TLP:CLEAR

España | digital 2026

Industrial control systems endpoints defence guide

Financiado por la Unión Europea
NextGenerationEU

MINISTERIO DE TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TLP:CLEAR

May 2023

INCIBE-CERT_ICS_ENDPOINTS_DEFENSE_GUIDE_2023_v1.1

This publication belongs to INCIBE (Instituto Nacional de Ciberseguridad) and is licensed under a Creative Commons Attribution-Noncommercial 3.0 Spain licence. For this reason you may copy, distribute and publicly communicate this work under the following conditions:

-Acknowledgement . The content of this report may be reproduced in whole or in part by third parties, citing its source and making express reference to INCIBE or INCIBE-CERT and its website: https://www.incibe.es/. Such acknowledgement shall in no way suggest that INCIBE supports such third parties or endorses their use of their work.

Non-Commercial Use . The original material and derivative works may be distributed, copied and displayed for non-commercial use.

When reusing or distributing the work, you must make clear the terms of the licence for this work. Some of these conditions may not apply if permission is obtained from INCIBE-CERT as the copyright holder. Full text of the licence: https://creativecommons.org/licenses/by-nc-sa/3.0/es/.

Index

INDEX OF FIGURES

1. About this guide

This guide aims to explain more about *endpoints* and endpoint security on a theoretical level.

The wording is of a technical nature, but understandable for anyone who wants to understand both the *endpoint* concept and endpoint defences. In addition, different possible perimeter defences are listed and explained, i.e. both *endpoint* and external defences are explained.

The order of the contents is distributed in such a way that initially there is an introductory knowledge of *endpoints* in industrial control systems, together with general risks in ICS and defences for these end devices.

Finally, a conclusion is made in which this type of defences on *endpoint* devices is assessed.

2. Organisation of the document

This study has a structure focused on gradual learning, starting with a brief **3.- introduction** to *endpoints* both at IT and OT level, focusing on the latter. This introduction is followed by a brief but concise explanation of **4.- what an *endpoint* is** and what kind of general security measures these devices require.

Subsequently, in order to provide a closer approach to security measures, different **5.- industrial-level risks** that may affect this type of device are introduced. This is complemented by the following section on *endpoint* protection in terms of **6.- defence in depth.**

Focusing the study on defences, a list and explanation is given of different **7.- *endpoint-specific* solutions**, as well as physical and operating system security. It also details certain limitations that can affect this industrial equipment in order to include different security methods. In turn, and to counteract the limitations of implementing agents on the equipment itself, different solutions for **8. -defending *endpoints* at the perimeter level** are detailed.

Finally, to conclude the study, some **9.- conclusions** are drawn based on the different *endpoint* defence solutions.

3. Introduction

For several years now, there has been talk of Industry 4.0 and the digitalisation of industrial processes. This evolution has meant that the devices responsible for controlling industrial processes have gradually been replaced by others with better capabilities and greater intelligence, as well as being able to interconnect with each other through a network; these devices are known as **IoT** (*Internet of Things*) **devices** or as **IIoT** (*Industrial Internet of Things*[1]) devices if they are in an industrial environment. To specify the magnitude of growth, both in terms of devices and interconnections between them, the INCIBE-CERT article Predictions in Industrial Security in 2023[2], indicates a forecast of the number of smart devices connected in **2025, which concludes that the figure of 21.5** billion connected devices **will be reached**.

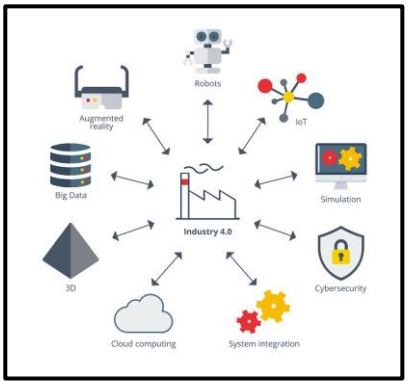


Illustration 1: Industry 4.0 and its connectivities

From the moment a device is connected to a network, it must be properly protected to prevent malicious actions on it, and this applies not only to devices in any network, but also to industrial devices. There are multiple protection measures that adapt to the different needs that a network device may present, so the **objective of this study** is to **present solutions for the defence of end devices or "*endpoints*".**

The protection of industrial devices is one of the biggest challenges in terms of security in the industrial field due to their particularity, as they are usually devices designed to perform a specific task, which does not allow much leeway when it comes to configuring them. Moreover, until a few years ago, cyber security has not been a factor in the design process of industrial devices, resulting in equipment with poor cyber security capabilities.

Added to this is the **intrinsic difficulty of updating and patching industrial devices**, which results in the persistence of vulnerabilities detected in the equipment. As in the IT sector, the industrial sector also suffers from attacks, often with a direct impact on people, as many of the activities of the industrial sector are dedicated to providing basic services to society, such as electricity, water, etc.

CrashOverride, the attack on Colonial Pipeline[3] or a sewage treatment plant in Florida are some examples of attacks on industrial control systems in the last decade, all of which had a direct impact on people.

[1] https://www.incibe.es/en/incibe-cert/blog/improvement-iiot-industrial-environments

[2] https://www.incibe.es/en/incibe-cert/blog/what-expect-industrial-cybersecurity-2023

[3] https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/supply-disruption-colonial-pipeline

4. What is an *endpoint*?

When we talk about an ***endpoint*** device, we are talking about an end asset present at the network level. Among these devices we can find from engineering *workstations* to servers, HMI, SCADA, PLC and others. These devices are key points from a security point of view, as their vulnerabilities could affect other assets within the network.

With the **exponential growth of IoT and IIoT devices,** the exposure surface in industrial environments has increased. Forcing the bastioning of equipment following the concept of defence in depth or deploying *endpoint* defence solutions. The set of end devices forms the first line of defence of any communications network at the logical level, whether industrial or not, as most attacks attempt to breach these poorly protected devices.

***Endpoint* protection solutions refer** to **defences for these core industrial assets**. Nowadays, it is no longer sufficient to simply introduce a firewall for perimeter protection to deny access to potential malicious actors, but an additional layer of security is required, which is where *endpoint* defences come in.

As mentioned above, in general terms *endpoints* refer to any device connected to the network. Looking at this from the IT perspective and the higher levels of the Purdue model, *endpoints* could be desktops, laptops, mobile phones, printers and routers. But when referring to the lower layers of the Purdue model and more on the operational side, *endpoints* include programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, safety instrumented systems (SIS), remote terminal units (RTUs), intelligent electronic devices (IEDs) and human-machine interfaces (HMIs).

All these devices in the industrial part of any company are a very critical point in terms of functionality and security, which is why defending them is critical, and although many are proprietary devices (whose configuration is difficult to modify to improve security) and legacy devices (designed and implemented before there were concerns about the cybersecurity of these systems), there are different solutions, mechanisms or tools to protect them.

