Detailed Measures

Cybersecurity for Industrial Control Systems

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Table of Contents

Section 1

Introduction

1.1 Context

This document is based on the findings of the working group on Industrial Control System cybersecurity, directed by the French Network and Information Security Agency, ANSSI[1][2]. Composed of actors in the field of automated industrial process control systems and specialists in IT Security, the group has undertaken to draft a set of measures to improve the cybersecurity of ICS[3].

The document is intended for all actors (e.g. responsible entities, project managers, buyers, manufacturers, integrators, prime contractors) concerned with the design, implementation, operation and maintenance of ICSs.

1.2 Scope

The working group did not focus on a specific business sector; the contents of this document are intended to apply to all sectors. Some sectors have specific characteristics that may not have been detailed or considered in this document. **Therefore, in some cases, a sector-specific version of this document may be required to clarify the application and to take specific constraints into account.**

All of the measures presented have been designed for new ICSs. It is quite possible that these measures cannot be directly applied to existing ICSs; therefore, an exhaustive impact evaluation should be carried out before any implementation.

It is also possible that situations may arise (e.g. compatibility issues with existing ICSs, business-specific constraints) in which measures cannot be applied without adapting

[1] Agence nationale de la sécurité des systèmes d'information.

[2] The working group is composed of the following companies and organisations: Actemium, Airbus Defence and Space, Arkoon-Netasq, A.R.C Informatique, Atos Worldgrid, Hirschmann, Cassidian Cybersecurity, CEA, CLUSIF, DCNS, DGA Maîtrise de l'information, Euro systems, EXERA, GDF SUEZ, Gimélec, INERIS, Itris Automation Square, Lexsi, Schneider Electric, Siemens, Sogeti, RATP, Solucom, Thales, Total.

[3] Industrial Control Systems.

them. These special cases should be the object of specific studies and the resulting measures should be submitted to the cyberdefence authority for approval.

1.3 Structure of the set of documents

The production of the working group is divided into two documents. This document contains detailed technical and organisational measures to be implemented for ICSs according to the classes defined in the classification guide [14].

It is therefore important to first carefully read the classification guide, which defines the basis for the approach and provides definitions of terms used in the remainder of this document.

1.4 Note to the reader

The cybersecurity measures presented in this document are conventional measures, but they have been adapted for ICSs. This document is not intended to be a training course in cybersecurity for ICSs. It is therefore assumed that readers have basic knowledge of information and communication technology, as well as cybersecurity, or that they can obtain support from people with these skills. The proper application of certain measures will certainly require teamwork between "computer engineers" and "automation engineers."

Note

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.

Important

This document is a courtesy translation of the guide *Cybersécurité des systèmes industriels : Mesures détaillées*. In case of divergence, the French version prevails.

Section 2

Cybersecurity considerations for industrial control systems

This section aims to provide a succinct overview of cybersecurity for ICSs. A list of constraints existing in these systems is provided in section 2.1. These constraints are one of the key differences between ICSs and Information Management Systems (IMS). It is important to identify them in order to propose appropriate measures.

Section 2.2 lists the principal vulnerabilities encountered in these systems. They may arise from the constraints listed in the previous section, though not exclusively. In particular, this section identifies vulnerabilities commonly encountered in IMS.

2.1 List of constraints

Constraints are a set of events that cannot be altered and that can have a serious impact on the security of the concerned ICS. It is very important to consider these constraints when choosing the security measures to be implemented.

Reference	Category	Constraints
C1-MI	Control of ICSs	• Multiple users use ICSs, making it more difficult to control the actions performed. • Multiple isolated sites, particularly in the transport, water distribution and energy distribution sectors, having limited physical protection. • ICS' technical documentation may be limited. This results in a loss of knowledge when personnel leave and makes it more difficult to handle incidents. • Some suppliers carry out remote maintenance from abroad. • For some ICSs, two different operators coexist; this can sometimes give rise to legal problems if the ICS is modified. Additionally, the systems they manage can also pose a threat to one another. • ICSs are often heterogeneous because devices come from multiple suppliers or because they have evolved over time. Heterogeneity may also be imposed for reasons of operational safety.

Reference	Category	Constraints
C2-CO	Contracts	• Suppliers require remote maintenance access to their devices. Otherwise they may not guarantee them. • Modification of systems without the supplier's prior agreement may void the guarantee. • It may be contractually forbidden to modify the existing ICS, even for the implementation of cybersecurity measures. • Some customers require remote access to information (logging) concerning the site's production. For simplicity, data transfer often takes place over a public network such as the Internet.

Reference	Category	Constraints
C3-REG	Regulations	• Certain regulations require operators to export data to a third party. For example, waste collection centres must provide certain data to the Regional Department for Industry, Research and the Environment (DRIRE[1]). • There are extensive traceability requirements in sectors such as food processing and pharmaceuticals. • Note: functional security measures imposed by regulations in a given sector can improve the ICS's security level and provide an acceptable level of residual risk. • Safety regulations may limit the possibility of modifying ICSs. Modifying an ICS may even result in loss of approval.
C4-GCH	Change Management	• There is no test environment for verifying ICS non-regression. • Interventions on an ICS can only occur during maintenance periods. • Suppliers offer operators meagre support to assess the impact of security measures on ICS.

[1] Direction Régionale de l'Industrie, de la Recherche et de l'Environnement

Reference	Category	Constraints
C5-OPE	Operations	• Certain environments require high responsivenss from operators, in particular when incidents occur. Security measures should not inhibit this responsiveness. • Operators often share devices, which can have a significant impact on traceability (e.g. use of generic accounts). • Operators often need to view the ICS's status in real time and respond quickly. Therefore, they cannot lock the workstations they are using.
C6-CECO	Economic Constraints	• Updates to existing systems and changes to installations entail significant costs for the customer.
C7-GOUV	Security Governance	• While IT management is assigned the task of securing ICSs, it has no hierarchical link with the teams that operate them. This complicates or slows the implementation of cybersecurity measures. • When this task is assigned to the management of a business unit, cybersecurity often has a low priority and the responsibility for managing the interfaces between ICSs and management systems is unclear. • Few personnel are responsible for industrial IT at an industrial site.

Reference	Category	Constraints
C8-CTECH	Technical constraints	• Devices are deployed for a 15 to 20 year lifecycle. Obsolescence limits the possibilities for updating them or integrating security functions. • Some devices (such as PLCs) and protocols have limited, or even non-existent, security functions. • Suppliers offer few technical solutions for centralised management of security functions. For example, it is often impossible to change the password for geographically distributed devices. • On some systems, performance imperatives require zero latency.
C9-CULT	Security Culture	• In environments with a heightened focus on safety, there is often a feeling that this also helps to deal with cybersecurity issues. • Information system security is not covered in professional training, in particular for automation engineers.
C10-MAT	Maturity of technical solutions	• ICS cybersecurity is not fully mastered. • Few suppliers incorporate the notion of a secure development cycle when they develop their products.

2.2 Vulnerabilities

Vulnerabilities in industrial information systems identified by the working group are listed below.

Important

Boxes entitled *Why is this a vulnerability?* are not intended to be exhaustive. They are only intended to illustrate the vulnerability in question.

2.2.1 Plant Control

Security fixes management

Vulnerability management in ICSs is complex. In many cases, updates can only be installed during maintenance phases and their installation may sometimes require re-verifying the ICS's safety.

Priority is given to ICS's integrity and availability and, as the responsible entity rarely has a test platform, it cannot perform non-regression tests on fixes released by suppliers.

For all these reasons, most ICSs do not have procedures or technical mechanisms to install security updates. In particular, automatic update systems are often incompatible, especially with older ICSs.

Why is it a vulnerability?

The presence of known unfixed vulnerabilities in an ICS increases the risk of an intrusion.
Many generic malware exploit such vulnerabilities and the risk of the ICS becoming contaminated is greatly increased when security updates are not installed.
In a targeted attack, the attacker often begins by seeking known unfixed vulnerabilities, in an attempt to penetrate the system. Following proper policies for installation of security updates can eliminate these vulnerabilities, thus significantly complicating the attacker's task.

Note

In 2013, many ICSs were still vulnerable to viruses such as Conficker, which appeared in 2009, despite the fact that the corresponding security update is available.

Lack of monitoring for vulnerabilities and threats

The entities responsible for ICSs rarely implement active monitoring of vulnerabilities for the products and technologies used, even though specialised information sources are now available.

Moreover, they do not monitor trends concerning threats and attack techniques.

Why is it a vulnerability?

The lack of monitoring regarding vulnerabilities and obsolescence of the products and technologies in use prevents rapid response when new issues of this kind occur.
Active monitoring of attack techniques and trends in threats can improve the relevance of risk analysis for ICSs. It also allows better adaptation of protection measures and reduction of the system's exposure time to vulnerabilities.

2.2.2 Inadequate logical access control

Inadequate password management policy

Password management policies are often insufficient or incomplete. This may entail the following problems:

- the use of default passwords;
- changing passwords infrequently (e.g. due to the lack of a tool to update passwords for an installed base of PLCs);
- the use of weak passwords (sometimes due to limitations of the devices or software).

Why is it a vulnerability?

The attacker's first step is often an attempt to compromise a user's account to gain at least partial access. One technique for this is to try to retrieve a password.
Using a default password may thereby provide him direct access to the installation's default accounts, which often have elevated privileges. If the passwords have been changed, the attacker can try dictionary attacks in an attempt to obtain a valid password and thereby gain access to the account in question. This is why we recommend using a strong password and, to the extent possible, changing it regularly.

Lack of account management

An ICS's account management policy is often inadequate or non-existent.

To facilitate operations, due to the rotation of operators or the multitude of sites managed by maintenance teams, generic accounts may be used.

Often, there is no procedure for managing arrivals and departures of employees. In particular, a former employee may retain his account long after his departure.

It is also common for personnel to use privileged accounts. This may be done to simplify user account management or due to the technical limitations of a product. For example, numerous applications only run under "administrator" level accounts.

Why is it a vulnerability?

The use of generic accounts greatly increases the risk of compromise, in particular due to the widespread knowledge of the password. In practice, the passwords used for generic accounts are often too weak, or noted on pieces of paper that are easy to misplace. A disgruntled former employee could make use of his account after his departure if it has not been deleted. Additionally, the lack of an account management policy reduces visibility within the ICS concerned (who has access to which resources?). If problems occur, it is very difficult to trace their origin.

