Use Case

Cybersecurity for Industrial Control Systems

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

Table of Contents

INTRODUCTION

This use case supplements the document entitled *Managing cybersecurity for Industrial Control Systems1*.

It is designed to present situations that pose a risk for businesses and provide pertinent recommendations to help them secure their Industrial Control Systems (ICSs).

Many of the best practices described here are similar to those used for Management Information Systems[2], but their implementation must be adapted to the constraints of the industrial environment.

Concrete examples and situations presented in the following study illustrate the implementation of cybersecurity in the industrial context**. The proposed approach and recommendations can be applied in any industrial context, but they must always be adapted to the identified issues and risks.**

This study concerns an industrial site that has existed for several decades. Its systems are heterogeneous; some are obsolescent. The systems are controlled by PLCs and supervised by SCADA systems grouped together in an control room. Some of these systems, such as production lines in an assembly shop, have real time constraints, while others, such as a distribution unit for hazardous materials, have dependability and availability constraints.

The site has a storage unit geographically located a few hundred metres outside its main perimeter. This unit is located upstream of the hazardous material distribution unit.

The abbreviations and acronyms used in this document are set out in Appendix A.

[1] http://www.ssi.gouv.fr/systemesindustriels

[2] Management Information Systems (MIS): information systems for office applications and services, human resources management, customer relationship management and integrated management.

1 CONTEXT

Site management has requested upgrades to the SCADA system so that it can communicate with the Intranet corporate system, with the objective of reducing costs and production time. The information collected from the SCADA system must be accessible by all site managers from their office work stations, as well as those at other corporate sites. Finally, they have requested that remote maintenance solutions be studied in order to optimise operating costs.

The company has an IT department responsible for managing the Intranet corporate system infrastructure (office systems and interconnections between sites, email and Internet access).

For several years, at the request of corporate management, this service has implemented an IT Security Policy.

Following recent incidents, management requested expansion of the IT Security Policy to industrial plant, some of which are under the responsibility of the Technical Manager, others under the responsibility of the Production Manager, and some directly under the responsibility of the Site Manager. A few months ago, the spread of a virus introduced by a USB key on a SCADA work station generated heavy network traffic and caused malfunctions in the ICSs.

In addition, a consulting firm carried out an internal penetration test and identified two ways to break into the office network: by injecting SQL commands into the extranet database engine and by sending booby trapped PDF files to some users. Some work stations, where security updates to the PDF reader had not been installed, were compromised. The auditors tried to expand the compromise and identify vulnerable devices on the office network via network discovery and vulnerability scans. They quickly identified the vulnerability of a set of devices, based on older systems and not updated, and the presence of numerous administration interfaces not protected by authentication. During these tests, a PLC halted, causing a production line to shut down for half an hour. The vulnerability was finally traced to the SCADA systems. The PLC halted as a consequence of running the vulnerability scan. The office and industrial networks were interconnected due to an incorrect configuration, unknown to the site managers.

This misadventure demonstrates why ICSs need to be better protected. It also shows why external attacks are not the only threats.

A coordinator, recently hired, with experience in IT and background in industry, was appointed to lead the project. His assignment required a pedagogic and diplomatic approach. The coordinator would report directly to site management. He began by learning about the plant and associated business constraints. While still learning about the IT Security Policy, he wondered how to extend it to industrial plants with very specific characteristics, while respecting their constraints and customs. He realised the differences in culture and approach between the IT, production and dependability groups. Yet they all have the ultimate goal of providing products and services to customers in a timely and cost effective manner.

2 THE FOLLOWED APPROACH

The first step was to understand the business needs, and to take an inventory of devices and services. The objective was to assemble a physical and logical mapping of plant and the data streams between the various elements, and then to establish levels of criticality for each one.

This was a significant project, which would be carried out together with the plant managers. Some of them already had information at hand, for example from the Failure Modes, Effects and Criticality Analysis (FMECA).

During the second step, this mapping would allow an evaluation of sensitivity levels and an initial analysis of existing vulnerabilities.

In the third step, analysis of new requirements would allow identification of the necessary security measures (technical or organisational) that should be implemented to reduce discrepancies with existing systems and potential impact on the plant.

These three steps were formalised in a security improvement plan that the coordinator will put forward to management.

He understood the extent of the work involved, but also the repercussions of his actions on his colleagues' daily tasks: "More new rules to follow... there are already too many... this will make our work even more complicated..."

He decided to start by communicating about his project, with a simple explanation of its purpose and how he intended to proceed. He organised a presentation for key managers and informed them of his plans to conduct a site visit, so that they can relay the information to their teams. He could thereby make contact with the personnel and directly communicate the importance of cybersecurity in their daily activities. **Educating personnel was a key part of his approach. Since they were very concerned about system availability and security, he emphasised that cybersecurity does not impair availability, but rather contributes to it.**

3 OBSERVATIONS (SITE VISIT)

The coordinator, accompanied by foremen from the shops, began the site visit at the control room, with its SCADA work stations staffed by operators 24/7.

3.1 The control room

Walking past the network wiring closets in the control room, he noted that the SCADA bays were properly identified and separated from the adjacent ones for the Intranet system.

However, he noticed a network cable from the SCADA racks going towards the intranet racks.

He asked the control room manager for an explanation. Seeming uncomfortable, the manager explained that for certain operations, it was useful to access SCADA from an office PC located in another room.

The coordinator pointed out that there had already been an incident caused by network interconnections. The manager explained that it was just a SCADA machine with two network cards, one connected to the office network and the other connected to the SCADA network; therefore, the networks were not interconnected. The coordinator explained that an individual or a *rootkit* that compromised this machine would have control of the entire SCADA network. This was a major risk, with the same consequences as the spread of a malware.

The Intranet components have measures to address external threats (e.g. antivirus software, regular updates, strong authentication, etc.), while that is surely not the case for all SCADA devices. One non secure machine with two network interfaces provides an attack path and facilitates the spread of viruses.

Solutions (e.g. based on Web technologies or RDP), together with network segregation mechanisms, provide better security for SCADA access from office work stations (see Appendix B).

This connection, which allows industrial systems to be compromised from the Internet by way of the office network, should therefore be removed.

The coordinator also noted a USB drive plugged into a work station. Someone had clearly forgotten it. He asked why USB drives were used in the control room. **He was told that the team needed to retrieve data from SCADA for reporting purposes. Examination of the key revealed that it contained personal data, as well as a virus!** Fortunately, it was not a particularly dangerous one, but all machines needed to be checked, and disinfected as necessary. The head of the control room said that USB drives were the only way to retrieve data from SCADA or to import updates for configuration files for example.

The coordinator explained that, short of banning USB drives, it is possible to disable Autorun for removable media, a function is exploited by many viruses (see Appendix B). Software restriction policies could be configured to whitelist specific programmes (e.g. SCADA functions and certain utilities).

It is also possible to implement a secure data exchange station and disable the USB ports on all critical SCADA machines. Solutions can be found!

USB drives are a primary vector for the spread of viruses. Numerous incidents bear this out!

The coordinator asked how internal personnel and subcontractors were made aware of cybersecurity issues. The manager responded that, theoretically, they undergo limited training, but it is mainly oriented around the IT side and that training should take place on a regular basis in order to be effective. The coordinator said that the same hygiene rules used for IT systems are applicable to industrial systems.

The "IT hygiene rules" for ICSs (see Appendix D) could be posted in the control room and in the production units. Pictograms, like those regarding dependability, could also be used to remind personnel that USB keys are prohibited on critical plants, that laptop computers cannot be connected without authorisation, that all anomalies must be reported, etc.

From the control room, numerous actions and configurations could be performed on the plant. The SCADA applications were numerous and inconsistent. The coordinator asked what would happen if an operator executed an erroneous command or incorrectly entered a setting (e.g. 10,000 RPM for an engine speed instead of 1,000).

The manager replied that checks are built into the system to limit the risk of operator error. The coordinator commented that this could also be valuable against attackers.