At a high level, we can define different actions to improve *endpoint* security:

- Use of a well updated asset inventory[4] , both *hardware* and *software*, to know what versions and possibilities exist to protect the device.
- Control of external connections to the industrial network both to the Internet and via remote access. Minimise connectivity to a greater extent and strictly control security authorisations.
- Configure correctly, and whenever and wherever possible, the security of end devices.
- Implement solutions to continuously monitor all *endpoint* devices in real time.
- Develop and improve policies and procedures on end-device security.

[4] https://www.incibe-cert.es/en/publications/guides/guide-asset-inventory-management-industrial-control-systems

5. Risks in industrial control systems

Within the infrastructure of any industrial company, **two very clear environments coexist, the IT** (*Information Technologies*) **environment** and the **OT** (*Operation Technologies*) **environment**, which is why there are a large number of connected end devices, and although this advance in interconnection between these two very different environments has generated an improvement in visibility, efficiency and speed in communications, it has also led to **greater exposure to different threats to the ICS** (Industrial Control Systems) **environment**, as this connectivity means that the threats that loom over the IT environment can affect industrial systems.

This link between environments referred to above implies a connection between management, control and business processes and the physical processes of the operational environment. This results in the exchange of data, the control of different operations and the monitoring of industrial processes from the IT environment. *Endpoints* in industrial environments are responsible for development, control and monitoring.

To gain a better understanding of ***endpoint* devices and the risks they can pose to industrial control systems**, in Figure 2, we can see how they can be used to control **industrial control systems.** Illustration 2is shown highlighted in red for different industrial *endpoints* within the Purdue model.

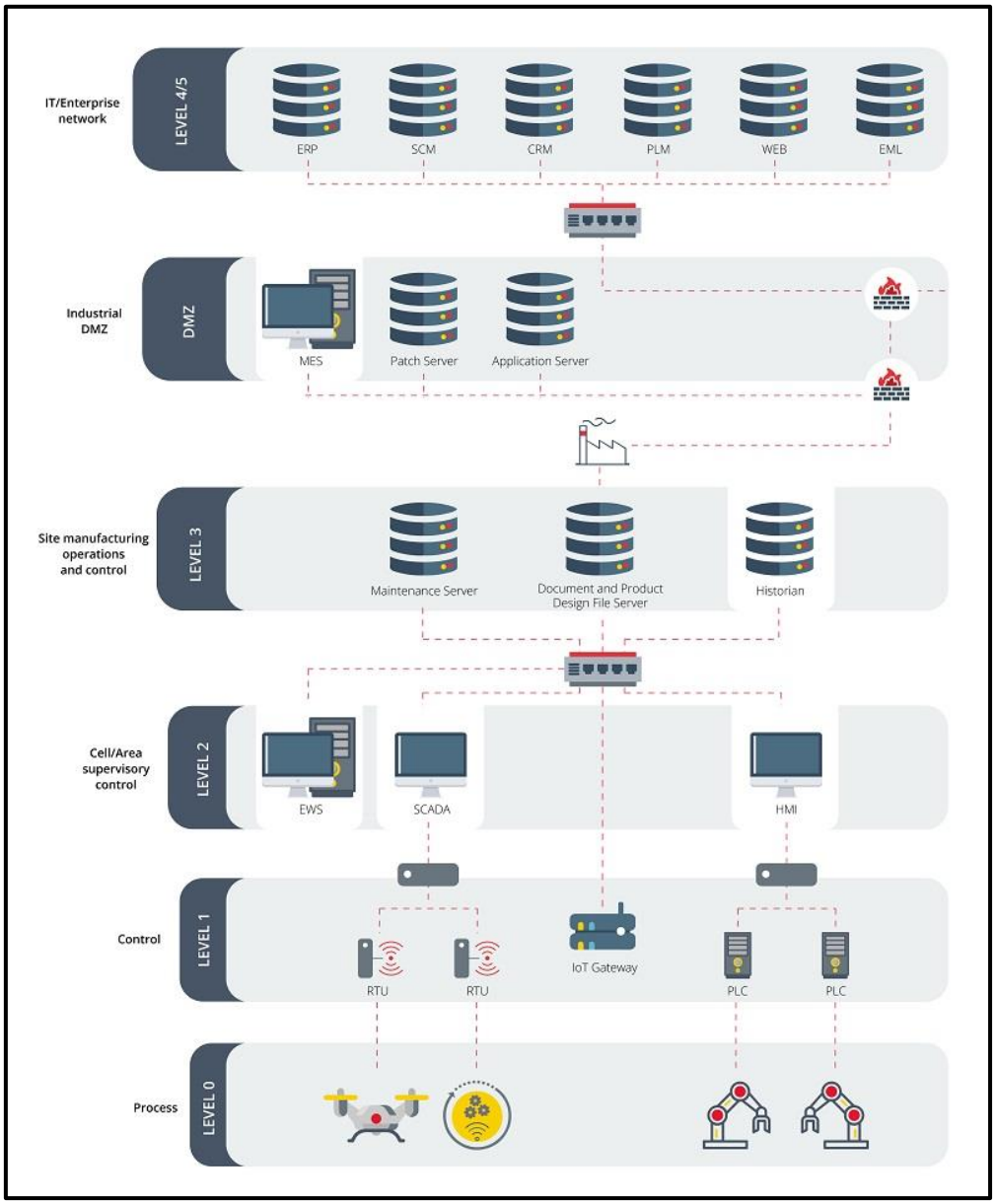


Illustration 2: Highlighted endpoint devices in an IT/OT environment[5]

Focusing on the risks or vulnerabilities that can affect industrial control systems, and why to use mechanisms or tools for the protection of industrial systems, a set of risks or vulnerabilities that are common in industrial environments are presented below:

- **Internet exposure:** Originally, industrial environments were isolated environments and limited to plants. As can be seen in Illustration 2as mentioned above, industrial evolution and the integration with a wider range of systems and platforms (between IT and OT environments) to facilitate access, has led some companies to connect their industrial systems or parts of them to the Internet without any security measures.
  The existence of insecure connections opens a gateway to entities with malicious intent.

[5] https://www.trendmicro.com/en_us/research/22/a/cybersecurity-industrial-control-systems-ics-part-1.html

It is also very common to provide external access to suppliers for maintenance purposes, which can result in an access point for attackers with malicious intent. Systems used by external providers can threaten the security of the client company. On the other hand, misconfigurations in VPNs, where the users or machines to be accessed are not restricted, also pose a risk.

