The Positive Way

WAVESTONE

FEEDBACK FROM THE FIELD AND GOOD PRACTICES FOR THE **PROTECTION AND SECURITY MAINTENANCE OF INDUSTRIAL CONTROL SYSTEMS**

For several years now, we've been supporting the far-reaching changes affecting Industrial Control Systems (ICS) which are being increasingly forced to open up to the broader market and corporate IS technologies. As levels of exposure and threats increase, protecting these systems in the long term, in coordination with business functions, is becoming critical.

What can we learn from experience in the field and what are the good practices for the protection and security maintenance of ICS?

AUTHORS

BENOIT BOUFFARD
benoit.bouffard@wavestone.com

ALI FAWAZ
ali.fawaz@wavestone.com

Opening up to corporate ISs is now a necessity ... but it also carries risks

Historically, ICSs were not connected to corporate ISs, either because there was no need or as a way of limiting the exposure. The majority of interventions were local, with work taking place directly on equipment, or remotely, using specific tools. The management of this work and the operations themselves were mostly local too.

Business functions' changing needs and the optimization of production processes have brought with them new and less localized requirements (such as remote supervision, remote maintenance, the emergence of the IoT[1], the standardization and rationalization of technologies and skills, cyber threats, etc.), which are designed to improve performance and facilitate operations. These challenges have led to a need to digitalize and interconnect industrial and corporate ISs.

Although this is now essential so that a company can operate effectively, our discussions with operational staff highlight the fact that such changes have also led to **risks of intrusion and the propagation of threats between these interconnected ISs.** These affect:

- **Operations and quality** – with potential shutdowns and modifications of production resulting in financial, reputational, and even people impacts;
- **The security of installations**, where production equipment being seriously compromised can have impacts on both people and the environment.

Mitigating these intrusion and propagation risks and their consequences means implementing security measures in several different stages:

1. Mapping ICS;
2. Putting in place secure network architecture;
3. Hardening and setting up security maintenance of the various systems over time;
4. And, lastly, putting in place the measures to detect incidents and respond to them.

Regulatory authorities have also been considering these risks. For the most sensitive installations, they are now mandating these types of measures and others too.

Interventions (such as patch management, account audits, integrity control, etc.), sometimes done remotely and often frequently, may now need to be carried out by teams more distant from site operations. These quickly come up against a traditional operating model designed to prioritize the continuity and integrity of operations, quality, hygiene and safety – while minimizing disruptions to production.

How can these measures be implemented without losing sight of the ICS's core purpose – to operate a physical process in the way designed?

[1] Internet of Things

1. Mapping, a prerequisite for dealing with cybersecurity risks on ICS

To assess the risks and control the potential impacts of implementing any new measures, the first step is the **IS mapping of your industrial installations,** which enables you to:

/ Know the systems that need to be administered and kept up to date;

/ Identify the users (operators, maintainers, etc.), and therefore those who need to be involved when a change takes place, to manage the operational impacts;

/ Evaluate the potential impacts of new vulnerabilities and security breaches in terms of safety, operations, and quality.

Feedback from the field

Our feedback shows that mapping an IS can be a long process. Initially, it's a question of identifying your industrial IS's macro-systems and then prioritizing the detailed mapping work. An **analysis of the macro-systems** enables them to be **grouped into different categories**:

1. Elements with a quality or safety role;
2. The supervision and maintenance systems for these quality/safety elements;
3. Other industrial ISs

Prioritizing also considers the degree of exposure (interconnection, remote access, online exposure, etc.).

Once the mapping process is underway, you will also need to develop **formal procedures for updating the map**. This means defining the update frequency, according to the level of criticality, and then actively managing the risks.

This is a substantial piece of work requiring **dialog and close collaboration with automation and other engineers involved with the installation**.

You should note that this mapping work can take longer and be more complicated than the types of mapping normally carried out by an IS department (ISD). An industrial IS can't be compared directly with a traditional IS, and there are several particularities that make mapping difficult:

- Equipment may be isolated behind filtering systems that prevent them from being detected or simply switched off for long periods (for example, an equipment used only for an annual production batch);
- The management of such equipment has traditionally been carried out locally and may not necessarily use the same standards and tools as the ISD.

2. Mitigating risks on an ICS by putting in place security architecture

Security isn't a new concept and it makes sense to follow the established principles for corporate IS architecture and security while adapting them to the particularities of ICS:

- Reducing the risks of propagation and intrusion by clearly **partitioning the ICS** and restricting access to it;
- Securing the administration of the IS by putting in place **dedicated administration architecture**;
- Equipping administrators with **appropriate tools** that enable them to make interventions across the entirety of the industrial assets;
- Integrating from the start (as far as possible) **interventions made by external maintainers**.

