Telefónica Tech

Cyber Security for Industrial Digitalisation

Keys to a successful approach

01 **Context**

› Factors motivating the digital transformation of industry
› No industrial sector can evade this dynamic transformation
› Cyber security risks in operational environments
› The importance of a holistic cyber security approach

02 **Telefónica Tech proposal for OT cyber security**

› Why Telefónica Tech?
› METEO methodology
› Evaluate and Plan
› Implement
› Manage

03 **METEO implementation in OT environments**

Executive Summary:

Digital technologies, and in particular what has been agreed to be called IoT (Internet of Things), bring a world of possibilities that organisations of any sector cannot fail to exploit in order to increase their flexibility and capacity to adapt to the tastes and habits of their customers, improve the services they provide through continuous monitoring or become more efficient.

All these technologies have the need for greater connectivity in the environment of organizations in, both externally, that is to say, with their customers and suppliers, and internally. Therefore, achieving greater coordination and integration between different organizations and departments.

This increased interconnection between areas that were recently isolated (i.e. information systems and operating systems) as well as between organisations that up to date have used less digital and automated interoperation processes means that, in parallel with the digital transformation process, there is an increase in their attack surface and, consequently, in the cyber security risks they are exposed to.

This time, unlike previous waves of digital transformation (TI systems explosion, personal devices, cloud), changes are taking place in the core of industrial organisations, that is, in their operational systems. These are responsible for supervising and controlling production processes, which traditionally had been more isolated.

Telefónica has been supporting its customers in this process of digital transformation since its very origins, offering them specialised solutions and services to deal with cyber security risks. Likewise, we continue to adapt and improve our offer to remain at the cutting edge.

This document starts by explaining the forces driving the industry towards digital transformation and the associated cyber security risks. Then it introduces the methodology followed by Telefónica Tech to help our clients address this challenge, highlighting the differential aspects of the proposal. Finally, two model scenarios are put forward that exemplify two different types of cyber security projects: organisations with traditional factories that must adapt to the new environment and organisations that are building new factories where cellular connectivity is a key element.

01 Context

01.1. Factors motivating the digital transformation of industry

The competition to which industrial companies are exposed forces them to constantly come up with initiatives to adapt and improve, those that pursue one or more of the principles that characterise the concept of the "Factory of the Future" (s.f.):

Greater flexibility to adapt to changing consumers' tastes and habits

Organisations must be aware of what is happening around them, following the changes in the tastes and interests of their clients and making available to them the possibility of personalising the product to their likings.
One of the examples that best reflects this trend is "Nike by you". An initiative launched by Nike that allows final consumers to personalise their shoes online with their own design, which will then be delivered to their homes.

Design, production and product digitalization

The main exponent of this concept is the "digital twin". On the one hand, it facilitates the conception and simulation of the product's properties without resorting to physical models, as well as digitising production, increasing savings and efficiency. On the other hand, it allows the creation of virtual replicas of the products in order to monitor them during their useful life to anticipate problems that may arise. This has great applications in fields such as automobiles, aviation or any other where the wear and tear of parts can have an impact on human lives.

Sustainable or zero waste manufacturing

In this current world, it is more important than ever to properly manage limited raw materials. This requires digital solutions that allow them to be fully tracked, from extraction to recycling. Electric car batteries are an example. The metals they are made of could suffer a shortage sooner rather than later, and this has led some manufacturers to make moves to secure their supply. Furthermore, the management of batteries after they have been built and throughout their life cycle helps to optimise their use and subsequent recycling.

All these initiatives share the need for greater connectivity and integration between the different areas that make an organisation up. Likewise, with its customers and suppliers in order to facilitate the flow of information necessary so the business processes flow with maximum agility.

01.2. No industrial sector can evade this dynamic transformation

As we have seen, the need for connectivity and integration with third parties pushes for constant transformation, however, this is not exclusive to a vertical or particular sector.

To a greater or lesser extent, any sector of the economy whose operations are susceptible to automation is immersed in this transformation process. Some of these sectors are:

Health sector

It may seem to be one of the least affected by digitisation, however, in any hospital large networks of PCs, servers and IoT devices can be found. As well as special medical systems such as sensors, monitors, x-ray machines or scanners. The correct functioning of all systems is essential for a safe operation that has a direct impact on people's health.

Transport sector

Nowadays it depends heavily on the use of communication networks and real-time information sharing. We could talk about networks in airports or those inside and outside trains, which control systems so common to passengers like screens and loudspeakers, but also critical automatisms such as braking or door controlling.

Retail sector

It is also fully engaged in a digital transformation which has filled distribution centres and plants with wireless IoT devices that enable full-speed operation of the entire logistics process.

01.3. Cyber security risks in operational environments

The same transformation that affects all industrial sectors and helps them to improve their competitiveness requires a major challenge to be tackled: cyber security.

Most of these risks are caused by the increased connectivity of industrial systems and the integration of technologies with one another. This translates into a larger attack surface, both in traditional systems and in newly created environments. In this same sense, we distinguish two types of scenarios.

TRADITIONAL INDUSTRY

It has made progress by maintaining the systems and networks, let´s call them legacies, which can be up to several decades old.

These systems coexist to a greater or lesser extent with flat networks and ad hoc extensions that have been added over the years. All this results in a lack of knowledge about what is really connected to the network. In addition, the principle of "if it works, don't touch it" generally applies, so systems are often out of date.

MODERN INDUSTRY

Such as those in the automotive sector, which have been designed to implement the latest automation technologies and great connectivity between their systems. However, time to market, budget limitations and availability requirements do not always allow to keep an adequate state of security. Some of their weak points are insecure remote access without adequate control and traceability, the use of potentially infected USBs and the large number of IoT devices to be managed.

What kind of problems can be found?

Lack of visibility: We do not know exactly what is connected in our network and how it is being communicated. It is impossible to defend something that you do not know exists.

Flat networks: A flat network means that any device can communicate with any other device without restrictions. An attacker or virus can move around the network without any problems.

Unsafe protocols: The use of old, previous proprietary, unencrypted and unauthenticated protocols carry an enormous risk. For example, variables can be supplanted, privileged information can be read, and acted upon automatons.

Old and outdated software: Due to the nature of the operation of these environments it is common to find old and outdated software which implies the accumulation of vulnerabilities that can be exploited by an attacker in order to take control of the systems.

Malware (USB or email): Most attacks are caused by malware infections through infected email or USBs that can also spread over an industrial network.

Unsafe remote access: Remote access by unsafe and uncontrolled means open security gaps in industrial networks, as we cannot be sure who is accessing and what they are doing.

Unprotected physical assets: nguarded control cabinets, open computer rooms, switches with activated openings...
All this can also be exploited by an attacker to cause damage.

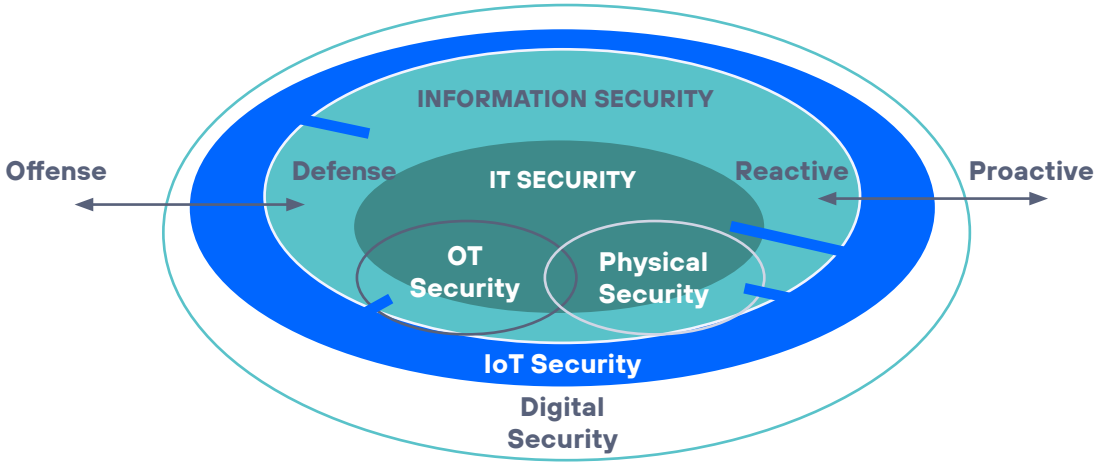
Social engineering: People are the weakest link; the lack of awareness makes us fall into the trap of cybercriminals.

Lack of response to cyber incidents: The impact of a cyberattack is much greater if we do not have an adequate response plan to recover and resolve the emergency as soon as possible. Many organisations are likely to be overwhelmed by the size of the problem and perceive that any small change can upset the precarious balance of the organisation which, although inefficient, barely survives on a daily basis.

01.4. The importance of a holistic cyber security approach

When considering the digital transformation and its risks, it is clear that we can no longer speak of isolated organisations with few points of connection with the outside world and which can easily defend themselves. Today, we have organisations that are hyperconnected with all the agents with which they interact, and which must learn to manage their risks and protect themselves in this new context.

One of the consequences is the need to integrate traditionally separate areas of security, for example physical security and IT security. These areas can now be connected by elements such as IP cameras or digital access control systems. To manage these risks, it is useful to consider the security model created by Gartner. It represents the different security domains that must be considered in order to carry out an end-to-end management of cyber security risks.



Modern IT security model by Gartner

Under this diagram, not only must the risks of each domain be treated independently, but also the risks arising from new connections between them. In this sense, by connecting the IT domain with the physical domain, we could be opening the door to an attacker, from the corporate network or Internet, to manipulate physical access control systems or video surveillance.

However, connecting different domains also bring new possibilities for cyber security. It allows the integration of different technologies, to orchestrate and automate more complex and effective actions in all domains.

An example of how this integration between technologies is exploited:

1. DETECTION

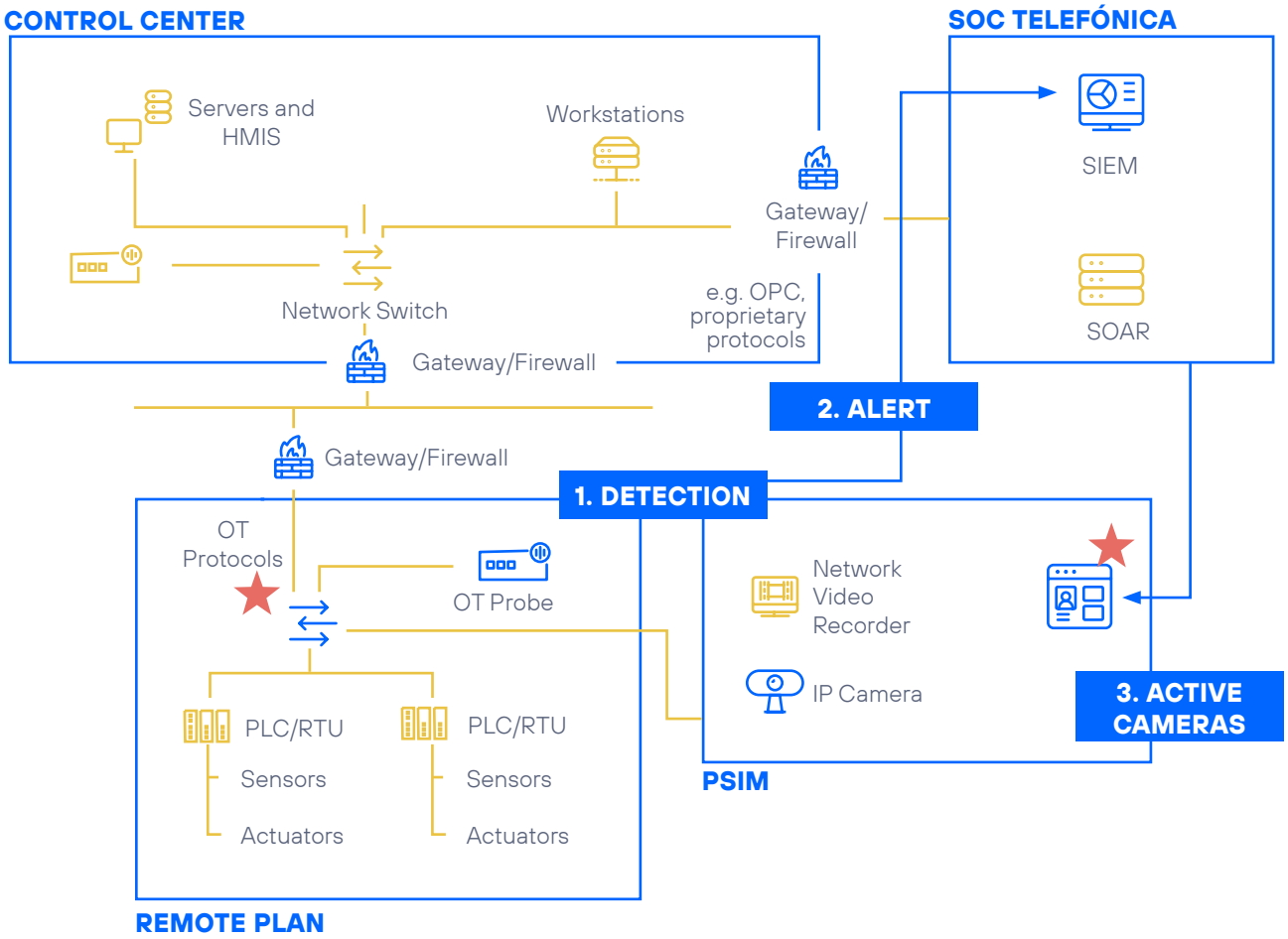
A network anomaly detection system installed in a plant detects that there has been an unauthorised reconnection to a switch in the control network of the OT environment.

2. ALERT

This system generates an alert that is sent to a central SIEM that receives and processes IT and OT events, which checks if there is an active work order.

3. ACTIVATE CAMERAS

If there is no work order, one is sent to the video surveillance camera control centre to focus on the room where the switch is located.



02 Telefónica Tech Proposal for OT Cyber security

Faced by an evident difficulty in addressing the problems and management of cyber security in this type of industrial environments and in full digital transformation, Telefónica Tech has created a proposal to help its clients in this complicated task.

02.1. Why Telefónica Tech?

Telefónica Tech, as part of Telefónica group, and now integrated in the new Telefónica Cyber Security Tech, has experience in the operation and security of complex environments and critical infrastructures such as telecommunications networks. The commitment to availability, SLAs, care in the implementation of updates and the protection of the infrastructure against attacks of any nature have been part of Telefónica's DNA for more than one hundred years. For this reason, our team understands the concerns and needs of its industrial customers,

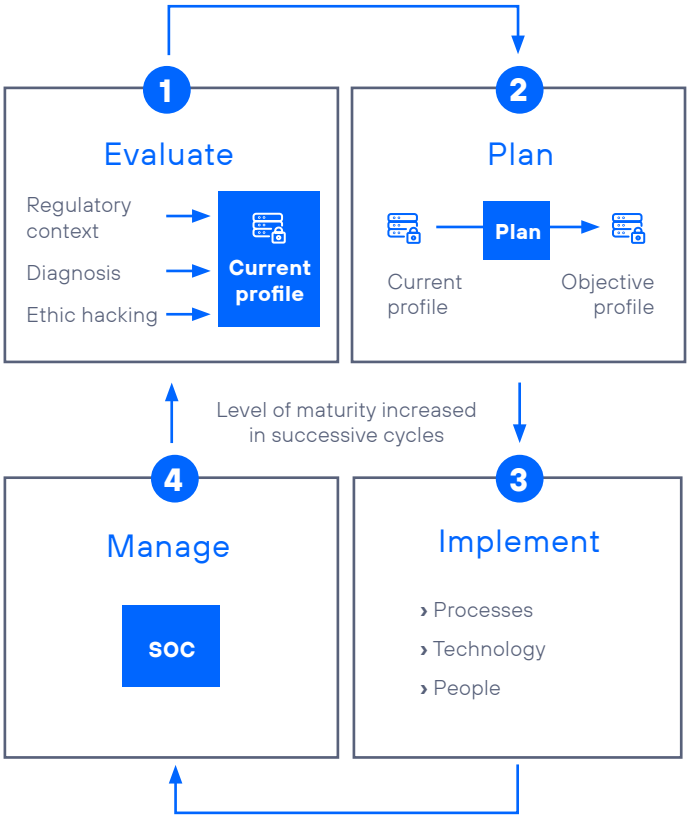
In fact, Telefónica is not only dedicated to protecting the networks in a logical way, but also physically. For more than 30 years, Telefónica Security Engineering has operated physical security projects for critical infrastructures, such as oil wells, airports, high-speed train tunnels, among many others. Telefónica is also a supplier of Cloud services, connectivity and management for IoT device networks and, of course, security for all of them.

Therefore, in Telefónica Tech we have a multidisciplinary team with a wide experience in cyber security applied to many sectors such as banking, IoT networks, online shops or industrial networks. Likewise, we can create a complete proposal for the current and future security of industrial organizations.

02.2. METEO Methodology

To tackle the challenge of industrial cyber security Telefónica Tech has created METEO (Telefónica Tech Methodology for Operational Technologies and Environments), a customised methodology based on a cyclical process to increase the level of security with each iteration.

The process consists of four steps:



› **Evaluate:** The current safety status is evaluated using applicable standards such as IEC 62443 or NIST 800 82 as a reference to generate a report on the safety status and recommendations for improvement.

› **Plan:** In the planning phase, an objective level of maturity that is to be achieved in the iteration is set and a decision is made as to which measures are to be used to achieve it, both technological and organisational.

› **Implement:** During implementation, planned changes and cyber security solutions are executed, with detailed monitoring of objectives and verification tests.

› **Manage:** Finally, the management of the measures that have been adopted is left. For this purpose, all the necessary documentation and training is provided and Telefónica from its SOC offers its full management.

For each of these steps, Telefónica Tech has a series of technologies and procedures that have been improving and adapting over time, assimilating the experience acquired in different projects and clients. The following sections will highlight these differential values of the Telefónica Tech proposal.

02.3. Evaluate and Plan

At Telefónica Tech we believe that the process of evaluating an industrial infrastructure should include two main aspects.

The first one is **classic consultancy work**, based on an understanding of industrial processes, risks, cyber security practices and, ultimately, all information collected from interviews.

The second one is **technical analysis,** using the latest tools to inspect assets and OT networks, always in an eminently passive way, carefully controlling any impact on production.

For this purpose, we have created a tool called ASPI_™ (Industrial Plant Safety Analyser). This tool incorporates various technologies to assess the cyber security of networks and assets, such as OT, IT or medical IoT protocol analysers, packet sniffing and remote connectivity. ASPI_™ allows us to make a technical diagnosis quickly and, if necessary, remotely, minimizing costs. This diagnosis allows us to have an initial idea of the most notable points of improvement in the organisation's cyber security, and so, we can prioritise and plan the next steps to be taken, which will enrich these classic consultancy tasks:

› **Maturity evaluation:** The maturity analysis allows us to know up to what extent the best practices of industrial cyber security are applied in the organization. In order to know this, we use some of the most recognized and used references and regulations in the field. The result is a 'GAP analysis' that allows for a roadmap to be drawn to improve the organization's cyber security posture, at technical, organizational and cultural level.

› **Risk Analysis:** While the maturity analysis evaluates the organisation's activities and processes against good practice, the risk analysis allows for the identification of specific risks affecting the organisation in its industrial assets to make better decisions: optimizing resources and directing investments to the most relevant risk mitigation projects.

› **Audit:** An audit allows a rigorous comparison of the level of security and compliantce under some standards, such as ISO 27000 and IEC 62443.

Once the results of the evaluation activities have been obtained, the planning phase begins. Our team of experts, together with the staff designated by the client, tackles these results in order to obtain the keys to the current situation.

The objectives to be reached in this iteration are then established based on multiple criteria such as the urgency of some risks, regulatory needs, implementation time and available budget in order to maximize the benefits obtained.

Finally, given these objectives, a project plan is created as a way forward to achieve the initial goals.

02.4. Implement

The implementation phase can be tremendously complex, starting with the question of which technology to install, which manufacturer, or how it will integrate with the rest of the company's systems and processes.

In recent times we have seen how the security solutions landscape changes almost from one week to the next, with acquisitions of new companies by larger and more established ones, inclusion of new functionalities, turns to cover new environments, announcements of integrations between various technologies, etc.

That is why it is very important to keep up to date, to know in depth all the available solutions, their differences and strengths and to apply in each case the most convenient one, taking advantage of the synergies between them.

For this purpose, at Telefónica Tech we have several laboratories in which to test all the technologies we work with. In these laboratories we verify the announced functionalities, make performance comparisons between each other and try out the latest developments and integrations. Likewise, generating very useful knowledge for us and our customers.

In addition, Telefónica Tech has partnerships with leading manufacturers and participates in multiple alliances to collaborate on improving cyber security technologies.

Telefónica Tech offers a wide range of solutions, adaptable to all environments and maturity levels, to help its customers improve specific aspects of their cyber security.

Segregation
Allows **OT networks to be made accessible only by the strictly necessary connections,** thus improving perimeter security.

Segmentation
Segmentation divides the network into areas and channels, **grouping assets for easier management and total control of communications** between them.

Monitoring
Monitoring **allows the detection of attacks on the OT and IoT networks,** looking for both known malignant patterns and anomalies on the normal operation of the network indicating a possible attack.

Safe remote access
To secure remote accesses with a unified platform that not only provides security for connections but also **monitors them, controls users and gives access only to the necessary assets.**

USB Protection
This solution **defends assets from malware infection through USBs** and also from electrical attacks such as those of the USBKiller.

Cyber Deception
It allows to anticipate the attackers, creating custom-made deception campaigns to discover their techniques and interests and to carry out an active defence.

Training and awareness
Training and raising awareness of people is a fundamental measure for the security of an organisation. General or specific courses can be given, for example, on industrial cyber security.

Cyber Range
The cyber range exercises are used to **train people through cyber security games with realistic environments, tools and attacks.**

02.5. Manage

The management of cyber security is as important as the implementation itself. As no matter how much technology is implemented, if it is not properly managed, it will be less and less useful in defending the organisation, and will only hinder workers and processes.

For that is why we have SOCs or Security Operations Centres. These centres manage technologies such as firewalls or monitoring probes, keeping them always updated and well configured for daily use. Thus, reducing the inconvenience for the client and freeing up their systems or IT area.

On the other hand, these centres also work on the integration of technologies so that, for example, firewalls, probes and logs from other devices are coordinated and used together in a SIEM.

Finally, the SOCs are responsible for coordinating and responding when a cyber security incident occurs, in which case they also work on automating the response to make it faster and more effective.

Telefónica Tech has a smart global SOC, distributed in several locations around the world, for 24/7 operation throughout the year.

These are some of its features:

Global Unified Costumer Portal: The client is provided with a unified portal that gathers panels with detailed information and indicators, complete vision of the security posture of the organization and with integrations of all the necessary sources.

Threat Intelligence Platform: The threat intelligence platform allows to know the context of adversaries that apply to the risk profile and generates TTPs and IoCs focused on customer cases to improve their defences.

Orchestration and automation: The orchestration and automation of the response to cases of use as phishing, port scans or SIEM alerts allows for great improvements in operation, reducing exposure time and standardizing response.

Managed Detection and Response: Managed detection and response is at the core of the iSOC offering, with EDR and rapid telemetry detection capabilities, against intelligence and deception campaigns to learn from adversaries and DFIR services where appropriate.

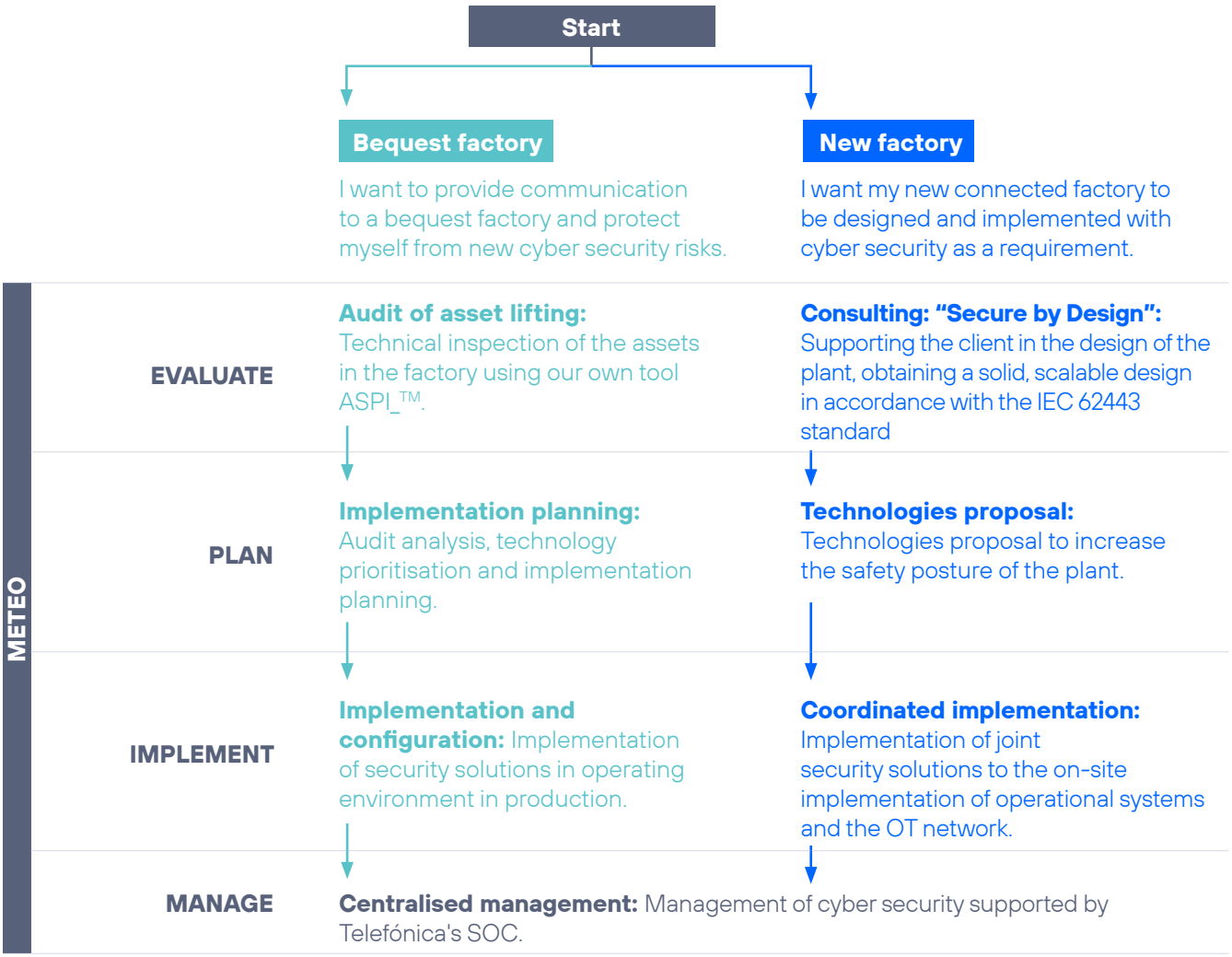
.

03 METEO Implementation in OT Environments

Telefónica Tech's methodology is applicable to all kinds of sectors, maturity levels and clients. When planning an industrial cyber security project on a specific production environment, we must differentiate between newly created factories and factories that are already running. In both cases, actions can be identified, planned and executed to improve the level of resilience of the environment. However, in the first case, they can be carried out from the design phase, which is highly recommended.

The following diagram summarises the different phases of the process to be followed in each case.

METEO: Telefónica Tech Methodology for Technologies and Operational Environments



If you want to know more about our methodology and portfolio and how it can be applied to your case, do not hesitate to contact us at hello.telefonicatech@telefonica.com

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. The company offers a wide range of integrated technological services and solutions in Cyber Security, Cloud, IoT, Big Data and Blockchain.