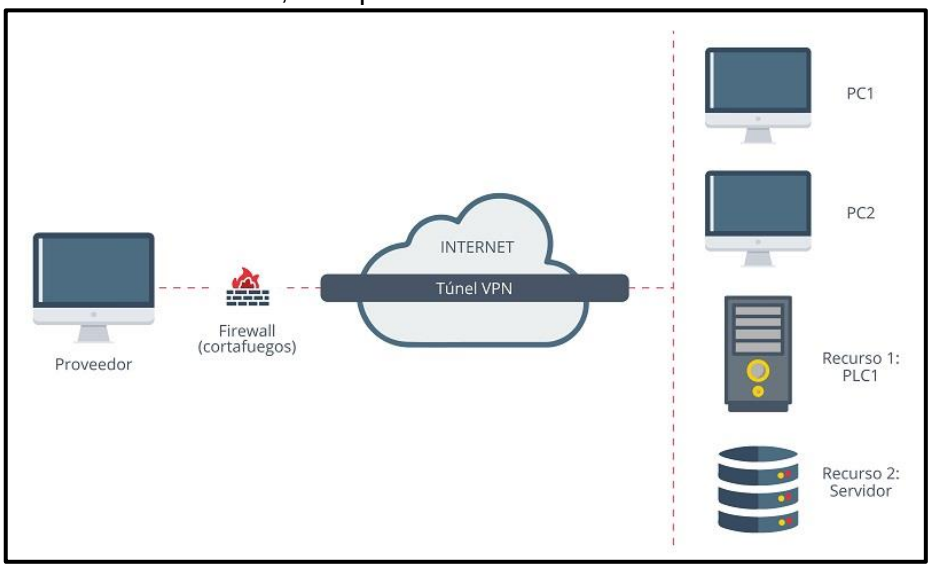


Illustration 3: VPN tunnel between a provider and the devices in an industrial environment[6]

- **Weak segregation:** Weak segregation between IT and OT environments is one of the most common factors that compromise industrial networks. Weak access control can allow a machine connected to the IT network to reach a device on the ICS network, and a *malware* infection in the IT system can allow it to spread to OT.
- **Outdated equipment and default configurations:** Not all companies can afford the downtime to upgrade equipment, as it leads to decreased production and lost revenue. Other companies feel that their industrial systems are securely isolated, and do not apply patches issued by manufacturers to fix vulnerabilities, or maintain the default configuration of equipment.
- **Lack of data integrity:** In the industrial world, a possible alteration of data can mean serious problems in different processes. Ensuring data integrity allows stored information or data in progress between devices to be complete, accurate and reliable; guaranteeing its protection against attacks or unauthorised external access. This is why end devices, or *endpoints,* must have the ability to ensure data integrity.
- **Weakness in ICS protocols:** The original protocols used in ICS were not designed with security in mind. Years have passed, and the same protocols are still used as before.

[6] https://www.antiun.com/vpn/

Illustration 4: Industrial protocols[7]

For example, the MODBUS protocol uses unencrypted text communication, which can allow an attacker to eavesdrop on traffic, and also lacks proper authorisation, which can lead to unauthorised actions such as updating the ladder logic program or shutting down the PLC.

- **Weakness in ICS applications:** ICS-related applications are sometimes vulnerable, such as the web interfaces that some devices rely on for management, which can be vulnerable to attacks because they implement unsecured protocols such as HTTP. This can lead to the disclosure of credentials over the network or session hijacking.
- **Lack of security awareness:** Due to a lack of security awareness, employees often become victims of social engineering, *phishing* and *spear-phishing* attacks. Sometimes, an attacker only needs one click from a victim to achieve his goals. Once a machine has been compromised, an attacker can try to move into the network and breach new machines.

[7] https://www.logicbus.com.mx/pdf/articulos/Protocolos-de-Comunicaci%C3%B3n-Industrial.pdf

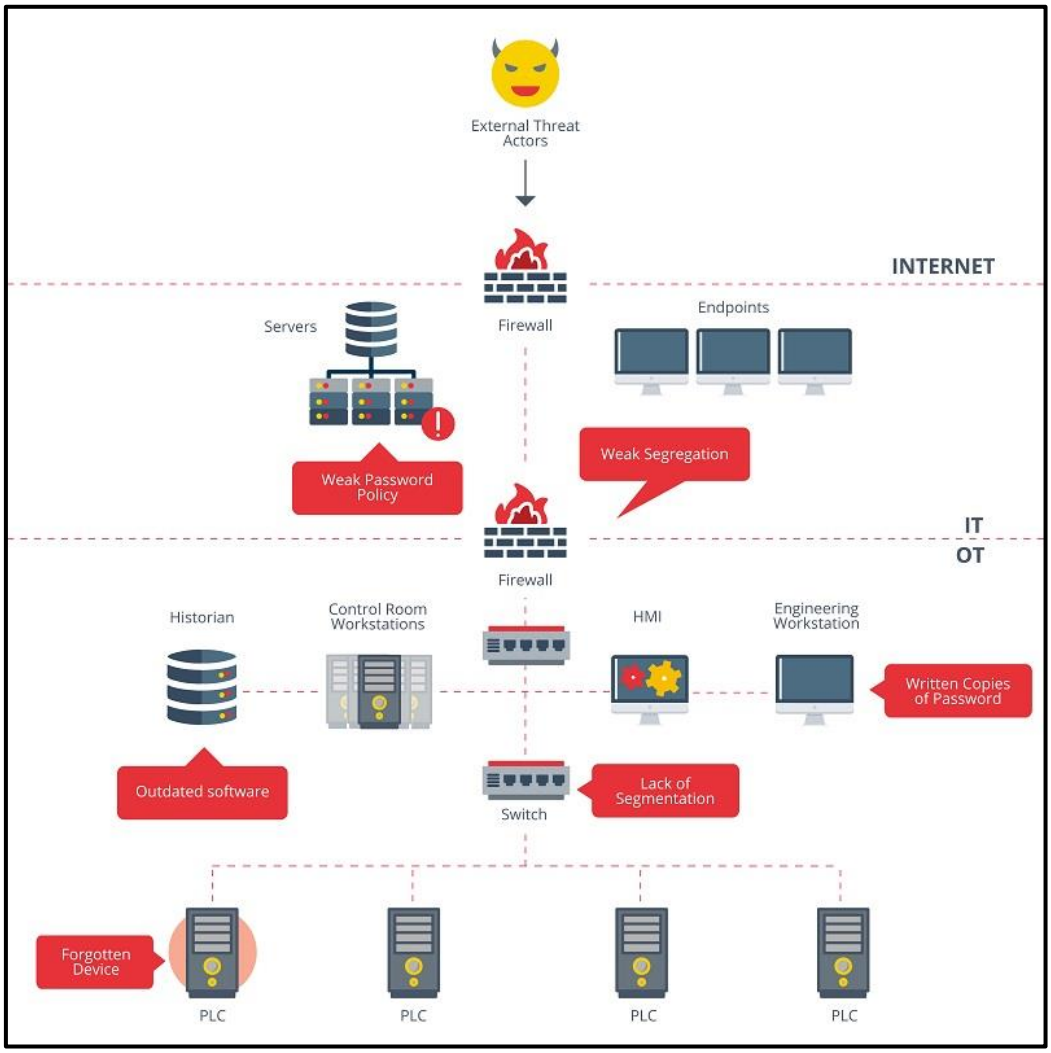


Illustration 5: Different hazards in industrial environments[8]

[8] ttps://www.wizlynxgroup.com/mx/ciberseguridad-mexico/evaluacion-de-la-seguridad-de-los-sistemas-de-control-industrial

6. *Endpoint* protection: defence in depth

In order to provide complete *endpoint* protection, a philosophy based on the concept of **defence in depth will be** followed. This means that protections will be applied at multiple layers, starting from the lowest level, from the operating system itself and its applications, to the highest level, corresponding to the defences on the outside of the device, in its environment.

