurity culture and management throughout the whole lifecycle of industrial automation and digitalisation projects.

The electricity sector forms part of a market that is changing very quickly. This makes it necessary to reorganise internally and adapt the industrial culture in such a way that it becomes possible to understand that it is no longer a sector of service operators, but has become a sector of service managers. The sector must attend to clients with an ever increasing tendency towards digitalisation and with increasing demands in terms of what consumers want: to have information made available practically in real time and not simply in the periodic bill.

Although it may seem obvious, in general the regulations do not usually recognise the new costs that this generates for organisations within the electricity sector, stemming from the need to embark on digitalisation projects and also to incorporate cybersecurity, or even from the purchase of new technologies or assets which will also increase maintenance costs, and not only affect the initial investment.

2.5. Types of cybersecurity incidents and the lessons learned

As already mentioned, irrespective of the type of company or the sector, everyone is constantly at risk of attack, and the most useful tool that exists when it comes to defending oneself is knowledge itself. When an incident is made public, the problem becomes visible and it is put out in the open for discussion by other companies. Sharing the knowledge that a certain technology which was implemented was, nonetheless, not configured optimally or that the area of cybersecurity needs to be more involved in a certain project or process, has shared common benefits for the whole sector.

The work of the areas devoted to cybersecurity is complex because it is based on providing protection for internal systems, for systems purchased from third parties and for systems hosted by third parties (such as cloud services), as well as for what happens to people, cultural change, communications, roles, etc.

While we could cite many cases in the public domain that have affected companies, both large and small alike, the following examples are of the types of incidents suffered by companies in the electricity sector over the last five years:

- **Unauthorised system access.** The attacker (or attackers) gained access to sensitive information related to a limited number of company clients, including: name, personal ID number, telephone number, email address, postal or service address, products contracted and the corresponding dates, invoicing dates, tariff charged, amount and status of payments, and even the IBAN.

- **System alterations.** The cyber incident not only involved the disruption of 90% of corporate systems (mail and telephone services remained affected for weeks), but also, according to the information published, 25 years of historical data were lost from the system. Although services related to the power grid and the fibre network were not affected, the major impact that corruption of documentation had on corporate systems affected the organisation in relation to billing, customer services, historical consumption information, taxes, etc.

- **Ransomware.** Ragnar Locker is ransomware that has generated serious consequences. The literature shows that the systems of the companies affected were compromised and encrypted, and that some 10 terabytes of information was exfiltrated from one specific company. It was also made public that the ransom demanded by the cybercriminals to decipher the information on the computers and not make the incident public was around 10 million euros.

The different cases cited here and those that can be found in various reports published on the situation within the sector make it evident that the electricity sector has experienced an increase in cyber incidents and threats. It is likewise clear that it is necessary to increase investment, enhance staff awareness and training strategies, improve incident response procedures and, above all, involve all employees in cybersecurity. The examples show the importance of improving procedures and also personnel training.

In connection to this, in June 2021, the United States Secretary of Energy, Jennifer Granholm, warned: “There are thousands of attacks on all aspects of the energy sector and the private sector generally. It's happening all the time. This is why the private sector and the public sector have to work together.”

In 2017, ESET announced the discovery of potentially extremely damaging malware that targets industrial control systems, which it dubbed Industroyer, and which the company claims was behind the blackout that lasted almost an hour and a half in the Ukrainian capital, Kiev. The objective of the malware was to take control of electricity substations and interrupt power distribution, but also to damage infrastructure.

Unlike the other cases mentioned here, this ransomware was specifically designed to affect this type of industry. Last year, many researchers referred to it, although mainly to warn of the existence of a second version that is now being used in times of war.

> In general the regulations do not usually recognise the new costs that this generates for organisations within the electricity sector.

2.6. The position of the European Union given this risk situation

In light of the increase in risks and attack vectors against critical infrastructures of the European Union that has been occurring in recent years, the Union itself has approved many regulations concerning cybersecurity, security and resilience that mark a change in approach for all sectors, especially critical infrastructure, both at the European level and at that of Member States. Each country will have to adapt its regulations to the new European regulatory framework, although the configuration of this new European cybersecurity and resilience framework began back in 2019.

To make understanding of the whole framework easier, we can classify it into cybersecurity of services, resilience of critical infrastructures, product security and cybersecurity, and finally data protection. This will be laid out schematically in Section 5.3 of this document.

Specifically with regard to critical infrastructures, due to their vital importance, the following regulations should be highlighted:

- **Directive NIS2** (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148).

- **Directive (EU) 2022/2557** of the European Parliament and of the Council, of December 14, 2022, on the resilience of critical entities and repealing Directive 2008/114/EC of the Council and Council Recommendation 2023/C20/01 of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructures.

- The **proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity** requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act), which applies to products with digital elements that are introduced in the market.

3.
Current challenges

The electricity sector faces different challenges, although there are three main areas that stand out: renewable generation; distributed generation and the virtual power plant; and lastly, the digitalisation of networks.

3.1. Renewable (non-synchronous) generation

- The contribution of renewable energy production to electricity systems is increasing every day in many developed countries, and this will continue in accordance with emission reduction targets. This is producing a change in the traditional way of managing the contributions of the different energy vectors, but also in the assessing of risk associated with each such vector, with cybersecurity one of the key elements to be taken into account. In fact, photovoltaic solar energy and wind power are sources that were already born linked to the outside world.

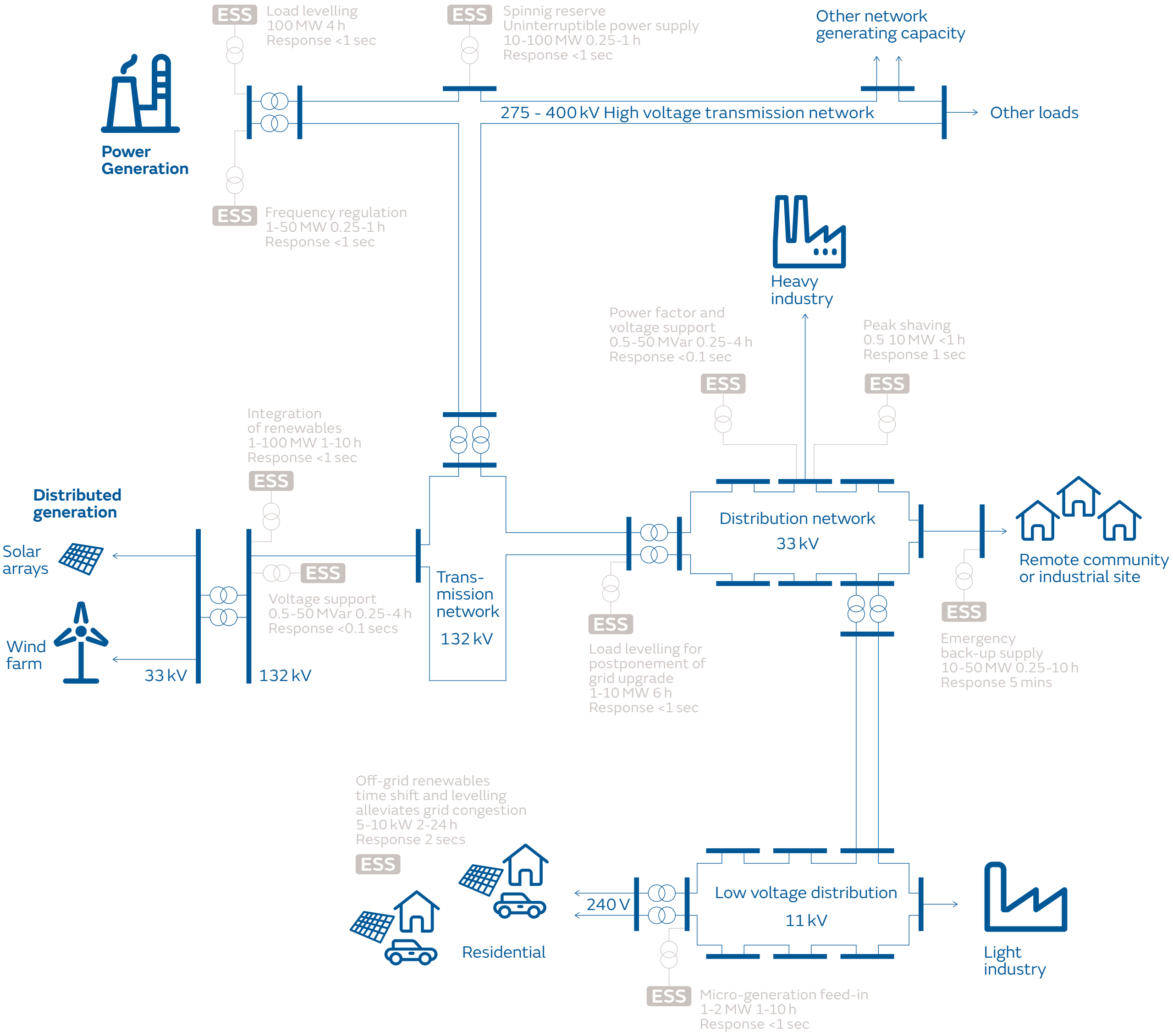
- Wind power generation was born connected to original equipment manufacturer (OEM) suppliers, mainly via satellite links—which up until 2022 were considered safe—and depends on service contracts, guarantees and maintenance over periods of several years that require the sending of data and remote access to assets.

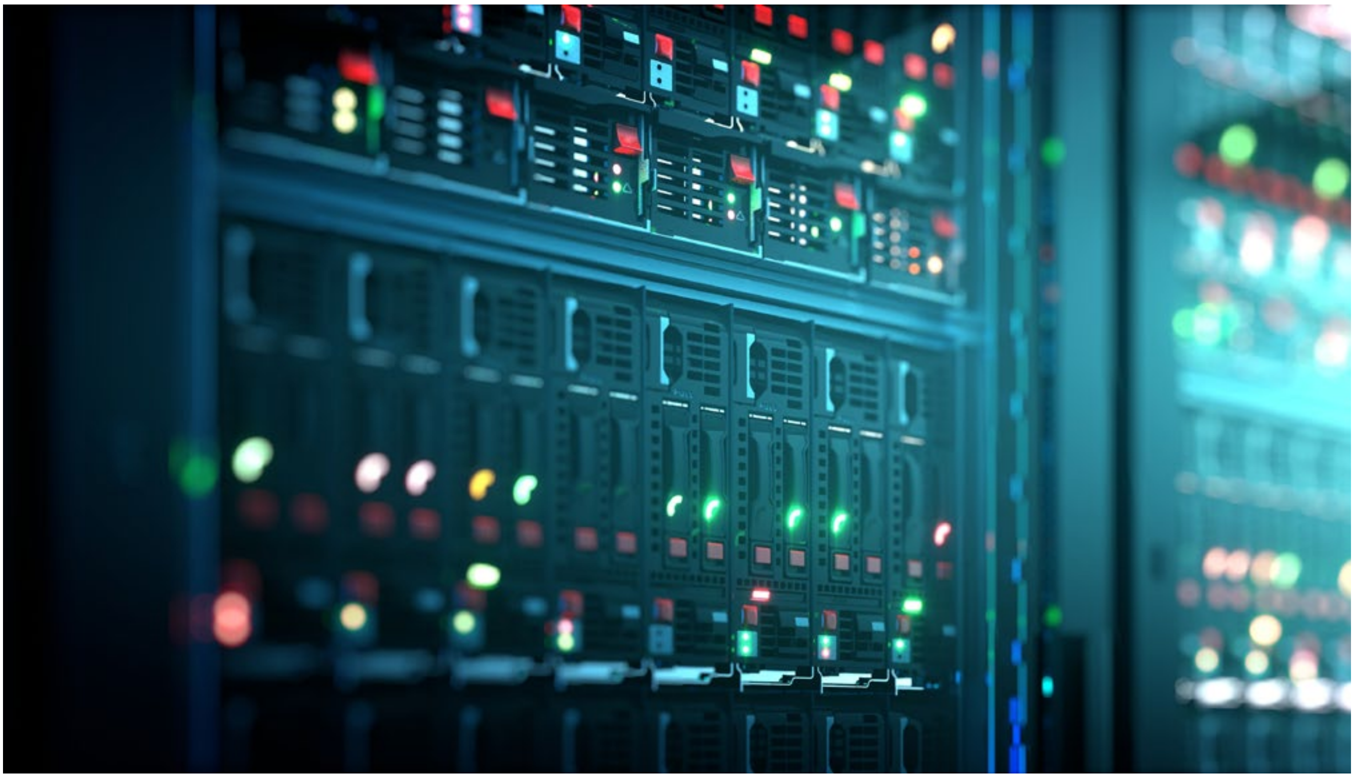
- Solar energy was born linked to the cloud, especially considering that it is a greatly changed setting where there is no longer one main technological provider—as is the case for all other technologies—but rather there are often up to four technologies (SCADA, power electronics, trackers and weather station). That said, the main responsibility rests with the integrator or owner of the asset, who in no way controls the external connections of those technologies.

3.2. Distributed generation and the “virtual power plant”

- The emergence of the figure of the “prosumer”. The paradigmatic chain of electricity generation, transmission, distribution and commercialisation in which the flow of energy always went in one direction and which had allowed knowledge of the grid, its dynamics, failure prediction and consumption forecasts is changing radically as distributed generation becomes affordable and starts to have a significant impact, not so much at the level of energy matching, but at the level of grid stability in the local setting.