2.2.3 Inadequate control over connection interfaces

On certain ICSs, we regularly observe a lack of management policy for connection interfaces. For example, USB ports are not blocked and unused Ethernet ports are left active.

Why is it a vulnerability?

When interfaces are not controlled, the attack surface is increased. For example, unblocked USB ports favour the introduction of viruses into the system, while enabled Ethernet ports provide the potential for unauthorised connections that could disrupt system operation. This could also be used to subsequently launch an attack from outside the site (e.g. by connecting Wi-Fi devices).

2.2.4 Inadequate control of mapping

The mapping of an ICS is not necessarily controlled. The following can be seen in particular:

- carrying out the installation of network cabling like electrical wiring, with a lack of consideration for documentation constraints;
- insufficient mapping of the ICS, and notably:
  - network topologies,
  - flow matrices,
  - hardware and software inventories;
- operating procedures not catalogued;
- lack of vision concerning coexisting technological generations and their inherent vulnerabilities.

In addition, when a mapping does exist, the procedures and tools that could allow them to be kept up-to-date are not necessarily implemented.

Why is it a vulnerability?

A system mapping is a fundamental component of information system security.
Proper knowledge of an ICS notably helps quickly determine if a vulnerability concerns the system in question, enables a pertinent risk analysis to be made and helps to quickly and efficiently determine the scope of the compromise if an incident occurs.

2.2.5 Inadequate configuration management

Lack of integrity or authenticity checks

Mechanisms to check integrity and authenticity are rarely deployed for firmware, software, PLC programmes and SCADA applications.

Why is it a vulnerability?

The lack of an integrity or authenticity checking mechanism allows an attacker to disseminate a corrupted update.

Lack of back-up

Back-ups are often partial, non-existent or only available from the supplier. When back-ups exist, the proper functioning of post-incident recovery procedures is rarely tested.

Why is it a vulnerability?

If the system is compromised, back-ups can permit a rollback of the ICS's configuration to its prior clean state.

Lack of control over online modification

It is possible to make on-the-fly modifications to PLC programmes and SCADA applications, without authentication or logging mechanisms. This feature is very useful

when systems operate 24/7, but often incorporates very few cybersecurity mechanisms.

Why is it a vulnerability?

The lack of authentication or logging allows an attacker to surreptitiously modify the PLC programme. This modification may not be detectable by the SCADA applications and users.

2.2.6 Use of vulnerable devices

Devices developed for ICSs often incorporate robust safety constraints but rarely include cybersecurity constraints. In particular, the security functions are often limited or even non-existent and the development techniques used rarely consider the presence of an attacker on the system as a threat.

The configuration of the devices or software in the network is rarely hardened. In particular, unused services are often left enabled in the default configuration.

Why is it a vulnerability?

Devices that have been developed without cybersecurity objectives are more likely to contain vulnerabilities that can be exploited by an attacker.
To reduce the attack surface, unused software and services must be disabled or uninstalled. Thus, if a vulnerability is discovered in one of these components, the ICS is not vulnerable.

Note

Installing only essential components favours safety. It reduces the failure risks and makes ICS easier to understand and maintain.

2.2.7 Use of vulnerable protocols

ICSs often use network protocols that do not incorporate any security mechanisms. These can be standard protocols like Telnet, but can also be specific industrial security protocols such as Modbus, Profibus and EtherNet/IP.

Note

EtherNet/IP is the name of an application protocol used by some devices (e.g. industrial PLCs and SCADA software).

Various wireless technologies (Wi-Fi, GSM, Zigbee) may have been adapted for use without carrying out a risk analysis or without deploying appropriate protection measures.

Why is it a vulnerability?

The use of unsecured protocols can allow an attacker to modify frames on the fly or to forge frames that disrupt the operation of the ICS. This can also allow an attacker to obtain login information transmitted over the network in plaintext.
The use of wireless technologies exposes the system to availability issues as it is easy to jam a signal, intentionally or otherwise. Moreover, when a wireless device is not properly secured, an attacker can potentially modify legitimate traffic or inject illegitimate traffic more easily than for a wired infrastructure.

2.2.8 Inadequate physical access control

In many cases, external providers (e.g. maintenance workers, operators) need to physically access industrial installations.

Depending on the activity involved, the ICS or its components may be located in factories, on public streets or in other places that do not allow effective physical access control to be established.

Why is it a vulnerability?

The absence of physical access control allows an attacker to directly access the ICS, thus bypassing all perimeter protection that may have been implemented.

2.2.9 Inadequate segregation

Frequently, there is no effective segregation between an ICS and the IMS. This access from industrial networks to the IMS or a public network such as the Internet may

be due to operational reasons such as schedule constraints or tool sharing, or cost reduction reasons to simplify the transmission of information from the ICS to the IMS.

Moreover, it is very common to have no segregation within the ICS (e.g. between modules). This may also be due to cost reduction needs or a lack of understanding of the need to partition systems.

Why is it a vulnerability?

The lack of segregation between systems facilitates the work of an attacker, who can more easily move through the system to reach her target. Effective partitioning can also help limit the spread of a virus.

Note

Segregation should also be best practice for safety, since it limits the effects of a system dysfunction, in addition to its cybersecurity benefits.

2.2.10 Remote Maintenance

Remote maintenance and remote management are increasingly common for ICSs. Some are even connected to public networks such as the Internet or mobile networks. This remote access may have been established for internal purposes but also to allow the manufacturer or integrator to perform maintenance operations.

The technical solutions used for remote management and remote maintenance have, in many cases, a low level of security.

Why is it a vulnerability?

The use of remote access greatly increases the attack surface of a system. It is difficult to implement physical protection measures for this type of access.

2.2.11 Inadequate mobile terminal control

It is increasingly common for users to use mobile terminals such as smartphones or tablets to increase their productivity in the field. This is especially true for large distributed installations.

The security of these terminals is not necessarily controlled and the use of personal equipment to carry out professional duties, sometimes called "Bring Your Own Device" (BYOD) has started to be observed.

Why is it a vulnerability?

The use of mobile terminals, with no control over their security, increases their risk of compromise and offers a potential point of entry for an attacker.

2.2.12 Use of standard technologies

For reasons of cost and ICS–IMS interoperability, the technologies used for the former are increasingly standardised. Thus, Ethernet and TCP/IP are increasingly used for networking, replacing previously used proprietary technologies. Development and maintenance tools also increasingly use generic blocks.

Why is it a vulnerability?

The use of standard blocks exposes the systems to all the vulnerabilities they contain. ICSs are thereby vulnerable to generic malware attacks.
Conversely, the use of proprietary or uncommon technologies is not in itself a means of protection, but increases the complexity or cost of an attack as it obliges the attacker to develop malware.

2.2.13 Users

Users of an ICS are not always aware of information system cybersecurity issues and do not necessarily know the ICS Security Policy for their system.

Why is it a vulnerability?

When users are not aware of cybersecurity, it fosters risk behaviours that can facilitate an alteration of the target system. Numerous incidents, based on a lack of awareness and application of best practices, are regularly observed.

2.2.14 Insufficient supervision of cybersecurity events

If an incident occurs on an ICS, operators and maintenance workers do not necessarily consider a malicious action as a possible cause. Users are often not sufficiently qualified to identify cybersecurity events.

Logging of security events is often limited and underexploited. Systems to detect incidents or malfunctions are rarely present.

When supervision of cybersecurity events is effective, the multitude of parameters and the complexity of the environment may limit the analysis of the incident.

Why is it a vulnerability?

When ICS's cybersecurity events are not supervised, it greatly limits the ability to detect and, a fortiori, to react to incidents. Early intervention can help to limit the impact of an incident. In addition, in some cases, when business or technical constraints make it impossible to deploy protective measures, supervision is the only control possible.

2.2.15 Lack of a Business Continuity Plan

Business Continuity Plans (BCP) or Business Resumption Plans (BRP) do not necessarily take cybersecurity events into account. Operational teams rarely have instructions for responding to such events. Drafting a Crisis Management Plan (CMP) for the loss of ICS control due to a malicious event is rarely anticipated.

Why is it a vulnerability?

The establishment of response plans for security events reduces the reaction time and the time taken to return to a normal situation.

2.2.16 Lack of consideration for cybersecurity in projects

During the specification and design phases of the ICS, the documents generally do not include any cybersecurity requirements.

Why is it a vulnerability?

To deploy effective defence mechanisms, cybersecurity must be considered in the initial stages of projects, and in particular as of the project specifications. Increasing the security level of existing ICS is often more complicated and expensive.

2.2.17 Lack of cybersecurity tests

Tests prior to the entry into service (FAT and SAT) rarely include cybersecurity tests. During maintenance operations, security or compliance tests for information systems are often planned, but cybersecurity audits are not.

Why is it a vulnerability?

For cybersecurity of an ICS to remain at an acceptable level, the mechanisms deployed must be tested throughout the lifecycle of the ICS.

2.2.18 Inadequate control of suppliers and service providers

In ICS projects, an audit of the cybersecurity level of suppliers and service providers is rarely envisaged. Moreover, secure information exchange procedures are not considered. Traceability of modifications during the different project phases is not forseen.

Why is it a vulnerability?

In some cases, it may be easier to attack the supplier in order to gain access to the target ICS than to attack the target system directly.

2.2.19 Unsecured development environment

In ICS projects, the development environment is rarely dedicated or secured, either internally or at the supplier facility. For example, development machines are often also the office workstations and are therefore connected to the Internet.

Why is it a vulnerability?

The use of a single working environment for tasks of different exposure and sensitivity increases the risk of alteration. An unsecured development environment (e.g. connected to the Internet) can allow an attacker or malware to corrupt developments (e.g. firmware, PLC programme, SCADA application).

2.2.20 Presence of development tools

In numerous ICSs, development tools are present on the network. This may be because some products do not distinguish between production and development environments. However, it can also result from operational practices. Engineering stations are sometimes simultaneously used as supervision stations.

Why is it a vulnerability?

The presence of development tools on the network facilitates the attacker's task: he can change the behaviour of the ICS, while retaining a legitimate appearance.

2.2.21 Administration machines not partitioned

ICSs often do not segment their administration machines. Frequently, these same machines are used for SCADA applications and device administration.

Why is it a vulnerability?

Inadequate partitioning facilitates the attacker's task, making it possible for him to access device administration functions from the SCADA supervisory stations, which are potentially very exposed.