The following image shows schematically the different layers of protection applicable to a device, and how each layer forms a wall that protects all the previous ones.

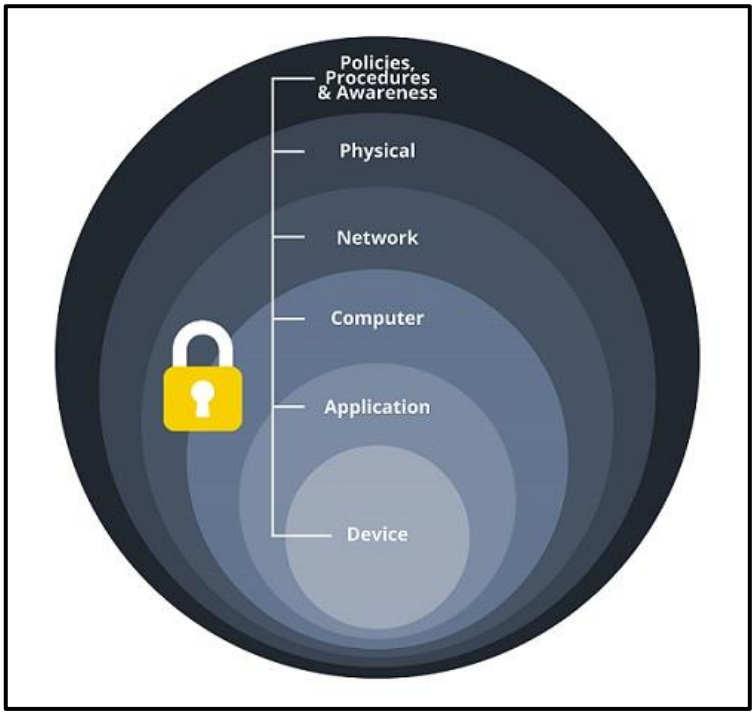


Illustration 6: Layers for defence in depth[9]

Throughout the study, several types of defences applicable to industrial devices will be presented. These defences will vary depending on the "layer" to which they belong and the asset itself that is to be protected, as the protection that would be applied to the defence of SCADA systems is not the same as the protection that would be applied to a PLC. Therefore, the following sections will show protection measures for *endpoints* applicable to the devices themselves, i.e. at the level of configurations or installable protection *software*, or protection from the outside and in their environment.

[9] https://www.networkaccess.com/defense-in-depth/

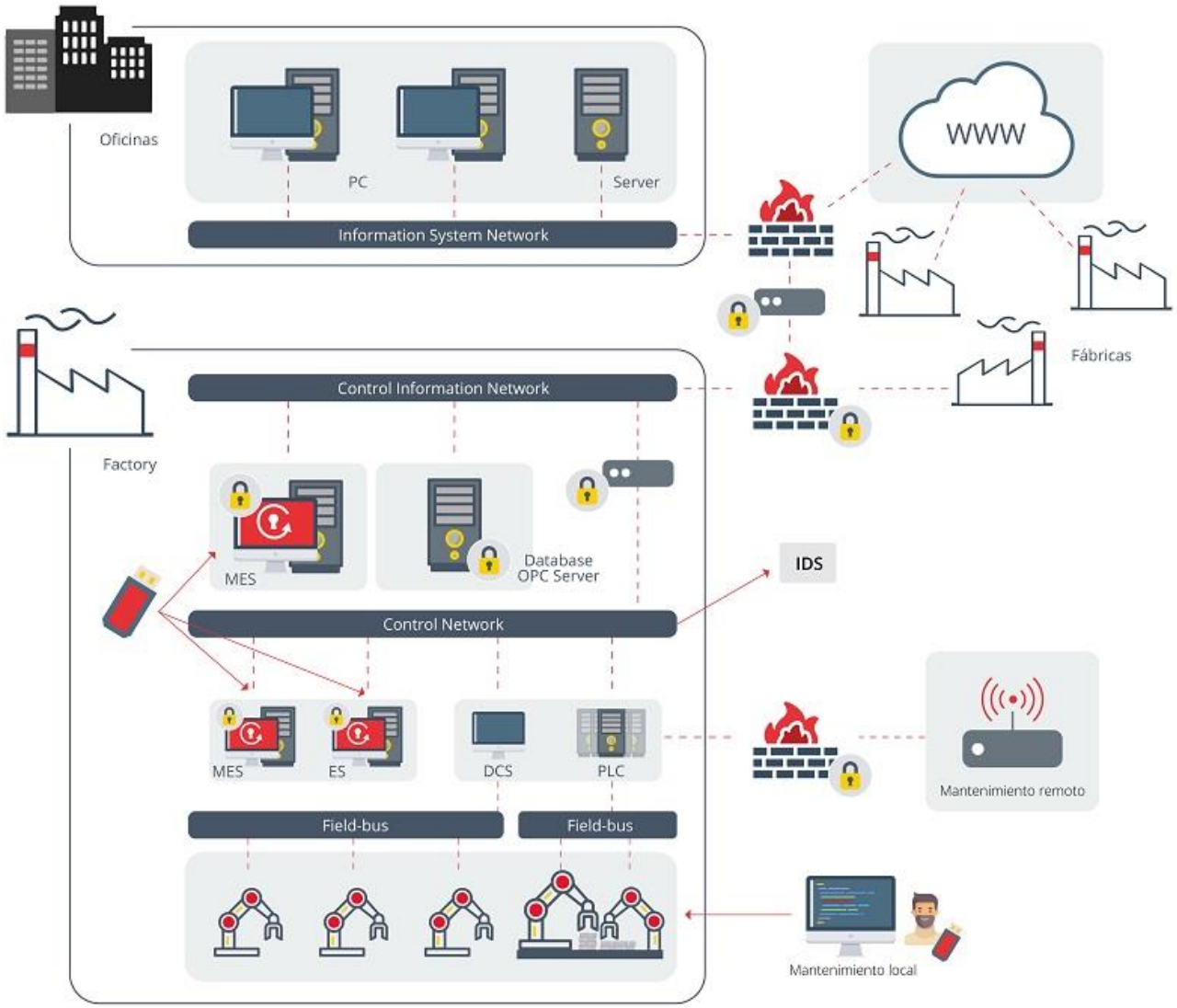


Illustration 7: Multi-layered endpoint protection[10]

[10] TrendmicroSolution.pdf

7. *Endpoint* defences

This section focuses on the protections that can be applied to the *endpoints* themselves. It presents ways of protecting the operating system itself or *firmware* of the equipment, and the applications installed on them, without neglecting the installation of specific *software* for the protection of the equipment, and also taking into account the physical protection of the assets.

7.1. Application and operating system security: bastioning

Hardening is the procedure by which vulnerabilities in a system are reduced. The development and management of industrial equipment hardening is necessary in order to control the security of individual assets individually and collectively to improve the overall security of industrial systems.

The application of bastioning to industrial equipment reduces the exposure of assets to possible attacks, vulnerabilities or misconfigurations that can be exploited. This is achieved by applying secure configurations to the equipment, which must take into account different main aspects:

- Network applications, services and protocols.
- Local access.
- Remote access.
- AAA authentication.
- Operating system and *firmware*.
- The event log.