These four principles **form the cornerstones of securing ICS architecture**.

Partitioning, the first step in reducing exposure

Corporate IS and ICS have different goals: one is designed to facilitate the operation of a business (by providing messaging, management systems, collaborative tools, etc.), while the other is used to operate physical processes. In theory, these should be separated, and only certain types of information should be allowed to flow between them. However, feedback from the field tells us that this is rarely the case.

As in any work on IS security, the **strict necessity principle** should be adopted to limit exposure to cyber threats. Any interconnection between an ICS and a corporate IS should serve a specific purpose, for example:

- Sending production orders to the SCADA[2];
- Transferring CAM[3] files to digitally controlled machines;
- Collecting production data to enable the control of operations.

A current good practice is to set up a DMZ[4], including the filtering of flows through a firewall, but also a file-sharing solution that meets the needs of the business. This file-sharing facility can be secured by carrying out systematic anti-virus analysis of the files placed on the system before they can be recovered on the industrial side.

An ICS must also be internally partitioned to reduce the risk of threat propagation. To do this, you can use the principle of zones and conduits described in the IEC 62443 standard.

In practice, **this partitioning has to be carried out in several steps**:

- The listing of relevant business activities according to their different levels of sensitivity;
- Grouping activities requiring the same security level into zones (with, potentially, a "legacy" zone and associated sub-zones);
- Putting in place security rules for each zone according to their needs, as described in standard IEC 62443;
- Checking that the interconnections (conduits) between the different zones comply with security rules;
- Migrating the applications. Ensuring applications are compliant can be a long and difficult task, and it's best to use a risk analysis to prioritize and manage the work, as well as documenting the nonconformities and associated remediation plans. In addition, the migration process itself may be complex, if you are to avoid an impact on operations.

Here, it makes sense to take a step-by-step approach with associated observation phases:

- Before migrating industrial applications to their target zones – to verify that a change of IP address will not impact operations (hard-coded IPs, IPs configured in a given asset, etc.);
- After migration and before activating the filtering rules – again to verify that filtering itself will not impact operations.

[2] Supervisory Control And Data Acquisition
[3] Computer Aided Manufacturing
[4] Demilitarized Zone

The particularities of safety ISs

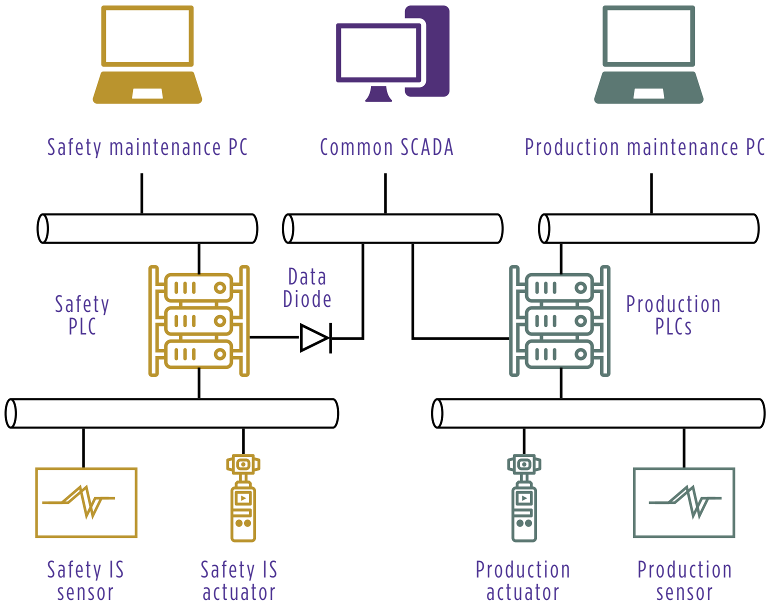
Safety ISs are ICSs that enable industrial production systems to be put into a safe state. Before the advent of today's digital systems, such systems had long been used in mechanical, pneumatic, and electrical forms. Ensuring their digital integrity is therefore of prime importance. A final partitioning step can be considered to achieve this. However, existing systems often act as a brake that complicates the work.

When done rigorously, such separation reduces the risks of propagation and enables distinct levels of security to be implemented for the production IS and safety IS according to their risk levels. However, a disadvantage is that doing this requires a dedicated SCADA system, which is both expensive and not operationally friendly.

Good practice:

A separation that leaves room for a common SCADA means the usability of the ICS can be ensured, while reducing the risks of propagation from the production IS to the safety IS, by the installation of a diode.

