OT SECURITY

Designing and implementing technological and process solutions
to reach industrial plants and operational infrastructures' Cyber resilience,
by protecting their operativity and integrity.

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

WHAT ARE WE TALKING ABOUT?

AUTORI

Elio Di Sandro

Director of Offering & Solutions
Cybertech an Engineering Company

elio.disandro@cybertech.eu

Elio Di Sandro

With over 35 years' experience in the IT business, Elio has covered Technical, Sales and Managerial roles in Italy, Europe and US. He successfully ran international software and IT service business units. Elio currently is responsible for the IT Security offering and solutions' portfolio at Cybertech.

Aldo Lentini

Principal Security Architect - R&D Manager
Cybertech an Engineering Company

aldo.lentini@cybertech.eu

Aldo Lentini

Aldo is the Principal Security Architect in Cybertech since 2019, with a 20-year experience in the IT industry, that has started in IBM as Product Specialist. He is specialized in IT Security solutions, Identity Access Management, design of technological solutions for complex systems, feasibility verifications of critical technological solutions, design of complex technological components, and definition of Cybersecurity strategy and methodology.

Riccardo Morsicani

Principal Security Architect - Presales Manager
Cybertech an Engineering Company

riccardo.morsicani@cybertech.eu

Riccardo Morsicani

Riccardo is an IT and IT Security professional with over 15 years of experience in Identity Management, Identity Provisioning and De-Provisioning/Workflow, IT Security, Security Audit and Penetration Testing, SIEM technologies, Data Security, Architecture of the Company System, Design of the Security Infrastructure, Authentication and Authorization technologies, as well as customized Security frameworks.

1 TRENDS, CHALLENGES AND OPPORTUNITIES

The industrial world is facing a time of rapid and radical changes. The production process has evolved thanks to new operational technologies, with interconnected systems, data analytics, SCADA, ICS (industrial control systems), IIOT (Industrial Internet of Things) and intelligent sensors. The quantity and the quality of data generated by the new technologies means greater efficiency, but at the same time expose the infrastructure to greater security risks.

Industrial automation and control systems and operational technologies in vital sectors of our economy (transport, manufacturing, energy, and utilities) are currently not adequately protected, and as a result are becoming one of the main targets of hacker attacks. Critical facilities are increasingly under threat from individuals and organised groups. Hacker attacks directed at infrastructure systems can result in exponential economic damage for companies, creating malfunctions and interruptions to services and production lines, and compromising intellectual property. On a large scale they can cause losses of sensitive personal data or even endanger the health of individuals and the security of the environment.

According to Statista, in 2020 94.5% of respondents in a global survey say that the protection of initiatives digital transformation is a cyber security priority for the organizations after the pandemic of COVID-19. The epidemic has greatly accelerated the digitization of organizations around the world, since millions of employees work in digital workplace mode

This data demonstrates one of the problems that was amplified during the pandemic and the time of remote working: namely how to provide secure access to the applications and OT systems of critical infrastructure to operators and third-party maintenance staff, who connect via access points and unsecured networks, and often through unmanaged devices.

The vulnerability of the industrial control systems is a result of old operating systems, such as obsolete versions of Windows that are no longer supported and for which it is difficult to create patches. Cybercriminals understand these potential vulnerabilities and how best to exploit them.

Some sectors have a much larger attack surface than others. For example, the Energy & Utilities sector: in addition to IT risks (business applications, data, server/data centre infrastructures), at the level of operational technology the sector may also be subject to significant threats to the network needed to transport resources (power lines and acqueducts), which increasingly features ICS and IoT devices (SCADA and PLC system, Industrial, switches) that are possible targets for cyber attacks.

Companies that operate in the sector of critical infrastructures such as water, energy, transport, and communications depend heavily on systems located on both IT and OT networks to drive and control the day-to-day operation of their facilities. The same goes industrial networks, or for the healthcare structures themselves, such as hospitals and clinics, where the presence of OT and IoT devices is pervasive. Now, although most OT networks use legacy and proprietary protocols, many systems are migrating to standard protocols based on TCP and the IP stack, in a progressive IT-OT convergence. This has allowed IT teams to provide remote access or cross-network access more easily to OT systems. Organisations often use solutions that are accessed via VPN or services based on RDP (Remote Desktop Protocol) such as TeamViewer.

It was through a remote connection via TeamViewer that a hacker was able to penetrate the control systems of a water treatment plant in Oldsmar, Florida, at the beginning of 2021 and briefly increase the amount of sodium hydroxide fed into the plant by a factor of more than 100. The attack was quickly detected and blocked by service staff before any kind of damage could be done, but this incident demonstrates once again how obsolete control systems within operational networks that were designed without particular attention to security aspects can enable remote connections via the Internet through remote access tools, designed for use by administrators and maintainers, but exploitable by malicious actors.

Before 2020, hackers were already taking advantage of the vulnerabilities of services with remote access based on RDP and VPN, in order to compromise OT/ICS environments. These techniques became more popular during the pandemic as remote working also became widespread among companies in critical infrastructure management sectors. After all, a VPN system is an entry point frequently used by OEMs and integrators to gain access to operational environments and other settings. As many companies are reluctant to adopt adequate security measures and appropriate network segmentation techniques, access to an infrastructure through a compromised VPN allows attackers to move with sufficient and dangerous freedom within an industrial network, with a good chance of escaping detection.

Since 2020, cyber incidents have continued to represent the most important risk factor for Italian companies. At the end of 2020, many Italian companies found themselves targeted by cyber attacks aimed at data theft, disruption of web services, and ransomware with extortion. The situation is a concern for many countries besides Italy. The US Department of Justice has stated that in the first 6 months of 2021, hacking activities at a global level increased by 102%.

2021	2020	2019	2018	2015
Colonial Pipeline, United States	National Operator of gas, US	ASCO Belgium	Automotive giant	Ukrainian electricity grid
Belgium: parliament and a number of universities	Ekans ransomware on Honda	PILZ manufacturing, Germany	Cathay Pacific	
Ireland: health service	Water treatment plant, Florida	Deutsche Bahn		

Figure 1
The reality of cyber attacks on industrial infrastructure since 2015 (at a global level)

The consequences of cyber attacks on industrial infrastructure

If the IT sector is now the area where most attacks are concentrated, the OT sector should be of most concern, because an attack on critical infrastructure can cause damage to an organisation's business but also to the population of an entire geographical area.

Consequences for companies:

1. **Loss of operational continuity and the availability of critical systems and components with unplanned periods of inactivity.** An attack on the OT infrastructure involves shutting down the installation or the infrastructure connected to it for a certain time and/or for a part of the installation, before resolving the problem and restarting. This is the case when it comes to shutting down parts of a plant, or where threats from the production area may compromise corporate servers (e.g. CED).

2. **Data integrity and confidentiality, including the violation of data, manipulation of data, and configuration.** The subtraction of data and information from the production process (subtraction/diffusion of confidential data by machines, including configurations).

3. **Problems of quality and performance.** The presence of malware or the generation of unwanted traffic can introduce latencies of even a few milliseconds. This cannot be tolerated in an industrial setting, leading to a degradation of performance or a drop in production quality.

4. **The health and safety of individuals.** Threats may directly or indirectly involve the alteration/inhibition of security functions on machines, systems or environments, exposing personnel and all those interacting with such systems to risks in terms of their health and safety.

5. **Compromised environment.** The manipulation of production and control equipment can lead to dangerous environmental emissions, such as the discharge of toxic gases, the release of pollutants into the water table, or the introduction of excessive quantities of substances, or even block the introduction of substances (e.g. a dam), endangering both people and the environment.