For the development of device bastioning, a set of **bastioning guides** must first be developed, which specify which configurations should be applied to each device, why they are being applied and what they are trying to avoid with such protection. Since each device is different and task-oriented, the bastioning guides must be customised for each device, as they take into account the particularities and situation of each device.

For the elaboration of the bastioning guides, it would be necessary to have the device to be protected and its manual, in order to be able to explore all its parameters, applied configurations, services, *software*, etc. Thanks to this, all possible protection points for the equipment can be identified, and which configurations should be applied to each of them. All of this will be collected in a customised document for each equipment, indicating all the steps to follow to bastion the equipment.

For the elaboration of these guides, it is possible to rely on existing guides such as the **STIG guides of the DISA (*Defense Information System Agency*)**. There are several guides applicable to different operating systems or *software*, which list different protection measures or configurations applicable to the equipment. These configurations are catalogued according to their severity, allowing to prioritise which of them should be applied.

Regarding the application of the basing guides developed, given that the equipment to be protected is industrial equipment in which availability is a top priority, it is recommended that it be tested in a secure laboratory environment, and not in production. This is because

some configurations applicable to the equipment could limit its functionalities, affecting not only the equipment itself, but also others that may depend on it.

7.2. Endpoint Security (EDR)

EDRs are a very comprehensive type of defence for industrial assets. They have several capabilities or characteristics that motivate their use in industrial environments. Some of these include the following:

- Monitor problem areas and traffic movements.
- Anomaly detection and blocking capability.
- Protection of data stored on equipment.
- Firewall.
- *Sandboxing* of infected or ambiguous programs.
- Integration with antivirus.
- Protection of equipment with *software* mechanisms that affect the physical part to some extent, such as blocking USB devices.
- Centralised administration (not all).

Now that the capabilities that EDRs possess have been mentioned, it is possible to go a little deeper by listing some of the techniques or tools they have at their disposal to perform all the tasks mentioned above. These are some of them:

7.2.1. Whitelisting

It is **one of the most widely used protections at the industrial level because it does not have a major impact on the system** where it is deployed. It consists of a list or register of entities that, for one reason or another, can obtain a particular privilege or access. It is a security mechanism that allows control over the processes executed, *software* installed, etc.

WHITELISTING	
ADVANTAGES	Blocks most *malware*.
	Prevents the use of unauthorised applications.
	It does not require daily updates.
	The equipment administrator is responsible for authorising new applications.
DISADVANTAGES	Adds load to equipment performance.
	It requires regular maintenance.
	It can sometimes be annoying for users.
	Permitted applications are susceptible to compromise.

Table 1Characteristics of Whitelisting

7.2.2. *Anti-malware* protection

This protection, as its name suggests, is responsible for detecting, protecting and eliminating malicious *software.* It does this by detecting and managing malicious files or actions that may affect a system.

To do this, it scans the files on a computer and compares them with its signature database. In order for a piece of *malware to be* detected, it will need to be included in the signatures of the *anti-malware software*, so it is vitally important that it is constantly updated.

Due to the capabilities of some older systems, it may not be possible to deploy agents, so external tools can be used, such as the use of a USB device containing an *anti-malware* tool in portable mode that allows an exhaustive analysis of the system and does not require installation on the system itself. Some manufacturers already provide this option, which has functionalities such as *antimalware* scanning, obtaining system information, file integrity, etc.

7.2.3. HIDS (Host-based Intrusion Detection System)

A HIDS, also known as a **Host Intrusion Detection System**, seeks to detect anomalies that indicate a potential risk by reviewing the activities on the host machine. It can take protective measures. Compared to other *endpoint* solutions, this type of *software* is very similar to IDS.

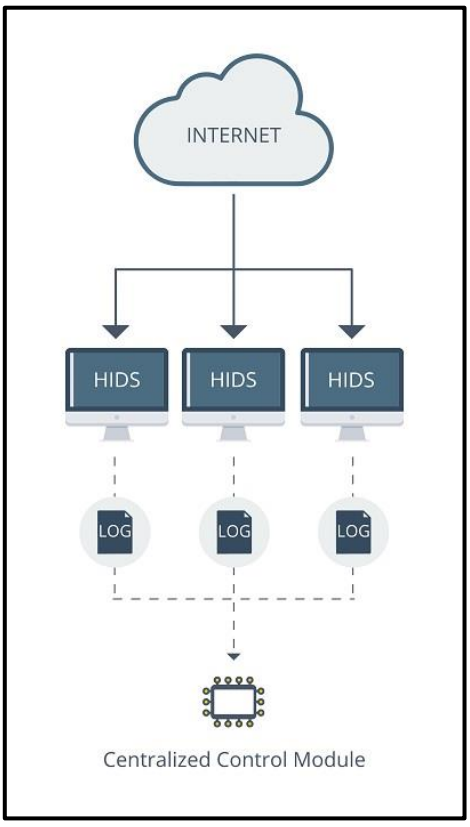


Illustration 8: Architecture with HIDS solutions installed[11]

[11] https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

HIDS have the following functions:

- Virus management.
- Analysis of local *logs*.
- File integrity check.
- Policy monitoring.
- *Rootkit* detection.
- Network monitoring, from the host's point of view.
- Real-time alerts.
- Active response.
- Inventorying the system.

7.2.4. AI and Machine Learning

Advanced techniques such as artificial intelligence or machine learning can be employed to enable early proactive detection of advanced persistent threats (**APTs**) at the industrial level.