The SCADA system's input fields incorporate bounds checking: a user cannot enter a value outside the device operating limits. These limits are also integrated in the PLCs and are unchangeable. They cannot be modified without changing the PLC source code.

Moreover, to avoid certain erroneous operations, the SCADA application asks for confirmation before sending the command. Although this reduces the risk of errors, they can still occur. The command request must be sent (bit = 0), and then when the PLC has accepted it, the command is sent (bit = 1). The manager explained that this mechanism allowed the shutdown of an plant to be avoided during a recent intervention. An automation specialist reloaded the PLC data from a backup. In the backup, the stop bits were set for several plant, but the command request bit was not. The production shop did not stop and an alarm concerning this discrepancy was sent to the SCADA system, which allowed detection of the problem. The coordinator said that this is an example of how simple mechanisms can sometimes prevent problems. This measure would be ineffective against an attacker with in depth knowledge of the system, but could allow detection of many other less sophisticated attacks.

3.2 The production shop

During his visit, the coordinator noticed a work station located in a corner of the production shop. Next to it, an interim employee of the cleaning service was dusting. The coordinator asked the shop foreman what the work station was used for. The latter replied that it was a "remote" SCADA work station used by team leaders and maintenance technicians.

Taking a closer look, he found that the SCADA application was running under a "Maintenance" login. The shop manager explained that maintenance had been carried out on a production line the previous day. It ended late and the technician had probably forgotten to log out.

The coordinator pointed out that, as a result, anyone could use the application even the interim custodian who was working nearby. Wouldn't it make sense to include an automatic timeout in the application that locked the screen after a period of inactivity?

The manager replied that it would have little effect because the logins are generic, assigned to a team and thus known by numerous people.

The coordinator explained that it would still be judicious to implement automatic disconnection of this isolated work station and limit the remote control and remote configuration functionalities for these generic logins. And, most importantly, this work station should be moved to a more visible location in the shop, e.g. a zone under video surveillance.

Other approaches should be studied, because all employees have a badge for physical access to the premises and certainly have their own login for the office network. The SCADA application could take advantage of these approaches, instead of using generic logins, which are often an obsolete artefact.

The shop manager said that these suggestions were interesting and that he would like to pursue them.

The coordinator came across a technician using a touch screen on the new assembly line. The technician said he really liked the touch screen, which gave him the same functionality as a SCADA work station while being physically in front of his process.

It could be used to modify a set of process parameters, view trends and execute commands. The technician explained that he could force certain operating modes, inhibit sensors and force values, which he could not do on the SCADA work station. Very interested and curious, the coordinator asked how this touch screen was connected to the system.

The technician said he believed that it was connected to the PLC that controls the production line. He opened the low voltage cabinet of the production line and pointed out the PLC. It was connected to an Ethernet switch, clearly integrated into a fibre optic backbone. A second copper cable runs from the switch to the touch screen. **In summary, in the present configuration, the touch screen and the PLC were accessible from the office network!**

This touch screen (Operator Panel OP) is very similar to a PC and has a standard operating system, but is physically more robust. It surely has easily exploitable vulnerabilities that need to be considered in access policies and when installing updates. It could be useful to perform penetration tests from this type of device. The OP has USB ports; what would happen if a keyboard were plugged in? Does it provide access to system functions or to the list of programmes installed on the OP, for example?

The coordinator asked how the control room was informed when particular modes of operation are used. The technician replied that, in general, he calls the operators to inform them, because the system does not send this information to the control room.

The shop manager explained that this new assembly line is much faster than the old ones, but it stops more often and requires more precise and more frequent configuration. Therefore, in order to avoid swamping the control room, not all information is sent to the SCADA system.

The coordinator explained that, on the contrary, more traceability and more data sent to the SCADA system could help identify malfunctions and detect abnormal operation. Today's systems and software are capable of handling large volumes of data. Data storage is no longer a major constraint.

The coordinator said he was surprised to see one SCADA application in the control room for shops A and B, and a different application for shop C. The manager said he would like to have a single application and especially the same level of functionality for all three. That would make it easier to correlate production data. However, the PLCs in shop A and B interact with the SCADA system via specific protocols not supported by other manufacturers or by the new SCADA equipment.

The shop manager said that, from his point of view, SCADA systems using specific protocols are not vulnerable. The coordinator explained that, in reality, proprietary systems are not immune from attacks. They are often developed using standard components and run on standard operating systems that are not specific to ICSs. Their security mechanisms are often weak. An analysis of this system is needed. An upgrade study is also needed, conducted together with the manufacturer.

3.3 The hazardous material storage unit

Next, the coordinator visited the hazardous material storage unit, located a few hundred metres from the production building, outside the site's main perimeter.

He noted that the devices (radar) for measuring the levels of hazardous materials in the tanks were situated "out in the open," easily accessible to individuals outside the company. He pointed out to the unit manager that these levels could be modified by malicious individuals and asked what the impact would be.

The manager replied that invalid level readings could disrupt the operation of the system. For example, the PLC could close the distribution valves if it detects a low level in a tank. In the past, a sensor malfunction gave rise to erratic system behaviour without the cause being apparent. Diagnosis was difficult because this unit does not send any data to the control room. In the wake of that incident, a second set of sensors was installed to increase reliability.

The coordinator said that physical protection of remote or exterior devices seemed necessary, as well as a minimum report of data to the control room.

The unit manager observed that a planned expansion project would provide an opportunity to improve the monitoring of the system. This would also free operations teams from having to frequently visit the plant to check for anomalies.

Meanwhile, the coordinator noticed a modem connected to the PLC. The integrator had installed it to allow remote intervention and thereby reduce maintenance costs and response times.

Analysis revealed that the password to access the PLC programme was blank (which is the default). Neither the operator nor the integrator had thought to change this configuration. The coordinator said that it is urgent to implement a password policy for PLCs and other field devices (e.g. sensors and actuators).

An attacker scanning the range of telephone numbers used by the company could identify the modem, take control of the PLC, modify the programme and provoke malfunctions in the system. **Fortunately, the PLC modem has a callback function**[3]. Thus, an attacker cannot take control of the PLC, even if he knows the password.

The manager explained that the integrator would like to connect the PLC Web management interface to the Internet (e.g. via a VPN), which would give them access to more advanced diagnostic functions.

The coordinator understood the need and the request. Nevertheless, it is paramount to assess the associated risks.

The use of Web services on a PLC can be extremely dangerous.

The Web layer is undoubtedly a standard component (not specific to the PLC) that may engender vulnerabilities for the entire PLC (e.g. denial of service). On *IT* systems, Web services regularly require installation of updates; that is surely not the case for PLCs.

These functions, which are often optional, must be disabled on critical plants!

3.4 The hazardous material distribution unit

In the hazardous material distribution unit, the coordinator noticed several SCADA work stations unlike those he had seen so far. The unit manager explained that in this unit, **the SCADA system is maintained by the company that integrated it.** The integrator intervenes at their request if a work station does not function properly. Sometimes the integrator replaces the work stations. The coordinator was surprised and asked why this service was not provided by the IT department. Since they are on site, they could act more quickly; moreover, they could provide standard equipment that would certainly be less expensive.

[3] Callback: A maintenance telephone number is configured; when the modem receives a call, it hangs up and dials the configured number.

The manager explained that historically, this unit's SCADA systems were not in the IT perimeter. Also, **the applications have specific needs (e.g. specific software, obsolete OS) that are not compatible with IT standards.** While PCs are standard equipment in typical IT environments, they do not support industrial environments and they are equipped with antivirus software that conflicts with the applications. Furthermore, administrator rights are necessary to use these applications.

The coordinator explained that he understood the issues of application incompatibility with the "hardened" configurations provided by the IT department. However, these work stations represent a vulnerability that could spread to all the SCADA systems. Antivirus software or OS updates may not be compatible with these older applications, but there are certainly countermeasures that can be taken. These solutions must be studied in collaboration with the IT department and the integrator. At minimum, event logs must be implemented, the machines must be monitored and a framework must be defined for cooperation with the IT department in order to benefit from their expertise without detriment to the company operational activities.

The coordinator asked how hazardous materials are distributed and how the entire system is operated.

Distribution is fully automatic, in response to the needs of the production lines. The plant, which requires high availability, is operated by three high availability PLCs.

The coordinator asked whether there was a link with the storage unit. The manager replied that the majority of servos are independent. However, there is still a link, since, in case of leakage, the distribution unit shuts down and sends a stop command to the storage unit, closing the safety valves. Leak detection signals (on off logic) are wired directly to the valves. A bus or Wi Fi connection is in the plans for expansion of the storage unit. This would provide more flexibility for operating the system.

The PLCs communicate with the SCADA system via an Ethernet network that appears to be the same one used by the other PLCs on the site.

The coordinator asked how maintenance of this unit was managed. The unit manager replied that maintenance is provided by the company that placed the systems in service, the same as for the SCADA systems. Because the system is robust, maintenance interventions are relatively rare and are limited to equipment failures. Sometimes the Ethernet cards are at fault. If they become unavailable (e.g. due to frame overflow), the PLC must be restarted to reinitialise them. The coordinator asked whether these overflows were identified. The manager replied no, because users do not necessarily have sufficient network skills to diagnose the problem.

The coordinator explained that analysis and monitoring tools must be configured on the network. They can be simple to deploy and fully transparent for the plant. They enable event detection, prevent incidents or simply provide data to analyse behaviours that currently have an impact on the process.

A diagnostic channel independent of the SCADA system is needed to detect incidents, e.g. if the SCADA system is compromised. The widespread use of Syslog and SNMP (v3) protocols in industrial devices allows this second channel to be implemented to detect "system" failures of the components and applications.

The coordinator asked how interventions are carried out. The manager replied that in general, a technician from the company goes to the location in question, connects his console to the PLC or network, makes a diagnosis and corrects the problem. The coordinator was concerned whether this connection also provides access to the site's other PLCs and if access to PLCs is protected (e.g. by passwords). The manager did not know; he said he would ask the integrator.

The integrator indicated that no password was configured for the PLCs. This simplifies interventions. In addition, these PLCs, like the SCADA system, are connected to the same Ethernet network as the other PLCs on the site.

The coordinator concluded that, during very specific and infrequent interventions, external users connect to the SCADA network with their own tools and have access to every PLC on the site, since no password is configured. This constitutes a major vulnerability. These interventions must be governed by procedures, access to the PLCs must be limited and protected by passwords, and most importantly, the maintenance consoles must be controlled and made available to users when necessary.

Physical access to PLCs, fieldbuses, SCADA and other devices must be limited to the full extent possible.

4 CONCLUSIONS

4.1 Initial analysis

After his visit to the plants, the coordinator made a rough and rapid assessment:

- both users and management had fully cooperated with him. However, the coordinator felt that his presence may have sometimes been stressful as he pointed out vulnerabilities;
- systems are heterogeneous and not managed in the same way;
- control over systems is relatively weak. Many issues solely concerned the integrators, or even those who initially placed the plant in service, several decades ago;
- to address their needs which seem legitimate users are using insecure approaches that create vulnerabilities;
- the various personnel he interviewed were motivated, but there is high staff *turnover* and numerous interim employees;
- it is fairly easy for anyone to connect to the SCADA system (open sessions on work stations with high access levels);
- physical protection is incomplete;
- there is no notion of segregation. All components seem to be on the same network, regardless of their level of criticality and their functionality. The PLC halt during penetration testing confirms the need to implement a solution as quickly as possible to filter between the networks and limit access;
- it is indispensable to create a process to monitor vulnerabilities (e.g. monitoring information from CERTs and from the manufacturer's site, bringing in subcontractors specialised in this domain);
- there is a need for a procedure (e.g. to be posted in the control room) to handle incidents and an alert hierarchy to be followed;
- it also appears useful to prominently display the 10 "healthy network" rules for ICSs (see Appendix D);
- awareness training tailored to ICSs is needed.

4.2 Overall reflections

Overall, the coordinator tried to understand the issues faced by users and demonstrate a pedagogic approach. However, this is not enough. There are significant business constraints. He must show users how cybersecurity provides solutions and reassure them again: the measures will be undertaken as a joint project and will not impair business objectives.

Although certain actions immediately spring to mind and seem simple to implement, such as the networks segregation or defining a policy for managing removable media, the constraints of certain shops and the obsolescence of certain equipment mean that a more comprehensive analysis is required. That will involve several areas of expertise and require him to restructure the approach he had envisioned into three steps.

In particular, the need to upgrade the SCADA systems in shops A and B, as well as the automation of the hazardous material storage and distribution unit, seem more complex. The hazardous material unit involves issues regarding the safety of assets and individuals. A coordinated approach with safety experts is necessary.

Moreover, the subject of backups and documentation has not been addressed. During the debriefing that he will organise with the various managers concerned, he expects to cover this, as well as other transversal themes.

4.3 Mapping

The first step of his approach remained unchanged. He established a mapping of the industrial systems from different viewpoints that will help identify weaknesses and areas for improvement. Pre existing FMECA studies have already clearly defined levels of criticality for the plant, allowing an initial mapping of the systems to be carried out rapidly.

4.3.1 Macroscopic view of criticalities

Data streams with dotted lines represent requested upgrades.

Systems located in the "High Availability" section have a strong impact on production if there is a shutdown. The assembly shop he visited is in this section.

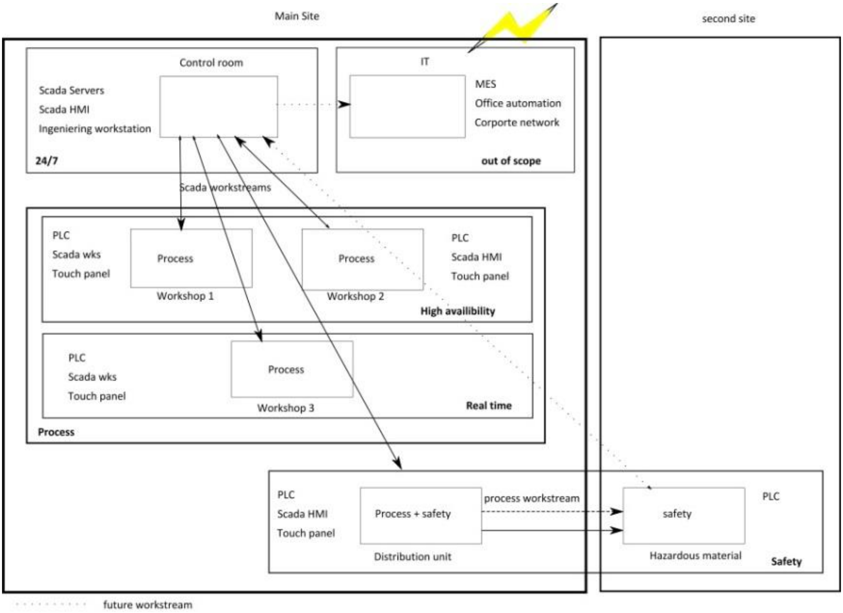


Fig. 1 Macroscopic mapping of plants based on criticality

The hazardous material distribution plant located in the "safety" zone also strongly affects production in case of a shutdown. It must ensure high availability, but priority is given to safety functions.

The control room is considered strategic because it makes it possible to view the status of plants and ensure that they are all functioning correctly. A high level of availability is required, even if it is possible to stop the SCADA for a few minutes without a significant impact on the site's proper operation. The procedure in case of total loss of SCADA functions in the control room for more than 15 minutes (as happened in the past due to a network outage) calls for evacuation of the production building upon the decision of the safety manager.

4.3.2 Physical view of network topology

A deeper analysis of the network topology is needed to understand how various devices are connected. Currently, the situation is not very clear. In collaboration with IT department personnel accustomed to this type of exercise, the coordinator obtained the following topology.

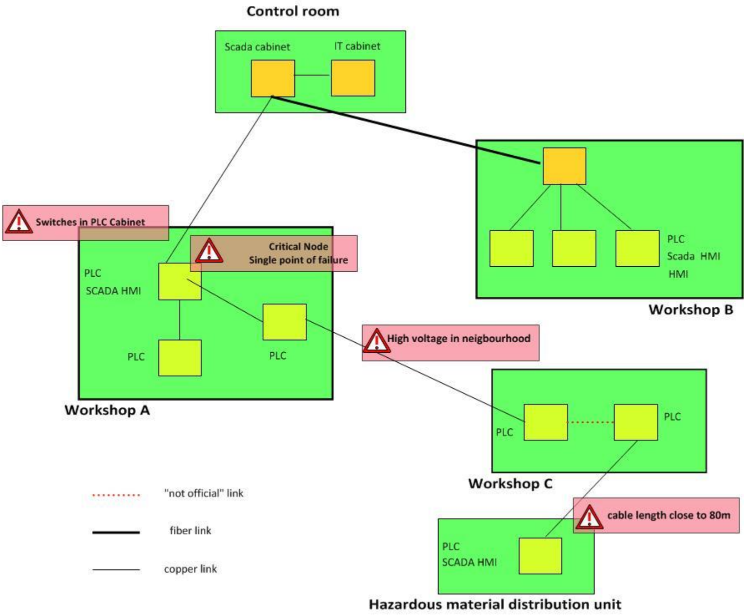


Fig. 2 Physical view of the ICS network

The network topology is inconsistent and seems to lack robustness. It has developed along with the shops, but has not been subject to overall planning.

Some devices are connected to switches placed in network wiring closets while others are connected to hubs placed directly in electrical cabinets.

Failure of a hub in workshop A means the loss of SCADA in shop B and the hazardous material distribution unit.

Continuing to work together with IT teams and shop foremen, he established the logical topology of the plants.

3.3 Logical view of ICS

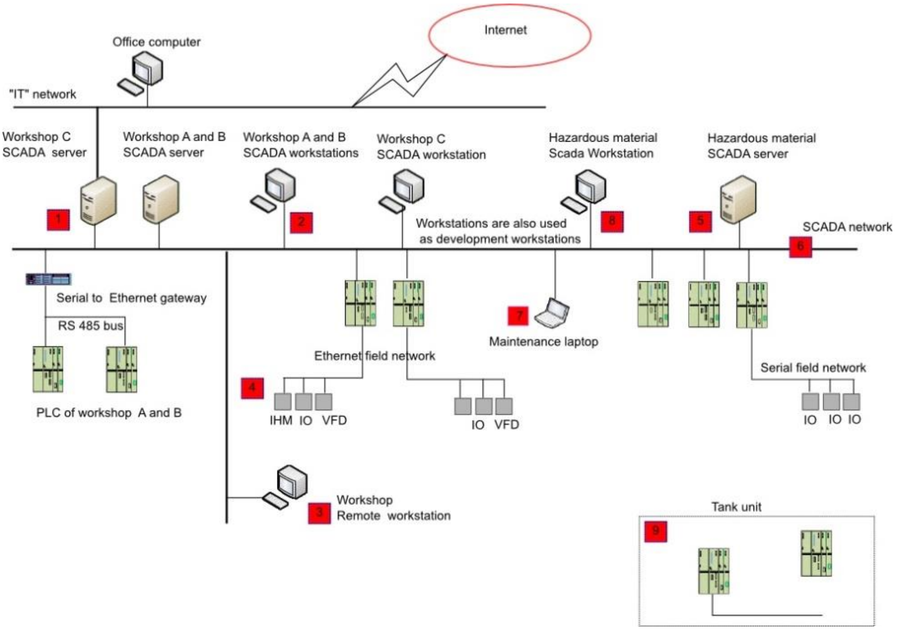


Fig. 3 Logical view of the ICS network

In this diagram, the coordinator indicates the vulnerabilities he identified:

1. potential compromise from the office network, which can extend to the industrial network, and vice versa;
2. obsolete systems are not maintained, configuration and development software installed on work stations allows applications to be modified;
3. generic login, work station easily accessible;
4. "standard" machines and systems not updated, inadequate traceability of actions performed;
5. server in technical zones, not updated, inadequate control over the configuration, not consistent with other servers;
6. all devices are connected to the same network without any distinction for level of criticality. A network incident makes the entire control room unavailable and can impact PLCs;
7. console belonging to a subcontractor, no control over its configuration, risk of introducing viruses;

8. access to PLC programme and configuration not authenticated by password;
9. no physical access control, inadequate control of configurations.

This mapping allows principal vulnerabilities to be quickly located and explained to personnel. The coordinator will use it as a teaching tool to explain risks to the managers.

4.4 Analysis of new requirements

4.4.1 Wi Fi connection

The expansion project includes the implementation of a Wi Fi connection between the PLCs handling the storage unit and the distribution unit. Installing optical fibre would be complex and expensive due to the physical configuration of the site.

However, Wi Fi is not the recommended solution for sensitive systems. Risks for Wi Fi are higher than those for "wired" connections, both in terms of availability (ease of causing interference to radio signals) and integrity of upstream plant (ease of physical access).

The Wi Fi coverage area is often underestimated. Current technologies can capture Wi Fi signals at significant distances (hundreds of metres or even several kilometres depending on configurations). Wi Fi is sometimes used when it would be complex (or impossible) to use optical fibre or other approaches. **It is important to analyse the risks presented by this type of solution and to implement measures to limit them.**

Studies conducted with the safety managers show that to ensure the protection of assets and individuals, the loss of the data connection between the PLCs of the storage unit and the distribution unit must cause the safety valves at the storage unit to be closed (fail safe principle).

Cybersecurity risks identified for this connection are the disruption of the connection (hardware failure or radio interference) and penetration of systems by exploiting a vulnerability in devices.

Disruption the connection would not impact safety functions.

Configuring a firewall behind the access point would be a positive step, but the PLCs use a layer 2 protocol (Ethernet frames) and for maintenance reasons, MAC address filtering is not desirable. Protection is principally provided by the encryption in the WPA2 protocol and the configuration of clients and Wi Fi access points. If the protocol is not properly implemented, it could introduce numerous vulnerabilities.

It is essential to segregate the hazardous material distribution plant with respect to other

plants in order to avoid any risk that its compromise via Wi Fi could be extended to the entire site.

Analysis of devices' data streams and connections and monitoring of potential vulnerabilities for Wi Fi devices are even more imperative, since the only protection is based on the WPA2 protocol.

An application firewall and installation of a Radius server are solutions under consideration to raise the security level.

4.4.2 Remote maintenance

Although the new topology allows it, remote maintenance on safety PLCs via Web service access to the CPU[4] is out of the question.

Previous FMECA analyses and lessons learned show that, in most cases, failures of PLC plants are due to the hardware. These failures require physical intervention on the system to return it to service. There are few failures related to software bugs; after the intervention, the system must be re qualified. For critical systems, even minor modifications are subject to a validation process that cannot be conducted remotely.

This is why the acceptance process for systems requires comprehensive on site testing, sometimes very intensive, to ensure that no anomalies remain.

The security study concluded that remote maintenance on critical plants is not acceptable given the risks (e.g. the difficulty of establishing secure plants channels to the process plants, the difficulty of guaranteeing the identity of the individual logging in, the complexity of defining the limits of responsibility in case of incident). On the other hand, a remote diagnosis solution could be implemented.

The coordinator had explained that it was necessary to deploy analytical and diagnostic tools. These will allow SCADA and PLC events to be centralised at a work station in the control room. This information can be accessed via a DMZ by remote maintenance teams that can qualify the incident and, if an intervention is necessary, organise it more efficiently.

4.4.3 SCADA and MES interconnection

Data exchange with the MES system (Manufacturing Execution System) can use protocols such

[4] CPU: Central Processing Unit. This is the part of the PLC containing the processor and the programme being executed.

as OPC or SQL. The SCADA application sends data to the MES system or vice versa. It is also possible to use a repository server located in a DMZ between the ICS and MES networks; this would be a more secure solution.

The IT teams prefer the SQL solution, although it is no more secure than the OPC solution. However, the IT teams are familiar with the associated issues (e.g. code injection, privilege elevation) and already know the countermeasures to apply, while they have not mastered the OPC solution.

The coordinator explains that, in general, the more the protocols are standardised and used by a majority of people, the easier it is to master them and find personnel with pertinent skills. This also leads to more rapid identification of vulnerabilities and availability of updates.

5 THE ACTION PLAN

5.1 Improving the architecture

Still in collaboration with the IT department, he worked on an improved topology that would reduce vulnerabilities by partitioning the network, while integrating new needs with an view to the future:

- allowing desktop PCs to access SCADA HMIs;
- linking SCADA databases and corporate MES applications;
- sending data from the storage zone to the control room;
- deploying a data connection between the hazardous material storage zone and the hazardous material distribution zone to benefit future plants;
- potentially implementing remote maintenance.

These points will also be studied with plant safety managers. Also, improvements in physical protection of devices should be made.

5.1.1 Architectural proposal

The work carried out with IT teams and various users led to the architectural proposal described below. The urbanisation and segregation model for the network and systems is divided into zones and Sections organised according to criticalities and functions.

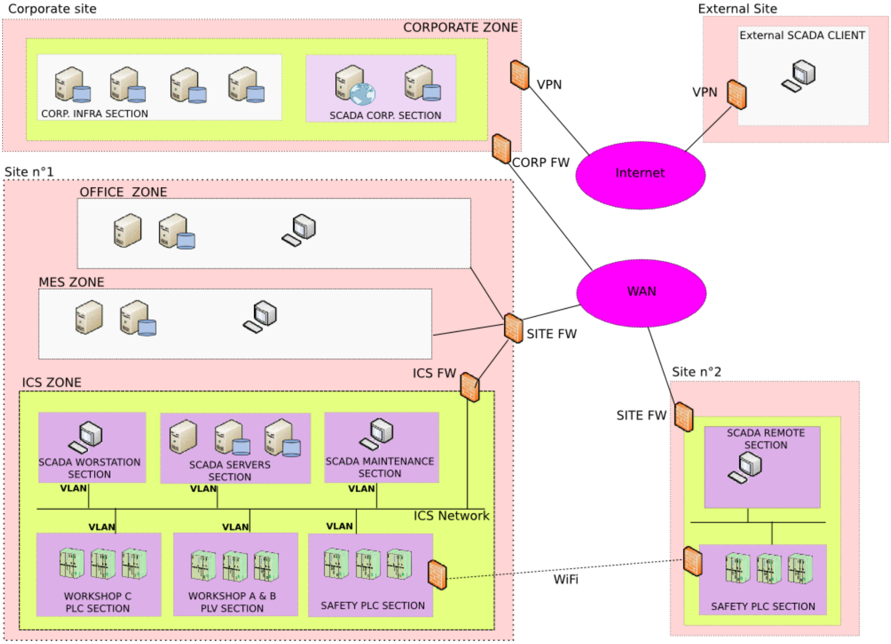


Fig. 4 Proposed architecture for ICS networks and interconnections

This architecture will facilitate integration of future systems and will permit implementation of the policy defined below.

The various networks in the industrial zone (ICS) can be implemented with LANs or VLANs. To ensure high availability, firewalls can be deployed redundantly.

It is strongly recommended to create an "admin network" VLAN containing all ICS network devices (for simplicity, this VLAN is not shown in the diagram).

The rules presented below set down basic principles and should be made more specific in view of each plant needs.

Filtering example:

SCADA STATION SECTIONS: no incoming data

- RDP and Web outgoing data to SCADA SERVERS SECTIONS;
- WSUS outgoing data to INFRA CORP SECTIONS;
- LDAP, Kerberos, other infra services outgoing data to Corp zone based on application requirements.

REMOTE WORKSTATION SECTION: no incoming data

- Web outgoing data to SCADA CORP SECTION;
- WSUS outgoing data to INFRA CORP SECTION;
- LDAP, Kerberos, other infra services outgoing data to INFRA CORP SECTION based on application requirements.

SCADA SERVERS SECTION:

- RDP and Web incoming data from SCADA STATION SECTION;
- data stream allowing access to SCADA from office work stations (see Appendix B): Attention, the risks related to this rule must be clearly identified and accepted with knowledge of the facts;
- PLC communication protocol outgoing data to all PLC SECTION;
- SQL outgoing data to SCADA Corp SECTION;
- Syslog and SNMP outgoing data to SCADA Corp SECTION;
- SQL or OPC outgoing data to MES ZONE.

Under current versions of the OPC protocol, data streams can be complex to manage. They rely on DCOM components that use dynamically allocated ports in a given range. The data streams can be bidirectional. In this case, the risks stemming from this rule must be clearly identified and accepted with knowledge of the facts.

PLC ISLANDS:

- PLC communication protocol incoming data from SCADA SERVERS SECTION;
- Syslog and SNMP outgoing data to SCADA Corp SECTION and SCADA SERVERS SECTION;
- NTP outgoing data (to synchronise clocks) to SCADA SERVERS SECTION.

MAINTENANCE (or ADMININISTRATION) SECTION: no incoming data

- LDAP, Kerberos, WSUS and other infra services outgoing data to INFRA CORP SECTION;
- PLC programmes outgoing data to all PLC SECTION;
- SCADA programmes outgoing data to SCADA SERVERS SECTION;
- administration data (HTTPS, SNMP, SSH) outgoing to ADMIN NETWORK VLAN;
- data for administration of servers and applications (e.g. RDP) outgoing to SCADA SERVERS SECTION.

SCADA CORP SECTION:

- Syslog and SNMP incoming data from ICS ZONE;
- HTTPS incoming data from External SITE.

Most SCADA applications run under a Microsoft operating system. Group Policy Objects (GPO) can be used to deploy and manage some system configurations; Microsoft tools can be used to deploy updates. Centralised management will be more effective than the current approach.

There are not a sufficient number of operator work stations and servers to create and manage a specific SCADA domain. However, if they are grouped together with the machines in the MES zone, it could be advantageous to create a specific domain (e.g. Production) independent of the office domain[5]. **This assumes that the MES and SCADA zones have the same level of confidence.** If special skills are needed to manage a domain, it should be handled by the IT department.

This pooling will facilitate administration, in particular enabling more effective user account management. This may help resolve certain issues (e.g. generic logins).

5.1.2 Proposal for a new physical network topology

Each shop and unit will be connected to the SCADA network via a wiring closet connected in a loop to improve availability. The wiring closets will be physically locked and a dry contact will send an alarm to the SCADA system if one is opened.

Devices (PLC, OP, SCADA work stations) will be connected with copper cables to the switches in the wiring closets.

Several VLANs will be created to implement the segregation proposed above. Routing between VLANs will be complemented by filtering.

Interconnection with the office network will also pass through a firewall.

This topology will facilitate the addition of future plants.

[5] Domain management can be complex and can be a source of significant vulnerabilities if not properly mastered. Appendix C provides further explanations on domain architecture.

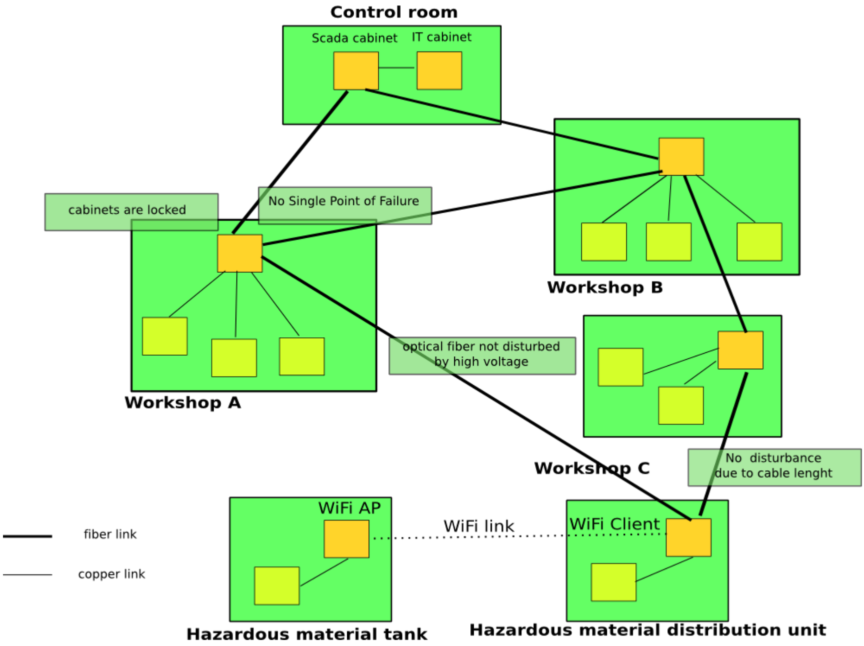


Fig. 5 Proposal for a new physical topology for the ICS network

5.2 Adapting the IT security policy

In combination with technical measures, a consequential project concerning methodology and definition of responsibilities for the operation and maintenance of the SCADA systems must be undertaken (e.g. operating procedures, intervention procedures for subcontractors). There is also the question of the level of involvement of IT teams who have useful skills and can provide effective support to users. These teams could also assist with the deployment of the IT security policy, giving proper consideration to the business specific adaptations required.

The IT security policy should be adapted, in particular, by:

- defining a policy for removable media management;
- defining a policy for password management, addressing generic accounts (with restrictions), PLCs, subcontractors, etc.;
- implementing management and especially traceability of changes in applications and documentation;
- defining a monitoring policy (who? how? what?);
- defining a policy for event log analysis;
- defining a process for manage incidents and an alert hierarchy;

- defining a policy for antiviral protection. This is more complex due to the sensitive nature of applications. We can anticipate undesirable interactions between the antivirus software and applications (often from earlier generations) that have not been designed to coexist with it. The coordinator prefers to work on hardening the production systems' configurations and limiting the deployment of antivirus software to engineering stations and programming consoles;
- defining a data backup policy and associated restoration procedures. This will be needed in order to draft a DRP (Disaster Recovery Plan).

5.3 Improving applications

Finally, improvements are planned for SCADA applications. Some are simple, such as:

- implementing automatic disconnection;
- improving traceability for the use of degraded modes allowed by the touch screens in production shops.
- However, merging the SCADA applications for production units A and B with those of unit C appears more complex. The PLCs are from an earlier generation and the communication protocol is proprietary.

The manufacturer of these PLCs has recently introduced protocol converters incorporating an OPC server. This solution would enable the SCADA application of unit C to interact with PLCs in units A and B without migrating devices (OPC UA) to the current generation.

This protocol is known to be vulnerable, although improvements incorporating security mechanisms are ongoing. The implementation of a filtering policy and hardening of configurations are possible temporary measures pending these improvements.

5.4 Audits and penetration tests

The coordinator proposes to call upon an external provider to audit the plant and perform penetration tests once all improvements have been implemented. To avoid plants being affected again during penetration testing, the audit protocol will be validated in advance.

A FEW MONTHS LATER...

The coordinator considers the overall impact of the actions to be positive.

Users access SCADA data from their office work stations in a more secure manner, simplifying numerous tasks. Handling shops A, B and C from a single SCADA application gives operators and shop foremen better visibility for the plants. The OPC protocol in use has vulnerabilities, but its risks have been significantly reduced by hardening machines and segregating networks. The data sent from the storage unit has greatly simplified the work of maintenance and operations personnel. Malfunctions are detected more quickly.

The "process" networks are limited to data streams between PLCs and remote I/O. The implementation of filtering between these networks provides useful diagnostic information and enabled detection of many device configuration problems (e.g. transmission of unwanted *broadcast* and *multicast* frames, IP address conflicts). Downtime has been reduced on the new production line. The new penetration tests were negative. Scans performed on the office network and then extended to the SCADA network had no impact on PLC networks. Attempts to penetrate the office network from the SCADA network failed.

As site management pointed out, the most important consequence is surely that personnel now understand the overall importance of cybersecurity: in their everyday life, but especially in the industrial context. They understand that it is a tool to promote availability and dependability, an indispensable accompaniment to new technologies.

The company "re appropriated" its systems. Thanks to the studies carried out for this project, users have a better understanding of the plants and the procedures to follow. Together with remote diagnostics, this has reduced maintenance costs.

IT security policy is a continuous process. There are still many areas for possible improvement. Other projects are planned:

- analysing statistical data (e.g. sensors, actuators and alarms) to detect erratic behaviour;
- further developing the "monitoring system" functions of the SCADA and PLCs;
- deploying a centralised solution for updating PLCs, touch screens and other automation components;
- creating a plan to manage obsolescence, in order to progressively replace the oldest and most vulnerable devices and software;
- regularly planning non regression tests;
- creating an audit plan based on attack scenarios and negligence scenarios;
- planning exercises to test the alert hierarchy and the procedures for handling incidents;
- studying virtualisation solutions for server applications, which, combined with thin

clients, can improve availability and quickly restore configurations in case of a disaster. These solutions also facilitate the deployment of system updates.

All these projects will be led by the coordinator, who will be the cybersecurity contact for industrial users. He is responsible for ensuring compliance with the rules that have been set down and the consistency of actions with the IT department.

APPENDIX A: ABBREVIATIONS AND ACRONYMS

ADSL	Asymmetric Digital Subscriber Line
FMECA	Failure Modes, Effects and Criticality Analysis
PLC	Programmable Logic Controller
CPU	Central Processing Unit
DoS	Denial of Service
DRP	Disaster Recovery Plan
EIA	Electrical Industry Association
ERP	Enterprise Resource Planning
RMAS	Reliability, Maintainability, Availability and Security
FMEA	Failure Mode and Effects Analysis
FAT	Factory Acceptance Test
GSM	Global System for Mobile
CAPM	Computer Aided Production Management
CTM	Centralised Technical Management
BMS	Building Management System
HAZOP	HAZard & OPerability method
ICS	Industrial Control System
MES	Manufacturing Execution System
MTBF	Mean Time between Failure
OPC	OLE for Process Control
OPC UA	OPC Unified Architecture
OLE	Object Linked & Embedded

P&ID	Process & Instrumentation Diagram
PID	Proportional Integral Derivative
PLC	Programmable Logic Controller
STN	Switched Telephone Network
RDP	Remote Desktop Protocol
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition
SPC	Statistical Process Control
DCCS	Digital Command Control System
SNMP	Simple Network Management Protocol
SIL	Safety Integrity Level
SOAP	Service Object Access Protocol
SQL	Structured Query Language
SIS	Safety Instrumented System
VFD	Variable Frequency Drive
WSUS	Windows Server Update Services

APPENDIX B: RESTRICTING FUNCTIONALITIES RELATED TO THE USE OF REMOVABLE MEDIA

The use of CD ROMs, DVDs and USB mass storage devices (e.g. external hard drive, USB drive, PDA, smartphone, digital camera, MP3 player) is now widespread. These media, easily transportable and difficult to control, can be used to illegitimately collect data from an information system; they are an important vector for malware.

While CD and DVD drives can be removed from systems (like floppy disk drives before them), it is more difficult to do without USB connectors, employed today by legitimate peripherals such as keyboards and mice.

However, logical measures can be implemented on the Windows operating system in order to address the threat of malware introduction or data leakage.

Blocking the detection of USB storage devices

If no USB storage device has been previously installed on the computer (carry out the following operation on the %SystemRoot%\Inf folder), simply assign the user <<~Deny~>> permissions for the following files:

%systemroot%\Inf\Usbstor.pnf

%systemroot%\Inf\Usbstor.inf

Disabling the device driver for USB storage devices

To prevent the use of USB drives, set the Start value in the following registry key to 4 (this will take effect after restarting the work station):

HKLM\SYSTEM\CurrentControlSet\Services\UsbStor

Keyboards, mice and other USB peripherals will still work. For more information, refer to the Microsoft website.

Blocking writing to USB devices

Starting with Windows XP SP2, you can connect USB devices in read only mode. This requires creating or modifying the WriteProtect value (type DWORD), by assigning it the value 1 in the key:

HKLM\System\CurrentControlSet\Control\StorageDevicePolicies

Disabling Autorun

Autorun and Autoplay features can be completely disabled for all types of readers by changing the group policies. The parameter is located in Computer Configuration, Administrative Templates, System, and is named << Turn off Autoplay >>. It must be set to <<~Enabled~>>, specifying <<~All drives~>>.

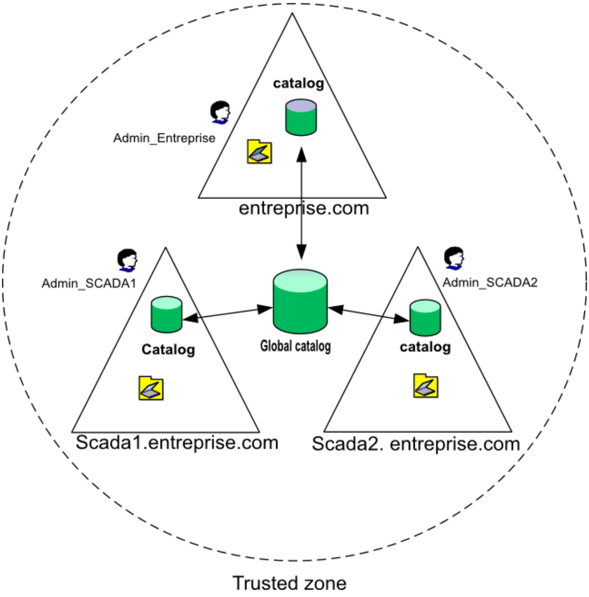
Windows security updates must be also installed to correct vulnerabilities regarding USB media. The software restriction policies can also be configured to prevent the execution of programs from media other than hard drives.

APPENDIX C: MICROSOFT WINDOWS DOMAINS

Several domain architectures are possible, each with its own advantages and disadvantages. It is important to choose the architecture that addresses security and functional requirements.

The diagrams below show the main characteristics of solutions in common use.

Domains and subdomains (this architecture is strongly discouraged):



Relationships between all domains are implicit.

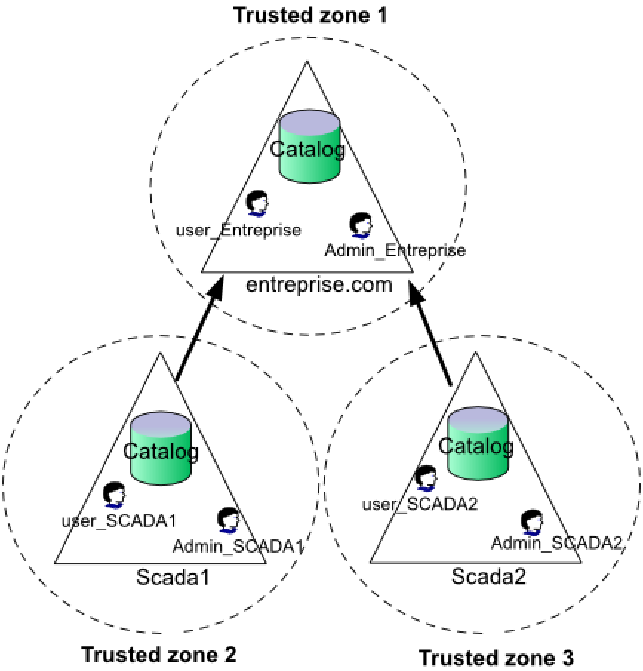
There is a global catalog for all domains, plus a catalog per domain with replication mechanisms for certain objects.

The enterprise.com domain policies implicitly apply to the SCADA1.enterprise.com and SCADA2.enterprise.com domains.

The user of one domain can access the other domains when they are authenticated on one of the domains.

The compromise of one domain compromises all the others. Example: a takeover of account Admin_SCADA1 would allow execution of administrative tasks in other domains.

Independent domains (preferred architecture):



Relationships between all domains are implicit.

There is an independent global catalog per domain.

External trust relationship. They can be unidirectional or bidirectional.

The enterprise.com domain policies do not apply to domains SCADA1 and SCADA2.

The user of a domain can only access other domains if they are explicitly granted rights for the other domains.

If a domain is compromised, the compromise is limited to that domain.

Warning: if the admin_enterprise account is declared a member of the administrative groups in the SCADA domains, a compromise of that account means that the SCADA domains are compromised.

APPENDIX D : IT AND SCADA INTERCONNECTIONS

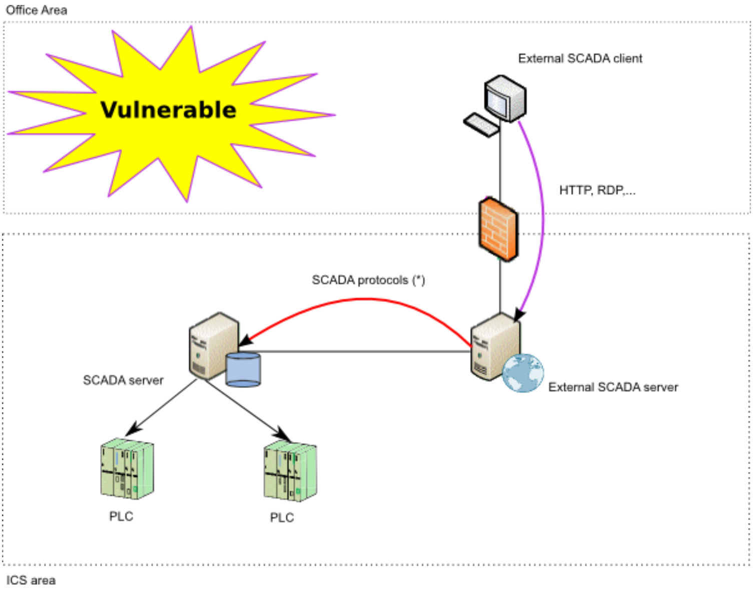


Fig . 6 Access to SCADA data by a simple filtering solution:

NOT SECURED (highly not recommanded)

Advantages:

- Possible with the commercial SCADA software.

Disadvantages:

- It allows incoming connections in the ICS area;
- A vulnerability in the firewall permits access to the ICS zone;
- A vulnerability in the "Internal" server can conduct to the takeover of the entire ICS area.

Warning: taking control of the client (possible if the station is connected to the Internet or uses email and has no hardening or has never be updated) provides legitimate access to the SCADA Web server.