6. **Economic losses caused by significant impacts on the performance of the industrial plant and the loss of quality.** Threats may alter the production process, with modifications to the product in terms of quality (an increase in non-confirming products) and quality, or they may manipulate the management of conforming/ non-conforming products.

7. **Damage to the company's image.**

8. **Loss of clients.**

Consequences for some specific sectors:

1. **Energy -** impacts on the entire supply chain (generation, transmission, distribution, sale) related to power outages to consumers
2. **Gas -** temporary blocks on gas supplies for the winter period, efficiency reduction compared to production
3. **Water -** damage that may be caused to the population (water quality for human use) and the environment (spillage of waste water into rivers, parks, etc.)
4. **Waste -** blocking the life cycle of municipal waste (smart bins, logistics management) and industrial waste (environmental damage from hazardous waste)

The financial impact of a cyber attack

Let's start with the fact that the average cost for one hour of downtime can reach hundreds of thousands of dollars.

Now, unavailability may have various causes and impacts, as illustrated in Figure 2, where the most common and frequent malfunctions are to be found in the plant's operating activities, which are subject to equipment misconfigurations or unstable process values on a daily basis, albeit (fortunately) in a limited way. Then there are less frequent but longer-lasting or more significant downtimes due to the industrial network and the plant infrastructure as a whole, such as connectivity problems at gateway level or the unavailability of certain field devices, or communications using poorly formed or non-conforming protocols.

But undoubtedly the shutdowns that have the greatest impact are those caused by cybersecurity attacks which, although much less frequent, cause the most significant damage in terms of the duration of the unavailability of systems and the number and criticality of those involved.

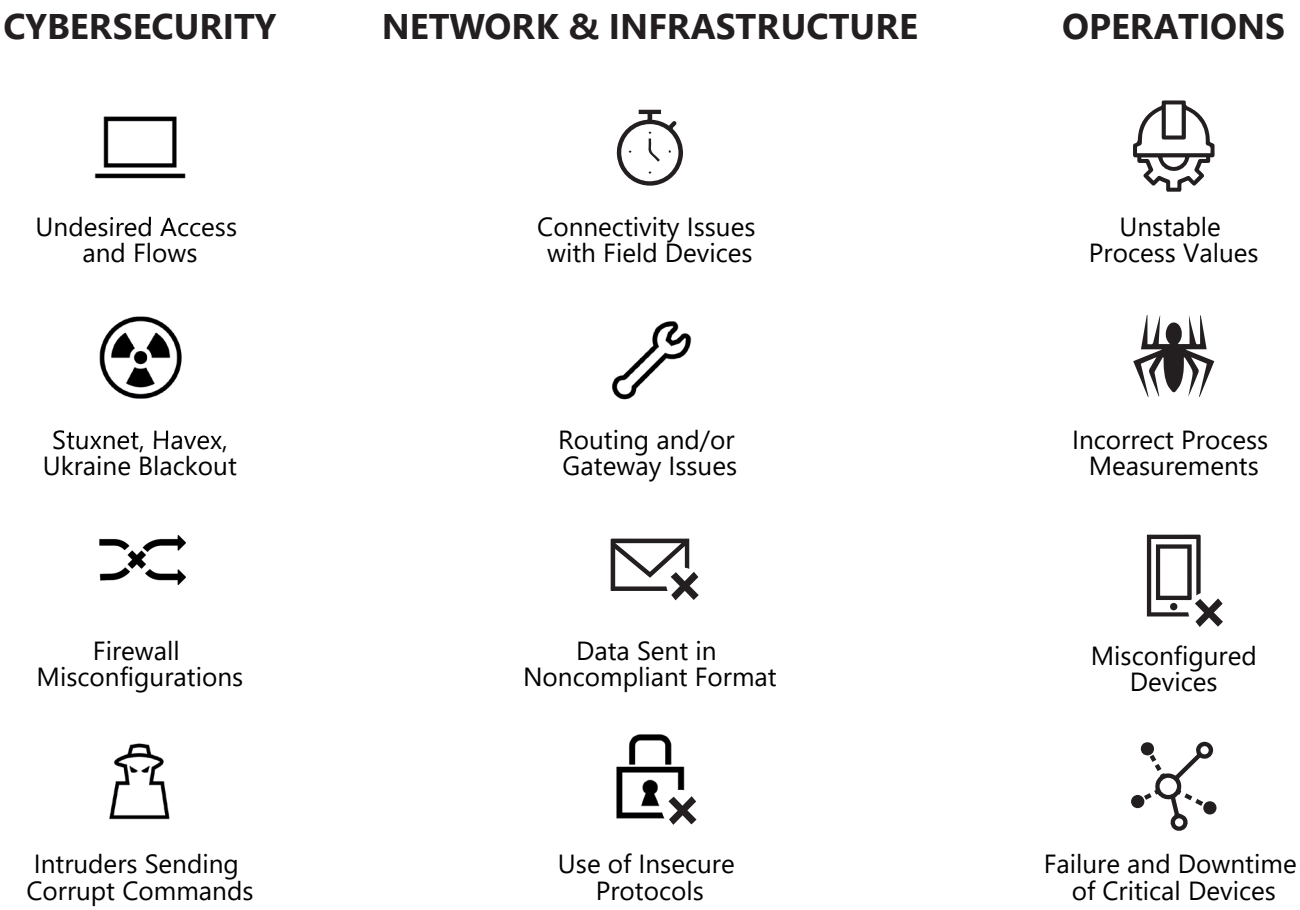


Figure 2
The cyber risk and the financial impact for critical infrastructures

Technological and market trends

The opening up of critical infrastructures to the IT world and to new technologies such as Cloud, IoT Mobile, wearable devices and ~~Smart Cities~~ has increased the level of risk exposure. In the past, the perimeter of attack was restricted to the physical site itself, but today there is a disjointed perimeter that is highly vulnerable and difficult to monitor.

In this expanded perimeter, the main technological and market trends fuelling cybersecurity risks in the OT world are:

1. **Convergence between ITand OT:** OT networks are no longer separate, threats have shifted from cyber to physical, assets are extremely critical and can rarely be upgraded or hosted by an agent.
2. **Threats targeting non-traditional devices and interconnected objects:** IoT and OT threats are constantly growing, new attacks are increasingly sophisticated, and companies have a limited ability to detect APTs and remedy threats in real time.
3. **he cyber risk becomes a risk in terms of performance, operational continuity and physical security.** The priority is to guarantee the continuous availability of systems, thus avoiding all potential operational problems, such as system errors and downtimes for critical devices, configuration problems with field devices, insecure protocols, and data sent in non-compliant formats.