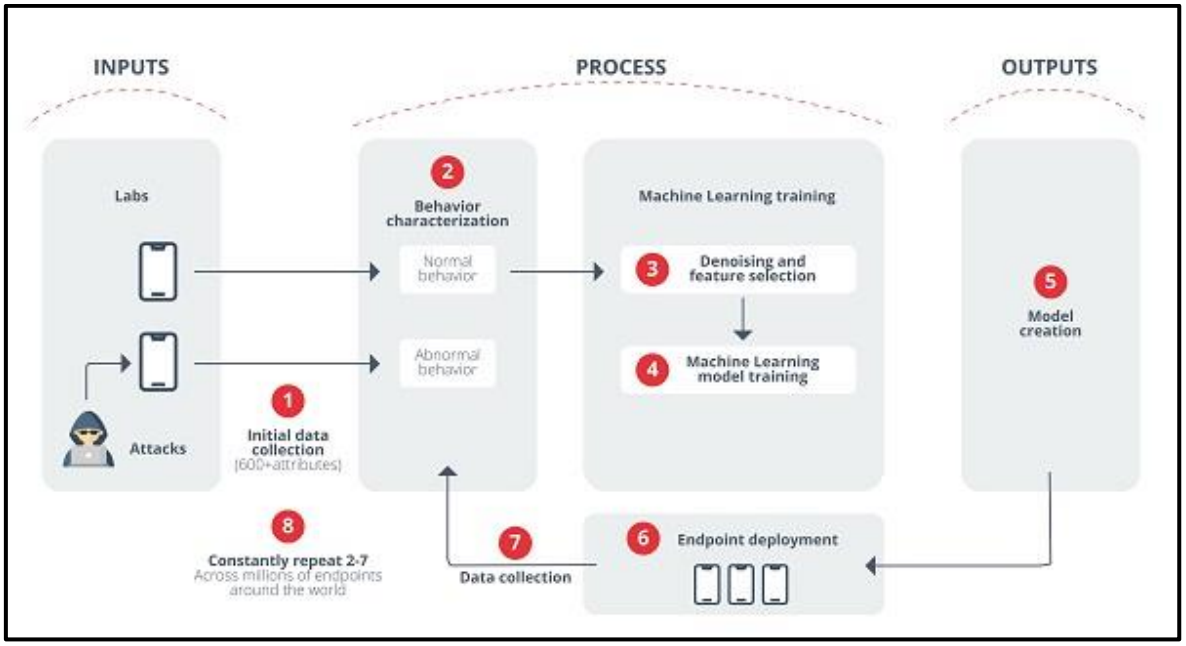


Illustration 9: AI training process using different behaviours and their modelling

7.3. Physical security

Physical security relies on any mechanism to ensure its integrity and preservation. This type of security has to be treated as a type of security in the field of industrial cyber security.

The main objective of physical security is to keep different operators or workers away from dangerous situations, as well as to protect equipment from possible malicious agents that want to access or physically interact with industrial equipment.

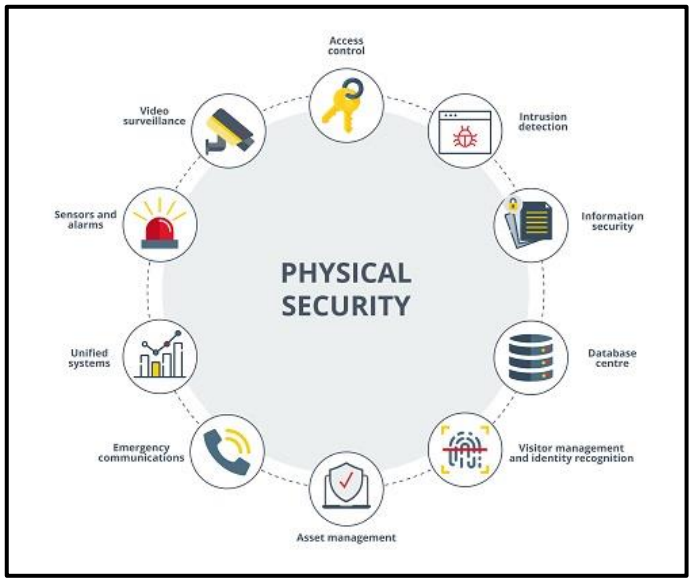


Illustration 10: Physical security.

The NIST 800-82 "Guide to Industrial Control Systems (ICS) Security[12]" lists the attributes to be considered when performing defence in depth applied to physical security. These controls are detailed below:

- Protection of physical locations.
- Access control.
- Access monitoring systems.
- Access limitation systems.
- Systems that allow the tracking of persons or assets.
- Management systems for environmental factors.
- Systems for monitoring environmental conditions.
- Current protection systems.
- Additional protection systems for control centre.
- Control systems for portable configuration devices.
- Cable protection systems.

As has become evident, the physical security of equipment is a very important aspect of the overall security of the devices and therefore, a good physical defence can be crucial in protecting both the equipment against possible attacks and the people working with it.

7.4. Limitations on industrial equipment

Once the mechanisms used by *endpoint* solutions and their capabilities have been identified, it is necessary to mention some particularities of industrial systems' equipment that differentiate them from equipment in corporate environments. These particularities must be taken into consideration, as they **can directly affect the way *endpoint* solutions operate, limiting their actions or making it necessary to use other types of solutions to defend the equipment**.

[12] https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

- **Processing capacity:** some industrial equipment lacks high processing capacity. This aspect is very relevant and should be taken into account when installing different security solutions on *endpoints*, as overloading the system or the device itself can lead to a lack of processing capacity.
- **Equipment with specific tasks:** industrial equipment is considered to be fixed devices, i.e. the ability to modify its configuration or the installation of external agents is considered complex and in many cases impossible. This problem or limitation is complemented by the processing capacity limitation detailed above. This case is very common in PLC devices.
- **Deployment on *hosts*.** Some industrial manufacturers' applications can be quite sensitive to the use of certain versions of operating systems, installed patches or installations related to changes in the system. Because of this issue, modifying the operating systems or versions of some devices without the express consent of the manufacturer can lead to a failure of the device and therefore the consequent shutdown of the industrial process or the activity being carried out. Moreover, in most cases, the modification of unauthorised versions leads to a loss of the device's warranty and therefore the consequent economic cost in the event of an accidental failure of the device.
- **Incompatibilities with manufacturers:** some industrial equipment has a base operating system such as Windows or Linux, on which its application is mounted. The inclusion of an EDR solution that includes the installation of agents may imply a limitation on the equipment. This may mean that the protection tasks performed by the EDR may directly affect the operation of the equipment. These affected functionalities may include communications with insecure ports, services or ports, etc.
- **Updating signatures:** Many industrial networks are isolated from the outside world and have no outlet to the Internet. This makes it difficult to update antivirus signatures.

8. Defences on the outside

For complete *endpoint* protection, it will also be necessary to defend endpoints from the outside, i.e. not to delegate all protection to computers, but to secure their environment as well.

8.1. Secure architecture

Endpoints will be connected to each other through a network, and their topology directly affects the security and exposure of the computers. It is therefore important that the computers to be protected are connected in a network whose architecture follows security principles and has been properly structured. The aim is to segregate the network into different sub-networks in order to be able to control all communications between the individual segments with the help of a *firewall.*

The recommended approach for equipment in industrial systems is IEC 62443-3-2 "**Standard addresses security risk assessment and system design for IACS**", which introduces the concepts of "zones" and "ducts"[13] for secure segmentation of industrial networks using defence in depth.

A zone is a grouping of physical or logical assets that share common security requirements, which have a defined physical or logical boundary. And conduits are the connections between zones, and must contain security measures that control access to them, resist attacks and protect communications.

8.2. Industrial firewall

These devices are responsible for isolating the different zones and allowing only authorised traffic between the different segments of the network, whether industrial or more corporate, or even the border between these two environments. They have certain characteristics that differentiate them from their general-purpose analogues, such as their operation in transparent mode or the deep packet inspection, in which each field of the packets is analysed and filtered according to the specific values of the protocol.