Figure 1 | Schematic representation of grid energy storage systems (ESS) and applications





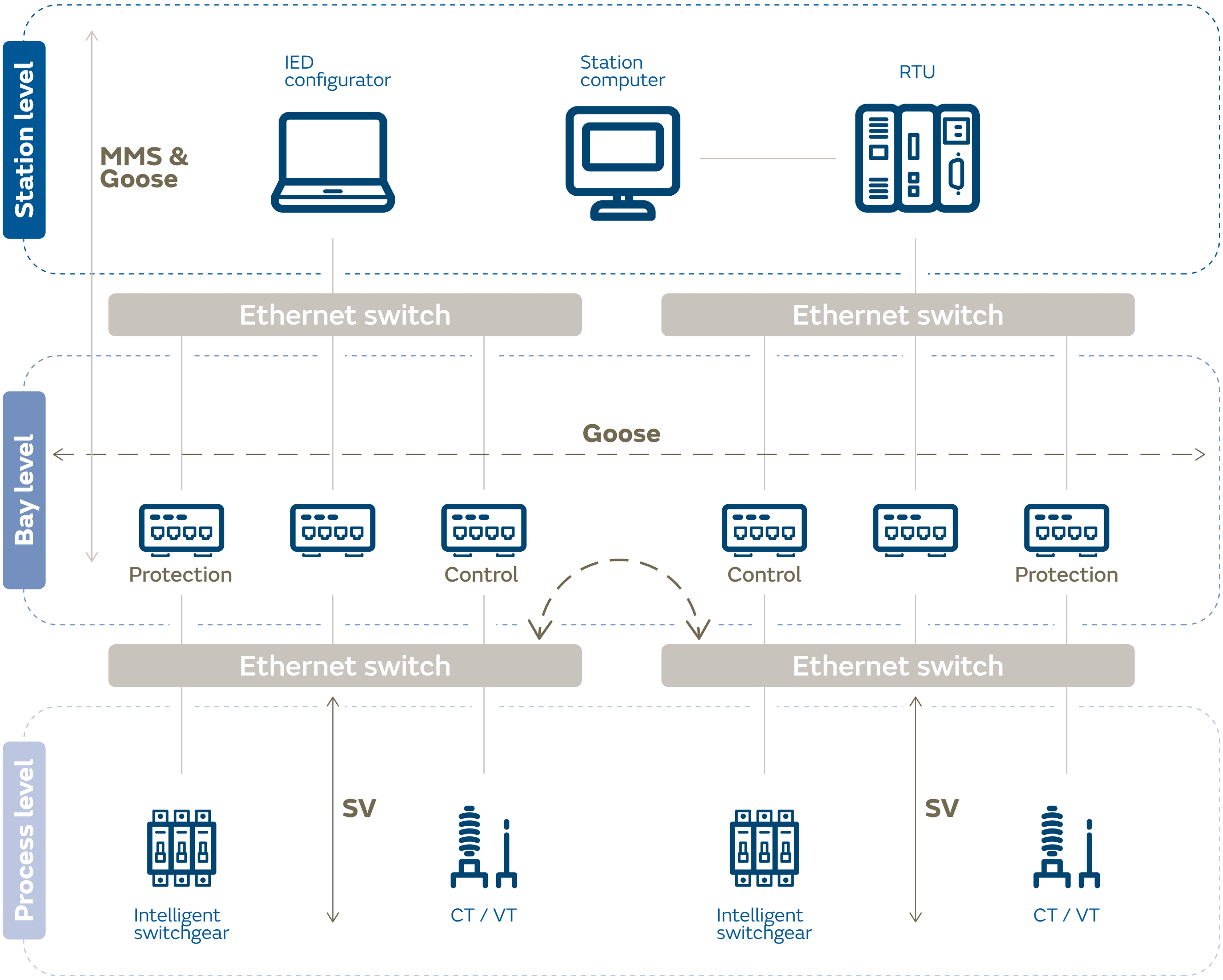
- The concept of the “virtual power plant” is on the rise, and those domestic consumers whose reference levels could be modified are considered to be a “negative” influence to be rectified, while maintaining comfort baselines. For example, turning down the air conditioning of one million consumers and changing the thermostat by just one degree could save 30 megawatts, with the consequent benefits in system stability, marginal prices and reduced emissions. However, this theoretical approach that is beginning to be implemented at a technical level once again demonstrates that the need to address the security of domestic devices and the reliability of their measurement, together with adopting these from cloud-based environments, could have an impact the electricity system.

3.3. Grid digitalisation

Smart grids. For years, electricity companies have been making large investments in so-called smart meters and advanced measurement systems. Such equipment, which offers considerable value for an adequate supply and potentially allows for the management of many of the new services demanded by consumers, also entails a need to increase communication security through encryption and security measures at the level of the application layer.

- **Distribution networks.** No one doubts the benefits in terms of operating and maintenance costs of the new digital substations, in accordance with IEC 61850. However, new challenges are emerging in terms of opening up traditionally tightly closed networks and serial communications to evolve towards Ethernet communications and allow third party access for maintenance or to send data to cloud computing environments. This has led to the development of specific cybersecurity regulations such as IEC 62351, which is being orchestrated together with the ISA/IEC 62443 standard, and which will be covered in more detail in later section below.

Figure 2 | Substation architecture in accordance with IEC 61850.[2]



- **Electric vehicles and the network of charging points.** This is a change that also brings challenges in various dimensions. On the one hand, inheriting issues mentioned before, digital transformation centres are required to process consumer data and manage load sharing. The recharging points that will be needed are fast-charging or superior, making planning requirements and concurrency coefficients to avoid overloads even more important. In addition, management models that are very different from each other are emerging: from models in which the utility owns and operates charging points, requiring third parties for supply and maintenance but treating the data internally; to charging points managed by the manufacturer, at both the electricity and data management level, who thus acts as an intermediary between users and utilities.

  For the different possibilities in between, and including these two extremes, the role of the regulator is very different. There are cases in which there is no direct regulation within the system, and others in which it is the responsibility of the system electricity operator or in which a distribution is proposed between the different operators of the system, utilities or not.

  On the other hand, the future impact, although still in its infancy, of the reversible use of energy from car batteries (vehicle-to-grid) must be considered. Although this future scenario can help to provide stability, it also poses challenges in terms of opening up types of communications between new actors.

> These new technologies make up new supply chains at the technological and cybersecurity level.

3.4. Cybersecurity challenges in these electricity scenarios

For the three areas presented here, it is clear that traditional systems need to open up and give way to models in which new opportunities are associated with new challenges that must be taken into account.

All of this entails a fundamental change in the supply chain in which the market must be opened up to a greater number of manufacturers in order to incorporate new technologies. These new technologies, such as IoT devices, are accompanied by connectivity with environments such as the cloud; and altogether they make up new supply chains at the technological and cybersecurity level that will be considered below..

- **The new digital supply chain.** This is a whole ecosystem that ranges from device manufacturers to application developers working in the cloud, and also includes firmware and device-embedded applications.

The main aspects of this supply chain will be:

  - Adequate identification of the actors in each process, their roles and responsibilities.
  - Identification of the new interdependencies between the new actors that must be taken into account.
  - The security levels to be established, at the level of device, application and system.
  - The need for a global approach to vulnerability management.
  - The adoption of a zero trust philosophy, both in the design of architectures and in their operation.

- **New schemes of roles and responsibilities.** The risks associated with the supply chain, the proliferation of actors and the dependence on both hardware and software should lead to seriously reflection and to ensuring a degree of transparency that allows us to identify those responsible for each stage of the design, operation, maintenance, provision of services and security lifecycle.

  Furthermore, the roles will not be singularly occupied at each level, as Figure 3 represents them, but different dimensions will open up at the level of firmware, applications, devices, computers, servers, communications, the cloud, etc.

Figure 3 | Schematic representation of the wind sector.

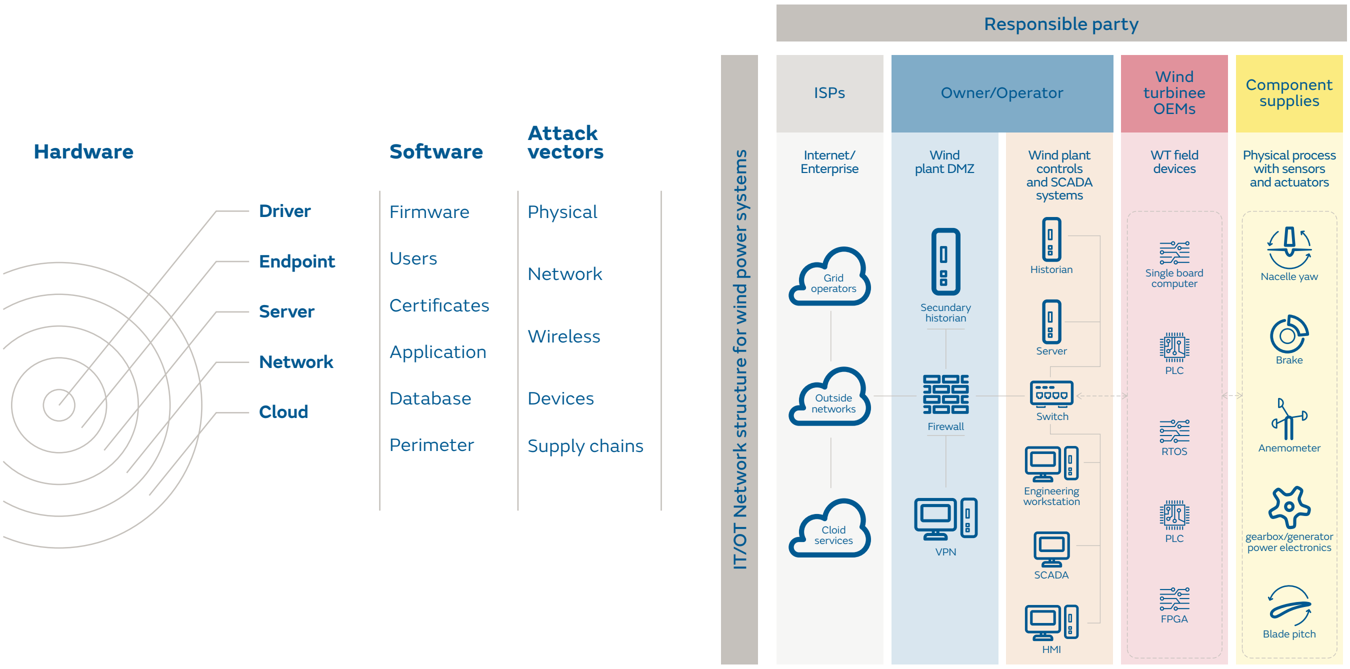
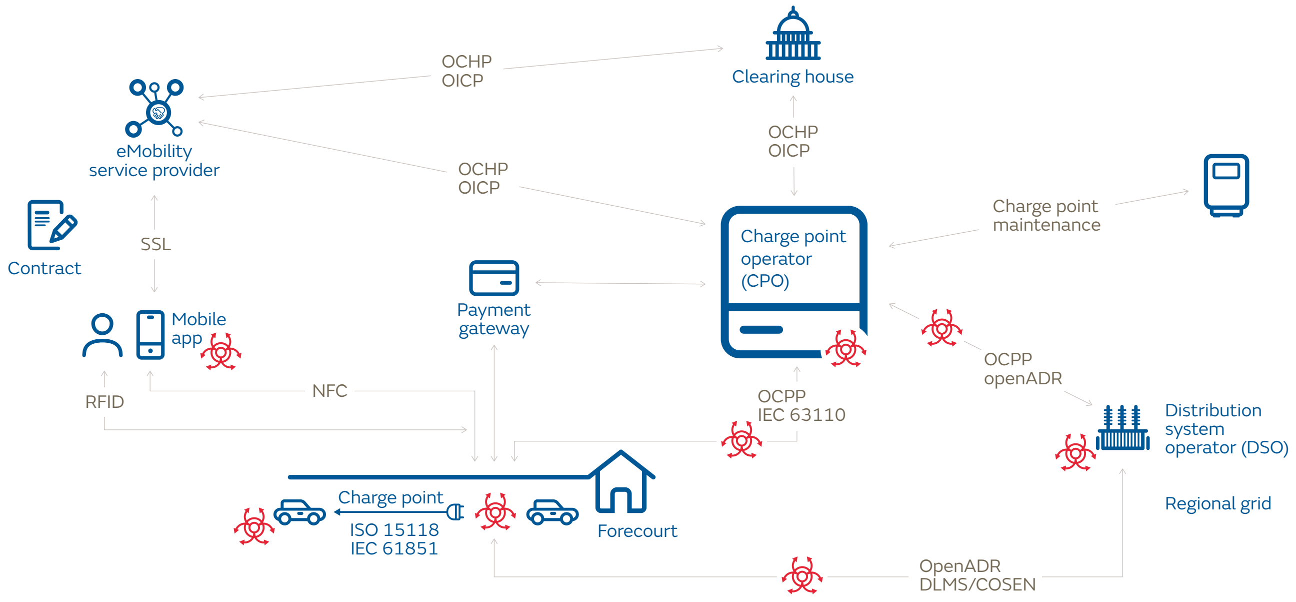


Figure 4 | Simplified diagram of the electric vehicle ecosystem.



- **New levels of interdependencies.** Figure 4 serves as an example of this. It is a greatly simplified diagram of the electric vehicle ecosystem which shows the interconnections between systems such as charging points, smart grids, distribution networks, payment gateway networks and 4G/5G networks that require a totally new approach to risk due to their complexity.

- **Security levels of devices and applications.** Traditional risk analysis is used to indicate how many security capabilities the equipment to be deployed should include. The massive surge in the Internet of Things and (commercial off-the-shelf) multipurpose automation systems obliges these methodologies to be standardised, both in terms of risk analysis and of establishing security requirements.

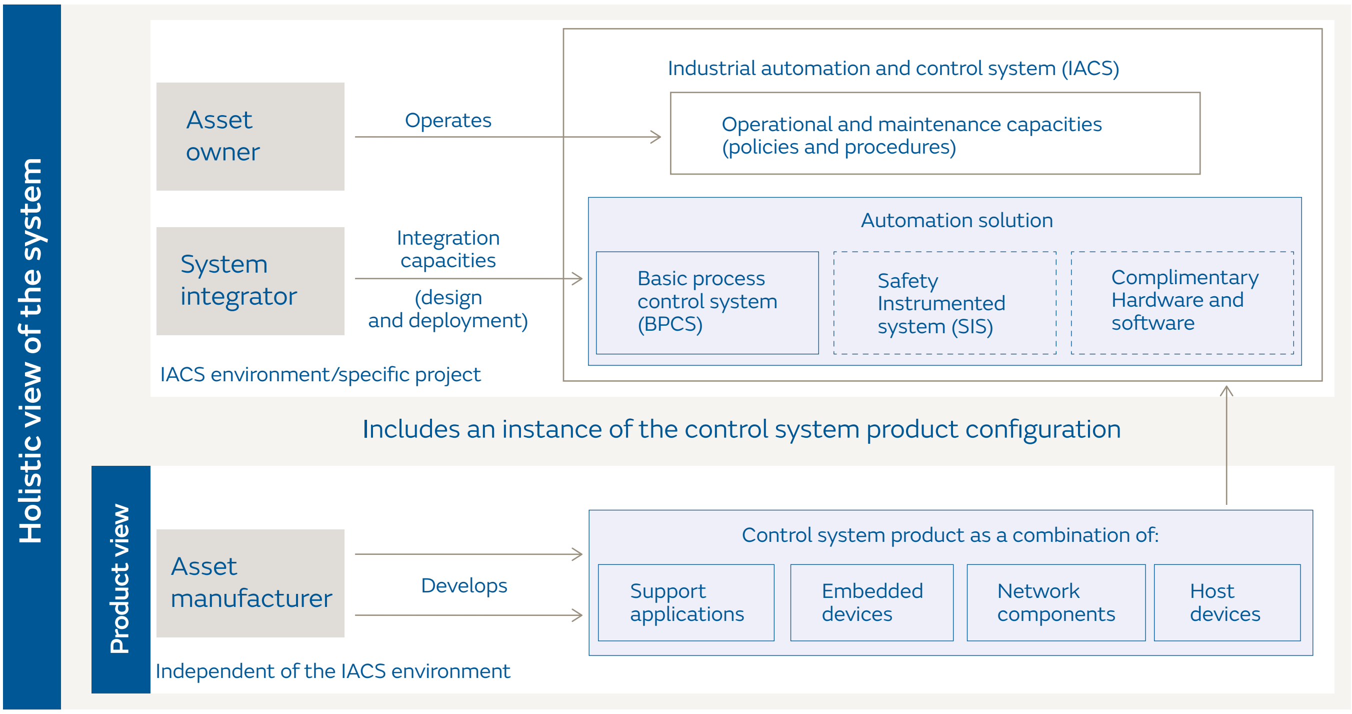
In can also be seen that carrying out an analysis considering the risk a device poses for the process is no longer effective: it is also necessary to analyse a set of threats (thousands or millions) for the entire ecosystem. By way of example, based on the previous points, consider small-scale solar panels, air conditioning equipment, aerothermal energy apparatus, domestic electric vehicle chargers, mobile phones and all the systems in which the lifecycles (and security cycles) of hardware, software and firmware are very different. As the European Union Agency for Cybersecurity already stated in 2019, the cyber risks associated with a massive event must always be considered.

Along these lines, the Cyber Resilience Act, or CRA, was recently published in Europe. Focusing on device security, it establishes a methodology whereby most of the devices cited here fall within the scope of self-assessment. In this case, manufacturers must evaluate a series of criteria and show compliance with them.

More specific devices and systems are classified as “critical” either in “Class I” or in “Class II” and these require third-party evaluation. All systems traditionally associated with critical infrastructures will be considered within Class II; however, it would be extremely expensive for all such devices to pass through a certification scheme. In this regard, positions adopted at the sectoral level will be key in order to allow the main actors in this new supply chain to combine criteria and requirements. Meanwhile, it is important to highlight the development of the ISA/IEC 62443 (4-1 and 4-2) standard, which provides cybersecurity levels and requirements for all industrial devices whose intrinsic safety aspects typically vary across large ranges. Therefore, it has become an ideal basis on which to establish the required sectoral model.

It is essential to bear in mind the role and responsibility of each of the different actors in the supply chain, where we will encounter the manufacturer of the asset who develops the technological product, applications and devices, and who must contemplate cybersecurity capabilities as well as configuration and integration recommendations. There is also the systems integrator, who designs the architecture and also deploys and configures the technologies. The third role is the asset owner, who operates and maintains the automated process technologies.

Figure 5 | **Holistic cybersecurity for IACS (ISA/IEC 62443 2-4:2015).**


Holistic view of the system
Asset owner
Operates
Industrial automation and control system (IACS)
Operational and maintenance capacities (policies and procedures)
System integrator
Integration capacities
(design and deployment)
Automation solution
Basic process control system (BPCS)
Safety Instrumented system (SIS)
Complimentary Hardware and software
IACS environment/specific project
Includes an instance of the control system product configuration
Product view
Asset manufacturer
Develops
Control system product as a combination of:
Support applications
Embedded devices
Network components
Host devices
Independent of the IACS environment

- **New approaches to vulnerability management.** There has always been talk of obsolescence as a key aspect of the electricity system given the goal of durability behind the design of all the equipment. However, many cases occur in which it is new computers that experience more notifications of security issues. Although this is due to improvements in the more mature versions of product security programs, it is also becoming apparent that there are technical difficulties in maintaining software updating cycles without affecting critical services.

So, the approach adopted is changing. On the one hand, it must be based on metrics that take into account the large number of new devices. And on the other, on prioritisation in terms of two dimensions: the situation of those assets that are most critical for the system and the situation with regard to existing weaknesses.
Finally, it is worth mentioning the use of technologies such as virtual patching, the virtual layer of security applied to industrial devices to prevent malicious code from reaching them, allowing adequate mitigation without losing process availability.

- **Proper understanding of the role of the cloud.** It is a reality that the cloud is present in the electricity sector to a greater or lesser extent; and it is important to foster an understanding of how to work with it.

  Cloud service providers have realised that the location of the data processing centres (DPCs) is a key aspect, and for this reason they are expanding the number of regions across the globe where they are present.

  In this way, cloud service providers are deploying their own technologies in the DPCs that belong to the utilities, thereby shedding some light on certain doubts regarding security standards or business continuity.

  However, it is essential to understand that the cloud is not a case of all or nothing. All cloud adoption models bare their share of the responsibilities. An example of this is the Amazon Web Services scheme which contemplates the distribution of responsibilities with respect to a critical IT service.

> It is essential to bear in mind the role and responsibility of each of the different actors in the supply chain.

- **Dealing appropriately with zero trust.** While there may be much talk of zero trust for data protection, information classification, access privileges and user characterisation, this philosophy must also be appropriately transferred to OT environments, with all the complexity that this entails.
  Taking on board this philosophy in this kind of environment will lead to a greater degree of transparency and visibility at all the levels already indicated, in such a way that everything is perfectly identified, validated, continuously verified and, of course, associated with a specific identity: from a laptop or cloud service to the industrial equipment.

  Therefore, associating identity control at points of access to industrial networks to the use of third-party devices, protocols and applications, will involve considerable effort and the deployment of inventory visibility technologies. But it will also make it possible to reduce the area of exposure to a level not previously achieved.

4. The model currently being implemented

Given all this, it is important to establish which components are necessary in the new model of electricity distribution. These include the regulations that affect it and the bases of the model from three points of view: human, legislative and technological.

4.1. Considerations, standards and regulations

The electricity sector in general is considered a critical national infrastructure because it provides a service that is essential for the functioning of our current society, especially given its increased use in the digital environment in which we live. Moreover, cyberspace has become the fifth theatre of war[3].

On the other hand, supporting national cybersecurity is the responsibility of everyone, not just of the state.[4] Therefore, every organisation in this sector should design its industrial cybersecurity model considering the elements required across three dimensions: people, processes and technologies. The goal is a model that allows assets to be protected via a security architecture that takes into account the regulatory aspects of their geographical locations, but that goes much further, starting with an assessment of the security requirements of each installation and field device according to its level of risk and importance for the electricity system of the country or region in which it operates. It should even consider coordination with public entities and security, regulatory and control bodies.

A few years ago, there were no elements to guide the development of a digital security model or an industrial cybersecurity management system that effectively responded to the needs of the electricity sector. Today, in contrast, a cybersecurity model for the transmission and distribution of electrical energy must take into consideration several relevant international standards that can be used in its development and which cover the different needs of industrial processes within the framework of the security requirements of the different stakeholders within the organisation to which they belong.

For this reason, a model should start by considering the risk management elements that can be found in the ISO 31000 regulations and develop the elements of the management system in accordance with ISO/IEC 27001 and the set of regulations contained in ISO 27000[5] to achieve integration into the digital security management system of the organisation with emphasis on analysis and the application of the technical references in ISO/IEC TR 27019.[6] But this is only the starting point for an environment that must evolve to genuinely protect the critical infrastructure for which it is responsible. Therefore, application of the NIST Cybersecurity Framework[7] provides important elements for the structuring of an industrial cybersecurity plan, since it helps us to consider identification, protection, detection, response and recovery in case of incidents.

But when we specifically aim to protect in an industrial setting, we must consider specific standards such as the set of standards ISA/IEC 62443. And when we are dealing with the electricity sector, that protection must take into consideration elements that are contained in commonly accepted international regulations, in NERC CIP regulations and specific standards such as IEC 62351.

For the distributed generation scenario and the changing context generated by the new reality of distribution networks with users who area “prosumers,” the models must be adapted to this reality and take on board that each part of the chain must be protected, if possible by design, to guarantee the security and resilience of the system.

All these regulations will guide the development of a complete model that considers the human, technical and procedural implications necessary for its creation and operation over time.

4.2. The bases of the management model

Every model is built on several cornerstones; and models related to the novel electricity distribution scenario are no exception. In this case, it is important to highlight the human, regulatory and technological dimensions, which constitute fundamental building blocks that support each other, and which will now be addressed.

4.2.1. Human dimension

The human dimension must be the basis of an industrial cybersecurity model for distribution, since all stakeholders must be aware of the threats and risks that are present in the setting. They must also support the reduction of vulnerabilities and particularly those which each person can influence in order to prevent them from being exploited to carry out effective attacks against the service or the organisation itself.

It is also vital to understand that achieving cybersecurity objectives is a joint responsibility that has to be addressed from senior management as a team together with those responsible for security, operations, maintenance, manufacturers and integrators. To this end, it is necessary to move beyond just awareness and to internalise the knowledge and skills required by each person according to their role.

The training of personnel must similarly include verification and simulation scenarios which make it possible to demonstrate that each person has the necessary skills and knowledge necessary to rise to the challenge and respond in a timely and effective manner to situations that may occur.

4.2.2. Regulatory dimension

This dimension is related to establishing a cybersecurity management system with an approach based on the risks of the industrial setting and which allows the initial level of risk level to be reduced to one that is acceptable to the organisation.

It is framed within the regulations that are to be applied in the geographical area where the facilities are located and in accordance with the norms and standards commonly accepted in the industrial setting.

It is therefore necessary that the different parties know and apply the principal norms and standards that facilitate a safe operating environment for their organisation. This is especially important when providing essential electricity generation, transmission and distribution services.

This section presents some recognised norms and standards that will help the reader to establish, maintain and monitor a cybersecurity management system that is applicable to industrial settings and adopting an international focus.

For this, the most important standards that allow for the identification, analysis and evaluation of risks (ISO 31000) are described, together with the standards that allow a set of controls to be established that are commonly accepted as the minimum expected within an organisation (ISO 27000). Later, standards that must be considered by an organisation categorised as critical infrastructure are incorporated (NIST CSF), as well as the specific guidelines for national smart grid environments (NIST) and those associated with the control of industrial scenarios (ISA/IEC 62443).

> The human dimension must be the basis of an industrial cybersecurity model.

These guidelines, regulations and standards must be applied in an effective and integrated manner, as mentioned in the section corresponding to the human dimension, by trained personnel, with skills and experience in industrial cybersecurity and knowledge of the electricity sector and the setting in which implementation is required, in order to achieve effective harmonisation, implementation in the specific setting and acceptance within the culture of the organisation.

The norms are the following:

ISO 31000. This is aimed at managing the risk that organisations face when integrating risk into all their decisions, activities and functions.

To develop an industrial cybersecurity model correctly, a risk analysis is required. By using the set of ISO 31000 standards as a basis, it is possible to follow the methodology they use, which can be integrated into the other management systems of the organisation and with the risk analysis in other areas. Through analysis of the organisational context and business criteria, it is possible to identify, analyse, assess and define strategies to treat them while establishing communication and consultation strategies within the organisation and the review and improvement mechanisms required to maintain them at an acceptable level for the institution.

ISO 27000. The ISO/IEC 27001 standard, which develops the information cybersecurity management system, builds on ISO 27002 to establish controls. But in the case of process control systems in the energy sector, the technical reference document ISO/IEC TR 27019 can be used, which applies directly to the process control systems used by the energy industry to control and monitor the production or generation, transmission, storage and distribution of energy and for the control of the associated support processes. Furthermore, it includes a requisite to adapt the risk assessment and treatment processes described in ISO 27001:2013 to the specific guidelines of the energy services sector in a better way.

Therefore, the development of an industrial cybersecurity system that can be integrated into the security management system of the organisation should be considered. It should also be guided by the ISO/IEC 27001 standard, which allows the system to be established taking into consideration the organisational context and the requirements of stakeholders, establishing management's commitment to the development of the plan in accordance with the risks and including the requirements to manage operations and support, to evaluate the system and improve it according to the findings.

NIST CSF. At its core, the NIST Cybersecurity Framework (NIST CSF) for improving the cybersecurity of critical infrastructures establishes the need to maintain the functions of identification, protection, detection, response and recovery in order to achieve effective cybersecurity management in the face of possible attacks.

Since this framework was specially designed for the protection of critical infrastructures, it can be seamlessly applied in the design of the protection model for the new electricity distribution scenario. This framework calls for reflection on the activities that we must take into account at each of the stages. Today's systems cannot only consider prevention, but must be ready to detect cyberattackers early on within a setting, respond before they have a significant impact, and recover in a way that provides the operations with resilience while maintaining essential services.

NIST Guidelines for Smart Grid Cybersecurity. These NIST guidelines[8] help in visualising the cybersecurity environment required in energy smart grids, with all their particularities. In addition, they allow the controls in this type of network to be mapped in accordance with cybersecurity objectives, selecting requirements according to the risks identified and they allow for responses to both regulations and standards as well as the existing cyberthreat setting. And they achieve all of this while taking into account the level of impact at each point.

The requirements range from access control and training to testing and certification of smart grid cybersecurity. Different procedures and technical elements are considered, as are others relating to management of personnel and governance.

IEC 62351. This cybersecurity series of protocols for smart grids is a set of standards that includes cybersecurity technologies for some of the most important protocols in this area, including DNP3, ICCP GOOSE and the common information model, CIM. It defines the cybersecurity requirements for the operating environment, including objects for network and system management, role-based access control, cryptographic key management, and security event logging. It is possible to reuse the standards, which facilitates interoperability.

Some of the technical reference documents for these standards, which are especially important for the development of new protection models, include IEC/TR 62351-12, which focuses on the resilience of power systems with distributed resources, as well as the essential architecture controls defined in IEC/TR 62351-10.

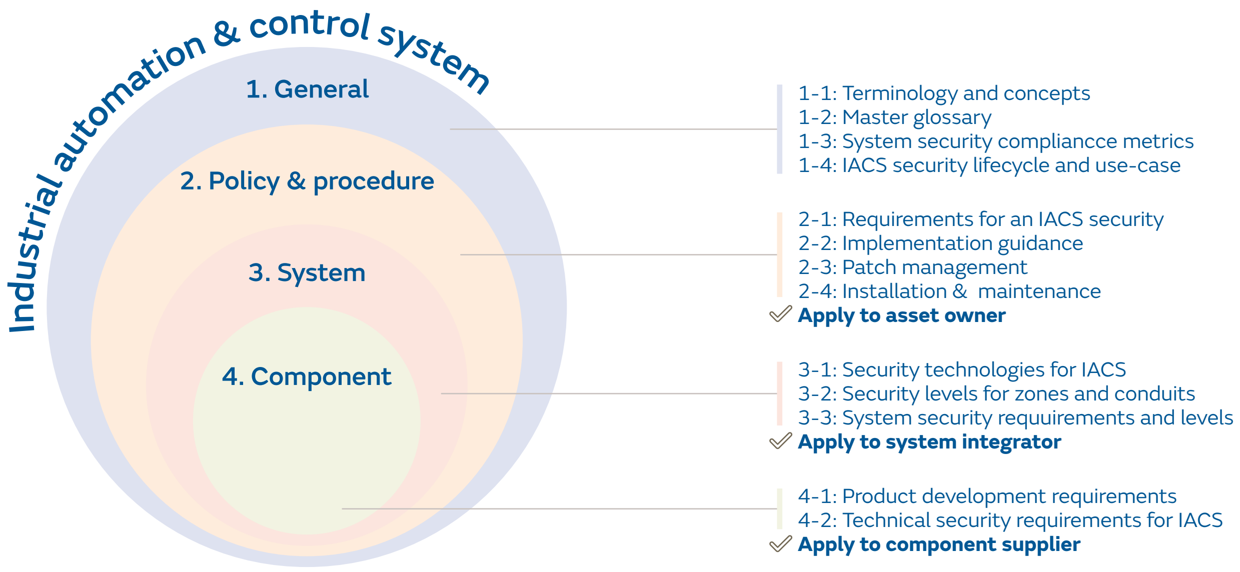
IEC 62443. ISA/IEC 62443[9] is an international standard for cybersecurity in industrial systems that focuses on the availability and integrity of systems. It is based on the principle of "defence in depth", which consists of providing different layers of security to prevent threats suffered by one layer from easily spreading to others and affecting critical assets. Each layer establishes an additional defence strategy and assumes that the preceding one could have been compromised. It must be implemented via a risk-based approach.

This standard identifies three instances that influence operational industrial processes: device and equipment manufacturers, system integrators, and system operators. It also provides a holistic approach for greater security and at the same time takes into consideration the different actors.

The standard was developed to protect industrial automation and control systems (IACS) and industrial communication networks through a systematic approach. It is organised into several documents, including: IEC 62443-1-1, which defines the terminology, concepts and models for IACS security; IEC 62443-2-1, which determines the elements necessary to establish a cybersecurity management system; IEC 62443-2-3, which describes the requirements for asset owners and IACS providers, and those who deal with patch management in the industrial setting; IEC 62443-3-3-1, which outlines various cybersecurity categories, inputs into the control system, the types of products available, and recommendations and guidelines for the use of these products; and IEC 62443-4-1, which provides requirements for secure product development lifecycles. It also includes IEC 62443-4-2, which is based on detailed requirements for control system components associated with the seven foundational requirements: identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events and resource availability.

The standard is organised as shown in Figure 6.

Figure 6 | **The scope of IEC 62443 standard.** Source: Alter Technology



1-1: Terminology and concepts
1-2: Master glossary
1-3: System security compliancce metrics
1-4: IACS security lifecycle and use-case

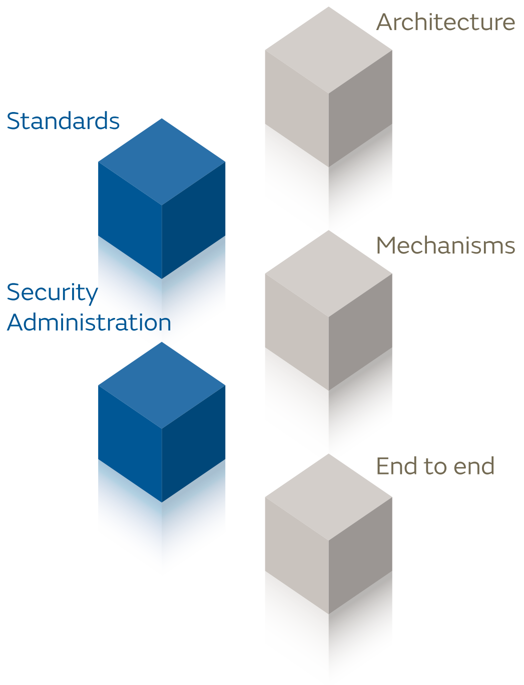
2-1: Requirements for an IACS security
2-2: Implementation guidance
2-3: Patch management
2-4: Installation & maintenance
✓ **Apply to asset owner**

3-1: Security technologies for IACS
3-2: Security levels for zones and conduits
3-3: System security requuirements and levels
✓ **Apply to system integrator**

4-1: Product development requirements
4-2: Technical security requirements for IACS
✓ **Apply to component supplier**

Considering all the requirements, elements and aspects included in IEC 62443, the energy sector is increasingly adopting this group of standards in order to reduce and mitigate technological risks in industrial settings.

Figure 7 | Technological dimension



4.2.3. Technological dimension

The technological dimension (see Figure 7) is another cornerstone of the model and should contemplate the implementation of protection mechanisms, beginning with the definition of a base architecture in accordance with industrial cybersecurity and information security norms and standards already identified in the regulatory dimension. After this, a defence-in-depth model will be built, establishing layers of protection that allow authentication and monitoring of access to supervision and control devices; monitoring of any change in device configurations; implementation mechanisms to guarantee the absence of malware; the best security practices defined by the manufacturers to be applied; and complete platform support.

The design of an adequate security architecture for these environments must consider the implementation of passive control measures such as firewalls and anti-malware systems, together with active measures such as intrusion detection and prevention systems that contain intrusions and signal their presence. These technologies should not affect the operational processes, so operation availability and continuity must be the priority.

Below are examples of some best practices recommended for technical protection:

- **Segmentation and defence in depth.** To guarantee the security of industrial control systems, it is essential to implement different layers of protection that allow for the development of defence in depth. These systems should be seen as high-security islands, separated from other company networks (such as administrative areas), as well as from supplier networks and external parties via control mechanisms.

> Monitoring of security aspects and communication networks in secure areas must be continuous: 7 days a week, 24 hours a day, 365 days a year.

It is important to design this segmentation taking into account the zones and conduits based on the IEC 62443 standard, where a zone is a logical or physical grouping of industrial assets (equipment, applications or information), which share the same security requirements; and a conduit groups together the communications that allow the transmission of information between different zones.

It is advisable to create an industrial DMZ, which will be the layer in charge of allowing the secure exchange of information between the industrial network and the corporate network, providing protection while limiting automation traffic. The servers and services that are exclusive to the industrial network are housed in this layer.

- **Strengthening.** The best security practices defined by manufacturers and specialised cybersecurity centres must be used from the initial configuration of all infrastructure components and verified during their lifecycle.

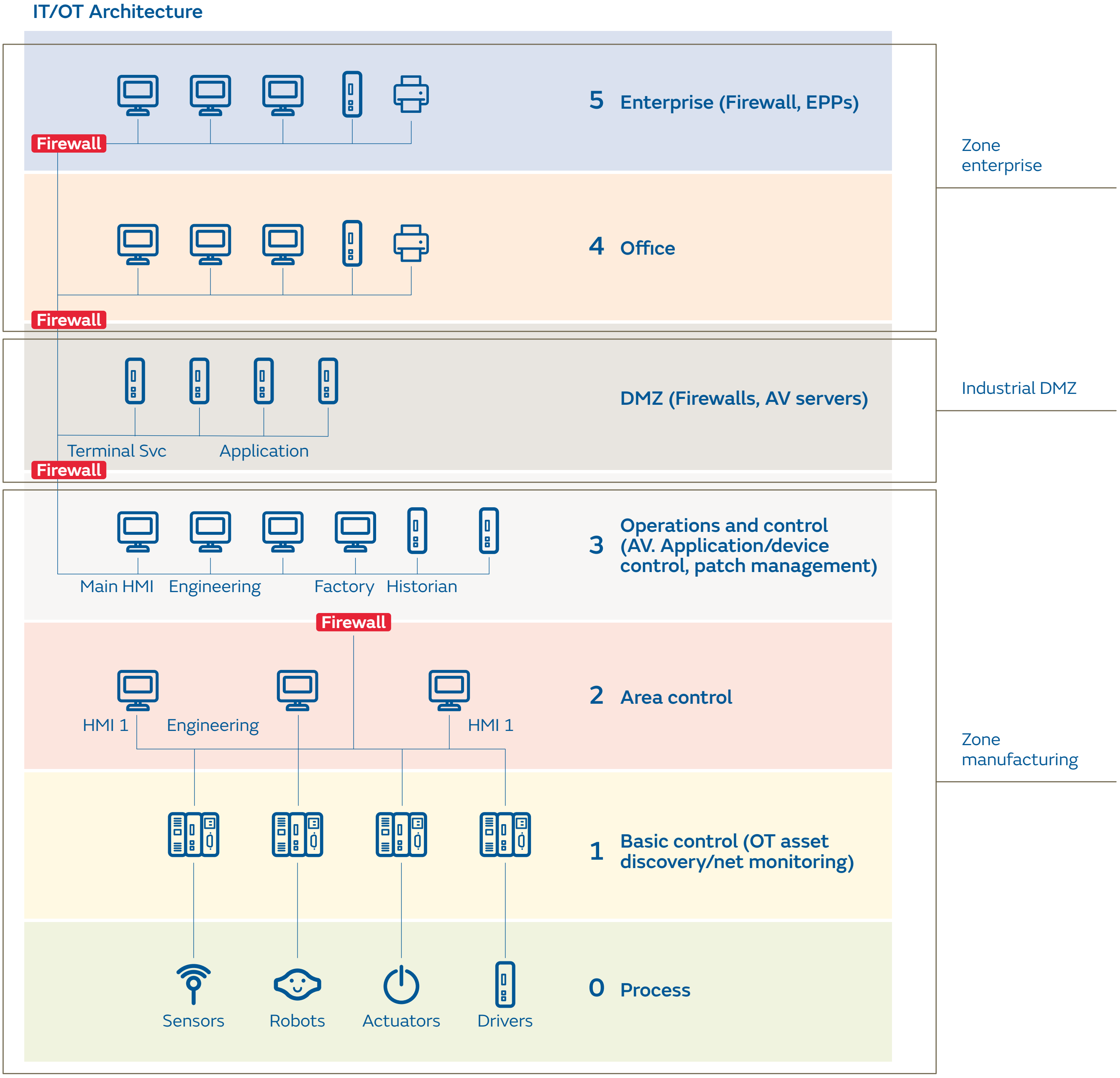
- **Configuration control.** Follow-up of any change in the configurations of the devices must be established to determine whether they are authorised; and if any anomalies are detected, they must be investigated as possible cybersecurity incidents.

- **Access and privilege control.** Access to supervision devices, and especially to control devices and remote access, must be authenticated, limited, monitored, and recorded for future investigations. This must be done in such a way that it allows identification of both attacks and improper or inappropriate actions by users, administrators, remote supports and third parties concerning the different management needs of the platform. Access to these systems should only be granted through secure mechanisms and only specific people and technologies should be granted access, according to the need to know and following the principle of least privilege.

- **Remote access control.** Remote access must be gained via control points that guarantee no unauthorised people or devices, or those which are contaminated, intervene in the infrastructure controlled by a “bastion” (jump-box), which is required for remote access to computers within the industry network. The industrial network has to log all the actions carried out within it.

- **Anti-malware management.** Mechanisms that guarantee the absence of malware within the network or devices must be implemented wherever possible, taking care that their automated actions can never affect service provision. Here, too, whitelists of applications have to be assessed.

Figure 8 | **Purdue Model.** Source: Gartner.



- **Vulnerability assessment and management.** The assessment of platform vulnerabilities must be constant and performed by passive means that do not affect operational capacity or integrity. It must also be performed periodically by active methods that can be synchronised with maintenance windows to keep the infrastructure as clean as possible through the implementation of the required patches offered by the manufacturers as soon as possible.

- **Monitoring.** Monitoring of security aspects and communication networks in secure areas must be continuous 24-7-365, specialised and with an understanding of industrial protocols in such a way that it allows centralised analysis and verification of any anomalies that may occur. Monitoring should not introduce traffic to control networks. In addition, real-time response mechanisms and personnel must be in place.

- **Continuity and resilience.** Full platform backup must be a priority. So too must verification of the backup, continuity and resilience mechanisms that have been designed to guarantee the continuity of the service and the safety of personnel, the environment and the installations.

4.3. Building the model

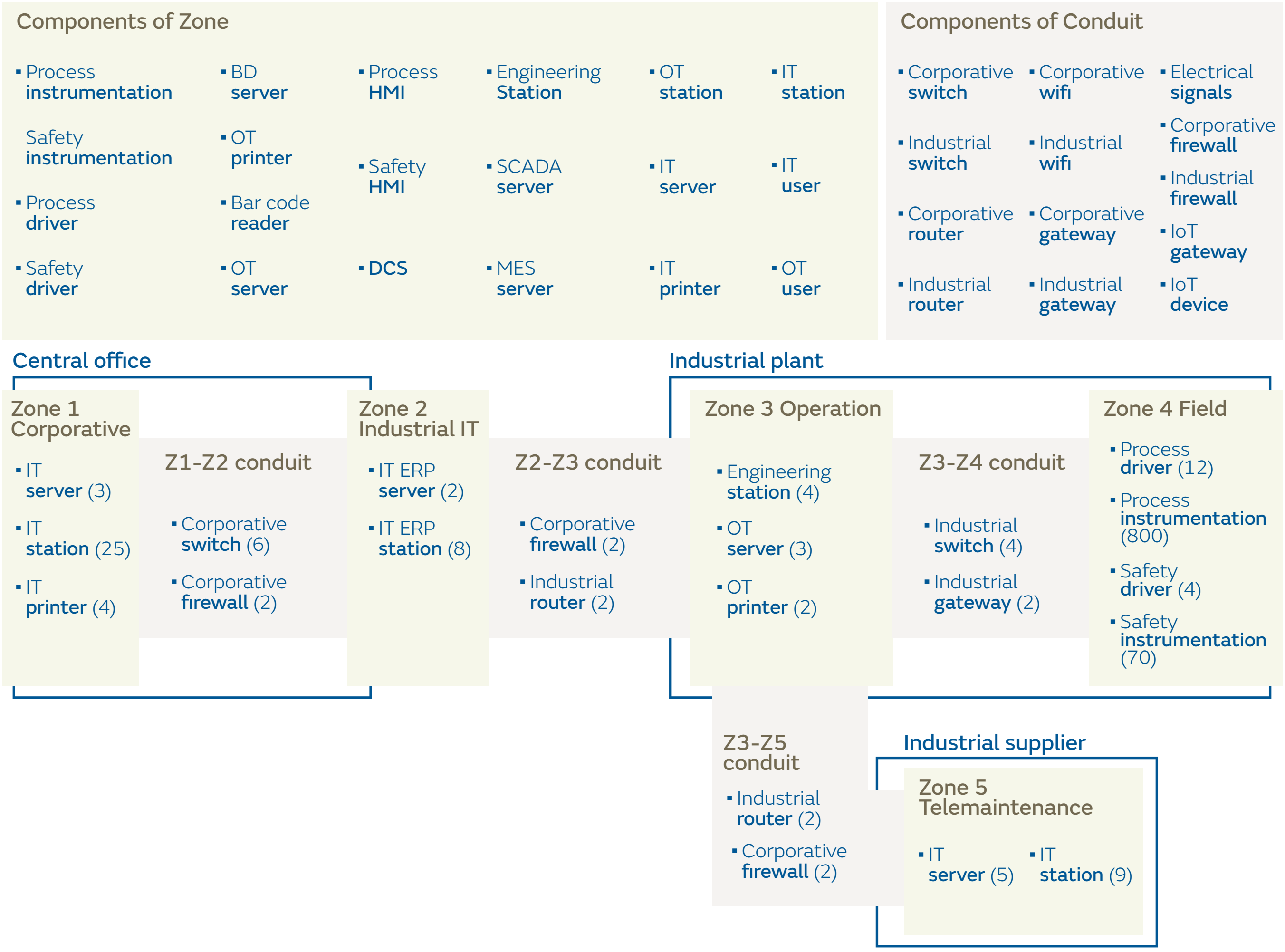
As already noted, when thinking of a model for the new electricity distribution scenario, we cannot only consider a model that is specific for the facilities needed to distribute power to consumers. Rather, we must think of protecting the entire chain, which sometimes acts as delivering to a consumer and at other times as a receiving from a producer. This adds significant complexity to the model but we can reduce it if we work on applying security by design and in each of the phases of implementation of new projects, as well as the necessary adaptations and renovations.

In various countries, regulations and technical standards have been established that include the definition of cybersecurity of energy meters, smart grids and devices that facilitate data exchange with measurement management and control centres. This is an element that must also be considered in the model to achieve complete protection of the electricity distribution scenario all the way to the points of consumption.

Protection of control centres in the electricity distribution setting and of the various field devices in substations can benefit greatly from the methodology proposed in the IEC 62443 standard. This standard makes it easier to identify the zones of these components with their appropriate security levels according to the threats they are exposed to and the conduits that allow the exchange of data, applying the principle of "defence in depth" to offer different layers of protection.

Just as with the growth of Industry 4.0, the convergence between IT and OT is absolutely essential in order to extract data from industrial control and supervision systems and manage it via IT for decision-making or management. Therefore, the cybersecurity model must include the aspects necessary to protect industrial networks and systems from attack vectors that may propagate via the IT network.

Figure 9 | **IEC 62443 zones and conduits.** Source: Industrial Cybersecurity Center.



To this end, the Purdue Model and the IEC 62443 standard separation into zones and conduits represent a fundamental basis that facilitates the definition of layers of protection for industrial systems by defining several levels at which cybersecurity measures will be applied, both in the systems at the OT levels (0, 1, 2 and 3) and at the IT levels (4 and 5), in order to provide protection for IT and OT convergence.

At each of the levels of this model, and of the zones and conduits, the appropriate cybersecurity measures must be defined, based on risk assessment and the definition of the target level to be reached.

To define the necessary measures, the following steps must be followed:

1. Evaluate the cybersecurity capabilities of each component or subsystem, considering the seven foundational requirements and contrasting each one with the cybersecurity requirements the standard presents.

2. Determine the target level of cybersecurity that you want to achieve (see Figure 10).

3. Determine the cybersecurity level achieved by each component or subsystem and determine whether it exceeds or is below the target security level.

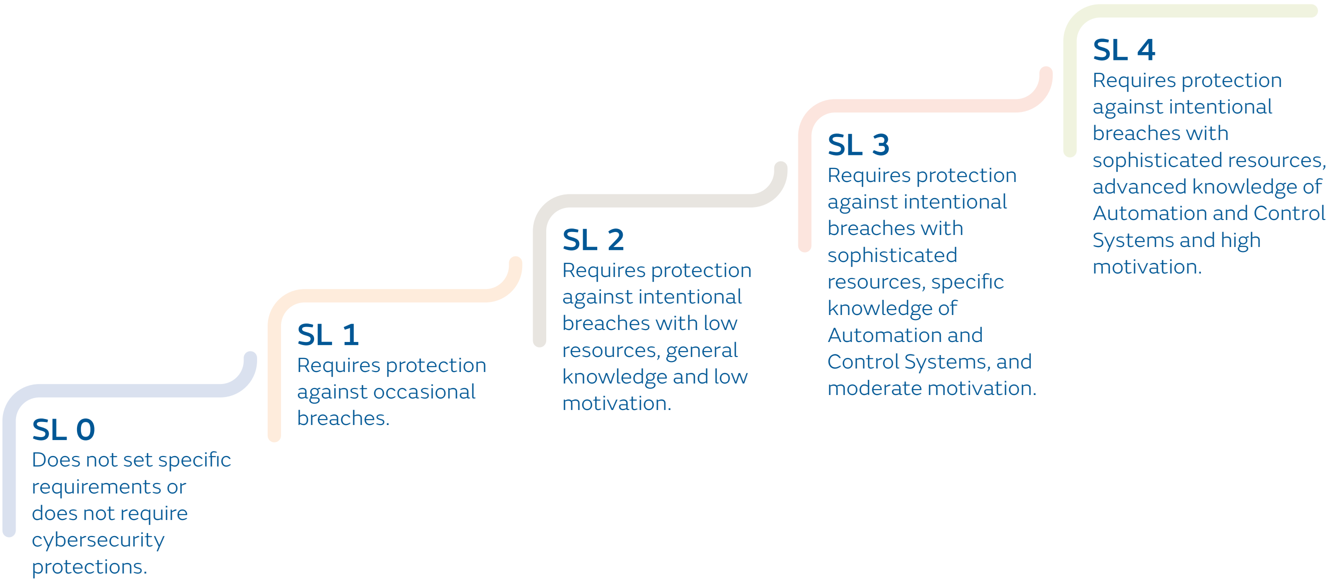
4. For components that do not reach the target cybersecurity level, compensatory measures should be considered to reduce the gap.

5. Carry out risk analysis on the components or systems that exhibit a shortcoming in order to determine priority in the implementation of correctional measures.

6. Define the action plan and implementation schedule.

7. Reassess the components and systems.

Figure 10 | **Cybersecurity levels.**



SL 0
Does not set specific requirements or does not require cybersecurity protections.

SL 1
Requires protection against occasional breaches.

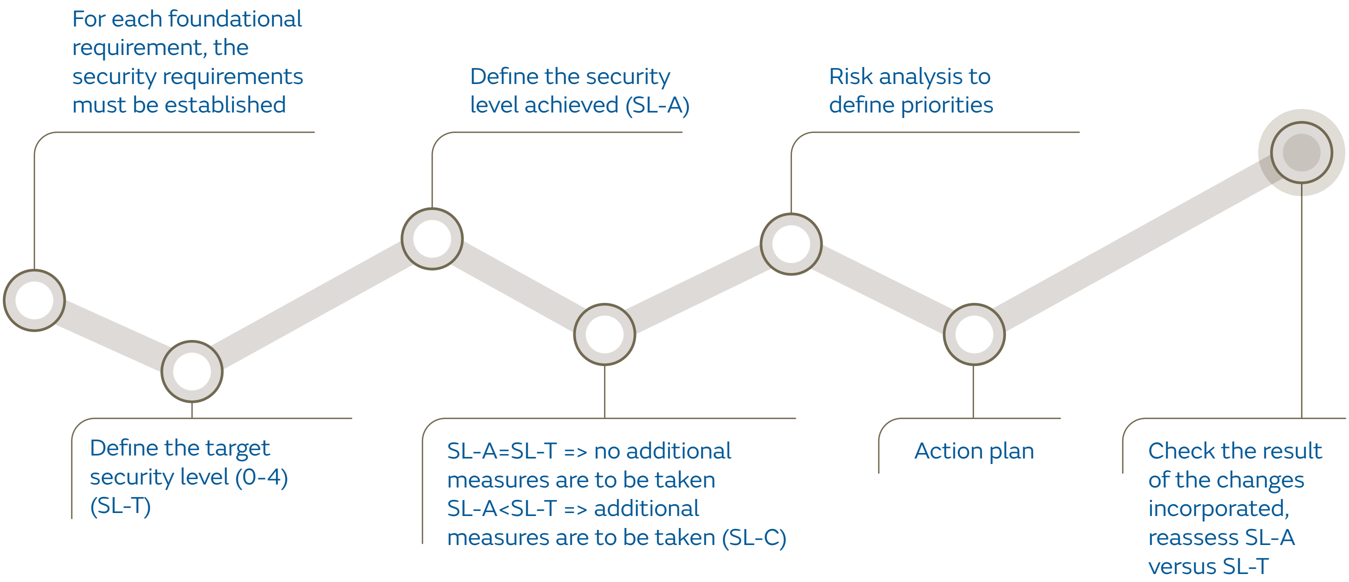
SL 2
Requires protection against intentional breaches with low resources, general knowledge and low motivation.

SL 3
Requires protection against intentional breaches with sophisticated resources, specific knowledge of Automation and Control Systems, and moderate motivation.

SL 4
Requires protection against intentional breaches with sophisticated resources, advanced knowledge of Automation and Control Systems and high motivation.

Every time an industrial system is modified, its security level must be evaluated. In this way the security level achieved (SL-A) will be determined and this can be compared with the target level (SL-T) (see Figure 11).

Figure 11 | Evaluation of cybersecurity levels.


For each foundational requirement, the security requirements must be established
Define the target security level (0-4) (SL-T)
Define the security level achieved (SL-A)
SL-A=SL-T => no additional measures are to be taken
SL-A<SL-T => additional measures are to be taken (SL-C)
Risk analysis to define priorities
Action plan
Check the result of the changes incorporated, reassess SL-A versus SL-T

> A comprehensive model is required that can respond to the range of regulations and new realities at different points in the chain.

In parallel, one aspect that accelerates safe digitalisation of industrial environments, especially of an electricity distribution system with field devices that can even be located in consumers' homes, is to consider the principle of "zero trust". This will allow potential attacks to be better resisted.

All of this encompasses three basic principles:

1. **Check explicitly.** The containment mechanisms to be implemented should include guarantee authentication and authorisation, considering that it is denied by default, always based on all the available data. This includes user identity, location, device status, service, data classification, and anomalies.

   As for the devices included in this network, they should have two-factor authentication mechanisms and be based on advanced encryption technologies that guarantee that only they can belong to the network.

2. **Use of least privileges access.** Limit access to users with sufficient permission and the time required, implement data protection and risk-based policies, enhance threat detection and improve defences.

3. **Assume a breach.** Applying the "defence-in-depth" principle, access is segmented and extent of a breach is minimised, end-to-end encryption is confirmed, and analytics are used to gain visibility, enhance threat detection and improve defences.

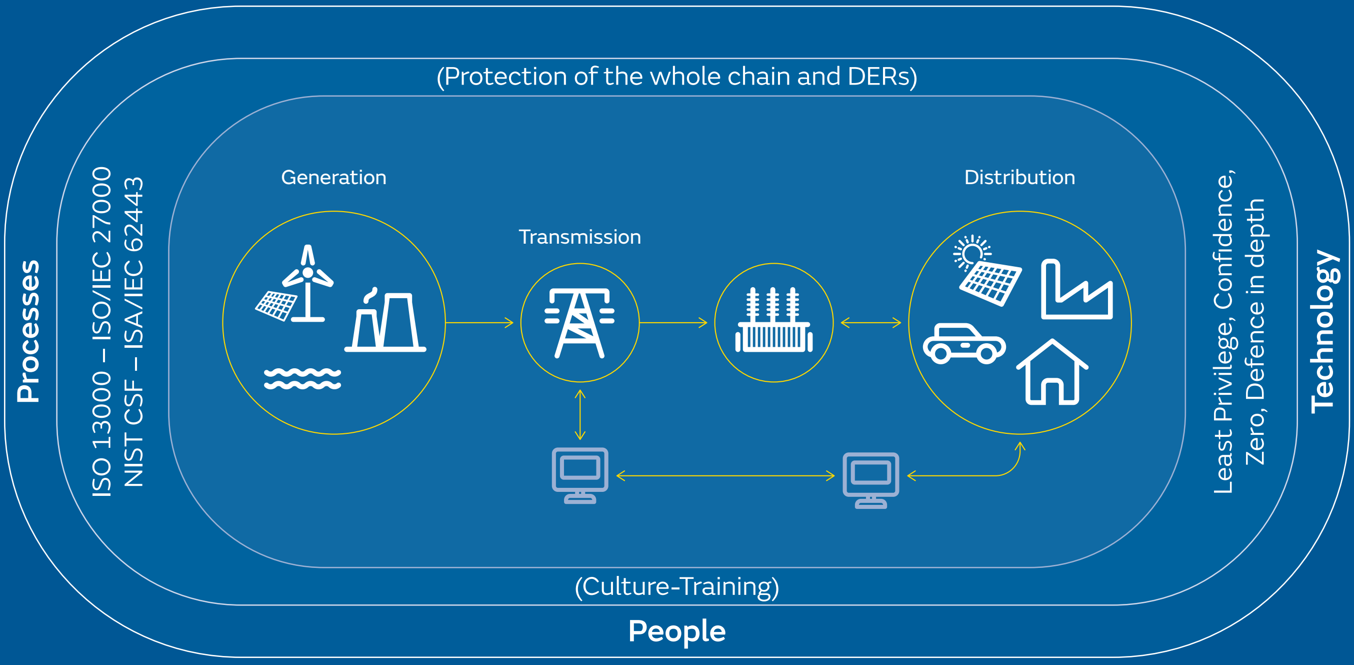
As the US Department of Energy suggests,[10] distributed energy resources face a number of attack vectors. These include ransomware, a compromised supply chain, botnets and worms. Any of them could affect the entire electricity sector supply chain on a significant scale. That is why security must be in the DNA of each electricity distribution and smart grid component.

Similarly, the European Commission, which aims at unified cybersecurity measures via the NIS2 Directive, requires security measures for critical entities. In fact, it makes the senior management of organisations responsible for their maintenance and includes supply chain management. Furthermore, it has already presented proposals for a Cyber Resilience Act that offers protection against products with inadequate security characteristics, and details products that will have to include cybersecurity by design, vulnerability management and security throughout the lifecycle of the product.

A comprehensive model is therefore required that can respond to the range of regulations and new realities at different points in the chain, considering the key elements and facilitating a timely response to events and incidents that may arise.

For all these reasons, it is necessary to take into consideration the people, processes and technology required to maintain the confidentiality, integrity and availability of the cyber–physical systems involved and of the information that allows continuous and resilient operation of the electricity system as a whole to be maintained in the new scenarios of two-way communications and of management, interconnections and continuous interaction throughout the whole chain (see Figure 12).

Figure 12 | **Cybersecurity model in electricity distribution.**



5. Regulations

The European Union has adopted a leading role in cybersecurity. One example of this is the range of regulations that it has recently implemented, all of which are of considerable importance. Essential services, cyber resilience or security by design are some of the elements that it promotes at the EU level.

5.1. Current cybersecurity regulatory framework

This section addresses the cybersecurity and resilience regulatory framework at the European level, which will determine regulations in the separate Member States.

In the last quarter of 2022, a plethora of European regulations concerning cybersecurity, security and resilience were approved. They indicated a change of emphasis for all the sectors involved, and especially for critical infrastructures, both at the European level and at the level of each Member State. Each of them will have to adapt their national regulations to the new European regulatory framework.

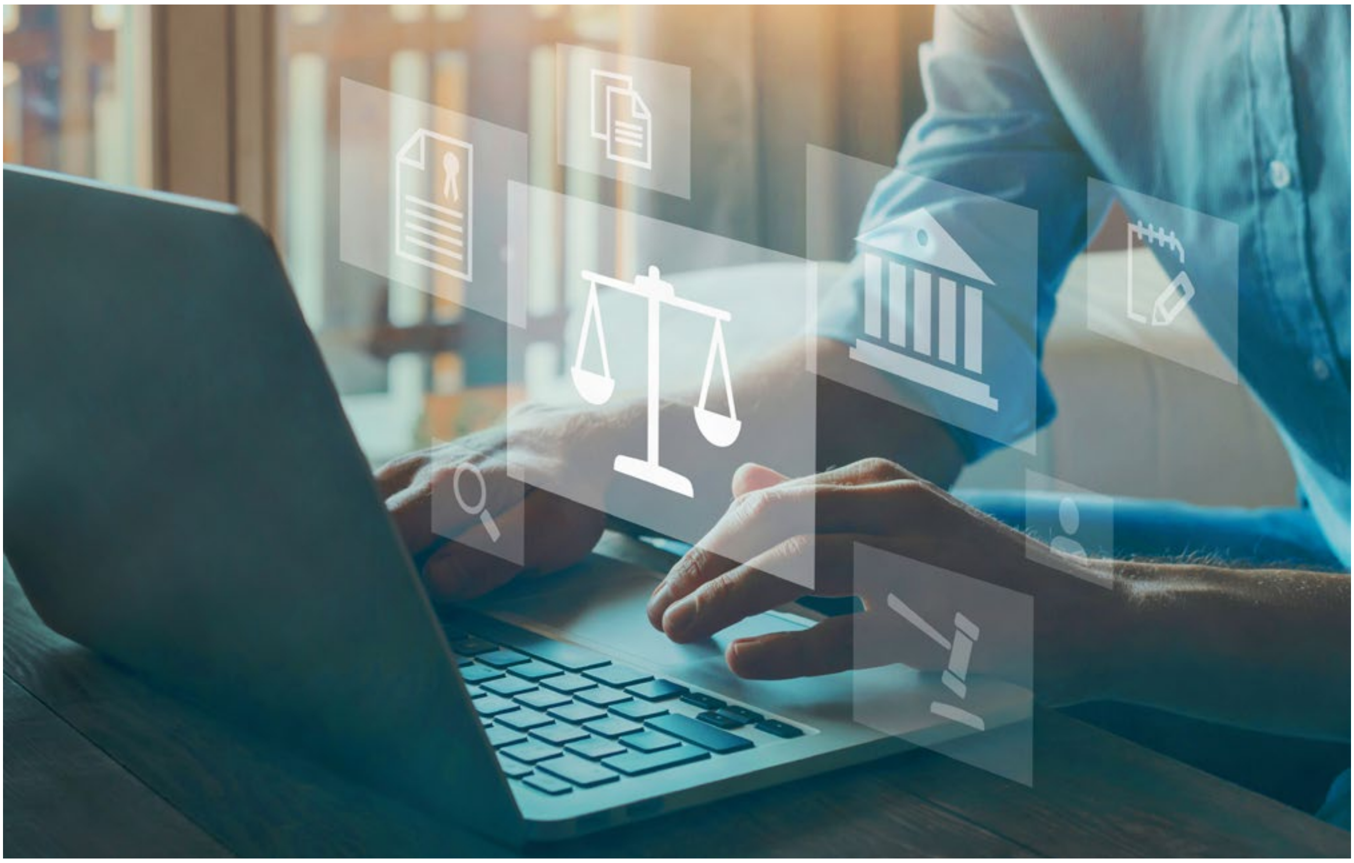
Furthermore, standards and best practices related to cybersecurity that have been promoted and adopted in other countries are contemplated.

5.2. European regulation of cybersecurity and resilience

Resilience is one of the cornerstones of cybersecurity that the European Union has aimed to strengthen. And with good reason considering that it is vital that organisations recover from a cyberattack if it occurs. Below, various different regulations related to this aspect are highlighted, some of them published recently.

Service cybersecurity. In this section two regulations stand out. The first is Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).

The second is known as the NIS2 Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148).



This latter regulation entered into force 20 days after its publication in the Official Journal of the European Union, on 16 January 2023.

In addition, no later than 28 October 2024, the Member States will adopt and publish the measures necessary to comply with the provisions of the Directive. And they will immediately notify the Commission of the text of those provisions, which will be applicable as of 29 October 2024.

Resilience in critical infrastructures. Here it is worth noting Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC and Council Recommendation 2023/C20/01 of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

The Member States will adopt and publish, no later than 28 July 2024, the legal, regulatory and administrative provisions necessary to comply with the provisions of this regulation. And they will immediately notify the Commission of the text of these provisions, which will be applicable as of 29 January 2025.

Cybersecurity and product safety. In this section we once again indicate two separate regulations. The first, known as the Cyber Resilience Act, is the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

And the second is the Proposal for a Regulation of the European Parliament and of the Council on machinery products.

Data Protection. Here the GRDP stands out. That is: Regulation (EU) 2016/679 of the European Parliament and of the Council of 17 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

5.3. Principal implications of cybersecurity

As previously mentioned, the European Union has adopted a leading role in cybersecurity. It has recently published several regulations of great significance for the sector, such as the NIS2 Directive, the Resilience Directive for critical entities and the Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements amending (EU) 2019/1020. We now highlight the most important points of these regulations.

5.3.1. NIS2 Directive

Information systems and networks have become a central feature of everyday life with the rapid digital transformation and interconnectedness of society, including at a cross-border level.

This development has led to an expansion of the cyberthreat landscape, generating new challenges that require adapted, coordinated and innovative responses from all Member States.

The authorities have established a series of minimum standards related to the operation of a coordinated regulatory framework, establishing mechanisms for effective cooperation between the responsible authorities in each Member State, updating the list of sectors and activities subject to cybersecurity obligations and providing effective remedies and compliance measures that are key to effective compliance with these obligations.

5.3.1.1. Prevention of vulnerabilities, and incident response and management

Cyber hygiene policies provide the foundation for protecting information system networks and infrastructures, hardware, software, and online application security, as well as business or end-user data on which entities rely.

Cyber hygiene policies that comprise a common core of practices, including software and hardware updates, password changes, managing new installations, limiting administrator-level access accounts, and backing up data, foster a proactive framework of preparation and security as well as general protection in case of incidents or cyber threats. Here it is ENISA that must supervise and analyse the cyber hygiene policies of Member States.

Awareness and cyber hygiene are essential in order to improve the level of cybersecurity within the EU, particularly in light of the growing number of connected devices, which fall prey to an increasing volume of cyberattacks. Therefore, efforts need to be made to improve general awareness of the risks related to such devices, while assessments at the EU level could help to ensure a common understanding of such risks in the internal market.

Member States have to develop a policy that tackles the increase in ransomware attacks as part of their national cybersecurity strategy. They must also address the specific cybersecurity needs of small and medium-sized enterprises.

As part of their national cybersecurity strategies, countries also have to adopt policies on promoting active cyber protection as part of a broader defensive strategy. Rather than responding reactively, active cyber protection consists of prevention, detection, monitoring, analysis and mitigation of network security breaches in a proactive way, combined with the use of capabilities deployed inside and outside the network at risk.

Since exploiting vulnerabilities in networks and information systems can cause significant disruption and damage, quickly identifying and remedying them is an important factor in risk reduction. Entities that develop or manage networks and information systems must therefore establish appropriate procedures to deal with vulnerabilities when they are discovered. Since these are usually located and revealed by third parties, manufacturers and providers of ICT products or services also have to establish the necessary procedures to receive third-party information on vulnerabilities.

In parallel, a risk management culture must be promoted and fostered that involves carrying out assessments and implementing management measures that are appropriate for the threats.

Cybersecurity risk management measures should take into account the degree of dependence of an essential or important entity on the network and information systems. They should also include measures to identify any risk of incidents, prevent, detect, respond and recover from them as well as mitigating their impact. The security of networks and information systems must include the security of stored, transmitted and processed data. Furthermore, cybersecurity risk management measures must provide for systemic analysis, taking into account the human factor, in order to have a complete image of the security of the network and the information system.

Therefore, cybersecurity risk management measures must also tackle the physical and environmental security of networks and information systems by including measures to protect these systems from failure, human error, malicious acts and natural phenomena. All this must be in line with European and international standards.

In order to demonstrate compliance with cybersecurity risk management and in the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council, Member States, in consultation with the Cooperation Group and the European Cybersecurity Certification Group, are to promote the use of the pertinent European and international standards by essential and important entities. Alternatively, they can require these entities to use certified products, services, and ICT processes and services.

To avoid imposing a disproportionate financial and administrative burden on essential and important entities, cybersecurity risk management measures should be proportional to the risks posed to the network and information system in question. And always taking into account the state of the art of such measures and, where appropriate, the pertinent European and international norms, relevant standards and the cost of implementation.

In short, cybersecurity risk management measures must be proportional to the degree of exposure of the essential or important entity to risks and the social and economic impact that an incident would have.

> Critical products with digital elements will be subject to specific conformity assessment procedures reflecting their cybersecurity risk level.

5.3.1.2. Supply chain

Organisations are required to address risks arising from an entity's supply chain and its relationship with its suppliers. Along these lines, essential and important entities must evaluate and take into account the general quality and resilience of products and services, the cybersecurity risk management measures integrated into them and the cybersecurity practices of their suppliers and service providers, including their secure development procedures.

In particular, essential and significant entities should be encouraged to incorporate cybersecurity risk management measures into contractual agreements with their direct suppliers and service providers. Those entities could consider risks derived from other levels of suppliers and service providers. Therefore, essential and important entities have to exercise greater diligence when selecting a provider of managed security services.

In order to continue tackling key supply chain risks and help essential entities to manage them appropriately, the Cooperation Group, together with the European Commission and ENISA, and where appropriate after consulting relevant stakeholders (including industry), must carry out coordinated security risk assessments of critical supply chains with the aim of identifying critical ICT services, ICT systems, ICT products, threats and relevant vulnerabilities by sector.

In order to locate the supply chains that should be subjected to a coordinated security risk assessment, the criteria that are to be considered are the following: the extent to which essential and important entities use and trust specific critical ICT services, ICT systems or products TIC; the importance of specific critical ICT services, ICT systems or ICT products in performing critical or sensitive functions, including the processing of personal data; the availability of alternative ICT services, ICT systems or ICT products; the resilience of the general supply chain of ICT services, ICT systems or ICT products to disruptive events throughout their lifecycle; and for emerging ICT services, ICT systems or ICT products, their potential future importance for the entities' activities.

In addition, emphasis should be placed on ICT services, ICT systems or ICT products that are subject to specific requirements derived from outside countries.

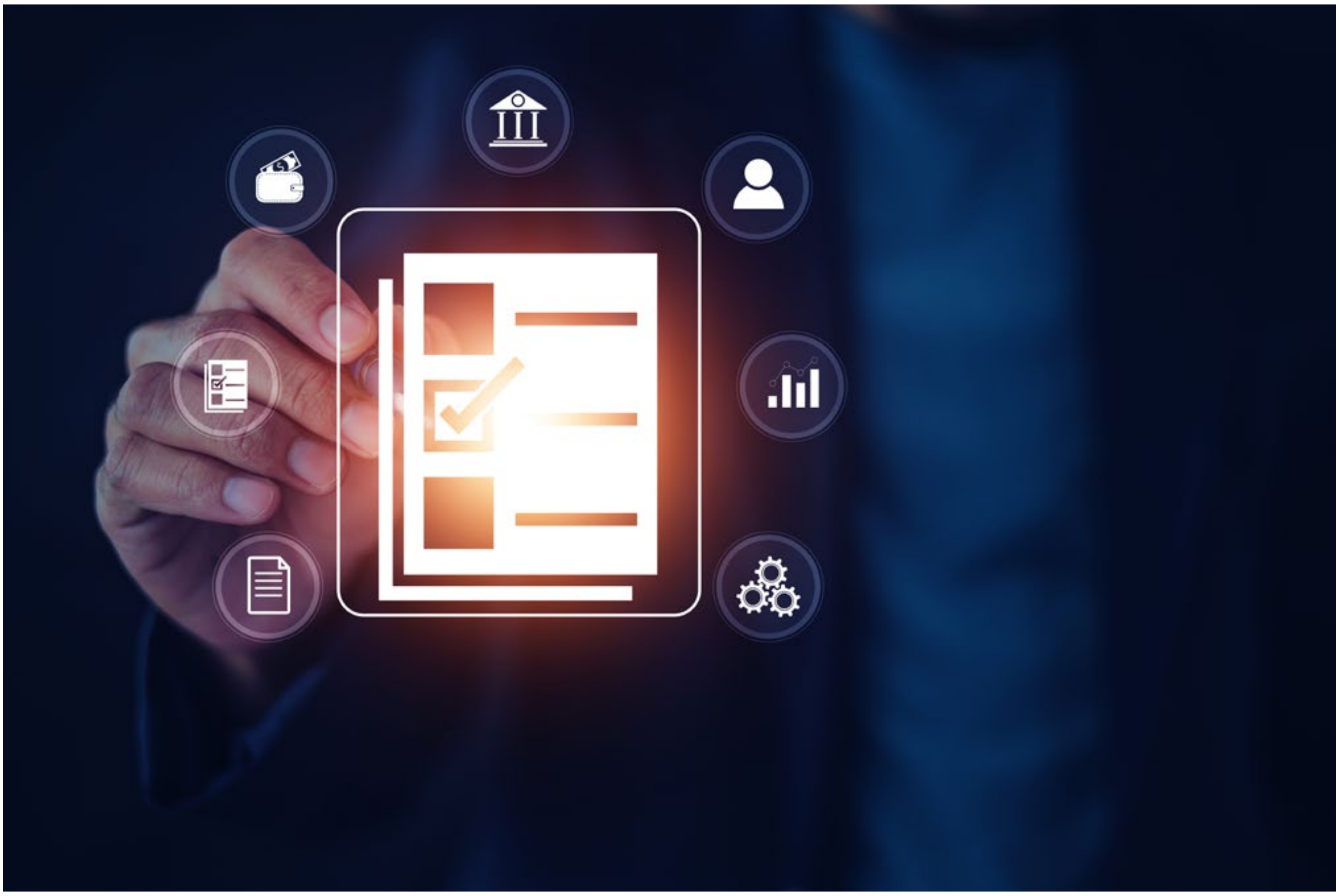
5.3.1.3. Incident notification

When essential or important entities become aware of a significant incident, they must be required to send an early warning without undue delay, and in any event within 24 hours. That early warning has to be followed by an incident notification. The entities affected will be obliged to submit an incident notification without undue delay, and in any case within 72 hours of becoming aware of the significant incident. The specific aim is to update the information sent in the early warning and indicate an initial assessment of the significant incident, including its severity and impact, as well as indicators of affectations where available. In addition, they will have to submit a final report no later than one month after notification of the incident.

Where appropriate, essential and important entities must notify the recipients of their services, without undue delay, of any measures or remedies they can take to mitigate the risks resulting from a significant cyber threat. Providing such information must be free and it must be in plain language.

5.3.1.4. Responsibility

The management bodies of essential and important entities must approve cybersecurity risk management measures and supervise their implementation. It is their responsibility to do so.



5.3.2. Directive on critical infrastructure resilience

On December 27, the Official Journal of the European Union published Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. This new legislation obliges Member States to adopt specific measures to guarantee the provision of essential services. However, above all, it establishes the identification of critical entities and addresses their compliance with the obligations imposed on them. We now highlight the most important elements.

5.3.2.1. Identification

This regulation establishes a procedure for Member States to identify critical entities using common criteria on the basis of a national risk assessment. In this regard, when identifying critical entities, Member States will take into account the results of the risk assessment and apply the following criteria:

a) The entity provides one or more essential services.

b) The provision of said service depends on the infrastructure located in the Member State.

c) An incident would have significant disruptive effects on the provision of the service or other essential services in the sectors mentioned in the annex that depend on the service.

National designated competent authorities will draw up a list of essential services in specific sectors. They will carry out, no later than 29 October 2025, and thereafter when necessary, at least every four years, an assessment of all relevant risks that may affect the provision of these essential services, with a view to identifying critical entities and assisting them to take necessary measures.

The Critical Infrastructure Resilience Directive is in line with the NIS2 Directive in ensuring that the competent authorities designated under the two Directives adopt complementary measures and exchange information in relation to cyber resilience and non-cyber resilience when necessary. And that especially critical entities in sectors considered essential, in the NIS2 Directive, are also subjected to general obligations to improve resilience to deal with non-cyber risks.

5.3.2.2. Analysis and management of risks to resilience

The objective of this Directive is not to protect a limited set of physical infrastructures the disruption or destruction of which would have a significant transversal impact. Rather, it is to increase the resilience of entities that are critical for the delivery of essential services in Member States so they can maintain vital social or economic functions in the internal market in a number of sectors that support the functioning of many others in the Union.

Critical entities are periodically to assess all relevant risks on the basis of national risk assessments and other relevant sources of information. In addition, they are to take appropriate and proportionate technical and organisational measures to ensure their resilience and they will describe these measures in a resilience plan or equivalent document.

5.3.2.3. Resilience measures of critical entities

Critical entities are to define and implement a resilience plan or equivalent documents that describe these measures in detail. When they have adopted them by virtue of the obligations contained in other acts of EU law that are also relevant to these measures, they will also describe them in these documents.

In parallel, critical entities must notify the competent authorities without undue delay of incidents that significantly disrupt or may significantly disrupt their operations. These notifications are to include all the available information necessary so that competent authorities can understand the nature, causes and possible consequences of the incident, including the determination of any cross-border impact. Notwithstanding, this notification will not imply any increase in the responsibility of the critical entity.

5.3.3. Proposal for Regulation on horizontal cybersecurity requirements for products

This Proposal amending Regulation (EU) 2019/1020 on horizontal cybersecurity requirements for products with digital elements establishes rules for the introduction into the market of products with digital elements aimed at guaranteeing the cybersecurity of those products. It also sets out essential requirements for the design, development and manufacture of products with digital elements and the obligations of economic operators in relation to those products with respect to cybersecurity. It further establishes essential requirements for the vulnerability management processes established by manufacturers to guarantee the cybersecurity of products with digital elements throughout their entire lifecycle and the obligations of economic operators in relation to these processes. Finally, it includes rules relating to market surveillance and the application of the aforementioned requirements and rules.

It will apply to all products with digital elements whose intended and reasonably foreseeable use includes a direct or indirect, logical or physical, data connection to a device or network.

Critical products with digital elements will be subject to specific conformity assessment procedures and will be divided into class I and class II as set out in Annex III, reflecting their cybersecurity risk level, with class II representing a greater risk. A product with digital elements is considered critical and therefore included in Annex III taking into account the impact of potential cybersecurity vulnerabilities included in the product with digital elements. The cybersecurity-related functionality of the product with digital elements and the intended use in sensitive environments such as an industrial setting, amongst others, is taken into account in the determination of cybersecurity risk.

The Commission is also empowered to adopt delegated acts to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers will be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme to demonstrate conformity with the essential requirements set out in Annex I of the Proposed Regulation, or parts thereof.

When determining such categories of highly critical products with digital elements, the Commission will take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria considered for the listing of critical products with digital elements in Annex III as well as in view of the assessment of whether that category of products is used or relied upon by the essential entities of the type referred to in Annex I to the NIS2 Directive or will have potential future significance for the activities of these entities; or relevant for the resilience of the overall supply chain of products with digital elements against disruptive events.

5.3.3.1. Obligations of economic operators

The essential cybersecurity requirements and obligations mandate that all products with digital elements will only be made available on the market if, where duly supplied, properly installed, maintained and used for their intended purpose or under conditions which can be reasonably foreseen, they meet the essential cybersecurity requirements set out in this Regulation.

The essential requirements and obligations would mandate manufacturers to factor in cybersecurity in the design and development and production of the products with digital elements, exercise due diligence on security aspects when designing and developing their products, be transparent on cybersecurity aspects that need to be made known to customers, ensure security support (updates) in a proportionate way, and comply with vulnerability handling requirements.

Obligations would be set up for economic operators, starting from manufacturers, up to distributors and importers, in relation to the placement on the market of products with digital elements, as adequate for their role and responsibilities in the supply chain.