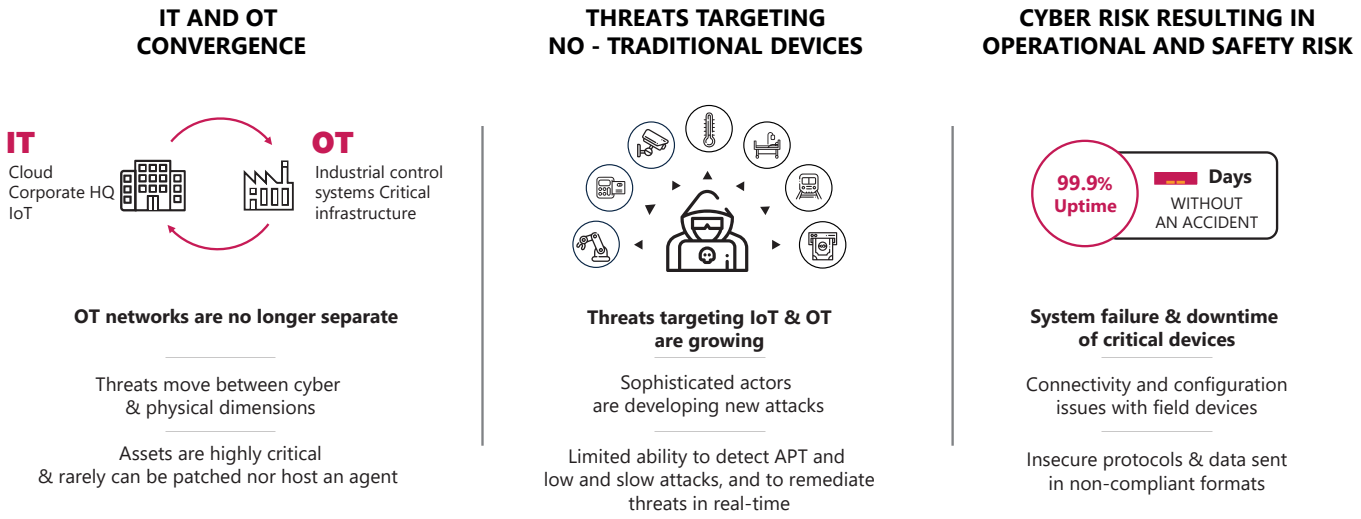


Figure 3

The challenges

In OT environments, cybersecurity challenges are combined with everyday network and operational problems. Below we address some of the main ones:

1. **Visibility and inventory of IoT/OT communications and assets.** The interconnection between devices (IoT, Smart City, Smart Products and Wearable) has disrupted the perimeter of attack, going beyond "on site" devices and multiplying the number of objects that are linked. The limits of segregation have been exceeded and managing the new, expanded perimeter is extremely complex. Furthermore, managing the security of such objects is often entrusted to the IT department, which has little if no visibility over the activities of introducing, removing, and modifying these objects by the OT department, which focuses on production issues.

2. **Management of risks and vulnerabilities.** Cyber-physical systems are connected and produce large amounts of data, while cyber attacks are becoming increasingly sophisticated and targeted.

3. **Continuous monitoring of IoT/OT threats, responding to incidents and intelligence regarding threats.** OT networks and devices were not designed with cybersecurity in mind, as evidenced by the lack of authentication systems, the limited use of cryptography to protect communications data, and the absence of network segmentation and segregation (OT networks are generally flat).

4. **The opening of OT networks and convergence towards IT architectures.** The communication of OT systems is increasingly based on the TCP/IP stack, making interoperability and access easier but less protected, and therefore increasing vulnerability to malicious intrusions. To guarantee operability, ease of access and the reduction of costs in the operation of OT facilities, what was once segregated and isolated is now increasingly open to the IT world and TCP/IP technology protocols, as this move allows greater interoperability and more flexible access to industrial equipment. The opening up of critical infrastructures to the IT world has increased the vulnerability of the OT system, given that a large quantity of malware travels across the protocols of the IT world. There is therefore a greater possibility of creating potential access points for attackers, who use IT protocols and architectures to enter the interconnected OT world with the same technologies

5. **Unified IT/OT security monitoring and governance.** Cybersecurity for OT machines and IoT devices involves challenges in terms of technology, people, and processes. These challenges start with the infrastructure and extend to involving complex and specialised operational processes.

Addressing these challenges, cybersecurity solutions for the OT world affect multiple domains and must be able to detect threats before they lead to operational or cyber incidents with disastrous consequences, providing the information that companies require to become more cyber resilient.

At the same time, however, cybersecurity technologies applied to Industrial Control Systems (ICS) and to and critical infrastructures can give companies with a high density of machines and operational and production assets full visibility within their supply chain, helping operators to visualise and segment their network and continuously improve operations, while maintaining system and configuration hygiene.

How, then, can the requirements of OT security be combined with the operability of industrial plants?
The advantages of an OT security solution can be divided into three key areas of interest: cybersecurity, networking, and operations.

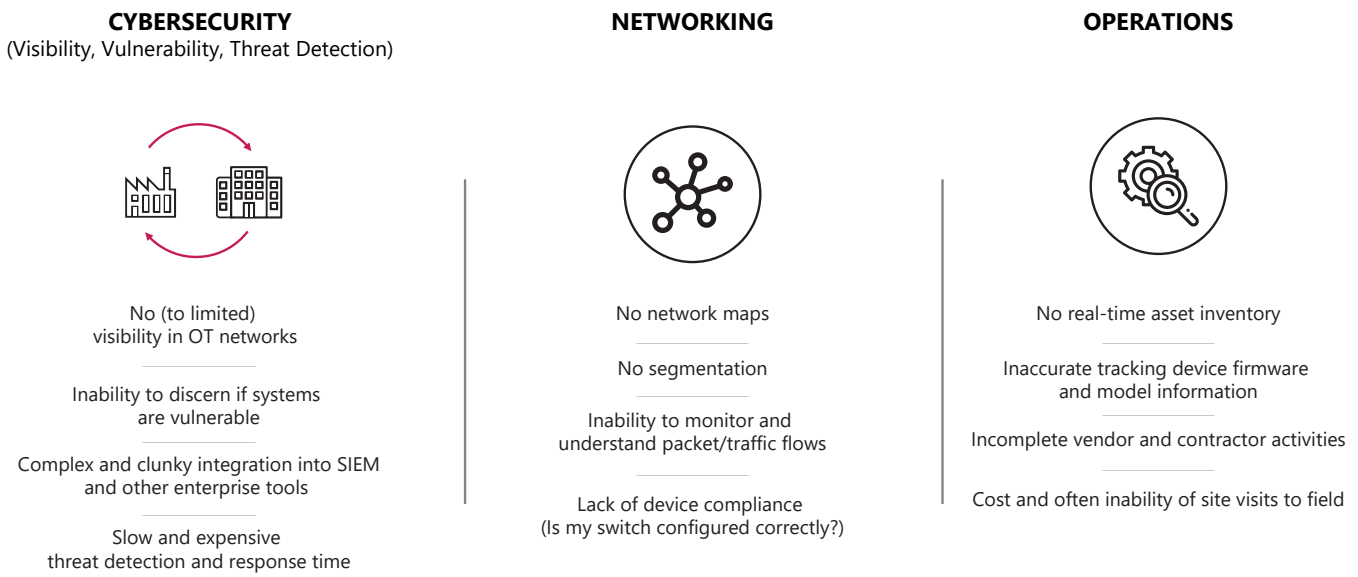


Figure 4
How we face the challenges of OT security

So, as outlined in the figure, the challenges and advantages of OT security can be subdivided into three key areas of interest:

1. **Cybersecurity**

   Cybersecurity for OT machines and IoT devices is confronted with unique technical challenges, but is also related to the human factor and industrial processes, including:

   - limited visibility or complete invisibility on OT infrastructure equipment and devices, and in general on assets connected to the OT network, their configurations and compliance, with little ability to identify critical vulnerabilities.
   - complex and specialised infrastructure and operational processes
   - OT networks and devices designed without considering elements of architectural security: lack of authentication, cryptography, networks
   - IoT, which has expanded the attack surface: cyber-physical systems are connected and produce data
   - cyber attacks that are targeted and more sophisticated
   - communication with OT systems increasingly based on the TCP/IP stack, making interoperability and access easier but also increasing vulnerability and the attack surface
   - need to maximise the use of limited resources.

2. **Networking and segmentation**

   - lack of mapping and visibility of OT network topology, with insufficient ability to identify network equipment configurations and conformities
   - difficulties in monitoring communications between components and analysing traffic flows
   - lack of network segmentation and segregation (OT networks are generally flat).