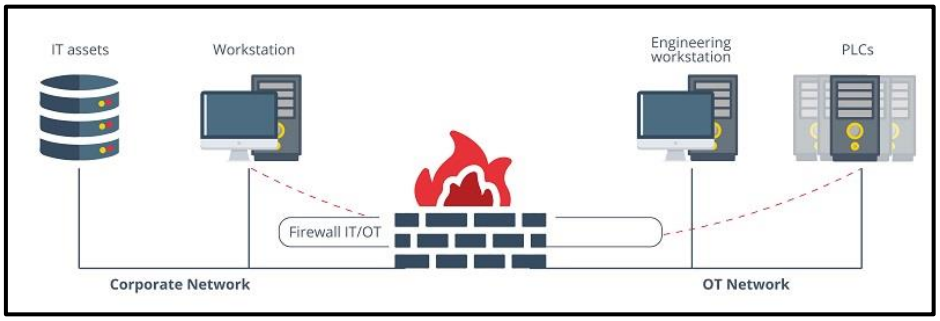


Illustration 11: IT/OT firewall[14]

[13] https://www.incibe.es/en/incibe-cert/blog/zones-and-conduits-protecting-our-industrial-network

[14] https://applied-risk.com/resources/4-ot-it-network-segmentation-techniques-selecting-a-cyber-resilient-configuration

8.3. IDS and IPS

IDSs (*Intrusion Detection Systems*) are systems that systems that monitor traffic in search of anomalies or suspicious activities that may indicate the start of an attack, in order to prevent it or, if this is not possible, to remedy it as soon as possible. These types of tools analyse the traffic flowing through networks in real time without the need to interrupt the data flow, acting passively, monitoring incoming, outgoing and local traffic.

When they detect any suspicious activity, they issue an alert to the system administrators, who must decide on the appropriate action to be taken. These accesses can be sporadic attacks by malicious users or repeated from time to time, thanks to the use of automated tools. These systems only detect suspicious accesses[15] by issuing early warnings of possible intrusions, but do not attempt to mitigate the intrusion.

There are also IPS *(Intrusion Prevention System)*[16], which, in addition to the capabilities of IDS, can act on communications by discarding packets or cutting connections. These systems are generally not widely used in industrial environments, and are limited to the use of IDS, which warn, but do not act, so as not to interrupt the industrial process.

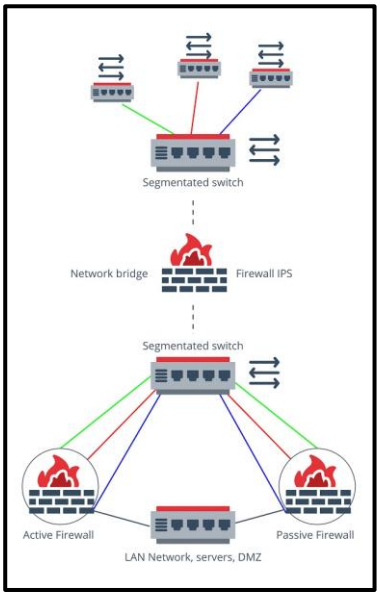


Illustration 12: IPS

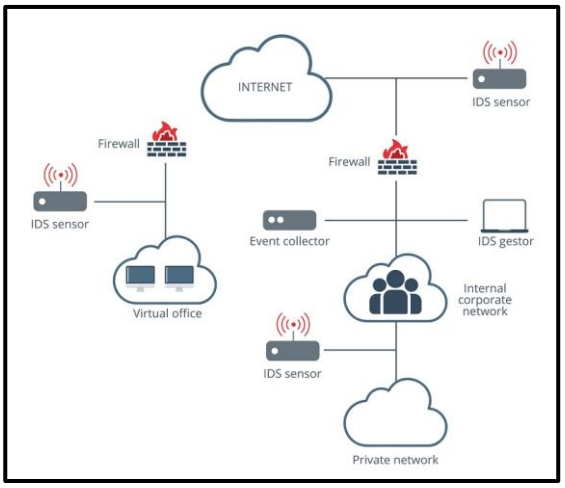


Illustration 12: IDS

8.4. Secure remote access

Secure remote access in industrial systems is one of the key security issues. An increasing number of suppliers are performing maintenance communications or operations through remote accesses. For the customer, this access is an access point to their network, so they must ensure that they are as secure as possible and that they are only used when strictly necessary.

[15] https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/certsi_design_configuration_ips_ids_siem_in_ics.pdf

[16] https://tr0n3t.wordpress.com/2020/04/28/firewall-transparente-con-pfsense/

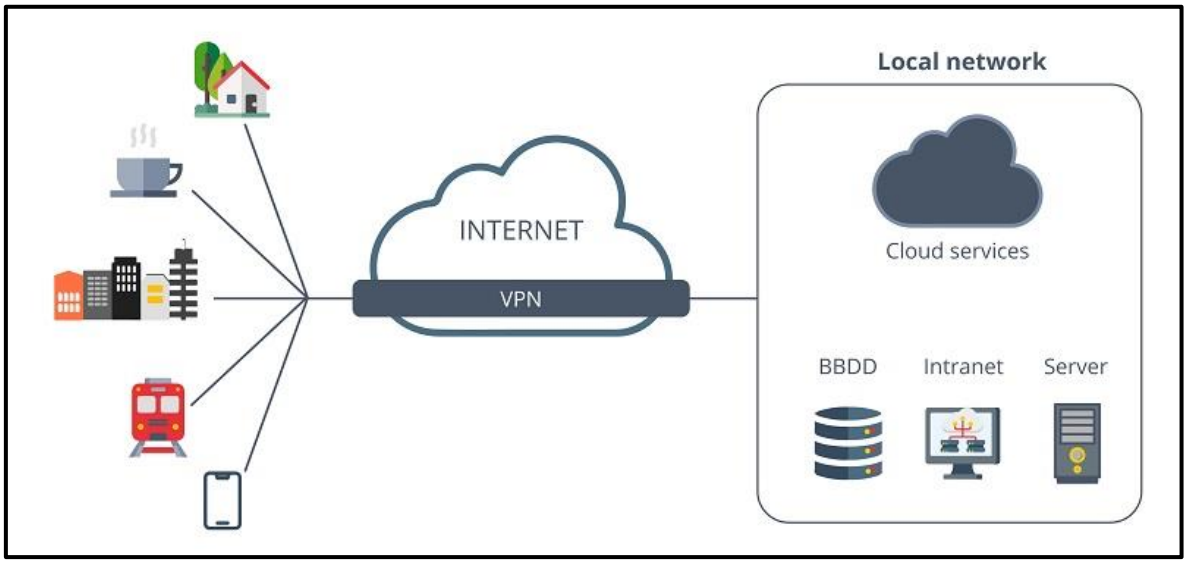


Illustration 13: Use of VPN for remote connection[17]

There are different methods of remote access for systems in industrial environments. Some examples are listed below:

- **Direct access to the industrial network:** this is the most common but also the most insecure, involving full access by the provider to the customer's industrial network. To be able to say that the connection is secure, point-to-point rules must be implemented and external access must be via VPN.
- **Use of a jump box:** with this solution, if a user from the corporate environment wants to access the operational environment, he/she must first access a jump box located in the OT DMZ.
- **Specific remote access solution:** There are specific equipment and solutions that can provide secure remote access by controlling the ports and applications to be used externally. The establishment of either a TLS tunnel or encapsulated HTTPS traffic are reliable solutions for secure remote connection.