An approach for ICS / safety IS (SIS) partitioning



© Wavestone 2020

Administration – the nerve center of network architecture

/ Good administration of an IS is essential to guaranteeing its availability and security. **When carrying out an IS security program, you must be clear about the objectives you want to achieve**. The good practices we observe in the field include:

/ **Creating an administration network isolated from the production network at central and local levels** to protect administration flows and avoid integrity losses on flows used to manage sensitive operations;

/ **Protecting the administrative equipment** to prevent an attacker from taking control of these critical elements directly;

/ **Standardizing, as far as possible, practices and equipment** to facilitate the deployment of secure, or even centralized, administration architecture, and to maintain security levels over time. This can be achieved by pooling resources within a central, dedicated team.

To note: here, we are discussing only the administration of industrial IS infrastructure.

Production PLCs, for example, are administered by the business functions in terms of configuration and will pass through the dedicated configuration and maintenance team, when updates are required.

/ The first step is to create the structure of the isolated and underlying administration network. This objective can be achieved by putting in place the following measures:

/ To optimize and pool resources, and especially to assure the **DRP[5], the administration network must be constructed around one or more datacenters.**

/ In order to reduce the propagation risk from an infected site, the WAN[6] placed between the datacenter and the industrial installations can be configured using the hub-spoke[7] model, which ensures the separation of each installation.

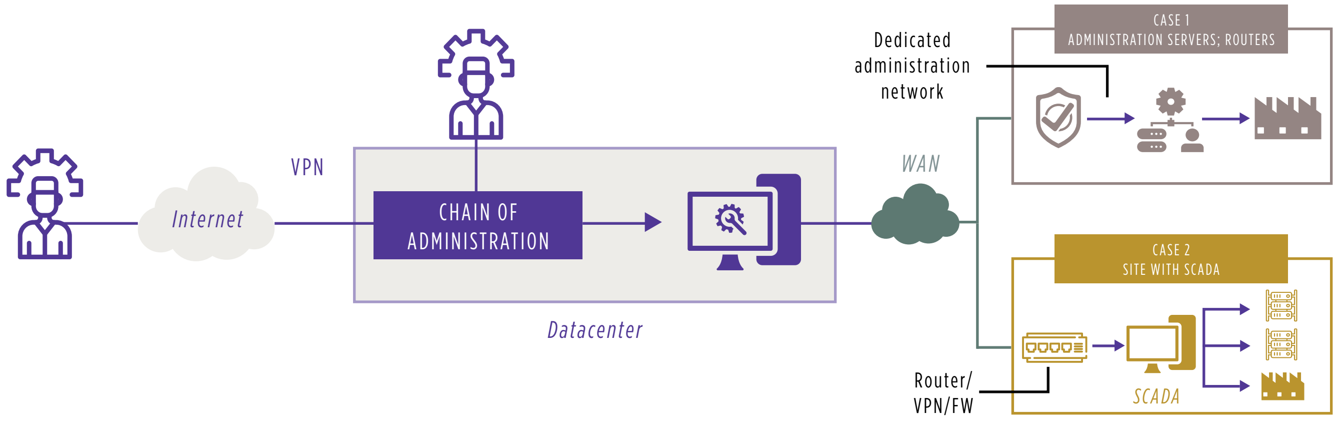
/ To guarantee the integrity and confidentiality of administrative flows, these must be isolated within a specific VRF[8] or on an administration VPN[9] between the datacenter and each site.

/ Setting up such a dedicated administration network relies on, in particular, the use of telecoms and security equipment, as well as dedicated interfaces on the servers.

/ For the most important sites, the risk of intrusion from the user LAN[10] can be reduced by setting up an administration LAN which is only accessible from the datacenter's administration LAN. However, such architecture must provide a resilient solution in the event that the WAN is cut to allow local teams to access it directly, as well as for equipments that simply cannot be maintained remotely.

/ Companies with multiple sites can also use a standardized box that embeds all the security functions required for the site to be interconnected. This facilitates configuration and security maintenance.

Diagram showing the interconnection of a site with or without a SCADA



© Wavestone 2020

[5] Disaster Recovery Plan
[6] Wide Area Network
[7] A network around the datacenter.
[8] Virtual Routing and Forwarding
[9] Virtual Private Network.
[10] Local Area Network.

The second step consists of connecting the administration tools and equipment to be administered to this network, while protecting it from compromise.

When done rigorously, this separation reduces the risks of propagation and enables distinct levels of security to be implemented between the production IS and the security IS, according to their specific risk levels. However, the disadvantage is that doing this requires a dedicated SCADA system which is both expensive and does not facilitate operations.

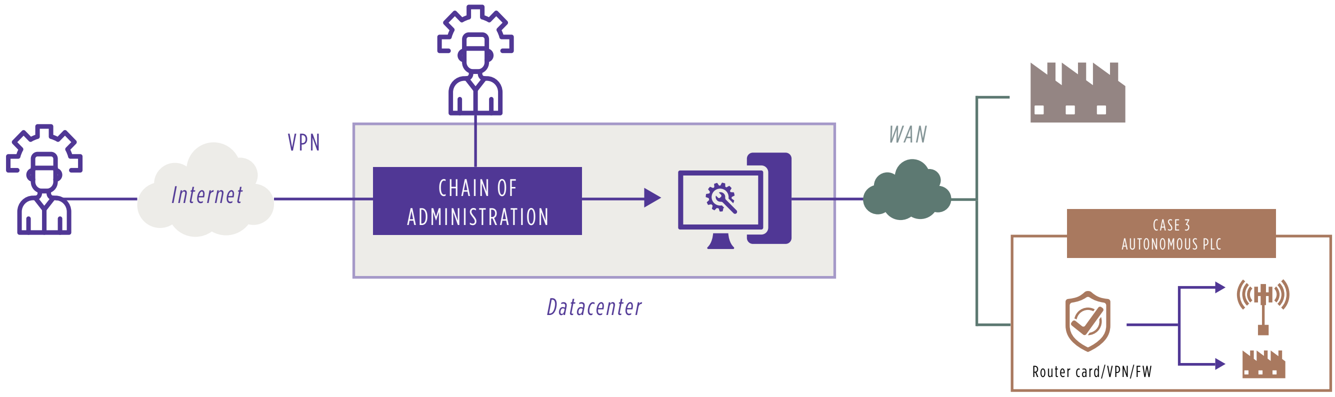
For sites with only one piece of equipment, VPN and filtering functions can be provided by a router card, sometimes directly added to the PLC.

Equipment that cannot be directly managed because of its operational constraints should be isolated in specific VLANs[11], access to which is filtered through a firewall that enables remote administrative actions to be carried out if required.

There may also be a variety of reasons to keep part of the IS fully separated. This isolation removes the ISS risks, leaving only business risks. Separation also lowers the level of exposure and therefore the risk of intrusion. A risk analysis should be carried out to determine how to proceed. The administration process will be modified consequently: from simple local administration procedure to a dedicated administration infrastructure – which can be costly.

These various network bricks, then, enable administrators to access the industrial equipment. However, they must also be given access to the necessary tools.

Diagram showing the interconnection of a standalone site



© Wavestone 2020

[11] Virtual Local Area Network (or Virtual LAN)

Administrator tools: how to meet needs while guaranteeing security

As corporate ISs and ICSs are generally managed separately, they each use their own tools – although these may be based on identical products. Setting up these tools meets several objectives. It:

/ Assures access control on the administration interfaces, reducing attacker chance to access to means of attack and the fraudulent use of the tools;

/ Tracks administrator activity to reduce the potential impact of an attack, by providing a means of detection and response capabilities, and facilitating investigation following an event.

This requires the implementation of an administration chain.

To centralize access and maintain close control of authorizations, an administration bastion must be set up. Generic accounts are handled by the bastion and protected in its digital safe.

The diversity of the equipment on an ICS can require specific and heavy clients or protocols whose administration cannot be supported by a bastion. To limit the risk of infection linked to connecting to unmanaged machines (supplier, maintainer...) on the IS, these tools can be installed on a dedicated administration workstation. Access to this station can be provided from the bastion using, for example, RDP[14]. Any flows that use obsolete protocols will need to be encapsulated in an IPsec VPN tunnel to be able to reach their targets.

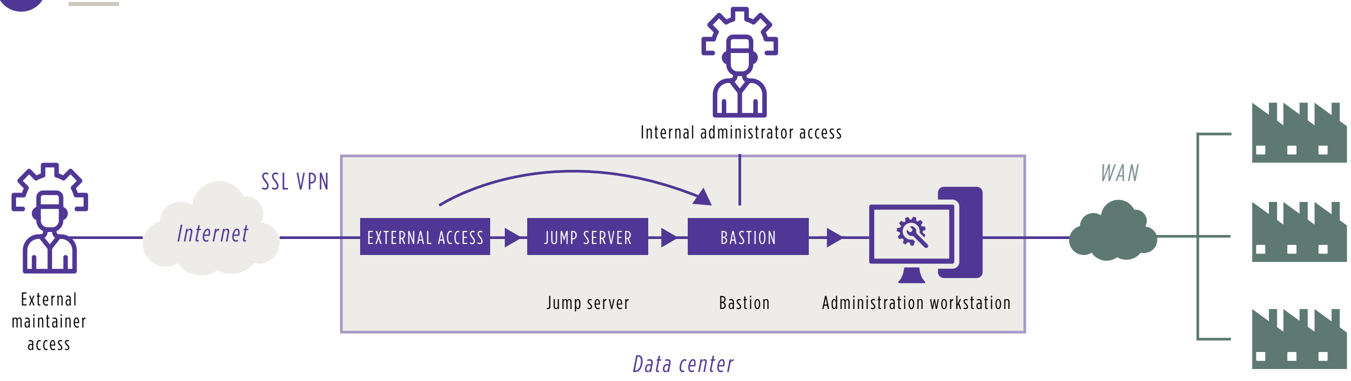
This also ensures the traceability of activity and reduces the risk of theft from generic, privileged accounts. The bastion can also secure administration flows by performing protocol translation (for example, from Telnet[12] to SSH[13]).

Equipment, especially telecom equipment, whose security levels are sufficiently mature (including detailed management of rights, traceability, individual accounts, etc.) can be directly administered without using a bastion.

The establishment of a dedicated administration workstation, where the tools needed by business teams will be installed, requires a process to be put in place for their creation. This will ensure the workstation can remain secure and that the list of tools being deployed on the IS can be documented.

Whether administration is carried out using a standardized bastion or a dedicated administration station, the resilience of the solution must be assured.

Diagram showing the main functions involved in a chain of administration


Internal administrator access
SSL VPN
Internet
EXTERNAL ACCESS
JUMP SERVER
BASTION
WAN
External maintainer access
Jump server
Bastion
Administration workstation
Data center

© Wavestone 2020

[12] Terminal Network, Telecommunication Network, or Teletype Network
[13] Secure Shell
[14] Remote Desktop Protocol

Integrating external maintainers

Lastly, **it's essential to secure access by third-party maintainers** in order to limit the risks that arise from improper or unmanaged access, such as infection of the IS after the installation of an unauthorized tool, data loss triggered by a malicious third party, the unavailability of equipment, etc.

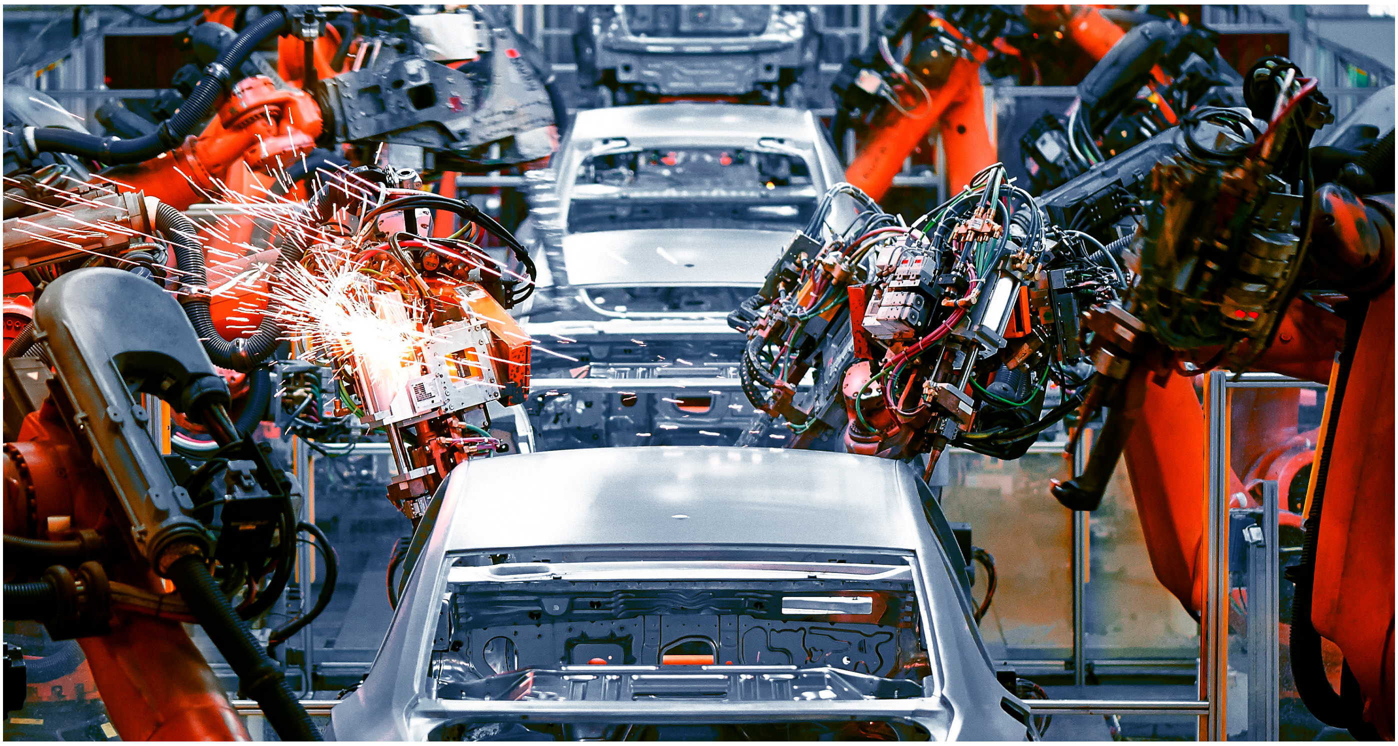
An **external access point** with **strong authentication** will be needed to confirm the identity of users. Such an access point allows maintainers to access a jump server which is controlled and hardened by the customer, while also ensuring the traceability of activity. Here, more sophisticated customers deploy solutions that allow the third-party access to the IS for the duration of the intervention only – and then only once access has been approved internally.

It should be noted, however, that remote access does not comply with The French Military Programming Law[15], that requires a dedicated and hardened administration server that is isolated from the internet (to be used by internal administrators too).

The **configuration and maintenance servers** that are dedicated to the site and PLCs must be rigorously monitored to keep them up to date and secure, especially in terms of the tools deployed on them.

For a variety of reasons, however, some suppliers may not agree to use a dedicated local maintenance server or a jump server with secure remote access. If this is the case, you must identify solutions that meet the security requirements of the ICS, the needs of business functions, and those of the supplier.

For more detailed information, note that there is an ANSSI[16] working group dedicated to the cybersecurity of industrial systems. Its **PIMSEC framework**[17] recommends a range of security requirements that can be incorporated into contracts with industrial IS service providers.



[15] A French law aimed at identifying and securing organizations and ISs of vital importance to the country

[16] The French National Cybersecurity Agency

[17] ANSSI's framework for security requirements for industrial systems integrators and maintenance providers

3. Managing risks in the long term

Equipment hardening

In addition to secure architecture and administration tools, security levels for each item of equipment should be increased according to the strict necessity principle. A generic hardening guide can be created and then adapted to each of the technologies identified by the ICS mapping. This allows some of the vulnerabilities to be remedied at configuration and system levels.

Additional security can be provided by adding complementary solutions, such as:

- / **Antivirus software**, which will cover industrial workstations against the most common viruses, whether connected to the network or not (although the latter will require manual updates);
- / Implementing strict rules on **local machine firewalls**, which can be used to prevent communications, and therefore intrusions, on unused ports, and to filter the origin of flows according to the protocols used – which means attempted attacks can be more easily detected;
- / **Local administrator account management solutions** (for example, LAPS for Windows) finally make it possible to manage native administrator accounts on workstations in a central and individualized way.

However, sometimes it may no longer be possible to harden equipment due to obsolescence. In such cases, there is a need to work with the relevant business functions on **obsolescence management** of the equipment – its potential replacement and, as a last resort, options to isolate it from the rest of the IS. On obsolete workstations, **configuration blockers** can be used to ensure the installation and use of components is limited only to those that are strictly necessary.

It's important to remember that, while ICSs have vulnerabilities, they are, above all, part of the company's means of production. Dialog with the relevant teams is therefore essential in understanding how equipment is used – in order to resolve the vulnerabilities while limiting effects on the business as far as possible.

Security Maintenance

Once equipment has been brought up to the right level of security, a plan will be needed to maintain this over time. **A choice of options for managing security patches** can be developed to meet the needs of the business (in terms of availability, integrity, etc.) and synchronized with the maintenance of the industrial equipment through:

1. **Integration into standard operating processes**, for example, an installation's qualification/quality processes may require that equipment be up to date regarding security. The updating and administering of equipment can therefore take advantage of plant shutdowns, especially when recertification is needed.

2. Planning a **"hot swap" update process** in the event of a critical security breach and a procedure for the preventive isolation of production lines – until it's possible to interrupt the production process;

3. The **identification of redundant or peripheral equipment** where interventions can be carried out on the basis of straightforward interaction with production managers.