3. **Operation and scope of the OT infrastructure**

   - lack of asset inventory, with absence of attributes and specifications on software and firmware installed on board
   - poor tracking of changes as well as update and maintenance activities by suppliers and contractors.
   - difficulties in accessing industrial infrastructures for maintenance and updating activities.

OT security solutions provide businesses and operators of critical infrastructure with full visibility of system technologies and their infrastructures. They help operators to visualise and segment their network via interactive maps, and detect threats before they lead to operational or cyber incidents with disastrous consequences, providing actionable insights with the information needed to become more cyber resilient.

At the same time, cybersecurity technologies applied to ICS and critical infrastructures provide asset managers with full visibility of their supply chain and help operators to visualise and segment their network and continuously improve operations, while maintaining system and configuration hygiene.

2 OT SECURITY: STANDARDS AND REFERENCE FRAMEWORKS

A defence strategy cannot be improvised. Extemporary solutions, i.e. to remedy a single flaw, are sometimes necessary in emergency situations but quickly become obsolete and lose their effectiveness.

Although tactical, all cybersecurity technology solutions - in the world of IT as well as for ICS and operational infrastructures - are aligned with and derive from sector standards that represent an established reference point, offer comprehensive coverage of use cases in the various IT and OT cybersecurity intervention categories, and are continuously updated following technological evolutions and changes to the threat landscape.

In the table below, all the **standards that already form the established reference point for OT security** are listed. The most important of these is the **ISA 99/IEC 62443**, which gives us the possibility of approaching security with a model guided by the priority of intervention (risk-priority) by focusing on the risk that must be controlled and the residual risk that can be tolerated, creating a map and a guide directed by priorities.

These references identify a series of models, methodologies, tools and practices that should be adopted to respond in a structured and effective way to a cybersecurity attack on an industrial plant or critical infrastructure, and to maintain an adequate safety and security position by design and by default in configurations and communications as well as in the software and firmware components of devices and equipment.

Making reference to the specific frameworks and standards for OT security, it is possible to carry out targeted risk analyses and assessments for the industrial mode, identifying intervention priorities and consequently implement **balanced actions that are synergic and multilevel**, making use of **technologies** as well as the **processes** and the **people** involved.

Figure 5.
The reference standards for OT security

3 THE VALUE OF OT SECURITY

Obiettivo cyber-resilienza

The ultimate objective of cybersecurity for operational and critical infrastructures is to obtain operational cyber resilience by mitigating the cyber risk through technological and process-based solutions that operate on multiple levels and can provide:

1. **Visibility and protection of devices and networks:** monitoring the activities of devices within the ICS in real time to prevent violations and mitigate the risk of unforeseen downtimes, thus reducing operational costs
2. **Threat and anomaly detection:** identifying known and unknown threats in their early stages to remain up-to-date with targeted and common threats
3. **The capacity to respond to and effectively resolve cyber incidents:** knowing what is happening at all times and easily sharing data with the organisation to be able to react quickly and effectively in the event of a breach and implement verifiable recovery.

DEVICE VISIBILITY, IDENTIFICATION AND PROTECTION

THREAT AND ANOMALY DETECTION

CONTROL, RESPOND AND RECOVER

The main functions and the technological areas

The main functions and the technological areas covered by OT security solutions are:

1. **VISIBILITY AND MONITORING OF THE OT NETWORK** with detection, profiling, classification, and monitoring of resources. Visibility, with automatic and recurrent discovery of plant assets, should include, as we were saying, profiling, classification and a continuously updated inventory of devices and systems in the various layers and segments of the OT network. This function is useful both for security, and for the performance and operability of the network itself by maintaining overall system hygiene. The visibility of the OT network must be considered as a key capability, rather than just a security requirement, as the availability of information regarding assets is essential for prolonging their life cycle and optimising performance management.

2. **SECURITY BASED ON THE DEFENCE OF THE OT NETWORK** (protection/detection/response), with segregation and control of the flow of data between IT networks and OT environments, and a network architecture based on the segmentation and isolation of critical sub-networks of the plant. Industrial network security includes basic functionalities and an architectural design orientated towards segmentation and segregation of the network, and the appropriate deployment of firewalls and IPDS specific to industrial protocols, to guarantee effective protection and blocking of malicious or malformed traffic based on known signature and attack patterns. On top of these basic functionalities it is possible to add further network protection systems or anomaly detection systems through network traffic analysis and deep packet inspection. These may include:

   – one-way gateway technology (data diodes), often used to ensure that traffic flows only in one direction;

   – Industrial firewalls and IPSs (Intrusion Prevention Systems), as well as advanced network traffic analysis (NTA) systems using behavioural and machine learning algorithms.

3. **DETECTION OF ANOMALIES AND MANAGEMENT OF VULNERABILITIES, consisting of:**

   - detection of threats and malfunctions in the OT infrastructure, including vulnerability management and continuous monitoring,
   - detection of data integrity manipulation, based on rules, attack patterns and known signatures (deterministic) and supported by advanced analytics based on behavioural analysis, as well as machine learning and artificial intelligence algorithms.

4. **AUTHENTICATION AND AUTHORISATION TO ACCESS SYSTEMS AND PLANT APPLICATIONS AND SECURE REMOTE ACCESS** which guarantees

   - secure remote access for partners and third party employees
   - full control for plant personnel to authorise, time limit, terminate and view recordings of any remote access connection
   - launch from the system of all network connections: no listening ports, no direct attack surfaces.
   - secure and granular remote access, more accurate than VPN or remote desktop services, controlled by protocol, user, application, destination node.
   - technical staff, off-site experts, technical support, assistance in the field, third-party support, everything everywhere.

5. **PROTECTION OF ENDPOINTS AND SERVERS** through system hardening techniques, as well as the adoption of industry-specific endpoint protection and EDR technologies, which provide advanced host-level malware detection and blocking, as well as safeguarding of files and system configurations and protection of on-board firmware. These enable:
   - advanced protection of the system, anti-malware, personal firewall, control of ports and devices;
   - cryptography, memory protection, configuration and management of security-related patches, portable media management; application control and whitelisting.
6. **OT ASSESSMENT OF THE TECHNOLOGICAL PROCESS AND RISK ANALYSIS** in compliance with industry reference standards, such as ISA99-IEC62443.

These are the main areas of technological intervention in the field of OT security, upon which we base the solutions that address the containment and mitigation of risks arising from cyber attacks to our industrial customers. For example, if it is necessary for maintenance workers to be connected remotely and securely, a client must decide whether to connect them using tools provided by the company and in a specific, dedicated environment, or using tools belonging to those responsible for maintenance, thereby allowing access to all of the company's IT environments. Addressing this specific example involves several of the areas of technological intervention just mentioned.

For example, the segregation and segmentation of the network, as well as strong authentication, granular and selective authorisation based on access profiles and the targeted use of plant systems, are architectural attributes that should be considered and implemented with particular care. These architectural attributes should include:

- **The isolation and control of traffic and of access to different network segments,** or the segmentation of the DMZ network from the IT network, and the segregation of the IT network from the OT network, with the ultimate goal of preventing and detecting undesirable lateral movements between the various network segments.
- **A component dedicated to the control of and secure access to OT** systems by users both internal and external to the organisation, and capable of:
  - **supporting** various user profiles (employees, contractors, third parties)
  - **providing access** only after establishing a safe channel with an authenticated user, normally through reverse-access technologies (outbound), which eliminate the need to open inbound ports to internal firewalls of critical infrastructures
  - **keep users** who have been given access (to certain data and applications on the basis of a specific profile) out of the network
  - **control** the use of legacy applications and remote access
  - **add** two-factor authentication to legacy and non-web applications that do not normally support MFA.

Consequently, even for an apparently targeted case, all the above issues must be considered. Cybertech, a company within the Engineering Group that specialises in cybersecurity, provides its clients with solutions based on technologies, processes and operational standards to avoid unauthorised access as well as possible malfunctions or damage to industrial equipment.

And that's not all: in fact, in addition to the emerging issue of guaranteeing secure and controlled remote access to the network and OT/ICS systems, we have seen that there are further technological and process domains of intervention that need to be addressed, and that represent as many core functionalities of OT/ICS cybersecurity architectures. In summary, the listed domains can be grouped as follows:

- **Visibility,** with automatic and recurring discovery of plant assets, including profiling, classification and a continuously updated inventory of devices and systems in the various OT layers and segments. This function is useful both in terms of security, as well as for the performance and operability of the network itself.
- **Industrial Network Security,** which includes basic functionalities and an architectural design orientated towards the segmentation and segregation of the network, and an appropriate deployment of firewalls and IPDS specific to industrial protocols, for the effective protection from and blocking of malicious or malformed traffic based on known signatures and attack patterns. It is also possible to graft additional systems for the analysis of network traffic and deep packet inspection onto this basic functionality.
- **Server and endpoint protection,** through system hardening techniques, as well as the adoption of industry-specific endpoint protection and EDR technologies, which offer advanced host-level malware detection and blocking capabilities, as well as safeguarding the integrity of system files and configurations, and on-board firmware protection.
- **OT process and technology assessment,** and risk analysis in accordance with industry reference standards, such as ISA99-IEC62443

4 ENGINEERING IN OT SECURITY

We have seen that the field of OT security presents many different challenges, which are also the drivers of security solutions in the OT world. **Our approach to OT Security is to design and implement technology and process** solutions and deliver managed services to support clients in:

- reducing the risk of business interruptions due to events or security breaches and avoid unplanned downtime
- ensuring that any abnormal behaviour in OT network flows and connected assets is detected in real time
- intercepting and blocking known threats and zero-days
- protecting the confidentiality/integrity of data and the configuration of critical resources
- quickly identifying vulnerabilities requiring responses, with priorities for action
- guaranteeing and demonstrating compliance with security and satisfying audit teams with the correct level of checks in place to be operationally effective
- increasing productivity in security operations
- limiting operational problems and improving the hygiene of the OT network and maintenance operations
- controlling remote access, blocking unwanted access, and minimising authorised access, while reducing unplanned maintenance due to misconfiguration of devices
- detecting equipment in an automatic and non-intrusive manner, and maintaining an up-to-date inventory of assets connected to the OT network, with sufficient details regarding hardware, software, and firmware components, functional attributes and configurations, for the purpose of correct classification and profiling of plant equipment
- gaining more control over device reconfiguration and non-synchronisation.

Taking into account the challenges and priorities of intervention imposed by the evolution of OT security for industrial and critical infrastructures, the above-mentioned approach of end-to-end integrators for OT Security solutions is declined in a value proposition articulated in two strands of intervention:

1. Risk assessment and planning of actions to improve the security position

Starting with business objectives and priorities, we assess which assets are fundamental to the business based on the critical scenarios that might occur and the impact they might have on business continuity, availability of critical components and systems, data confidentiality and integrity, data manipulation/exfiltration, environmental safety, and, finally, quality and performance.

Identifying the most critical areas within the plant/system, we define the consequences of a potential violation and the impact of this at company level. The evidence of the high-level risk assessment is presented to the company management. On the basis of these results, a risk assessment at a more specifically technical level is carried out on

specific critical systems to establish vulnerabilities on the basis of identified threats and to assess risks according to business criteria.

2. **Technological implementations with a multi-dimensional approach** to identify/protect/detect/respond to cyber threats, **based on market-leading OT cybersecurity platforms:**
   - visibility, profiling, classification, and monitoring of assets
   - security and segmentation based on the network
   - detection and blocking of threats and anomalies in network traffic
   - anomaly detection, vulnerability management, and protection of hosts (endpoints and servers) in the OT infrastructure
   - remote access control and security
   - convergence of SOC IT/OT

Designing and implementing technological and process solutions to reach industrial plants and operational infrastructures' Cyber resilience, by protecting their operativity and integrity.

5 WHAT WE DO

In terms of our skills and articulated value proposition in the two intervention directions indicated (i.e. risk assessment consultancy services and technological implementation), there are three categories or domains into which our services and portfolio of OT security solutions can be divided. In addition, there are "cross solution" services such as overall security governance or the implementation of a single, seamless security operation centre between IT and OT events.

Figure 7.
Service domains

- **OT assessment:** predominantly guided by the security frameworks and regulatory compliance, this aims to present a snapshot of the current security position (AS-IS), evaluate the security maturity level and the discrepancy compared to the objective (TO-BE), allowing the identification of an evolutionary roadmap based on risk reduction and the specific needs of the client
- **OT visibility, protection and anomaly detection** entails the introduction of technological and process-based solutions, enabling the visibility of all assets and their protection. They detect and block the threats travelling across elements of the network and the host, identifying possible errors using both a signature approach and deviation from a self-learned baseline.
- **OT secure remote access:** this refers to a functionality that emerges at times of access to critical infrastructures and plants through unsafe networks, or the securing and control of remote access to infrastructures.

These service domains are complemented by governance, risk and compliance services for the management of processes and staff, and Cybertech's SOC for the monitoring of client system security. Below, you can find several case studies that are explored in the three categories mentioned above, based on the real needs of customers we have supported.

OT Assessment

This is carried out to identify gaps, assess the current security maturity level, identify deviations from the target position, and draw up a response plan based on risk prioritisation, to bring the current state in line with the target state.

This activity is carried out by interviewing the client's "Key People" in order to identify the processes and evaluate the countermeasures present with respect to the reference framework adopted (NIST, ISO 27001). In addition, network diagrams and documentation are acquired to support the findings of the interviews. It is possible to increase the detail of the analysis by introducing a technical analysis consisting of a scan of a significant and representative part of the OT network, in order to obtain objective evidence about the state of the industrial lines scanned. The results of the analyses can be summarised as follows:

- risk assessment of both business-related and technological processes with the support of objective evidence gathered in the field
- analysis and reporting of the current security maturity level and deviations from the desired level
- intervention plan based on the risk priority to bring the security maturity level in line with the desired level

CASE STUDY: A company in the fashion sector required a technical evaluation of the OT/IoT devices physically distributed in each shop. The activities carried out:

- definition of the intervention perimeter
- mapping of the requirements and solution selection
- definition of the implementation roadmap
- Transformation of the roadmap into a detailed plan and drafting of a final report.

The OT Assessment solution offered by Cybertech was carried out according to intervention priorities based on risk mapping and classification. During the first phase, the security position was evaluated in general terms according to a process that entailed the following activities:

1. **definition of business objectives and business priorities:** we defined what was truly critical to the company on the basis of the scenarios that could affect the continuity and availability of critical components and systems: in particular the confidentiality and integrity of data, which could allow the manipulation/exfiltration of data, endangering physical safety, environmental sustainability, as well as quality and performance.

2. **identification of risks at a high level:** we identified the most critical processes and areas within the plant/ system, the consequences of a potential breach, and the possible impact of this on the business.

3. **presentation to the management:** we summarised the most significant concepts highlightedby the assessment of risk at a high level.

4. **definition of a detailed strategy:** on the basis of the results of the high-level risk assessment, we performed a detailed assessment of the risks to specific critical systems, in order to recognise vulnerabilities vis à vis identified threats and assess risks against business logic criteria. The detailed assessment established the likelihood of an attack, identified crucial vulnerabilities, and planned mitigation actions.

In this specific analysis phase, the technological risk assessment was carried out following the steps detailed below:

1. **network scanning and traffic acquisition:** to identify the network architecture, connected systems, typology of devices, protocols used, traffic data and potential threats.

2. **vulnerability assessment:** to compare detected vulnerabilities with effective threats to assess the real risks to the business.

3. **additional tests:** to complete the vulnerability assessment and assess other vulnerabilities or misconfigurations based on specific protocols and devices.

4. **detailed risk assessment:** assessment of the likelihood of a cyber attack in relation to existing vulnerabilities and countermeasures, where the high-level investigation has already identified the consequences and business impacts of a cyberattack.

01 BUSINESS RATIONALE		What's really critical for my company? Based on critical scenarios that might occur, impacting: • Business Continuity and Availability of Critical Components and Systems • Data Confidentiality and Integrity, Data Manipulation / Exfiltration • Safety • Environmental • Quality and Performance
02	HIGH LEVEL RISK ASSESSMENT (HLRA) DEFINES CONSEQUENCES / BUS IMPACT	What are the most critical areas inside my plant/system? Define the consequences of a potential breach and business impact
03	PRESENTATION TO MANAGEMENT	What has High Level Risk Assessment highlighted?
04	LOW LEVEL STRATEGY FOCUSES on CRITICAL SYSTEMS and DEFINES PROBABILITY of ATTACK, IDENTIFIES CRUCIAL VULNERABILITIES and PLAN to COUNTER	Based on result of the HLRA, Low Level Risk Assessment is performed on specific critical systems, so to recognize vulnerabilities against identified threats and assess risks against the Business Rationale criteria.

Figure 8
The risk-priority-driven approach

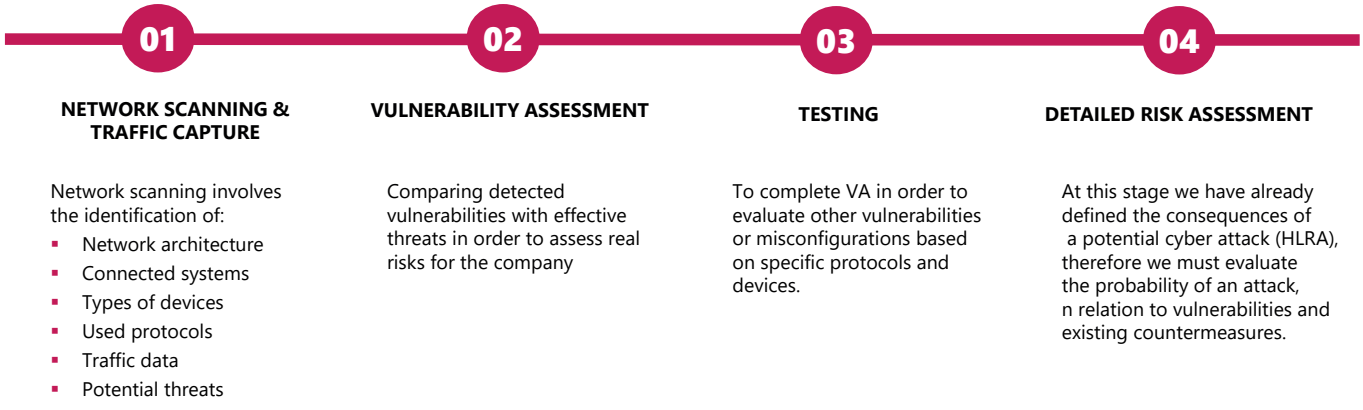


Figure 10
The key steps of the risk assessment

OT Visibility, Protection and Anomaly Detection

We ensure a solid and resilient overall security position by introducing specific technologies and designing customer solutions, such as:

- revision of the OT network and the introduction of segmentation
- the use of Intrusion Detection and Protection System (IDPS) devices
- the introduction of passive probes and/or active sensors to collect all OT traffic, monitor it, and analyse it
- the use of management consoles that allow for the centralised analysis of OT network traffic to identify anomalies and threats alongside the generation of related alerts, consolidation of a constantly updated and detailed OT inventory, evidence of possible vulnerabilities
- the activation of automatic responses for blocking anomalies and isolating suspicious traffic
- monitoring of the integrity of firmware and alerting/blocking in the case of abnormal tampering attempts
- integration of the OT world in the processes of vulnerability management
- the extension of SOC and NOC centres, including in the context of the networks and OT/IoT devices

These types of intervention translate into a series of advantages for our clients, including:

- a complete and constantly updated inventory of all OT devices, including all specific details (Vendor, Firmware, Vulnerabilities), as well as networks, reconstructing their topology and communication flows.
- the possibility of automatically detecting new devices present within the networks as well as any unmanaged or suspicious devices.
- the detection of operating anomalies, either by algorithms that use signatures or by behavioural analysis, reporting any deviations from the base scenario. It is stressed that this methodology is particularly effective in a manufacturing world where operations are sequential and cyclical.
- blocking attacks automatically either by recognising known attack patterns (virtual patching) or through integration with devices such as firewalls to isolate suspicious traffic. In this phase, the design and configuration activity aims to avoid the introduction of false positives that could lead to unjustified production stoppages with an impact on the business.
- reconstruction of the network map in order to identify and introduce micro-segmentations within the network.

CASE STUDY: A global shipping company had to update the processes and the on-board systems to comply with the new IMO regulations. This required network remodelling and equipment renewal for more than 100 cargo ships. The activities carried out:

- evaluation, gap analysis and redesign of the architecture
- Introduction of OT/IT segmentation
- automatic OT asset detection and inventory
- detection of network threats and anomalies, all in air gap conditions.

OT Secure Remote Access

We introduced a solution for centralising remote access to all production plants in order to control and protect access to networks, devices and operating machinery, introducing security elements such as dual factor authentication and explicit access authorisation, as required by IEC 62443. In addition, these systems also allow for the continuous auditing and accounting of plant activities; simplify management by using a single outbound connection channel from the plant; implement the principles of least privileges by profiling the maintenance staff who have access, guaranteeing visibility of devices and specific access permissions for maintenance staff; and centralise cybersecurity skills without requiring the presence of dedicated staff within each plant.

To summarise, we intervened by enabling:

- the central system for access control and "reverse proxy" for installations
- the outgoing connection from the installation's firewall
- the management of passwords
- the management of sessions (control, four-eye principle, communication)
- access rules and MFA
- encrypted connection, controlled jump server
- IAM integration

CASE STUDY: A company producing food and beverages worldwide needed to provide external users and contractors with remote access to each plant, controlling sessions and landing connections to the "jump-server" equipped with an OT Tool for maintenance.

The activities carried out:

- request for qualification
- selection of software
- architectural design
- technical and financial offer
- project delivery

Monitoring and Response Incident Room (Security Operation Centre)

With the explosion of Cloud, Mobility, Big Data and - last but not least - the IT/OT convergence, the processes of digital transformation have radically changed the technological landscape of information security. On the one hand they have led to an explosion and fragmentation of the attack surface; on the other hand they have triggered the proliferation and stratification of point solutions, segmented and spread over a wide perimeter, which are often difficult to manage as a whole. I**t is therefore essential to centralise detection, i.e. the surveillance of critical infrastructures and the monitoring of assets, in order to identify and counter criminal activities.** With a long list of new tools, professionals must now process large quantities of information deriving from numerous security and control systems, while also making important decisions such as how to respond to alarms and incidents.

The emerging need is for an **integrated and multi-modal** approach to cybersecurity, encompassing information technology (IT) and industrial control systems and operational technologies (OT/ICS). This approach translates into more intelligent IT solutions, able to operate synergistically.

We started, therefore, from the vision that a greater accessibility of devices and interoperability of systems on decentralised networks virtually eliminates boundaries and interconnects IT and OT Operational domains. This was the context for the design of a **SOC**, Security Operation Center, which is able to **recognise** and **signal** any Indicators of Compromise (IoC), **analyse** alarms, and activate the processes of **responding to** and **containing** any threats detected.

By way of example, the specific characteristics that are required for a SOC for OT environments are the following: the ability to **collect** telemetry from the field (at all levels of the Purdue Model); to **correlate** this information and (most importantly) to harmonise it with the information collected by the IT/campus environment; and to offer **enrichment** with automatic processes that interrogate additional and external information sources (e.g. sources of threat intelligence, HR, asset management systems, identity systems, etc.), in order to use advanced analytics algorithms to **identify** each individual alarm in the operational and technological context of the client and **update** it in the external global cyber threat landscape.

The ability analyse data and to correlate and contextualise them with **automatic processes** is the real differentiating keystone of a modern SOC: not only does this allow false positives to be reduced to a minimum, but, most importantly, it considerably increases the heuristic potential of the SOC itself, extending the detection capacity to a whole series of advanced **and complex** threats that might otherwise be left to operate undisturbed.

Here at Cybertech, we have developed and consolidated an **"OT Ready" SOC** service that is capable of integrating and operating specific telemetry detection technologies in the industrial environment in cooperation with the IT environment. Our SOC allows to automatically operate contextualisation and enrichment actions with specific processes designed for the industrial ecosystem and to offer **detection of** and **responses** to the threats that can put our customers at risk in a global and convergent horizon.

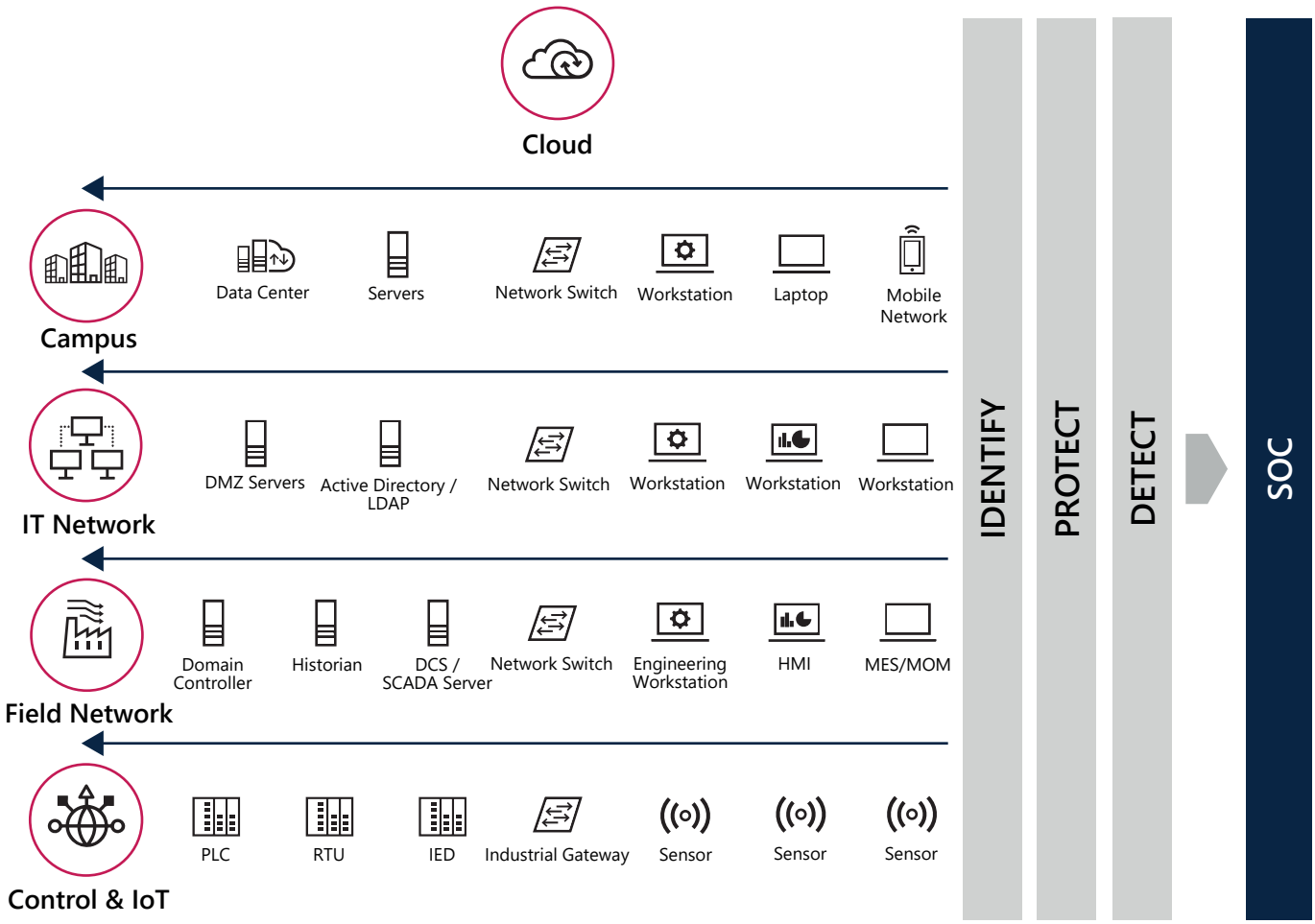


Figura 10
Integrazione verticale

Designing and implementing technological and process solutions to reach industrial plants and operational infrastructures' Cyber resilience, by protecting their operativity and integrity.

6 THE FUTURE OF OT SECURITY

The process of digital transformation that is affecting industrial realities, especially in terms of hyperconnection and interconnection, entails overcoming the historical phenomenon of "security by physical segregation" (air-gapped), which is becoming a structural and functional element of business. This is a trend that is showing no sign of abating: indeed, it is extending into other areas, from wearable collaboration systems to monitoring and control systems.

For example, advances in robotics or automation and monitoring processes based on machine learning engines are progressively shifting the management paradigm towards **"remote operations".** Or the fact that new CPSs (cyber-physical systems) are being designed to be connected, and the spread of **"retrofitted"** systems, i.e. originally standalone systems to which components are added to network them.

The number of connected devices and the connection patterns between devices are only set to increase: **smart products, smart buildings, and smart industry** are just a few examples that represent an underlying trend.

As in any other area of cybersecurity, the technological evolution of defence systems goes hand in hand with the evolution of threats, which are gradually becoming more sophisticated.

The common perception in the field of defensive security is that there remains an inalienable feeling of a profound **disproportion between "the attacker" and "the defender"**: the attacker, who is looking for the weak link, needs an opening, a small "crack" in the defensive mesh in order to opportunistically exploit a vulnerability and make a threat real. The defender, on the other hand, must ensure that myriad security challenges are addressed: they must continuously orchestrate an articulated series of initiatives involving technologies, processes, strategies, multitudes of assets and devices, and, of course, people. They must also manage budget requirements and maintain a balance between costs and benefits, and between risk and protection, which often require the sacrifice of some protection profiles.

The most effective approach for governing this transformation is a systematic one, in which a programme of progressive and consistent initiatives is structured to address the emerging complexity.

In other words, it is necessary to:

- carry out an initial broad assessment that involves processes, technologies, and people in order to assess the AS-IS status of risk exposure
- define a desired TO-BE status based on the organisation's risk tolerance and risk appetite
- carry out a gap analysis
- structure a roadmap of progressive interventions to direct both tactical and strategic initiatives over a multi-year horizon, keeping the principle of risk reduction in the background.

During the definition of the roadmap, and as part of its regular updates, it is important to remain mindful of the concept of the **"weak link"**, i.e. to maintain a high level of synergy between the chosen initiatives so that all the observation domains can evolve homogeneously, otherwise there is a risk of losing efficiency in the return actions. Using a metaphor, there is a risk of locking the door but leaving the window wide open.

Clearly, maintaining an adequate level of complex maturity is a challenge that will come up against the emerging tendency towards the fragmentation of initiatives as well as the exponential expansion of the perimeter, , as we were saying earlier, it is essential not to improvise but rather to rely on consolidated practices, methodological frameworks, and international norms.

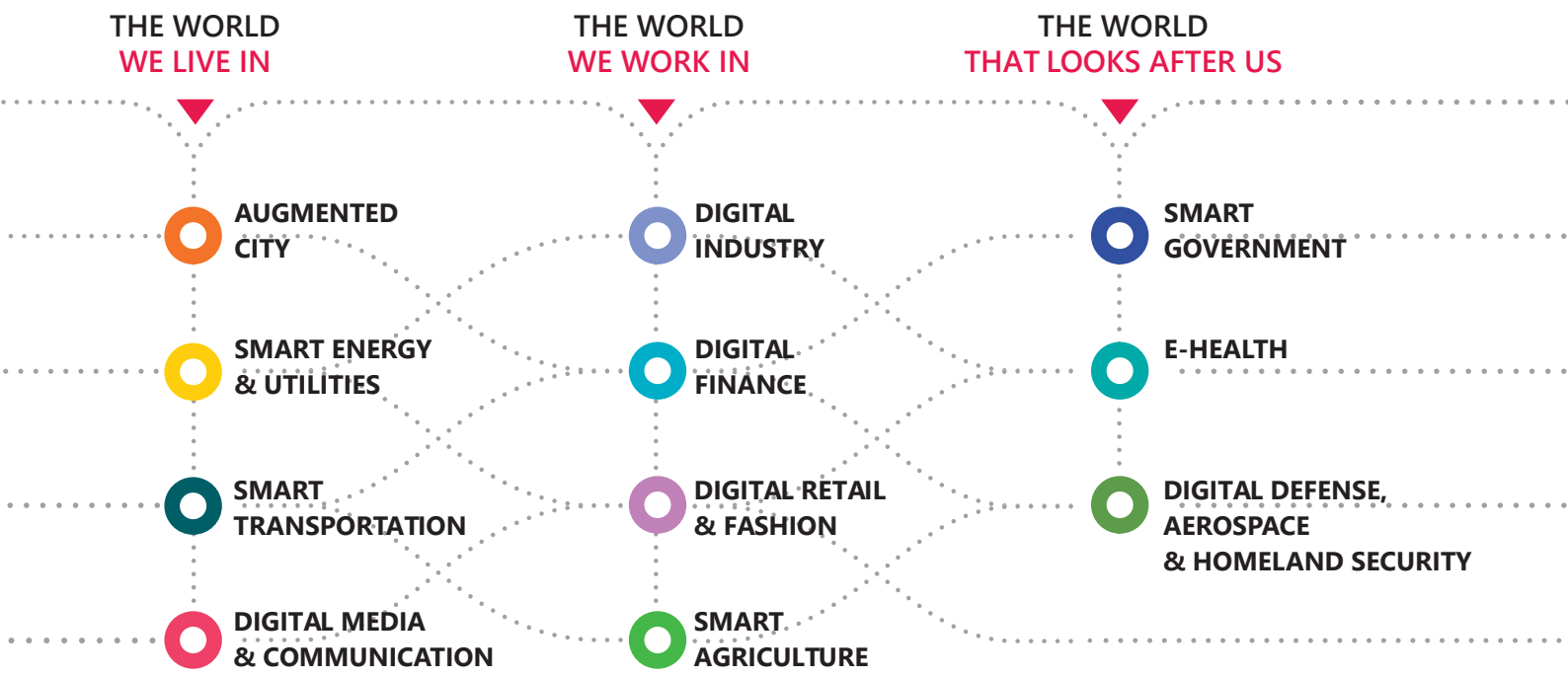
As a final note, from both an operational and a security point of view, the emerging need to govern the multitude of "intelligent objects" during the entire course of their life cycle introduces issues such as "object identity", which, like the classic concepts relating to people's identities and enabling permissions, require appropriate supporting tools and specific processes to keep operational and security risks under control. The cybersecurity challenges of the IT and OT fields are likely to be played out within this context in the near future.

ENGINEERING

For more than 40 years Engineering has been one of the main actors in the digital transformation of both public and private companies and organisations, with an innovative range of services for the main market segments.

With approximately 11,600 professionals in 40+ locations (in Italy, Belgium, Germany, Mexico, Norway, Serbia, Spain, Switzerland, Sweden, Argentina, Brazil, and the USA), the Engineering Group designs, develops, and manages innovative solutions for the areas of business where digitalisation generates major change, such as Digital Finance, Smart Government & E-Health, Augmented Cities, Digital Industry, Smart Energy & Utilities, and Digital Media & Communication. In the course of 2020, Engineering has supported its partners in the continuation and protection of their businesses and key processes, assisting in the design of their 'New Normal' and the mapping of new digital ecosystems. With its activities and projects, the Group is helping to modernise the world in which we live and work, combining specialist skills in the final frontier of technologies, technological infrastructures organised in a unique hybrid multi-cloud model, and the ability to interpret new business models. With important investments in R&D, Engineering plays a leading role in research, coordinating national and international projects with a team of 450 researchers and data scientists and a network of scientific and academic partners throughout Europe. One of the Group's strategic assets is the expertise of its employees, whose development is promoted by a dedicated multi-disciplinary training school that provided more than 15,000 training days over the last year.

www.eng.it



Designing and implementing technological and process solutions to reach industrial plants and operational infrastructures' Cyber resilience, by protecting their operativity and integrity.

Our point of view on

DIGITAL TRANSFORMATION

ENGINEERING INNOVATION

ENGINEERING THE NEW NORMAL

WHERE BUSINESS MEETS TECHNOLOGY

AUGMENTED CITY

DIGITAL DEFENCE, AEROSPACE & HOMELAND SECURITY

DIGITAL FINANCE

AUGMENTED MIXED AND VIRTUAL REALITY

BLOCKCHAIN

DIGITAL INDUSTRY

DIGITAL MEDIA & COMMUNICATION

DIGITAL RETAIL & FASHION

CLOUD

CYBERSECURITY

E-HEALTH

SMART ENERGY & UTILITIES

SMART AGRICULTURE

DIGITAL TWIN

ROBOTIC PROCESS AUTOMATION

SMART GOVERNMENT

SMART TRANSPORTATION

Coming Soon

AI & ADVANCED ANALYTICS

IOT INTERNET OF THINGS

DIGITAL WORKPLACE

DIGITAL WASTE

DIGITAL EXPERIENCE: CULTURE & TOURISM

SUPPLY CHAIN

DIGITAL AUTOMOTIVE

PROJECT MANAGEMENT

www.eng.it

@EngineeringSpa

Engineering Ingegneria Informatica Spa