8.5. SIEM

SIEM solutions are a hybrid solution between SIM (*Security Information Management*) and SEM (*Security Event Manager*). This technology provides real-time analysis of alerts generated by both *software* and network hardware.

The term SIEM encompasses different capabilities such as data collection, analysis and presentation of information from the network and the different security devices in it. In addition, it is also capable of managing identities and access, as well as vulnerabilities.

The characteristics of a SIEM described above are summarised and completed below:

- Identify between real threats and false incidents.
- Centralised monitoring of all potential threats.
- Redirect the action to qualified personnel for resolution.

[17] https://blog.segu-info.com.ar/2020/03/teletrabajo-escritorio-remoto-vs-vpn-vs.html

- To provide a greater degree of knowledge about incidents in order to facilitate their resolution.
- Document the entire process of detection, action and resolution.

Together with IDSs, SIEMs can assist in the work of monitoring computers and their external environments, so that potential threats can be detected even at an early stage and acted upon.

9. Conclusions

The **evolution of industrial systems and their connection to corporate environments and the internet has given way to new cyber-attacks**, which initially were not possible or required greater difficulty because they were in isolated environments. This, coupled with the age of many of the devices, creates a risk in industrial systems, which have had exploitable vulnerabilities for years.

As a mitigation measure to prevent the exploitation of these vulnerabilities, it will be necessary to use solutions to protect equipment, including *endpoints*.

As a summary of *endpoint* protection solutions for industrial systems, we can say:

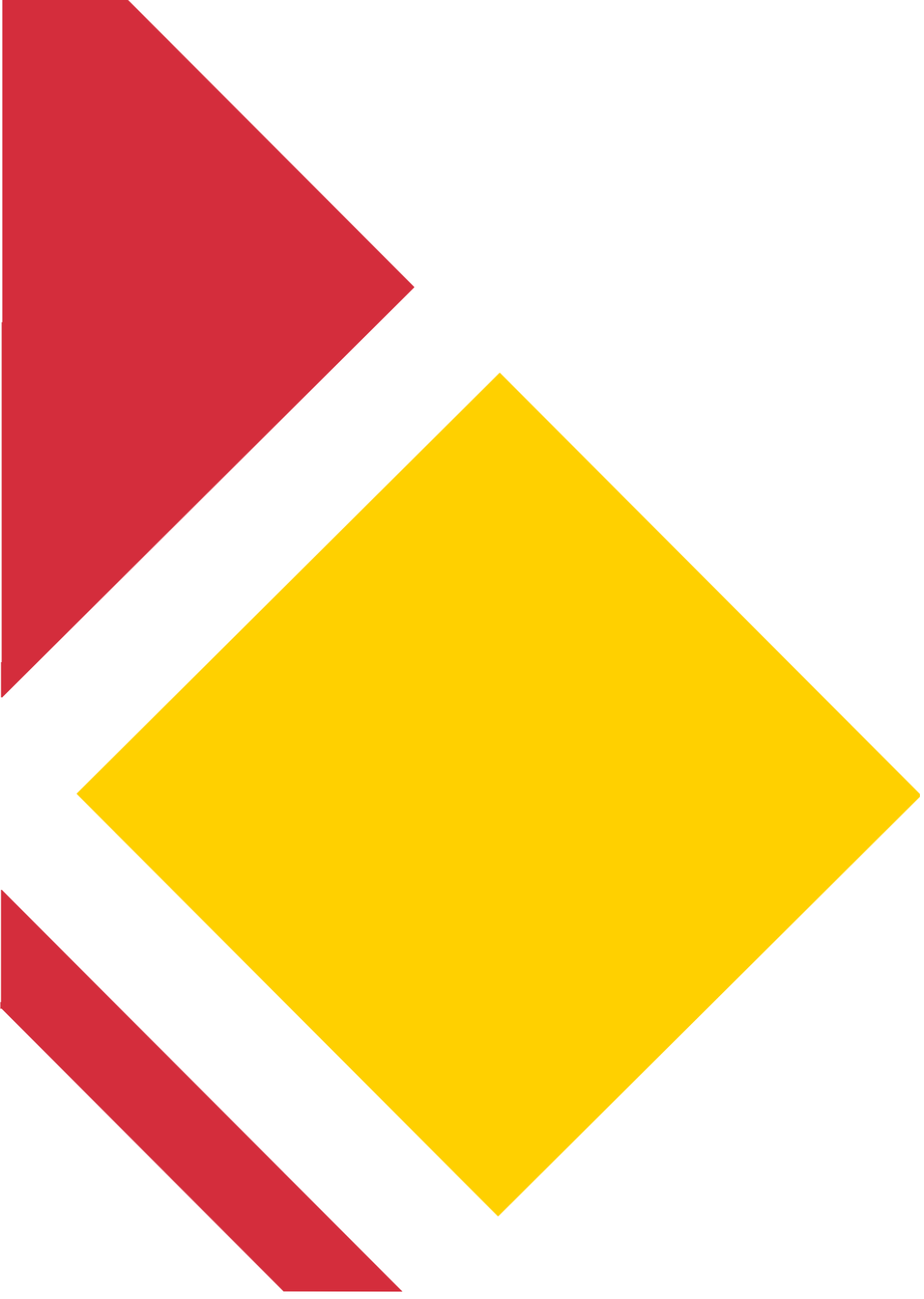
- **A defence in depth** approach to securing *endpoints* is possible.
- Equipment belonging to an industrial system has limitations that make it special when it comes to protection.
- The deployment of **EDR** and the application of **bastioning** on equipment, allows adding an **extra layer of security to** prevent malicious actions on industrial systems.
- ***Endpoint* protection from the outside** should not be neglected**.**

Glossary of acronyms

- **IoT**: Internet of Things
- **IIoT**: Industrial Internet of Things
- **IT**: Information Technologies
- **OT**: Operation Technologies
- **PLC**: Programmable Logic Controller
- **SCADA**: Supervisory Control and Data Acquisition System
- **SIS**: Safety Instrumented System
- **RTU**: Remote Terminal Unit
- **IED**: Intelligent Electronic Device
- **HMI**: Human Machine Interface
- **ICS**: Industrial Control Systems
- **ISP**: Internet Service Provider
- **VPN**: Virtual Private Network
- **XSS**: Cross Site Scripting
- **SQL**: Structured Query Language
- **HIDS**: Host-based Intrusion Detection System.
- **IDS**: Intrusion Detection System
- **IPS**: Intrusion Prevention System
- **SIEM**: Security Information and Event Manager

10. References

Reference	Title, author, date and web link
[Ref.- 1]	"Good Practices for Security of Internet of Things in the context of Smart Manufacturing" November 2018 URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
[Ref.- 2]	"Challenges and recommendations for the Industry Cyberdefense". URL: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations
[Ref.- 3]	"Protect your company: What IDS, IPS and SIEMs are and what they are for". URL: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips
[Ref.- 4]	"Malware InfoTech Product Scorecard". URL: https://resources.malwarebytes.com/files/2020/04/Malwa-rebytes-InfoTech-Product-Scorecard-Report-March-2020.pdf



Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO DE TRANSFORMACIÓN DIGITAL SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD