



Classification Method and Key Measures

Cybersecurity for Industrial Control Systems



Table of Contents

1	Introduction	5
1.1	Context	5
1.2	Scope	6
1.3	Structure of the Set of Documents	6
1.4	Terminology	6
2	Cybersecurity Classes and Associated Measures	9
2.1	Cybersecurity Classes for Industrial Control Systems	9
2.2	Measures	10
2.3	Security Approval	19
3	Classification Method	21
3.1	Context	21
3.2	Security Criteria	23
3.3	Scales	23
3.4	Primary Assets	26
3.5	Supporting assets	27
3.6	Determining the Class	37
A	Simplified Case Studies	39
A.1	Water supply plant	39
A.2	Manufacturing industry	40
A.3	Continuous process industry	40
A.4	Railway switch automation	42
	Acronyms	45
	Glossary	47
	Bibliography	55

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, the ANSSI¹². Composed of actors in the field of automated industrial process control systems and specialists in IT³ Security, the group has undertaken to draft a set of measures to improve the cybersecurity of ICS⁴.

These documents will be used to define the methods for applying the measures set out within the framework of French law No. 2013-1168 of 18 December 2013, known as the Military programming law (LPM⁵).

The objective is to subject all new critical ICSs to an approval process, thus ensuring that their cybersecurity level is acceptable given the current threat status and its potential developments.

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.

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

²The 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.

³Information Technology.

⁴Industrial Control System.

⁵Loi de programmation militaire.



1.2 Scope

The working group did not focus on any specific business sector. Therefore, the contents of this document are intended to apply to all sectors. Some sectors have special characteristics that have not been detailed or considered in this document. **In some cases, it may be necessary to establish a sector-specific version of this document, in collaboration with the coordinating ministries, in order to clarify how to apply techniques 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.

Situations may arise (e.g. compatibility issues with existing ICSs, business-specific constraints) in which certain measures cannot be applied without adapting them. These special cases should be the object of specific studies and the resulting measures should be submitted to the cyberdefence authority for approval.

As this work focused exclusively on cybersecurity for ICSs, the definition of organisations' overall IT security strategy is not concerned by this framework. It is therefore up to each responsible entity to integrate their ICSs and their specific constraints into their IT Security Policy. Please refer to the guide [6] for more information on this subject.


1.3 Structure of the Set of Documents

The production of the working group is divided into two documents. This document constitutes the basis and contains fundamental elements. Cybersecurity classes and key measures are presented in section 2 and the classification method is presented in section 3.

The Measures Guide [10] contains all the precise technical and organisational measures to be implemented according to the classes identified.

1.4 Terminology

In all documents, the term *Industrial Control System* (ICS) designates a set of human and material resources designed to control or operate technical installations (consisting of a set of sensors and actuators). Naturally, this covers the control-command systems that we find in many sectors (e.g. energy, transport, water supply, industry), as well as Building Management Systems (BMS).



Management Information Systems (MIS) are not within the scope of this document. Solely their interfaces with ICSs are discussed. For more information about the distinction between these systems, please refer to the ANSSI guide [8].

The term *cybersecurity* will be used in this document to avoid confusion with the term “security” which, in the industrial context, could have meanings besides the security of information systems (e.g. the security of assets or individuals).

Throughout the remainder of this document, the responsible entity is the natural or legal person that has legal responsibility for the implementation of cybersecurity measures for the ICS in question. It is not always the same person or organisation, depending on the circumstances. Additionally, please note that terminology can vary in different sectors of activity.

Technical terms used in this document are defined in the glossary. In particular, terms relating to information system security are based on the ISO 27000 standards series [5] and IGI 1300, a French government standard on classified information [3].

Warning

Recommendations and directives contained in this document are provided “as-is” and are adapted to known threats at the time the document was published. In view of the diversity of ICSs, there can be no guarantee that this information can be used without adapting it to the target systems. The responsible entity should undertake a preliminary analysis before implementing any of the proposed measures.

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 : Méthode de classification et mesures principales*. In case of divergence, the French version prevails.

Section 2

Cybersecurity Classes and Associated Measures

This section presents the cybersecurity classes and the applicable measures (technical and organisational) for each one. Some measures are simply recommendations; others are directives.

2.1 Cybersecurity Classes for Industrial Control Systems

Some sources propose four or five levels of ICS classification. It is noted that the first levels of these classifications are quite often concerned with safety and contribute little from a cybersecurity point of view. It is assumed that safety issues have already been taken into account; they are not the subject of this document.


Note

Risks due to human negligence are considered as dependability issues, while risks due to malicious acts fall in the domain of cybersecurity. Nevertheless, cybersecurity measures can address certain negligence-related risks.

We therefore propose a simple division of ICSs into three classes, corresponding to their sensitivity. This classification can be applied to an entire site, to a specific portion, or to an ICS distributed over several sites. Details will be provided in the description of the scope, in section 3.1.1. It is up to each responsible entity to define the precise scope of the ICS concerned.

Important

Cybersecurity levels are defined in terms of consequences for the Nation, rather than consequences for responsible entities.



Each class systematically includes the measures of the class below it. Below is a brief description of the three cybersecurity classes for ICSs.

Class 1: ICSs for which the risk or impact of an attack is low. The measures recommended for this class must be able to be applied in complete autonomy. This class mainly corresponds to rules provided in the ANSSI Healthy Network Guide [9].

Class 2: ICSs for which the risk or impact of an attack is significant. There is no state control over this class of ICS, but in the event of inspection or incident, the responsible entity must be able to provide evidence that adequate measures have been implemented.

Class 3: ICSs for which the risk or impact of an attack is critical. In this class, the obligations are heightened and the conformity of ICSs is verified by the state authority or an accredited body.