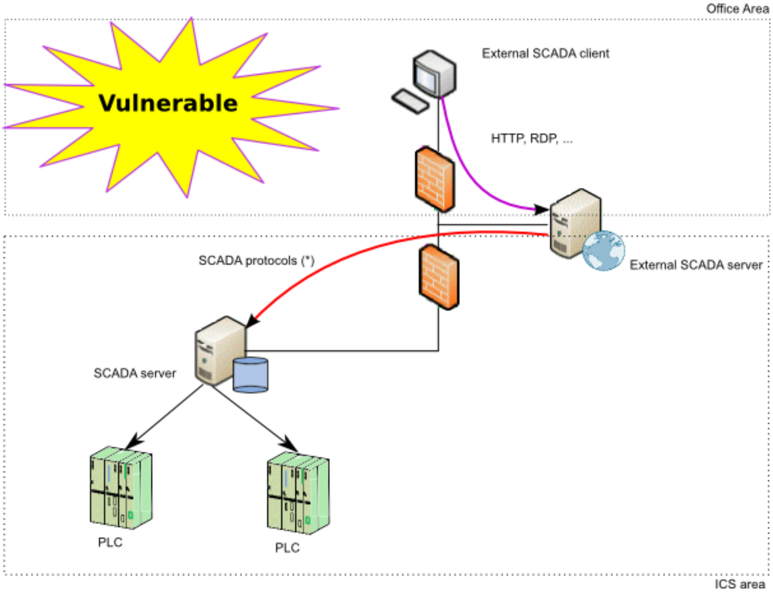


Fig . 7 Access to SCADA data by an intermediate zone:

NOT SECURED (highly not recommended)

Advantages:

- Possible with the commercial SCADA software.

Disadvantages:

- it allows incoming connections in the ICS area ;
- following the specific SCADA protocol (dynamic ports for example), the filtering for the internal firewall can be "soft " ;
- The takeover of the «External» server permits to send command to the PLC. If the SCADA protocole is vulnerable, it allows execution of arbitrary code and provides full access to the ICS area. Protocols used by SCADA were not originally designed to deal with cyber-attacks and may be very vulnerable.

Warning: taking control of the client (possible if the station is connected to the Internet or use email and has no hardening or has never be updated) provides legitimate access to the SCADA Web server.

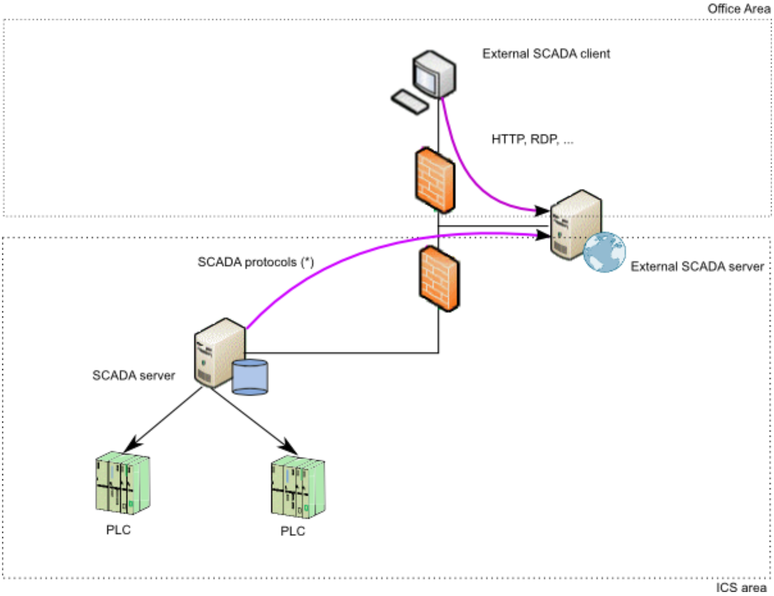


Fig . 8 Access to SCADA data through a DMZ:

SECURED

Advantages:

- No incoming connections to the ICS area which complicates malicious access to this area .

Disadvantages:

- It needs dedicated development to realize this architecture.
- Possible to take the control of ICS network if the protocol used to " replicate " data to this "external" server has some vulnerabilities.

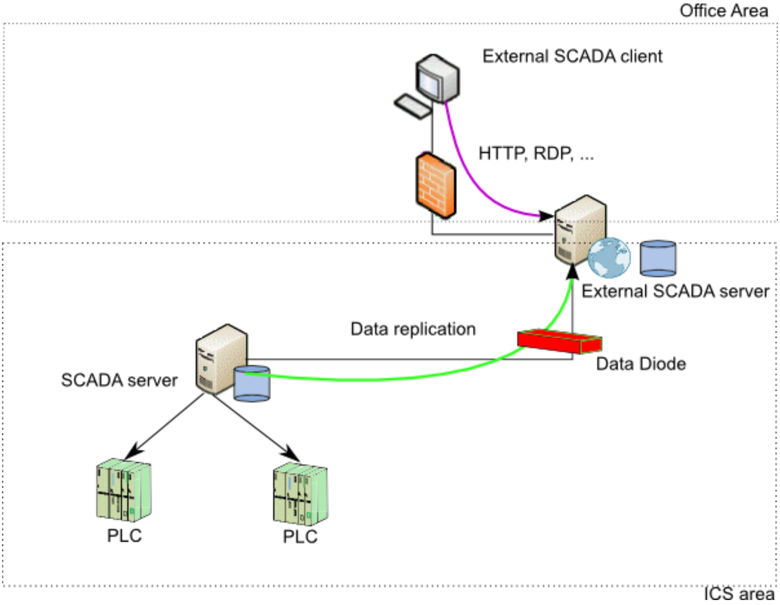


Fig . 9 Access to SCADA through a data diode:

VERY SECURED (preferred solution)

Advantages:

- No data coming from the area outside can enter the ICS zone.

Disadvantages:

- Specific developments may be required.

APPENDIX E: 10 RULES FOR THE USE OF SCADA

Example of 10 rules for using SCADA to display in the control room and in different areas of the site:

1. Lock or log off when you leave a station or a touch screen
2. Do not share the username and password to his colleagues
3. Do not connect a USB drive , external hard drives , mobile phones or other devices on the ICS
4. Use a specific station in order to exchange data with external systems
5. Do not use the programming and maintenance console outside of the site and do not connect it on other networks as SCADA. Store it in the plant (control room for instance)
6. Do not keep data on stations and programming devices. Use Shared storage space provided for this purpose
7. Close and lock PLC and "low voltage" cabinet and wiring closets
8. Do not restart a failed equipment (SCADA Station , OP , PLC ...) without the diagnostic of a specialist
9. Do not connect unsafe equipments on the SCADA network;
10. Report any abnormal situation to the control room center.

If in doubt, contact your manager!

This guide was produced by the Agence nationale de la sécurité des systèmes d'information (ANSSI)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION • ANSSI •

with the help of ministries

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ministère
de l'Écologie,
du Développement
durable,
des Transports
et du Logement

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR,
DE L'OUTRE-MER,
DES COLLECTIVITES
TERRITORIALES
ET DE L'IMMIGRATION

and companies

AREVA

EDF

EADS

GDF SUEZ
ÊTRE UTILE AUX HOMMES

suez environnement
Lyonnaise des Eaux

MICHELIN
Une meilleure façon d'avancer

NATIXIS

saur

TOTAL

VEOLIA
ENVIRONNEMENT

This document is a courtesy translation of the guide Cybersécurité des systèmes industriels: Maitriser la SSI pour les systèmes industriels. In case of divergence, the French version prevails.

ANSSI publications are available on its website: http://www.ssi.gouv.fr/publications/

Comments on this guide may be sent to systemes_industriels@ssi.gouv.fr

About ANSSI

The French Network and Security Agency (ANSSI / *Agence nationale de la sécurité des systèmes d'information*) was created 7 July 2009 as an agency with national jurisdiction ("*service à compétence nationale*").
By Decree No. 2009 834 of 7 July 2009 as amended by Decree No. 2011 170 of 11 February 2011, the agency has responsibility at national level concerning the defence and security of information systems. It is attached to the Secretariat General for National Defence and Security (*Secrétaire général de la défense et de la sécurité nationale*) under the authority of the Prime Minister. To learn more about ANSSI and its activities, please visit www.ssi.gouv.fr.

Version 1.0 - June 2012

Agence nationale de la sécurité des systèmes d'information

ANSSI 51 boulevard de la Tour Maubourg 75700 PARIS 07 SP FRANCE

Websites: www.ssi.gouv.fr and www.securite informatique.gouv.fr

E mail: communication [at] ssi.gouv.fr