5.3.3.2. Conformity of products with digital elements

Products with digital elements which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union will be presumed to be in conformity with the essential requirements of the Proposed Regulation. Where harmonised standards do not exist or are insufficient or where there are undue delays in the standardisation procedure or where the request by the Commission has not been accepted by the European standardisation organisations, the Commission may, by the means of implementing acts, adopt common specifications.

In addition, products with digital elements that have been certified or for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881, and for which the Commission specified via implementing act that it can provide presumption of conformity for this Regulation, will be presumed to be in conformity with the essential requirements of this Regulation, or parts thereof, insofar as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.

The manufacturer will perform a conformity assessment of the product with digital elements and the vulnerability handling processes it has put in place to demonstrate conformity with the essential requirements set out in Annex I by following one of the procedures set out in Annex VI. Manufactures of critical products of class I and II will use the respective modules necessary for the compliance. Manufacturers of critical product of class II have to involve a third-party in their conformity assessment.

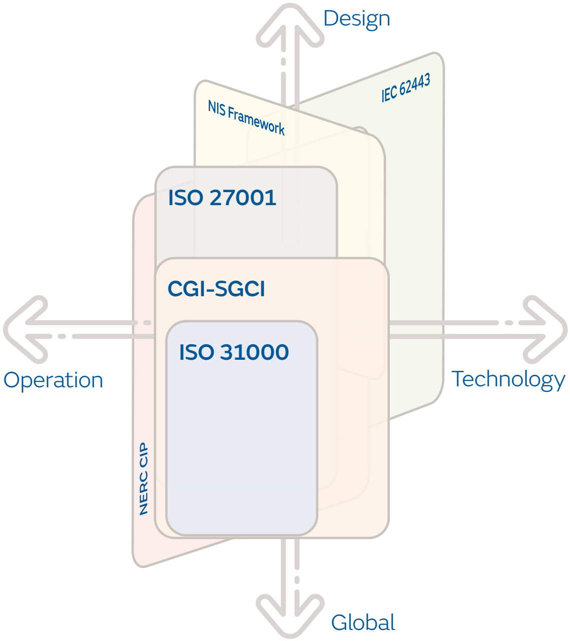
5.4. Good practices in other countries

Over the last decade, different organisations and entities, mainly in the United States and Europe, have developed standards and good practices for application in areas of industrial automation digitalisation such as that in electricity distribution. Figure 13 shows the most widely recognised and accepted practices at present. To facilitate identification of the strong points of each of these good practices, the axes have been labelled with four concepts: “design”, which contemplates the incorporation of cybersecurity requirements into new projects; “operation”, which includes measures to manage risk through cybersecurity operation and maintenance in an existing infrastructure or installation; “technology”, which could be applied to adopting technical configuration and implementation of cybersecurity measures; and "global", which includes cybersecurity strategy, compliance and good governance.

These good practices are the following:

- Operational Best Practices for NERC CIP BCSI (North-American Electric Reliability Corporation Critical Infrastructure Protection standards for BES Cyber System Information) CIP-004-7 and CIP-011-3
- Operational Best Practices for NIST 800 171. Protection of controlled unclassified information resident in non-federal systems and organisations
- Operational Best Practices for NIST 172. Enhanced security requirements for protecting controlled unclassified information: supplement to NIST Special Publication 800-171
- Best Operational Practices for NIST 800 181. Workforce Framework for Cybersecurity (NICE Framework).
- Operational Best Practices for NIST 800-53 Rev 4. Security and privacy controls for federal information systems and organisations.

Figure 13 | Best practices.



- Operational Best Practices for NIST 800-53 Rev 5. Security and privacy controls for information systems and organisations.
- Operational Best Practices for NIST 1800 25. Data integrity: identifying and protecting assets against ransomware and other destructive events.
- Operational Best Practices for NIST CSF. NIST Cyber Security Framework.
- Industrial Cybersecurity Management System of the Industrial Cybersecurity Center. This document also includes the requirements of the ISO 27001 (ISO 27002 controls) and IEC 62443 standards, as well as the CCI maturity model.
- IEC 62351. Management of energy systems and associated exchange of information – data and communications security.
- IEC 62443-1-1 “Models and Concepts”.
- IEC TR 62443-1-2 “Master Glossary of Terms and Abbreviations”.
- IEC 62443-1-3 “System Security Compliance Metrics”. Defines compliance metrics for security in industrial automation and control systems.
- IEC TR 62443-1-4 “Security Life Cycle and Use Cases”. Focuses on the lifecycle and giving examples of its use in typical applications within control systems.
- IEC 62443-2-1 “Requirements for an IACS Security Management System”.
- IEC TR62443-2-2 “Operating a Control Systems Security Program”.

- IEC TR 62443-2-3 “Patch Management in the IACS Environment”. A practical guide to carrying out an update management programme from the point of view of both the owner and the solution provider.
- IEC 62443-2-4 “Certification of IACS supplier security policies and practices”. Focuses on the certification of suppliers of security products for control systems and industrial automation.
- IEC TR62443-3-1 “Security Technologies for IACS”. Offers a description of existing technologies for the protection of industrial networks and systems, reporting their advantages and limitations. (Currently in the review phase.)
- IEC 62443-3-2 “Security Risk Assessment and System Design”.
- IEC 62443-3-3 “System Security Requirements and Security Levels”. Describes the technical system requirements to define the security level of the asset analysed.
- IEC 62443-4-1 “Product Development Requirements”. Defines the development process that new devices created for control systems have to undergo, although it can also be applied to existing devices.
- IEC 62443-4-2 “Technical Security Requirements for IACS Components”. Groups together the technical requirements to improve the safety of the components, individually, within the industrial network. It also addresses network segmentation to restrict data flows within and between networks.
- ISO/IEC 27001. Information Security Management System.
- ISO 31000. Risk management — Guidelines.
- CEN/CLC/JTC 13/WG 3. GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP) v1.0.
- Operational Best Practices for NCSC Cyber Assessment Framework. UK National Cyber Security Centre Cyber Assessment Framework Checks.
- Operational Best Practices for UK National Cyber Security Centre Cloud Security Principles. Cloud Security Principles from the National Cyber Security Centre.

6. Investment in cybersecurity by the electricity sector

Combating the increase and sophistication of attacks that critical infrastructures in general are suffering, and electricity distribution in particular, requires a more mature level of culture and management of cybersecurity in both current and future scenarios of automation and industrial digitalisation.

Furthermore, although cybersecurity regulations seek to minimise the financial and administrative burden, they require investment and imply expenses to manage this increasingly important risk. Such investments are justified to the extent that they contribute to increasing the resilience of operators and the system, including end consumers and the new ways they relate to the electricity system, and also to providing a more coherent approach and greater capacity to provide reliable services throughout the EU. Additionally, any additional burden from regulatory compliance is expected to be far outweighed by the potential costs associated with having to manage and recover from severe disruptions that could jeopardise uninterrupted delivery of services related to vital social functions.

Given this risk scenario, several operators in the European electricity sector have been consulted on the evolution of their investment and spending on cybersecurity. Some interesting results are included here:

- In-house staff dedicated to cybersecurity has doubled in the last two years, while external resources have also increased, but only slightly.

- Two years ago, 80% of cybersecurity resources were devoted to the corporate setting and 20% to operational aspects. This has changed so that now, 60% is corporate and 40% operational. This is due to both the regulatory requirements and the incidents suffered in recent years.

- There has also been clear evolution in the proportion of capital investment (CAPEX) compared to operational spending (OPEX), from a 30% CAPEX to 70% OPEX split two years ago to a 50:50 balance now.

These results indicate the significant effort being made by electricity operators to protect essential service infrastructure in compliance with existing and forthcoming regulations. But this effort will not one-off: the digitalisation of the sector, and the greater dependence on technology that comes with it, will require an increase in human and financial resources to tackle the associated risks, as indicated throughout this document.

This increased investment in resources to protect essential services will also need to include supply chain responsibility and investment.

The reorganisation of supply chains using advanced technologies has replaced the linear model from supplier to producer and from distributor to consumer, and vice versa, to a more integrated model, not only of the business model of enterprises, but also of their technological ecosystem. Suppliers have direct links to a company's networks or systems (including enterprise resource planning (ERP) systems, and ordering and billing applications) and in some cases they have access corporate data or even operational data. There are also similar interconnections between suppliers along entire supply chains.

This scenario significantly increases the scope that electricity distributors need to consider; that is, it multiplies the opportunities for an attacker to access their data or take control of their operation. For this reason it is also necessary to assess contractual relationships continuously with suppliers within the supply chains and to verify that they are also making the investments necessary to apply cybersecurity measures.

> These results indicate the significant effort being made by electricity operators to protect essential service infrastructure in compliance with existing and forthcoming regulations.

7.
Conclusions

The current situation of cybersecurity risk, together with the evolution of services demanded by electricity consumers, poses different challenges for electricity distribution that are driving actions, standards and regulations within the sector at all levels:

- Electricity is a sector in which a cyberattack can have important implications, not only due to a potential interruption in the supply that directly affects consumers, but also because of the consequences for other sectors. The electricity sector is therefore facing cyberattacks and threats with a very high potential impact. To combat this, it is necessary to develop a high degree of maturity in everything related to the culture and management of cybersecurity over the lifecycle of industrial automation and digitalisation projects, with the ultimate goal of minimising risks generated by the threats and guaranteeing essential services for society.

- The evolution of the end consumer of electricity towards the category of "prosumer" undoubtedly affects cybersecurity management in the sector. Customers, who are also undergoing a digital transformation, demand real-time information on their consumption. And this supposes necessary internal reorganisation and a readaptation so that the electricity companies are transformed from being service operators to being service managers.

- The growing activity of cybercriminals, together with their increasingly evident professionalisation, makes it strictly necessary to undertake significant investments. At the same time, it is also necessary to intensify awareness-raising strategies and staff training, incident response procedures and, above all, the involvement of all personnel in cybersecurity. Therefore, entities in the electricity sector must work as much on technology and procedures as with their personnel.

- The transformation in electricity distribution necessarily entails the implementation of a new digital supply chain, the definition of new roles, a consideration of the increasingly evident interdependencies, the standardisation of methodologies, consolidation of the cloud and the adoption of the zero trust principle.

- Therefore, when establishing a model for the new electricity distribution, it is necessary to consider protecting the entire supply chain in terms of cybersecurity, from the design stage and at each of the phases of implementation of new projects, as well as during necessary adaptations and renovations.

- Organisations in the electricity sector have been implementing a series of protection mechanisms for some time with the aim of reducing exposure to the activity of cybercriminals as much as possible. These include segmentation and defence in depth, tracking all changes in device configurations, controlling access and privileges, evaluating and managing vulnerabilities, monitoring all aspects related to security and guaranteeing continuity of service and the safety of people, the environment and installations.

- All of this means that the electricity sector, as a consequence of its categorisation as an essential service, faces a maelstrom of cybersecurity regulations. This has become more evident since the publication in the Official Journal of the European Union, at the end of last year, of what is known as the NIS2 Directive and the Directive on the resilience of critical entities.

- These new regulations at the European level require a greater investment when it comes to managing cybersecurity risks. Undoubtedly, these amounts are totally justified since they will reinforce protection, detection, response and recovery by organisations in the event of threats and incidents. In fact, the cost associated with managing and recovering after a cyberattack would far outstrip any additional burden resulting from regulatory compliance. Therefore, these costs resulting from continuous technological evolution must be adequately recognised in terms both of investment and of operating expenses.

> All of this means that the electricity sector, as a consequence of its categorisation as an essential service, faces a maelstrom of cybersecurity regulations.

8. References

1. Boston Consulting Group. Embracing Industry 4.0 and Rediscovering Growth. Available at: https://www.bcg.com/capabilities/operations/embracing-industry-4.0-rediscovering-growth

2. J. Julian Claveria and A. Kalam. GOOSE Protocol: IED's Smart Solution for Victoria University Zone Substation (VUZS) Simulator Based on IEC61850 Standard. Available at: (PDF) GOOSE Protocol: IED's Smart Solution for Victoria University Zone Substation (VUZS) Simulator Based on IEC61850 Standard (researchgate.net)

3. J. Andress and S. Winterfeld. Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners. Syngress; 2nd edition, 2011.

4. A. D. Campen. Uncommon Means for the Common Defense in Cyberwar: Strategy and Conflict in the Information Age (A. D. Campen, D. H. Dearth, and R. T. Goodden, eds.). Pages 71-75. Fairfax, Virginia: AFCEA International Press, 1996.

5. G. Disterer. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, nº 4. Pages 92-100, 2013

6. Tecnología de la información. Técnicas de Seguridad. Controles de Seguridad de la información para la industria de servicios de energía (ISO/IEC 27019:2017, Corrected version 2019-08) (Endorsed by the Asociación Española de Normalización in May 2020)

7. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, tech. rep., NIST, 2018.

8. Pillitteri, V. and Brewer, T. (2014). Guidelines for Smart Grid Cybersecurity, NIST Interagency/Internal Report (NISTIR). National Institute of Standards and Technology, Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.IR.7628r1 (accessed on: 9 December 2022).

9. Centro de Ciberseguridad Industrial. Estableciendo Zonas y Conductos, 2018

10. U.S. Department of Energy's, Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid, October 2022.

11. World Economic Forum - Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards. 2019.

12. DOE. Roadmap for Wind Cybersecurity. 2020.

13. Centro de Ciberseguridad Industrial. Guía de Ciberseguridad en el Ciclo de Vida de un proyecto de digitalización industrial. 2021.

Centro de
Ciberseguridad Industrial

Naturgy
Foundation