Potential challenges for long-term risk

The quality standard process should ideally:

- Request delivery of security maintenance procedures prior to production, as well as security policies;
- Plan for close working with security teams when evaluating the impact on integrity of any change related to the security maintenance of systems;

Mixed practice in the field:

- In less mature organizations, system patching is still optional in quality processes while projects do not deliver security maintenance procedures in a standard way;
- Conversely, in more mature organizations, standard operational quality procedures stipulate that cybersecurity patches must be installed in accordance with their application procedures (delivered by a security project), and that these do not alter the integrity or scope for using the industrial equipment.

Lastly, at a more detailed level, there are a few tips that can be applied to reduce the potential impact of updates:

- Identifying the architectural elements of an industrial system needed for business or operation functions may also enable the defining of parts that can help reduce unavailability risk following patching operations (high availability, cold spares, hot swaps of data redundancy/traces, temporary buffering of data and traces, offline backup, etc.);
- The non-intrusive installation of patches on the lower layers of systems, carried out during plant startup (between production batches) whenever possible, enables the time needed to install patches to be minimized within the available maintenance slot (the system reboot time being the only relevant measure here);
- The creation of regular backup infrastructure (each time the plant is restarted) can facilitate rollbacks when problems occur.

To put in place these patching processes, the mapping carried out previously must have generated a **precise equipment inventory**, including:

/ The identification of the equipment: type, location, and number of units;

/ The industrial processes that each item of equipment is used for, and the associated criticality;

/ The version of the operating system and/or firmware, and the tools and configurations deployed;

/ The cybersecurity needs of supported processes;

/ The availability of redundancy, data buffering, and cold spares;

/ The required patching frequency and patching history.

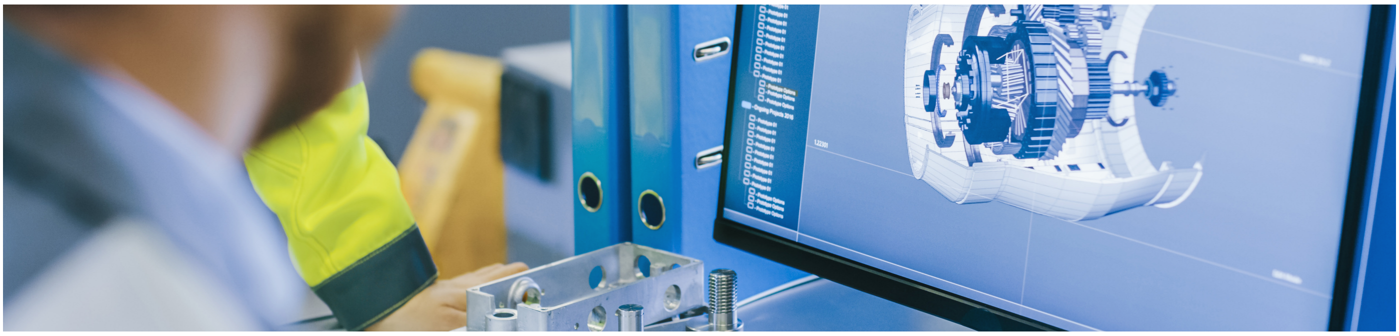
But maintaining security levels isn't simply about applying patches to equipment, it should also:

/ Define the process for updating the **security solutions installed** on equipment isolated from the network;

/ Install **removable media cleaning solutions**, given that these types of tool remain in widespread use on industrial sites. Here, the use of portable solutions allows such media to be analyzed while moving around the site;

/ Ensure the **safeguarding of equipment configurations** and their **integration into the DRP** in order to guarantee that equipment can be restarted following an incident while still meeting availability needs;

/ Set up **monitoring of the industrial IAM**[18] to ensure robust physical and logical access control. This can also be used to automate a number of time-consuming account reviews that are still sometimes done manually.



[18] Identity and Access Management

4. Detecting cybersecurity incidents

The measures set out above help reduce the likelihood of risks and increase the availability of equipment, which benefits the business. Nevertheless, there will still be a need to prepare for the worst and to have in place the tools needed to **detect an incident** – to be able to remedy such events as quickly as possible and minimize interruption times.

Putting in place detection

The first step is to activate the IDPS[19] functions on network equipment to ensure that a **first stage of detection, and potentially automatic blocking, is in place**.

The next step is to collect information by deploying a concentrator on site. The network equipments and server logs can then be sent to existing or dedicated SIEMs[20] where **correlation and detection** can take place. SOC[21] and CERT[22] teams can then carry out analysis and detection, and respond, if needed, to an incident, by working through standard scenarios.

It should be noted that sending logs can consume resources in terms of bandwidth; filtering can be applied directly at the concentrator level to ensure that only relevant information is sent to the SIEM.

Anticipating specific risks

However, detection based on standard scenarios may offer only limited value to the business functions. Considering the entirety of sources (PC, Linux, UNIX, etc.) and setting up dedicated industrial IS probes, capable of interfacing with the SCADA systems, can enhance the detection system. Such solutions, however, can be costly.

The key factor is to ensure a progressive and rapid increase in the SOC maturity and added value. Agile methods are a good fit here and involve the iterative application of the cycle described in the text box below.

Planning for remedial activities

Lastly, detecting an incident will only result in effective remediation if the business-function teams are involved. As with equipment updates, **emergency stop procedures** should be reviewed jointly with ICS users. A formal **Incident Response Plan** enables the actions for an industrial cyber-incident to be planned.

Dedicated **ICS crisis-management exercises** should also be carried out to ensure that teams are optimally prepared and to highlight any shortcomings.

Agile methods are therefore a good choice when putting in place an industrial SOC and involve the iterative application of the following cycle:

- Work with business functions teams to identify an undesired event;
- Analyze the ICS architecture and identify the relevant data sources;
- Collect the data required to detect the event;

Feedback from the field tells us that SOCs often rely on information from data flows or security equipment (firewalls, probes, etc.). However, we also observe that, "industrial" data sources, which are still under-exploited, may be easily accessible and can be a significant, complementary addition to information from data flows.

- Implement the detection scenario.

[19] Intrusion Detection and Prevention Systems
[20] Security Incident and Event Management
[21] Security Operations Center
[22] Computer Emergency Response Team

5. Taking a progressive and participative approach guarantees an initiative's success

The security maintenance of an ICS is a complicated task that can only be successful if it is carried out in partnership with the business functions. A progressive and participative approach should be taken to work with them in each of the following areas:

/ **Understanding the ICS**, by mapping and prioritizing the most critical elements;

/ **Mitigating the risks on the ICS**, by implementing state-of-the-art secure network architecture and defining the administration processes – due to their criticality, safety ISs must be given particular attention;

/ **Ensuring an adequate level of security**, by hardening and maintenance – in particular, this will involve discussions with equipment suppliers and manufacturers;

/ **Putting in place the tools needed to detect security incidents**, with the potential associated production stops, and define the response processes.

The actions above can't always be carried out in parallel. **Defining a clear roadmap** will enable such actions to be prioritized. This will aid cost control and maximize the added value for the business functions.

Given that such significant undertakings are often driven centrally, the challenge is to engage the individual industrial sites (which may be spread across the world) to ensure security levels can be maintained in the long term. In general, we observe that companies take a two-stage approach:

1. **A multiyear cybersecurity program** (typically carried out over three years), with a budget of €10m-15m, aimed at:
   - Creating the ICS inventory
   - Raising the security levels of existing assets by putting in place protective measures, often involving peripheral security and filtering, and remedying the most critical vulnerabilities – here, defining procedures is essential;
   - Putting in place an initial network of local cybersecurity coordinators;
2. Create an **industrial cybersecurity team** and its **associated management structures** that bring together:
   - A framework of key activities that local players will need to manage;
   - The participative construction of the tools that will help this network of local managers to carry out their cybersecurity activities;
   - The development of approaches to measure the increase in security maturity levels and perform change management (such as maturity matrices, site-level budget-modeling tools, the definition of steering indicators, central services that the sites can draw on, etc.).

Implementing the management processes can start immediately after the program and therefore benefit from the initial network of site-level cybersecurity coordinators put in place.

Once constructed, it becomes a question of energizing the initiative and steering progress on the sites and ICSs, in terms of both security and maturity levels.

Doing this typically involves:

/ A network of local cybersecurity coordinators, of size 0.5 to 2 FTEs[23] per site, who are responsible for carrying out projects, implementing ongoing cybersecurity activities, continuous security improvements, and reporting;

/ A central team of 3 to 10 FTEs, to provide overall steering and support local managers – especially in terms of expertise.

[23] These figures can vary significantly depending on the size and number of local sites; they are the typical arrangements we observe in the large international organizations that Wavestone supports

The Positive Way

WAVESTONE

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to inform and guide large companies and organizations in their most critical transformations, with the ambition of a positive outcome for all stakeholders. That's what we call «The Positive Way».

Wavestone draws on over 3,000 employees across 8 countries. It is a leading independent player in European consulting.

Wavestone is listed on Euronext Paris and recognized as a Great Place to Work®.