2.2.22 Definition of responsibilities

Responsibilities in cybersecurity are often poorly assigned between the supplier, the integrator and the entity responsible for the ICS. Similarly, division of responsibilities between business unit management and IT management is not always clear either.

Why is it a vulnerability?

When responsibilities are not clear, there is a risk that part of the ICS is under no one's responsibility and therefore is not subject to appropriate cybersecurity measures.

Section 3

Organisational Security Measures

The organisational measures presented below are intended for all stakeholders involved in ICSs (e.g. project managers, buyers, automation engineers, integrators, developers, maintenance teams, Information System Security Officers).

Important

It is the responsible entity's task to define who will be in charge of applying cybersecurity measures on ICS.

The measures refer to the sections of ISO 27002 [3], recommendations in the Healthy Network guide [13] and the best practices in the ICS cybersecurity guide [10] published by ANSSI. Some measures are also addressed in the classification guide [14].

These references are listed in a box like the one shown below:

References

Classification guide: refers to the classification guide [14].
Vulnerability: refers to vulnerabilities identified in section 2.2.
ICS guide: refers to the ICS guide [10].
Healthy Network guide: refers to the Healthy Network guide [13].
ISO 27002: refers to the sections of ISO 27002 [3] on the subject.

Measures are labelled as *recommendation* and denoted by **[R.x]** when they are advisory and *directive* and denoted by **[D.x]** when they are mandatory. The measures are cumulative. Thus, a class 2 ICS shall apply class 1 measures, and a class 3 ICS shall also apply class 1 and class 2 measures.

3.1 Knowledge of the ICS

This section includes all measures that favour improved knowledge of the ICS and its environment. To ensure a good defence, it is essential to have a thorough knowledge of the system, the risks it faces and the threats it is exposed to.

3.1.1 Roles and responsibilities

References

Classification guide: 2.2.1
Vulnerability: 2.2.22
ICS guide: 2.3.1
ISO 27002: 6.1.1

Class 1

[R.1] A chain of responsibility for cybersecurity should be implemented. It should cover all ICS.

[R.2] Cybersecurity responsibilities should be clearly defined for each of the stakeholders, regardless of the aspect concerned (e.g. development, integration, operation, maintenance).

Class 2

[D.3] Recommendation R.1 becomes a directive.

[D.4] Recommendation R.2 becomes a directive.

Class 3

[D.5] Directive D.3 is strengthened. The identity and contact details of the person in charge of the chain of responsibility for cybersecurity shall be communicated to the cyberdefence authority.

[D.6] Directive D.4 is strengthened. The limits of responsibility shall be reviewed periodically, at least once a year.

3.1.2 Mapping

References

Classification guide: 2.2.3
Vulnerability: 2.2.4
ICS guide: BP09, BP02, 2.2.1
Healthy Network guide: Rules 1 and 2
ISO 27002: 8.1.1

Class 1

[R.7] The following maps should be prepared:

- physical map of the ICS;
- logical map of the ICS;
- application map (flows).

Class 2

[D.8] The following maps shall be prepared:

- physical map of the ICS;
- logical map of the ICS;
- application map;
- system administration map.

[R.9] Mapping and documentation of the ICS should be reviewed regularly, upon each modification of the ICS and at least once a year.

Class 3

[D.10] Recommendation R.9 becomes a directive.

A more detailed description of the expected map content is found in Appendix A

Note

Implementation of industrial tools such as a Computerised Maintenance Management System (CMMS) to manage inventories can be useful. This provides access to all data in a single database, which can be shared with the "business" teams. In addition, the CMMS often already contains an inventory of hardware components such as PLCs, Human Machine Interfaces (HMI), smart sensors and smart actuators.

3.1.3 Risk Analysis

References

Classification guide: 2.2.2
ICS guide: 2.2.2
ISO 27002: ISO 27005

Note

Risk analysis for ICS cybersecurity should be integrated into the overall system risk analysis, which can handle aspects such as safety.

Class 1

[R.11] ICSs should be subject to a risk analysis for cybersecurity, even if it is succinct.

Class 2

[D.12] ICSs shall be subject to a risk analysis for cybersecurity using a method chosen by the responsible entity.

Class 3

[D.13] Directive D.12 is strengthened. The risk analysis shall be reviewed regularly, at least once a year.

[R.14] The risk analysis should be carried out in collaboration with a certified service provider.

3.1.4 Back-up Management

References

Vulnerability: 2.2.5
ICS guide: BP08
Healthy Network guide: Rule 36
ISO 27002: 12.3

Class 1

[R.15] A back-up plan for important data should be implemented to enable restoration of that data in case of incident.

[R.16] Configurations should be saved before and after any modifications, including those done "on the fly."

[R.17] The roll-back process should be tested regularly. It may be tested on a small but representative sample of the entire ICS.

Scope of application: This concerns all data necessary for reconstruction of the ICS after loss: programmes, configuration files, firmware, process parameters (e.g. servo settings), etc. This may also involve data required by regulations (e.g. required traceability data).

Class 2

[D.18] Recommendations R.15, R.16 and R.17 become directives.

Class 3 There are no additional requirements for class 3.

3.1.5 Documentation Management

References

Vulnerability: 2.2.5
ICS guide: BP09
ISO 27002: 8.1.1

Class 1

[R.19] The sensitivity level of documentation should be defined and should be clearly marked on the documents. Documents should be handled accordingly.

[R.20] All documents relating to the design, configuration or operation of the ICS should be considered sensitive.

[R.21] Documents should be stored in an information system whose sensitivity level is appropriate for ICSs.

> **Note**
>
> ICS documentation (e.g. functional analysis, organic analysis, address scheme) is often stored on the(office) management system, the cybersecurity requirements for which may be less stringent than for ICSs. Management systems are often an attackers' first target because they allow easy collection of a large amount of data in order to prepare, for example, a targeted attack on the ICSs.

Class 2

[R.22] The confidentiality of the documentation should be ensured.

[R.23] The documentation should be reviewed at regular intervals to:

- ensure that the necessary documents exist;
- eliminate documents that are no longer used.

Class 3

[D.24] Recommendations R.19, R.21 and R.22 become directives.

3.2 User Control

3.2.1 User Management

References

Vulnerability: 2.2.2
ICS guide: BP04
Healthy Network guide: Rule 3
ISO 27002: 15.1

Class 1

[R.25] Procedures for user management should be implemented, especially regarding their arrival and departure. These procedures should handle, in particular:

- creation and deletion of accounts (see 4.1);
- access management to premises;
- mobile devices management (e.g. telephones, tablets, portable computers);
- sensitive documents management.

[R.26] A skills management process should be implemented, in order to ensure that users have the skills necessary for their assignments. This process should include, in particular, skills transfer from users in charge of systems when they leave the company or change jobs.

Class 2

[D.27] Recommandations R.25 and R.26 become directives.

Class 3

[D.28] A regular review of users and their accounts shall be carried out at least once a year.

Note

In accordance with the regulations applicable to ICSs, a security clearance of users may be required.

3.2.2 Awareness and training

References

Classification guide: 2.2.4
Vulnerability: 2.2.13
ICS guide: 2.2.1
Healthy Network guide: Rule 39
ISO 27002: 7.2.2

Class 1

[R.29] Users should be trained and certified in cybersecurity.

[R.30] A good conduct policy should be established and signed by all users upon arrival.

Class 2

[D.31] Recommendations R.29 and R.30 become directives.

Class 3

[D.32] Directive D.31 is strengthened. User training is required **BEFORE** any intervention on the ICS.

[R.33] Cybersecurity training should be carried out by certified service providers.

[R.34] The ICS cybersecurity training and awareness sessions should take place at the same time as site safety and security training.

3.2.3 Intervention Management

References

Vulnerability: 2.2.6
ISO 27002: 12.1.2

Class 1

[R.35] An intervention management procedure should be implemented, allowing identification of:

- the person performing the work and the ordering party;
- the date and time of the intervention;
- the perimeter on which the work is performed;
- the activities carried out;
- the list of devices removed or replaced (including, where applicable, the ID numbers);
- the modifications made and their impact.

[R.36] All hardware and software used for interventions on ICSs should be inventoried as part of installed assets management, in order to be properly identified and kept up to date (see R.7).

[R.37] The intervention authorisation should be validated by the responsible entity.

[R.38] The intervention process should be audited at least once per year to ensure compliance with procedure.

Note

These elements can be integrated into work permits that are already implemented and required for certain ICSs.

Class 2

[D.39] Recommendations R.35, R.36, R.37, and R.38 become directives.

[R.40] For special cases where users provide their own tools (e.g. manufacturer-specific diagnostic tools), a procedure, however brief, should be implemented to verify that the devices involved have a satisfactory security level.

Such a situation should only occur in cases of absolute necessity and should be exceptional.

Class 3

[D.41] The use of special tools outside the framework provided for by the ICS's security policy is prohibited. Recommendation R.40 becomes irrelevant for class 3.

3.3 Integration of cybersecurity in the ICS life cycle

The integration of cybersecurity in ICS life cycle is a key step in addressing the established requirements. Particular attention should be paid to cybersecurity during the design phases of the ICS.

Cybersecurity should not be handled as an isolated issue. It should be integrated into the project like any other activity: electrical, mechanical, etc.

3.3.1 Requirements in contracts and specifications

References

Vulnerability: 2.2.18
ICS guide: 2.3.2 and 2.3.5
ISO 27002: 15.1.2

Projects can be executed in-house or be outsourced. In this case, the requirements should be established in the project specifications.

More generally, when external service providers are used, security requirements should be explicit and contractual.

Class 1

[R.42] The requirements identified during the specifications phase should be included in the project specifications.

[R.43] The project specifications should include a clause requiring a point of contact to be defined for the project's cybersecurity aspects. That person should be responsible for:

- liaison with the chain of responsibility of the responsible entity (see 3.1.1);
- ensuring compliance with cybersecurity policy;
- communication on discrepancies with requirements and other non-conformities.

[R.44] The specifications should include a list of documents to be provided, including:

- a risk analysis (see 3.1.3);
- a functional analysis;
- an organic analysis;
- an operation and maintenance guide;
- a system map (see 3.1.2).

[R.45] The project specifications should contain clauses requiring cybersecurity tests, particularly during FAT and SAT. The list of required tests should follow recommendation R.71.

Class 2

[D.46] Recommendations R.42, R.43, R.44 and R.45 become directives.

[D.47] The project specifications shall contain a confidentiality clause for all relevant project information, specifying the retention period for documents.

[R.48] The project specifications should include a clause for regular review of the risk analysis. The level of risk should be regularly submitted to the responsible entity (e.g. at the steering committee meeting).

[R.49] Specification documents provided by the contracting party should describe in detail the technical, human and organisational means mobilised to enable their traceability and enable their level of cybersecurity to be verified.

[R.50] The contracting party should provide a security assurance plan describing all measures addressing the required cybersecurity standards (see [8]).

[R.51] The contracting party should use a secure development environment (see 4.3.6).

[R.52] The contract should include a clause specifying that the responsible entity can audit the contracting party or suppliers to verify that all required cybersecurity measures are properly implemented.

Class 3

[D.53] Recommendations R.48, R.49, R.50, R.52 and R.51 become directives.

[R.54] The project specifications should include a clause requiring that supplied hardware and software is cybersecurity certified.

[R.55] The project specifications should require software developers to demonstrate that their development processes use state-of-the-art engineering methods, quality control processes and validation techniques to reduce software vulnerabilities and failures.

[R.56] In order to facilitate the application of recommendation R.55, the contracting party should be certified.

3.3.2 Integration of cybersecurity in the specifications phases

References

Vulnerability: 2.2.16
ICS guide: 2.3.2
ISO 27002: 14.1.1

Class 1

[R.57] The technical requirements should include all technical measures presented in Section 4. For example, the design should take into account:

- the need to authenticate users (see 4.1);
- the need to define a secured architecture (see 4.2);
- the need to secure devices (see 4.3);
- the need to be able to requalify an ICS after security updates.

[R.58] Procedures and technical means should be defined that allow preventive and curative maintenance operations to take place while maintaining the level of cybersecurity in the long term.

For example, provision could be made for degraded modes when performing updates, or PLC outputs could be configured to remain in their last states during a firmware update.

[R.59] The definition of the location of devices should take their physical security into account.

[R.60] The project specifications should require that functions not essential to the operation of the ICS be handled by another information system. The associated devices and software should not be present on the ICS. For example, office workstations with no connection to the ICS should be provided so that users can consult documentation, fill in tracking sheets, etc.

Class 2

[D.61] Recommendations R.57, R.59 and R.60 become directives.

[R.62] The design should incorporate tools and mechanisms to manage security and facilitate requirements such as:

- configuration control (see 3.3.6);
- configuration hardening (see 4.3.1);
- vulnerability management (see 4.3.2).

Class 3

[D.63] Recommendation R.62 becomes a directive.

3.3.3 Integration of cybersecurity in the design phases

References

Vulnerability: 2.2.16
ICS guide: 2.3.2
ISO 27002: 14.1.1

Class 1

[R.64] During the design phase, the interfaces and complexity of the system should be minimised to limit the introduction of vulnerabilities during implementation.

[R.65] The devices' cybersecurity features (e.g. authentication mechanisms, right segregation) should be considered in the selection process.

[R.66] Users roles should be defined. These roles should be integrated in the rights management of computer accounts. Roles should strictly correspond to assigned duties (principle of least privilege). In particular, users and administrators should be distinguished (see 4.1.1).

Class 2

[D.67] Recommendations R.65 and R.66 become directives.

Class 3 There are no additional measures for class 3.

3.3.4 Audits and cybersecurity tests

References

Classification guide: 2.2.5
Vulnerability: 2.2.17
ICS guide: 2.3.2
Healthy Network guide: Rule 40
ISO 27002: 12.7

To ensure that the security level does not degrade over time, cybersecurity tests and audits shall be conducted regularly. These can be integrated into the maintenance and functional testing phases.

Class 1

[R.68] Audits should be carried out regularly. These audits may be internal.

[R.69] Audits should be followed up with an action plan approved and monitored by the responsible entity.

Class 2

[D.70] Recommendations R.68 and R.69 become directives and are strengthened by recommendation R.71 below.

[R.71] An audit programme with the following components should be implemented:

- limit testing;
- error testing on operational functions;
- testing of exceptions verification and handling;
- simulated threat scenarios (penetration tests and takeover attempts);
- verification of security mechanisms (e.g. installation of fixes, analysis of event logs, back-up restores);
- evaluation of system performance.

> **Important**
>
> As penetration testing can lead to failures, it shall be executed in the framework of maintenance or before installations are started.

[R.72] Audits should be performed by certified external service providers.

Class 3

[D.73] Recommendation R.71 becomes a directive.

[D.74] Audits shall be conducted at least once a year.

3.3.5 Operational transfer

> **References**
>
> Classification guide: 2.3
> Vulnerability: 2.3.2

Note

The company tasked with operation may not be the ICS owner and therefore may not have been involved in the creation of the ICS. This may be the case for outsourced public service contracts, operating concessions or operating contracts with an obligation of result, for example.

Class 1

[R.75] Before bringing an ICS into operation, it is recommended to:

- establish a comprehensive inventory of the ICS's cybersecurity level;
- ensure sufficient resources to maintain it at an acceptable level.

Class 2

[D.76] The responsible entity shall obtain approval for ICSs.

Class 3

[D.77] ICSs shall obtain approval and require authorisation prior to the entry into service. Approval shall be carried out by an external organisation.

3.3.6 Management of modifications and changes

References

ICS guide: BP07
ISO 27002: 14.2.2

Modification management concerns PLC programmes, SCADA applications, configuration files for various devices (e.g. network devices, smart sensors, smart actuators), etc.

Class 1

[R.78] Tools should be used to quickly check the differences between the current version and the version to be installed and ensure that only modifications that are necessary and required have been installed.

[R.79] Updates and modifications to systems should be tracked.

Class 2

[D.80] Recommendation R.79 becomes a directive.

[R.81] A process to verify running programme versions against a reference version should be implemented. This ensures that the configurations executed by the ICS (e.g. PLCs, SCADA) are the correct ones.

[R.82] Modifications should be first evaluated in a test environment.

Class 3

[D.83] Recommandation R.78 becomes a directive. The impact of modifications shall be approved by the responsible entity prior to entry into production.

[D.84] Recommendations R.81 and R.82 become directives.

3.3.7 Monitoring process

References

Classification guide: 2.2.6
Vulnerability: 2.2.1
ICS guide: 2.2.6
ISO 27002: 12.6

Class 1

[R.85] A process to monitor threats and vulnerabilities should be implemented.

Note

In particular, this process should be based on available open sources such as national CERTs (CERT-FR, ICS-CERT) and manufacturer and software developer CERTs.

Class 2

[D.86] Recommendation R.85 becomes a directive.

[R.87] Contracts should require suppliers to provide vulnerability alerts for all hardware and software used in the ICS.

[R.88] A process to monitor developments in protection techniques should be implemented. This could also be based on available open sources such as the CERT-FR website.

Class 3

[D.89] Recommendations R.85, R.87 and R.88 become directives.

[D.90] A process to monitor evolutions of attack techniques and threats shall be implemented. In case of important changes, a reassessment of the risk analysis shall be undertaken.

3.3.8 Obsolescence Management

Obsolescence management is not directly a cybersecurity measure, but contributes to it. Obsolescent devices may contain numerous vulnerabilities that will never be corrected. Obsolescence management can therefore be a useful and necessary process in managing vulnerabilities.

References

Vulnerability: 2.2.1

Class 1

[R.91] Clauses relating to obsolescence management for hardware and software, indicating, for example, the date after which they are no longer supported, should be included in contracts with suppliers.

[R.92] An obsolescence management plan to replace obsolete devices and applications should be implemented.

Class 2

[D.93] Recommendation R.91 becomes a directive.

Class 3 There are no additional measures for this class.

3.4 Physical security and access control for premises

3.4.1 Access to the premises

References

Vulnerability: 2.2.8
Healthy Network guide: Rules 32 and 33
ISO 27002: 11.1

Class 1

[R.94] A physical access control policy should be defined. This policy should, in particular, provide a procedure for:

- collection of keys or badges from departing employees (see R.25);
- regularly changing of codes for the corporate alarm system;
- never giving keys or alarm codes to external service providers unless it is possible to track their access and constrain it to specified time periods.

[R.95] Access to premises should be logged and auditable.

Class 2

[D.96] Recommendation R.94 becomes a directive.

[R.97] Access control mechanisms should be robust. Please refer to the ANSSI guide on this subject [9].

[R.98] Entrances should be put under video surveillance.

[R.99] Access to devices should be strictly reserved to certified personnel.

Class 3

[D.100] Recommendations R.95, R.97, R.98 and R.99 become directives.

[D.101] An intrusion detection system shall be implemented for critical zones, especially those not occupied 24/7.

3.4.2 Access to devices and cabling

References

Vulnerability: 2.2.8
ICS guide: BP01
Healthy Network guide: Rule 34
ISO 27002: 11.2

Class 1

[R.102] Servers should be installed in controlled access premises (where possible within IT rooms).

[R.103] Work station central units, industrial network devices and PLCs should be placed in locked cabinets.

[R.104] Access points for the ICS should not be accessible to the public.

Class 2

[D.105] Recommendations R.102, R.103 and R.104 become directives.

[D.106] Recommendation R.104 is strengthened by the following directive: access points for the ICS shall not be accessible in zones not under surveillance.

[R.107] The physical integrity of cables should be protected (e.g. with a casing).

[R.108] When not in use, dedicated maintenance connectors should be blocked (e.g. with caps or cover plates). Unblocking them should follow a well-defined procedure and be subject to prior authorisation.

[R.109] Cabinets holding sensitive devices should be equipped with door opening detector and an alarm signal. At minimum, a means of visual inspection, such as seals, should be installed on external cabinets. Removal of these visual indicators should follow a well-defined procedure and be subject to prior authorisation.

Class 3

[D.110] Recommendations R.104, R.108 and R.109 become directives.

3.5 Incident response

3.5.1 Business Resumption Plan or Business Continuity Plan

A BRP or BCP ensures the resumption or continuity of service following a loss, whatever its origin. The BCP may already exist for non-cybersecurity losses. It should address all feared events giving rise to discontinuation of the service provided, as identified in the cybersecurity risk analysis. For more details, please refer to the guide published by the SGDSN [2].

References

Classification guide: 2.2.7
Vulnerability: 2.2.15
ICS guide: 2.2.7
Healthy Network guide: Rule 36
ISO 27002: 17.1

Class 1

[R.111] A back-up plan for sensitive data should be implemented to enable the ICS to be rebuilt after loss (see 3.1.4).

[R.112] The BRP and BCP should include cybersecurity incidents.

Class 2

[R.113] The BRP and BCP should be tested regularly and at least once a year.

Class 3

[D.114] Recommendations R.111, R.112 and R.112 become directives.

3.5.2 Degraded modes

Class 1

[R.115] Intervention procedures should include an emergency mode to enable rapid response when necessary, without significantly degrading the ICS's level of cybersecurity. In particular, this emergency procedure should not affect the traceability of interventions.

[R.116] Installations should incorporate degraded modes, enabling them to stop without causing damage (material or human) or continue to operate while being directed in "manual" mode.

Class2 There are no additional measures for this class.

Class 3

[D.117] Recommendations R.115 and R.116 become directives.

3.5.3 Crisis Management

References

Classification guide: 3.5.3
Vulnerability: 2.2.15
ICS guide: 2.2.5
Healthy Network guide: Rules 37 and 38
ISO 27002: 17.1

Class 1

[R.118] A crisis management process should be implemented. It should determine:

- what to do when an incident is detected;
- who to alert;
- who should coordinate the actions taken in a crisis situation;
- which initial measures to apply.

[R.119] The crisis management process should also contain an escalation procedure so that incidents are managed at the right level of responsibility and thus decide:

- whether a BCP should be instigated;
- whether legal action is necessary.

[R.120] Crisis management should also define a post-incident analysis phase to determine the cause of the incident and improve the ICS's cybersecurity.

Note

An ANSSI note sets out best practices in the event of intrusion into an information system [4].

Class 2

[R.121] The crisis management procedures should be tested regularly and at least once a year.

Class 3

[D.122] Recommendations R.118, R.119, R.120 and R.121 become directives.

Section 4

Technical security measures

This section brings together all technical measures intended for all stakeholders involved in ICSs (e.g. project managers, buyers, automation engineers, integrators, developers, maintenance teams, Information System Security Officers).

Important

It is the responsible entity's task to define who will be in charge of applying these measures on ICS.

Measures are labelled as *recommendation* and denoted by **[R.x]** when they are advisory and *directive* and denoted by **[D.x]** when they are mandatory. The measures are cumulative. Thus, class 3 ICSs shall also apply class 1 and class 2 measures.

The measures refer to the sections of ISO 27002 [3], recommendations in the Healthy Network guide [13] and the best practices in the ICS cybersecurity guide [10] published by ANSSI. Some measures are also addressed in the classification guide [14].

These references are listed in a box like the one shown below:

References

Classification guide: refers to the classification guide [14].
Vulnerability: refers to vulnerabilities identified in section 2.2.
ICS guide: refers to the ICS guide [10].
Healthy Network guide: refers to the Healthy Network guide [13].
ISO 27002: refers to the sections of ISO 27002 [3] on the subject.

The scope of application is specified for each measure or family of measures. It is the same for all measures in a family, unless otherwise specified. By default, the scope includes the following devices.

Devices that may be concerned by the measures include:

- servers, workstations and desktops;
- engineering stations and programming consoles;
- mobile devices: portable computers, tablets, smartphones, etc.;
- supervision software and applications (SCADA);
- CMMS and MES software and applications, if any;
- human-machine interfaces (touch screens);
- PLCs and remote terminal units (RTUs);
- network devices (switches, routers, firewalls, wireless access points);
- smart sensors and smart actuators;
- etc.

This list is an example and should be adapted to the context of each system.

Important

Some requirements use cryptographic mechanisms (e.g. encryption, signature, authentication). These mechanisms should comply with Appendix B of the General Security Guide [6].

4.1 User authentication: logical access control

4.1.1 Account Management

References

Vulnerability: 2.2.2
ICS guide: BP04
Healthy Network guide: Rules 8, 20 and 30
ISO 27002: 9.1

Accounts can be of various types:

- "session" accounts allowing access to Windows and Linux machines;
- "application" accounts allowing users to connect to a SCADA application, for example. These accounts are often managed by the application itself;
- "system" accounts allowing an application to run and communicate with other applications (e.g. service account). Normally, these accounts are not used by users.

These accounts may have different privilege levels. In particular, "administrator" level accounts are broken down into two categories:

- "system administrator" accounts, with elevated privileges, for IT-type administration of devices (e.g. servers, workstations and network devices) and operating systems;
- "process engineer" accounts, with elevated privileges, to access configuration or programming functions of PLCs and SCADA applications, for example.

> **Note**
>
> For expedience, the accounts are often combined, although they should be strictly separated. A "process engineer" does not need to be a "system administrator." This constitutes a poor practice.

Class 1

[R.123] Each user should be uniquely identified.

[R.124] All accounts with elevated privileges (e.g. administrator accounts) should be protected by an authentication mechanism such as a password. User accounts and administrator accounts should be strictly separated.

[R.125] Generic accounts, especially those with elevated privileges, are not recommended.

If they are indispensable, their application should be limited to very specific uses and should be documented.

[R.126] Roles should be defined, documented and implemented so that user accounts have privileges corresponding precisely to their assignments.

[R.127] An audit of events related to the use of accounts should be implemented.

[R.128] The accounts belonging to personnel who no longer work on the ICS should be deleted, or at least disabled (see R.25).

Class 2

[D.129] Recommendations R.123, R.124 and R.125 become directives. Default accounts and generic accounts shall not be used unless there is a strong operational constraint. Accounts with administrator-type privileges shall not be generic accounts and shall be separated from user accounts.

[D.130] Recommendation R.126 becomes a directive. In addition, accounts with elevated privileges shall be validated by the user's hierarchical supervisor.

[D.131] Recommendation R.128 becomes a directive and complements D.27.

[R.132] An annual review of user accounts should be implemented. In particular, it should allow verification of the proper application of directives D.129 and D.130. This review should pay particular attention to administrative accounts.

[R.133] Whenever possible, read-only access should be configured for level 1 maintenance tasks.

[R.134] If account management is centralised, the configuration of the centralised directory should be audited regularly and at least once a year. In the case of Active Directory, please refer to article [1].

Important

A centralised solution (e.g. Active Directory, LDAP) can facilitate the management of accounts and user rights. However, this type of solution can also give rise to a unique vulnerability and should therefore be studied with the greatest care.

Class 3

[D.135] Recommendations R.127, R.132 and R.134 become directives.

4.1.2 Authentication management

References

Vulnerability: 2.2.2
ICS guide: BP04
Healthy Network guide: Rules 9, 10, 11, 12 and 13
ISO 27002: 9.1

Class 1

[R.136] The various components (devices and software) should only be accessible after authentication using a username and password. Whenever possible, password policy should meet the following minimum requirements:

- passwords should be robust (see [12]);
- default passwords should be changed.

[R.137] A time-out delay should be favoured over a lockout in case of authentication failure.

[R.138] The password's confidentiality and integrity should be protected when it is transmitted over the network.

[R.139] When authentication cannot be applied (in particular, due to operational constraints), compensatory measures should be defined and documented. Some examples might be to:

- use physical access control;
- limit the functionality available (e.g. consultation without modification);
- implement authentication via smartcard with no PIN;
- partition devices more strictly;
- etc.

Example

In a control room operating 24/7, users must be able to take action quickly with SCADA applications. Individual accounts may be inappropriate. In this case, we might consider not requiring individual logins and passwords since only authorised users can access the control room, physical access is tracked, and the control room is occupied continuously.

[R.140] Files containing passwords or their hash value should be stored in a way that ensures their confidentiality and integrity.

[R.141] A secure procedure for resetting passwords in case of loss should be defined.

Class 2

[D.142] Recommendations R.138, R.139 and R.140 become directives.

[R.143] Whenever possible, strong authentication (e.g. smartcard, OTP) should be implemented on workstations and servers. This measure can be extended to devices in the field where possible (e.g. PLCs, remote I/O devices).

[R.144] When recommendation R.143 cannot be applied, the password policy in recommendation R.136 should be strengthened by:

- retention of password history (e.g. the last five);
- automatic verification of password complexity;
- periodic password renewal (e.g. after 90 days).

Note

When setting a new password, some tools can check whether it is too similar to the previous one. This may seem like a good idea because it is often easy to guess a password based on knowledge of the user's other passwords. However, this technique requires keeping a password log in plaintext, which can be dangerous. Simple visualisation of data history can be accomplished by only storing hash values.

[R.145] Security event logs should log authentication failures and successful authentications for privileged accounts.

Class 3

[D.146] Recommendations R.136, R.144 and R.145 become directives.

[D.147] Recommendation R.143 becomes a directive for exposed devices (e.g. desktops, portable computers, engineering stations, programming consoles, firewalls, VPNs).

4.2 Securing the ICS architecture

4.2.1 Partitioning ICSs

References

Classification guide: 2.2.10
Vulnerability: 2.2.9
ICS guide: BP02
Healthy Network guide: Rules 21, 25 and 29
ISO 27002: 13.1.3

Class 1

[R.148] ICSs should be divided into consistent functional or technical zones. These zones should be partitioned from each other.

[R.149] An inter-zone filtering policy should be implemented. To define a filtering policy, refer to the ANSSI firewall guide [11].

The following are a few key principles for data streams using IP protocol:

- data streams are identified by the source IP address, destination IP address, protocol (e.g. UDP or TCP) and, when appropriate, the source and destination ports;
- data streams are rejected by default;
- only data streams required for the operation of the ICS are authorised;
- rejected data streams should be logged and analysed;
- all data streams entering or leaving the ICS should be logged.

Example

Here are some examples of protocols and ports used by industrial protocols:

Modbus : TCP/502

S7 : TCP/102

EthernetIP : TCP/44818 et UDP/2222

OPCUA : TCP/4840

Profinet IO : TCP/UDP 34962, 34963, 34964

[R.150] When non-IP data streams must pass between two distinct zones, filtering should be performed on the source and destination MAC addresses as well as on the authorised protocols.

[R.151] Whenever possible, a physical segmentation should be favoured between functional zones of the ICS. Cybersecurity issues notwithstanding, physical segmenting also helps increase system availability.

[R.152] When physical separation is not possible between the functional zones of the ICS, a logical segementation should be implemented. The use of VLANs is one possible approach to logical separation.

[R.153] The device administration network should be separated from other networks (logically, at minimum). This includes standard computer devices such as switches, gateways, routers and firewalls.

[R.154] Administrative workstations should not be used for any other purpose. They should not be connected to the Internet or a MIS network.

Note

VLANs are not designed to be used as a security mechanism. They must be carefully configured to ensure effective segmentation.

Example

Here is an example of logical segmentation:

- 1 administrative VLAN for network components, administrative workstations and administrative servers;
- 1 VLAN for servers;
- 1 VLAN for operator workstations;
- 1 VLAN for development workstations;
- 1 VLAN per process for PLCs and other associated devices (e.g. remote I/O).

Class 2

[D.155] Recommendations R.148, R.149, R.150 and R.152 become directives.

[D.156] Recommendations R.153 and R.154 become directives. With certain devices, in particular from earlier generations, it may not be technically possible to implement this kind of partitioning. In this case, a specific analysis shall be conducted to investigate potential countermeasures and define the level of residual risk.

[R.157] Data streams should be unidirectional from class 2 ICSs to class 1 ICSs. The unidirectionality of the data streams can be enforced by a firewall.

[R.158] Device administration networks should be physically partitioned from other networks. At minimum, they should be logically separated using VPN tunnels. The use of certified products for the establishment of these tunnels is recommended.

Class 3

[D.159] Data streams shall be unidirectional from class 3 zones to zones of lower classes. The unidirectionality shall be physically enforced by a data diode.

[R.160] The data diode should be certified.

[D.161] Class 3 ICSs shall be physically separated from systems of lower classes. The use of logical partitioning is prohibited.

Important

PLCs are sometimes configured with two different network adapters to separate data streams, e.g. one for communication with SCADAs and the other for communication with process devices. This measure may address dependability needs, but it does not provide protection against certain attacks. This is because the isolation between the two network adapters cannot be guaranteed.

4.2.2 Interconnection with the MIS

References

Classification guide: 2.2.10
Vulnerability: 2.2.9
ICS guide: BP02
Healthy Network guide: Rules 21 and 29
ISO 27002: 13.1

The MIS and its networks are considered to be class 1 by default.

Class 1

[R.162] The interconnection should be protected by a filtering system (firewall).

[R.163] Data streams should be limited to the strict minimum.

[R.164] A filtering policy as described in recommendation R.149 should be implemented.

Class 2

[D.165] Recommandations R.162, R.163 and R.164 become directives.

[R.166] Data streams are unidirectional from class 2 ICS to MIS. The unidirectionality of the data streams can be enforced by a firewall.

Class 3

[D.167] Data streams shall be unidirectional from industial systems to MIS. The unidirectionality shall be physically enforced by a data diode.

[R.168] The data diode should be certified.

4.2.3 Internet access and interconnections between remote sites

References

Classification guide: 2.2.10
Vulnerability: 2.2.9
ICS guide: BP02
Healthy Network guide: Rules 4 and 24
ISO 27002: 9.4

Class 1

[R.169] Access to the Internet from the ICS should be limited. In particular, supervision stations and field devices should not have access to the Internet.

[R.170] Conversely, access from the Internet to the ICS should be limited.

[R.171] Interconnections between ICSs in different locations should ensure the confidentiality, integrity and authenticity of data communication. For example, an IPsec VPN could be used.

[R.172] A filtering system (firewall) should be implemented at the interconnection gateways.

[R.173] The interconnection gateways should be securely configured. Please refer to the ANSSI guide on this subject [7].

Class 2

[D.174] Recommendations R.169, R.170, R.171, R.172 become directives.

[R.175] Devices used for interconnection should be certified.

Class 3

[D.176] Direct interconnection between a class 3 ICS and a public network shall not be allowed.

4.2.4 Remote Access

References

Vulnerability: 2.2.10
Healthy Network guide: Rule 18
ISO 27002: 9.4

Remote diagnosis, remote maintenance and remote management

Remote diagnosis means diagnosing an ICS from a remote location, implicitly outside the buildings in which the ICS is located, and potentially passing through non-controlled networks. This does not include modifying configurations.

Remote maintenance means performing maintenance tasks on an ICS from a remote location, implicitly outside the buildings in which the ICS is located, and potentially passing through non-controlled networks. This implies the ability to modify configurations.

Remote management means taking control of the ICS remotely, with the ability to carry out all management of the system. If remote management is employed, the devices used for this purpose shall be included in the scope of the ICS. All security measures shall also apply to the entire system.

Class 1

[R.177] When remote management, remote maintenance or remote diagnostic operations are required, the following rules should be applied:

- connections should be made at the request of the responsible entity;
- remote connection devices should be certified;
- the connection password should be changed regularly;
- logging should be enabled;
- after a specified period of inactivity, the connection should be closed;

- devices should be partitioned and only necessary data streams should be allowed between the devices and the rest of the ICS;
- remote maintenance operations should only be performed using secure protocols, in particular ensuring the integrity and authenticity of the data exchanged.

[R.178] In the case of a modem connection that does not provide robust authentication, at minimum, a call-back system should be used to validate the telephone number of the incoming call.

[R.179] The connection devices used for remote maintenance should be certified.

Class 2

[D.180] The remote maintenance solution shall conform to the following rules:

- it shall ensure the confidentiality, integrity and authenticity of data communication (e.g. IPsec VPN);
- strong two-factor authentication shall be implemented;
- connection devices shall be partitioned from the rest of the ICS and only the data streams indispensable for remote maintenance shall be allowed;
- logging of security events shall be enabled.

[R.181] An intrusion detection sensor should be deployed on the connection gateway to analyse all incoming and outgoing traffic (see R.279).

Class 3

[D.182] Remote maintenance is prohibited. If remote maintenance operations are imperative, the remote devices and the connection shall be included in the scope of the class 3 ICS. All measures concerning class 3 shall be applied, and in particular those in section 4.2.5.

[D.183] Remote diagnostic solutions may be implemented. In this case, the solution shall implement the following measures:

- the remote connection shall only be made on a partitioned server;
- data needed for the diagnostics shall be pushed to the server through a data diode. This data diode shall be certified.

4.2.5 Distributed ICSs

An ICS is considered to be distributed when the physical protection measures are not applicable to all of the devices and connections that compose the system.

Class 1

[R.184] All data streams passing through physically unprotected or non-controlled networks should use secure protocols. They should ensure the confidentiality, integrity and authenticity of data communication.

[R.185] Whenever possible, VPN gateways should be deployed at the ends of connections to protect all traffic. Devices should be positioned behind a firewall that only allow indispensable data streams to pass. In particular, traffic external to the VPN should be blocked.

[R.186] For connections with availability requirements, the use of public networks such as the Internet should be avoided. The use of leased connections with dedicated resources should be favoured.

[R.187] The devices used in recommendation R.185 should be certified.

Class 2

[D.188] Recommendations R.185 and R.186 become directives.

[R.189] Deployment of intrusion detection sensors is recommended at connection gateways to allow analysis of all traffic flowing between sites. (See R.279).

Class 3

[D.190] The use of connections over public networks shall not be permitted.

[D.191] Recommendation R.189 becomes a directive.

4.2.6 Wireless communication

References

Vulnerability: 2.2.8
Healthy Network guide: Rule 22
ISO 27002: 13.1

Note

In certain cases, wireless networks may be used as a back-up for public wired networks.

Class 1

[R.192] The use of wireless technologies should be limited to the absolute minimum necessary.

[R.193] Depending on their use, data streams should be encrypted and signed, or only signed.

[R.194] Wireless access points should implement the following mechanisms:

- authentication of the access point and the device that connects to the infrastructure;
- network access control functions (e.g. EAP);
- logging of connections.

[R.195] Wireless communication should be partitioned to the full extent possible, isolating wireless peripherals in a separate physical or logical network.

[R.196] When security events are not supervised by a centralised system, events generated by wireless devices should be reviewed regularly.

[R.197] The wireless coverage area should be limited to the extent possible by reducing the transmission power.

Important

Even with reduced power, it is possible to receive broadcasts from a wireless network from far away using specialised antennas and techniques.

Class 2

[D.198] Recommendation R.196 becomes a directive.

[D.199] Security fixes shall be installed systematically on wireless network devices.

[R.200] An intrusion detection sensor should be deployed at the interconnection between the wireless network and other networks of the ICS.

Class 3

[D.201] Recommendation R.200 becomes a directive.

[D.202] The use of wireless technologies is strongly discouraged and shall be limited to cases where there is no other solution.

[D.203] The use of wireless technology shall be prohibited on all connections with critical availability requirements.

[D.204] Security events generated by wireless devices shall be centralised and supervised in real time.

[R.205] All devices used in wireless networks should be certified.

4.2.7 Protocol security

References

Vulnerability: 2.2.7
ICS guide: BP05
Healthy Network guide: Rule 23
ISO 27002: 13.2

Class 1

[R.206] Unsecured protocols (e.g. HTTP, Telnet, FTP) should be disabled in favour of secured protocols (e.g. HTTPS, SSH, SFTP) to ensure integrity, confidentiality, authenticity and the absence of replay flows.

Class 2

[R.207] For protocols that cannot be secured for technical or operational reasons, compensatory measures should be implemented, such as:

- implementation of perimeter protection (firewall);
- encapsulation of data streams with a VPN to ensure integrity and authenticity.

Class 3

[D.208] Recommendations R.206 and R.207 become directives.

> **Note**
> Secured protocols do not always need to encrypt the data stream. If the data stream passes through non-controlled networks, encryption is certainly necessary. However, on a controlled network, encryption is not always desirable, since it is incompatible with the use of intrusion detection sensors. Using signed data may be sufficient.
> The lack of encryption should not be incompatible with recommendation R.138 and directive D.142.

> **Important**
> Certain protocols include mechanisms for integrity verification based on CRC data. This measure, effective for promoting operational security, does not constitute protection against attacks in the context of cybersecurity.

4.3 Securing devices

4.3.1 Configuration hardening

> **References**
> Vulnerability: 2.2.7
> ICS guide: BP05, BP07, BP10, BP12 et 2.2.3
> ISO 27002: 12.6

Disabling unnecessary components

Class 1

[R.209] The following should be disabled on the devices:

- default accounts;
- unused physical ports;
- removable media, if it is not used;
- non-essential services (e.g. web services).

[R.210] On workstations, portable computers and servers, the following should be removed or, at minimum, disabled:

- debugging and development tools for production systems;
- test functions and data, and associated accounts;
- all non-essential programs.

> **Note**
>
> PDF readers and office software are often installed on SCADA stations in order to view documents such as operating procedures. It is preferable to provide users with workstations other than the SCADA stations to run office applications and PDF readers (see R.60).

[R.211] On PLCs and SCADA applications:

- debugging functions (for integrators and manufacturers) should be disabled;
- mnemonics and comments should not be loaded in the devices.

Class 2

[D.212] Recommendation R.209 becomes a directive.

Class 3

[D.213] Recommendations R.210 and R.211 become directives.

Strengthening protection

Class 1

[R.214] The recommendations for hardening operating systems should be applied to all devices. The ANSSI website[1] has many guides and technical notes on this subject.

[R.215] Applications should run with only the privileges absolutely necessary for their operation.

Class 2

[D.216] Recommendation R.215 becomes a directive.

[R.217] Defence in depth tools for workstations should be implemented. In particular, a white list of applications eligible to execute should be implemented on these devices.

[R.218] For PLCs, when devices allow it, the following mechanisms should be enabled:

- access protection for the CPU and/or the programme;
- restriction of IP addresses allowed to connect;
- disabling of the remote programming mode.

Class 3

[D.219] Recommendations R.217 and R.218 become directives.

[R.220] Tools should be certified.

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

Important

The use of antivirus protection may not be suitable for ICSs for the following reasons:

- mechanisms for updating signatures could give rise to vulnerabilities and require connections to external information systems that did not previously exist;
- antivirus protection may be incompatible with dependability principles and requirements.

Antivirus protection should certainly be used on dedicated workstations or servers as indicated in recommendation R.235 and directive D.241, but it is not recommended for the other components of the ICS. Configuration hardening, as described in recommendations R.217 and R.218, should be favoured.

Integrity and authenticity

Class 1

[R.221] The delivery process for all software, programs and configuration data, as well as their updates, should include a mechanism to verify the integrity and authenticity (signature). The components concerned in particular are:

- firmware;
- standard operating systems and software;
- SCADA software packages;
- PLC and SCADA programmes;
- configuration files for network devices;
- etc.

Class 2

[D.222] Recommendation R.221 becomes a directive.

[R.223] The integrity and authenticity of firmware, software and application programs (e.g. PLCs, SCADA) should be verified regularly. Ideally, this task should be automated and performed once per day.

Class 3

[D.224] Directive D.222 is strengthened as follows. The components whose integrity and authenticity must be verified shall be signed by the supplier (e.g. manufacturer, developer, integrator). The signature shall be verified by the responsible entity upon reception and by the device when it is loaded.

[D.225] Recommendation R.223 becomes a directive.

4.3.2 Vulnerability management

References

Vulnerability: 2.2.1
ICS guide: BP11
Healthy Network guide: Rules 6, 7 and 16
ISO 27002: 12.6

Class 1

[R.226] A process for vulnerability management should be implemented in order to:

- search for available fixes to correct these vulnerabilities;
- identify known vulnerabilities and measure their impact on ICS;
- install fixes starting with the most important ones;
- enumerate vulnerabilities for which correction has not been possible (due to lack of fixes, or because the fix could not be installed due to operational constraints).

Note

Installing fixes is not a trivial task. It is important to ensure their compatibility with the operation of applications. The deployment of fixes should be incorporated into ICS maintenance plans. It may be judicious to install fixes when the ICS is shut down (e.g. for mechanical maintenance). Today, PLCs and field devices such as smart sensors and smart actuators are also the object of software fixes.

[R.227] When installing security fixes, priority should be given to the most vulnerable devices (e.g. workstations, portable computers, engineering stations, programming consoles, firewalls, VPNs).

Class 2

[D.228] Unpatched vulnerabilities shall be clearly identified. Specific monitoring shall be carried out and remedial measures shall be implemented to reduce exposure due to these vulnerabilities.

[R.229] Fixes should be validated by the suppliers before deployment.

[R.230] The proper installation of security fixes should be verified. This verification could be a performance indicator for the ICS cybersecurity.

Class 3

[D.231] Recommendations R.226, R.227, R.229 and R.230 become directives.

[R.232] A test environment representative of ICS in production should be implemented to verify the non-regression of ICS after fixes are installed.

4.3.3 Connection interfaces

References

Vulnerability: 2.2.3
ICS guide: BP03
Healthy Network guide: Rules 5, 15 and 34
ISO 27002: 12.6

Management of removable media

Class 1

[R.233] A policy for use of removable media (e.g. USB keys, floppy discs, hard drives) should be defined.

[R.234] The use of removable media should be limited to a strict minimum.

[R.235] A decontamination station should be installed to analyse and sanitize all removable peripherals before they are used on the ICS.

[R.236] The connection of removable peripherals that have not been verified by the decontamination station should be prohibited.

[R.237] Portable media for use exclusively on the ICS should be made available to users. The use of this media for any other purpose should be prohibited. Conversely, the use of any other media should be prohibited.

Class 2

[D.238] Recommendations R.233, R.234, R.235, R.236 and R.237 become directives.

[R.239] Portable media ports should be disabled when their use is not necessary. If physical blocking is not possible, the port should be logically disabled.

Some examples of measures might be:

- blocking USB ports with physical or logical security mechanisms, such as USB port locks (with keys) or security software that can block the use of USB keys and other peripherals;
- removing or disconnecting drives for removable media.

Class 3

[D.240] Recommendation R.239 becomes a directive.

[D.241] A secure data exchange gateway shall be implemented to exchange data with ICSs. It shall be located in a controlled zone. Data exchange activities take place on specific occasions and shall be governed by a procedure.

[R.242] The secure data exchange gateway should be certified.

Managing network access points

Class 1

[R.243] The network access points should be clearly identified and enumerated.

[R.244] Unused network access points (e.g. switches, hubs, wiring closets, maintenance connectors on the fieldbus) should be disabled.

Class 2

[D.245] Recommendations R.243 and R.244 become directives.

[D.246] In case of connection or disconnection attempts on network ports, an alert shall be signalled and handled.

Class 3

[D.247] Network access points shall only be accessible in controlled locations.

4.3.4 Mobile devices

References

Vulnerability: 2.2.11
Healthy Network guide: Rules 5, 17 and 19
ISO 27002: 11.2.6

Class 1

[R.248] The use of all personal peripherals (e.g. smartphones, tablets, USB keys, cameras) should be prohibited.

[R.249] A policy for the use of mobile terminals and signage to remind users of this requirement should be implemented.

[R.250] Devices that are allowed to be connected to ICS should be clearly identified and validated.

[R.251] When devices contain sensitive data, its storage memory should be encrypted.

[R.252] A process for assigning mobile terminals should be implemented. At minimum, it should allow:

- validation of the terminal assignment by the hierarchical supervisor;
- for traceability between the terminal and its users;
- users to be made aware of the usage rules in force.

Class 2

[D.253] Recommendations R.248, R.249, R.251 and R.252 become directives.

[R.254] Devices in use should be dedicated to the ICS, including devices used by external service providers.

[R.255] These devices should not leave the site.

Class 3

[D.256] Recommendations R.251, R.254 and R.255 become directives.

4.3.5 Security for programming consoles, engineering stations and administrative workstations

References

Vulnerability: 2.2.20
ICS guide: BP13
ISO 27002: 11.2.6

Programming consoles are mobile devices; engineering stations are in fixed locations. In both cases, the workstations are dedicated to the engineering of ICS processes. Use of the term "administrative workstation" may lead to confusion.

Administrative workstations are dedicated to the administration of infrastructure devices (e.g. switches, servers, workstations, firewalls) within the ICS.

For technical measures regarding the partitioning of administration functions, please refer to section 4.2.1.

Class 1

[R.257] Engineering stations:

- should be dedicated to engineering activities;
- should not be connected to the Internet;
- should be installed in controlled locations (under access control);
- should be subject to the rules for workstation hardening;

- should be turned off when not in use.

[R.258] Programming consoles:

- should be dedicated to maintenance and operation activities;
- should not be connected to the Internet;
- should not be connected to other systems than the ICS;
- should be subject to the rules for mobile terminals;
- should be subject to the rules for configuration hardening and strengthening of protection;
- should be stored in a secured location;
- should be easily identifiable (e.g. via visual marking).

[R.259] Administration workstations:

- should be dedicated to the administration of infrastructure devices;
- should not be connected to the Internet;
- should be subject to the rules for configuration hardening and strengthening of protection;
- should be installed in controlled locations (under access control);
- should be turned off when not in use.

[R.260] Development tools should not be installed on production machines. For example, only the production (runtime) environment should be installed on SCADA servers and stations.

[R.261] Recommendation R.260 may be difficult to apply when Distributed Control Systems (DCS) are used. In that case, compensatory solutions should be studied in order to isolate the system and reduce its attack surface.

Class 2

[D.262] Recommendations R.257, R.258, R.259, R.260 and R.261 become directives.

Class 3

[R.263] Administrative workstations should not be used for continuous monitoring of systems.

4.3.6 Secure development

References

Vulnerability: 2.2.19
ISO 27002: 14.2

Class 1

[R.264] Best programming practices should be defined, implemented and verified. This could include the use of advanced options of certain compilers or tools designed to verify best programming practices.

Note

Some compilers and SCADA/PLC development environments have numerous options to display additional warnings to the user. These options are often disabled by default. Their use can help avoid multiple programming errors and bugs that could give rise to vulnerabilities.

Note

Applying and verifying best programming practices does not avoid all bugs that can give rise to vulnerabilities.

Class 2

[R.265] Development environments should be dedicated to the ICS.

Note

The development environment can be internal or located at the supplier. In this case, the expected requirements should be explicitly mentioned in the project specification (see R.51).

[R.266] In addition to best development practices mentioned in recommendation R.264, secure coding rules should be established and applied.

[R.267] Static analysis tools and robustness tests should be used systematically.

[R.268] Code audits should be conducted by external service providers.

Class 3

[D.269] Recommendations R.265, R.266, R.267 and R.268 become directives.

[D.270] The development environment's security level shall be verified by audits.

4.4 ICS Monitoring

References

Classification guide: 2.2.12
Vulnerability: 2.2.14
ICS guide: BP06, 2.2.4
Healthy Network guide: Rules 26 and 27
ISO 27002: 12.4

4.4.1 Events logs

Class 1

[R.271] An event management policy should be defined. It should allow for:

- determining which events are relevant and should be taken into account;
- organising event storage (e.g. volumetrics, data retention period);
- defining analysis conditions (e.g. preventative, post-incident);
- defining which events should generate alerts. Appendix B provides a sample list of events.

[R.272] Traceability functions should be enabled if the hardware and software allow it (e.g. syslog, SNMPv3, Windows Event).

[R.273] A centralised, secure system of event log management should be implemented. This system should, in particular, ensure the back-up, confidentiality and integrity of event logs. Please refer to the ANSSI guide on this subject [15].

[R.274] Parameter changes should be tracked and logged (e.g. for sensors and actuators, servo and regulation functions).

> **Note**
>
> In certain cases, some of the changes to process parameters may already be stored in the SCADA applications as events or curves.

Class 2

[D.275] Recommendations R.271, R.273 and R.274 become directives.

[R.276] Logs should be analysed regularly.

Class 3

[D.277] Recommendation R.276 become a directive.

[R.278] A Security Information and Event Management (SIEM) solution centralising all security event logs should be implemented. It should allow for correlating logs to detect security incidents. To avoid considering the SIEM solution as class 3, it should be placed behind a data diode as indicated in directive D.159.

Detection Methods

Class 1 There are no measures for this class.

Class 2

[R.279] Intrusion detection methods should be implemented on the perimeter of installations and at points identified as critical, in particular including:

- interconnections of remote ICSs;
- interconnections of remotely managed ICSs;
- interconnections between the MIS and the industrial information system;
- specific points of connection to the outside (e.g. industrial Wi-Fi);
- secure data exchange stations;

- the backbone network for industrial supervision workstations (SCADA);
- PLC networks considered sensitive.

[R.280] The implemented detection methods should be certified.

[R.281] Events collected by sensors should be centralised.

[R.282] A process should clearly describe how the events indicated by sensors are accounted for.

Class 3

[D.283] Recommendations R.279, R.281, R.282 become directives.

Annex A

Mapping

Teams that operate and maintain ICSs should be able to base their work on reliable and current documentation. This section presents four types of maps at different levels to provide an optimised understanding of the system concerned. Each of these maps consists of a list and a diagram organising the referenced elements.

A.1 A.1 Physical map of the ICS

The physical perspective focuses on the geographic distribution of devices within different sites. We can organise this map in the form of inventories and a diagram.

A.1.1 Inventory

This inventory should, in particular, include the following elements:

the list of communicating devices in the ICS:

This list will include, for example, PLCs, remote I/O, sensors, actuators, variable speed drives, meters, circuit breakers, switches, physical servers, desktops and storage units. For each element, specify:

- name;
- brand;
- model or reference[1];
- the version of the embedded firmware (software version) and the product version if appropriate;
- physical characteristics, if appropriate;
- physical location (building, room, cabinet, bay);
- list of switches connected;

[1] Some devices (e.g. modular PLCs) contains several references.

the list of network communication devices:

This list will include, for example, switches, routers and protocol gateways. For each device, specify:

- brand;
- model and reference;
- embedded firmware version;
- physical location (building, room, cabinet, bay).

For Ethernet switches, also specify the VLAN numbers for each port.

A.1.2 Diagram

This is a representation of the various geographical locations, showing:

- switches, associated VLAN numbers;
- links between devices;
- for inter-site plant, interconnection identifiers (MPLS, VPLS, telephone numbers);
- devices.

A.2 Logical map of industrial networks

This focuses on the logical topology of networks (e.g. IP and non-IP addressing scheme, subnet names, logical links, principal devices in operation). We can also organise this map in the form of inventories and a diagram.

A.2.1 Inventories

We suggest enumerating the following:

organisations:

with, for each one:

- the person responsible.

list of IP address ranges:

with, for each one:

- the list of switches concerned;

- the functional description of the IP range;
- interconnections with other ranges.

list of non-IP networks:
with, for each network:

- the list of MAC addresses or addresses specific to the industrial protocols on the network;
- the list of switches concerned;
- functional description of the network;
- devices connected to other networks (connectors).

list of non-Ethernet access points:
with, for each one:

- the list of access ports;
- addressing, if there is a special protocol;
- the list of connected devices.

list of logical servers and desktops:
with, for each one, if applicable:

- IP addressing (network, mask, gateway);
- operating system version;
- underlying physical server;
- business applications and their versions;
- services and versions.

list of connectors and communicating field devices[2]:
with, for each one:

- IP addressing (network, mask, gateway), the associated MAC addressing and network or the specific addressing, if appropriate;
- business applications.

[2] remote I/O, smart sensors, smart actuators, etc.

A.2.2 Diagram

This diagram is a representation of the IP ranges (networks and sub-networks) and their interconnections, showing:

- the functional description of the IP range;
- interconnections with other ranges;
- routers, switches and firewalls;
- IT security devices (e.g. filtering gateways, sensors, intrusion detection sensors).

In particular, this map must show interconnection points with "external" entities (e.g. partners, service providers) and all interconnections with the Internet.

A.3 Application map

The application perspective focuses on business applications and the data streams between them. As before, we can organise this map in the form of inventories and a diagram.

A.3.1 Inventories

In particular, we can list the following elements:

- the person responsible;
- the type of application (e.g. SCADA application, PLC programme, logging);
- the number of users;
- supporting devices (physical or logical);
- services listening on the network and associated network ports;
- application flows;
- application version.

A.3.2 Diagram

This is a representation of the application components and the flows between them:

- PLC programmes;
- SCADA applications;
- infrastructure services (e.g. DNS, NTP, Internet gateway);
- administration services (e.g. inventory service, remote administration).
- the flow matrix associated with each application and service.

A.4 Maps of IS administration and monitoring

This final mapping only applies if centralised management of administrative rights for devices has been implemented. If device rights are only managed by local accounts, this map is reduced to a list of accounts and related rights for each device.

The map should contain:

- directories (see below);
- key management infrastructures;
- single use password systems;
- systems managing logs and security events (log collection systems, SIEM);
- the supervisory systems (e.g. network alarms, intrusion detection sensors).

The "administrative domains" perspective represents the perimeter and level of privileges of the administrators for the IT base. This map will contain:

- where appropriate, an Active Directory diagram with:
  - Active Directory domains and their descriptions;
  - Active Directory forests;
  - trust relationships with domains external to each forest;
  - characteristics of trust relationships (e.g. bidirectional, filtered);
  - the Active Directory support servers.

- otherwise, the representation of the administration architecture with:
  - ones of responsibility for the various administrators;
  - the list of authentication secrets (e.g. passwords, keys) and rights associated with the administration of resources.

If an administrative account is compromised, this perspective identifies the privilege level of the attacker and the portion of the system potentially affected.

Annex B

Event logs

The following is a (non-exhaustive) list of audit events to configure, at minimum:

- authentication attempts (successful or failed);
- user actions in the system;
- use of privileged accounts;
- security mechanism failures;
- network connection attempts;
- startup and shutdown of audit functions;
- enabling, disabling or modifying the behaviour or configuration of security mechanisms (e.g. authentication, audit generation);
- actions undertaken due to audit storage failure;
- any attempt to export data;
- use of the management function;
- modification of a group of users with a given role;
- detection of a physical violation;
- any attempt to establish a user session;
- attempts to load, modify or collect programmes, micro programmes or firmware;
- modifications to system parameters (e.g. time, IP or non-IP address, cycle time, watchdog timer);
- modification or forcing of application data;
- change of device status to stop, run, standby or restart modes.

Note

Events can be centralised on a syslog-type server. In many cases, devices allow configuration of a syslog server target. For Microsoft event logs, there are utilities that allow each new logged event to be sent to a syslog server.

For more information, please refer to the CERTA information note [5] and the technical note with security recommendations for the implementation of a logging system [15].

Bibliography

[1] Gerard De Drouas and Pierre Capillon. Audit des permissions en environnement Active Directory (permissions audits in an Active Directory environment). In *SSTIC*, 2012.

[2] Secrétariat de la défense et de la sécurité nationale. Guide pour réaliser un plan de continuité d'activité (guide for drafting a business continuity plan). June 2013.

[3] ISO. ISO27002: Security techniques - Code of practice for security management. 2013.

[4] Agence nationale de la sécurité des systèmes d'information. Note d'information, les bons réflexes en cas d'intrusion (Briefing note: Best practices in case of intrusion). May 2002.

[5] Agence nationale de la sécurité des systèmes d'information. Note d'information pour la gestion des journaux d'événement (Briefing note: Managing event logs). May 2008.

[6] Agence nationale de la sécurité des systèmes d'information. Référentiel général de sécurité (General Security Guide). May 2010.

[7] Agence nationale de la sécurité des systèmes d'information. Définition d'une architecture de passerelle d'interconnexion sécurisée (defining a secure architecture for interconnection gateways). January 2012.

[8] Agence nationale de la sécurité des systèmes d'information. Guide de l'externalisation (Externalisation Guide). May 2012.

[9] Agence nationale de la sécurité des systèmes d'information. La sécurité des technologies sans contact pour le contrôle des accès physiques (Security of contactless technologies for physical access control). November 2012.

[10] Agence nationale de la sécurité des systèmes d'information. Mastering cybersecurity for industrial control systems. June 2012.

[11] Agence nationale de la sécurité des systèmes d'information. Note technique pour l'utilisation des pare-feu (Technical note on the use of firewalls). May 2012.

[12] Agence nationale de la sécurité des systèmes d'information. Recommandations de sécurité relatives aux mots de passe (Password security recommendations). May 2012.

[13] Agence nationale de la sécurité des systèmes d'information. 40 essential measures for a healthy network. January 2013.

[14] Agence nationale de la sécurité des systèmes d'information. Cybersecurity for industrial control systems: Classification and key measures. 2013.

[15] Agence nationale de la sécurité des systèmes d'information. Security recommendations for the implementation of a logging system. December 2013.

This cybersecurity guide for Industrial Control Systems was produced by the French Network and Security Agency (ANSSI / *Agence nationale de la sécurité des systèmes d'information*) with the help of the following companies and organisations:

- Actemium,
- Airbus Defence and Space,
- Arkoon-Netasq,
- A.R.C. Informatique,
- Atos Worldgrid,
- Hirschmann,
- Cassidian Cybersecurity,
- CEA,
- CLUSIF,
- DCNS,
- DGA Maîtrise de l'information,
- Euro system,
- EXERA,
- GDF SUEZ,
- Gimélec,
- INERIS,
- Itris Automation Square,
- Lexsi,
- Schneider Electric,
- Siemens,
- Sogeti,
- RATP,

- Solucom,
- Thales,
- Total.

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 – January 2014

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