Cybersecurity classes are estimated using the detailed methodology in section 3. The next section describes the *structural* measures that must be applied according to the three classes. The exhaustive list of measures is found in the Measures Guide [10]. For each measure presented in the remainder of this section, the relevant sections of the guide are indicated.

Important


All functional or technical modifications to ICSs must trigger a review of the cybersecurity level. Indeed, such modifications may have repercussions on the class that was previously estimated. For an example, please refer to the case study in Appendix A.3.

2.2 Measures

2.2.1 Roles and Responsibilities

Roles and responsibilities regarding cybersecurity must be clearly established.

Class 1: A chain of responsibility for cybersecurity should be implemented, covering all ICSs.



Class 2: A chain of responsibility for cybersecurity shall be implemented, covering all ICSs.

Class 3: A chain of responsibility for cybersecurity shall be implemented, covering all ICSs. The identity and contact details of the person in charge of this chain shall be communicated to the cyberdefence authority.

The corresponding detailed measures are found in section 3.1.1 of the Measures Guide [10].

2.2.2 Risk Analysis

Risk analysis is the core of organisational measures. It is the starting point for any cybersecurity strategy and many other measures are directly based on it.

Class 1: ICSs should be subject to a risk analysis for cybersecurity, even if it is succinct.

Class 2: ICSs shall be subject to a risk analysis using a method chosen by the responsible entity.


Class 3: ICSs shall be subject to a detailed risk analysis using a method chosen by the responsible entity. The risk analysis shall be reviewed regularly, at least once a year. It should be carried out in collaboration with a certified service provider.

The corresponding detailed measures are found in section 3.1.3 of the Measures Guide [10].

2.2.3 Inventory

A complete inventory of the ICS is a key component of a good cybersecurity policy as it provides detailed understanding of the system and its environment. For example, it allows rapid assessment of the impact of a vulnerability discovered in a product or measurement of the scope of a compromise access. Inventories of ICSs also permit faster incident resolution. For a brief explanation of inventories, please see Appendix A of the Measures Guide [10].

Class 1: Physical, logical and application inventories of the ICS should be prepared.



Class 2: Physical, logical and application inventories of the ICS shall be prepared. The inventories shall be reviewed regularly (frequency to be determined by the responsible entity) and at minimum each time the ICS is modified.

Class 3: Physical, logical and application inventories of the ICS shall be prepared. The inventories shall be reviewed regularly and at least once a year.

The corresponding detailed measures are found in section 3.1.2 of the Measures Guide [10].

2.2.4 User Training, Control and Certification

Training for users who work on an ICS is indispensable in ensuring the system cybersecurity. This training should include awareness of the risks inherent in information and communication technologies, as well as presentation of the ICS security policy. It should be formalised and approved by the responsible entity.

In the remainder of this document, we consider that personnel are **certified** if they have received specific training regarding their role in the ICS concerned and in awareness of IT security. This training must be officially recorded by the ICS's responsible entity. Personnel are considered to be **controlled** if they have been explicitly authorised to intervene and if their actions can be tracked.

Class 1: All users should be certified.

Class 2: All users shall be certified.

Class 3: All users shall be certified and controlled. Cybersecurity training for this certification shall be carried out by certified providers.

The corresponding detailed measures are found in section 3.2.2 of the Measures Guide [10].



2.2.5 Audits

Audits prior to the entry into service, during SAT¹ and FAT², and then regularly during the life cycle, allow the ICS's actual cybersecurity level to be verified. The audit should cover both technical and organisational aspects in order to verify the proper application of the measures listed in this document and in the Measures Guide [10]. Intrusion tests should also be carried out. The audit process should include suppliers (e.g. manufacturers, integrators).

Class 1: Regular audits should be implemented. These audits may be internal.

Class 2: Regular audits shall be implemented. These audits should be performed by external service providers.

Class 3: Regular audits shall be implemented and must be carried out at least once a year. These audits should be carried out by independent, certified service providers.

The corresponding detailed measures are found in section 3.3.4 of the Measures Guide [10].

2.2.6 Monitoring Process

A monitoring process allows the organisation to keep up to date on threats and vulnerabilities. The sophistication of the monitoring process varies according to the cybersecurity class.

Class 1: A process should be implemented to monitor the vulnerabilities of the products in use, in order to update them in case of flaws.

Class 2: A monitoring process shall be implemented to:


- keep up to date on vulnerabilities identified in the products and technologies used in the ICSs;
- keep up to date on developments in protection mechanisms.

Class 3: A monitoring process shall be implemented to:

- keep up to date on developments regarding threats;

¹Site Acceptance Test.

²Factory Acceptance Test.

- 
- keep up to date on vulnerabilities identified in the products and technologies used in the ICSs;
 - keep up to date on developments in attack techniques;
 - keep up to date on developments in protection mechanisms.

The corresponding detailed measures are found in section 3.3.7 of the Measures Guide [10].

2.2.7 Business Resumption Plan and Business Continuity Plan

A BRP³ and a BCP⁴ can guarantee resumption or continuity of service following a loss, whatever its origin. These plans sometimes already exist in response to other losses. They should address all incident scenarios causing interruption or degradation of the service being provided, as identified in the cybersecurity risk analysis. For more details, please refer to the guide published by the Secretariat-General for National Defence and Security (SGDSN⁵) [2].

Class 1: A BCP or BRP, however succinct, should be implemented.

Class 2: A BCP or BRP shall be implemented. Its effectiveness shall be tested regularly.

Class 3: A BCP or BRP shall be implemented. This plan shall address all incident scenarios that cause an interruption of the service provided and have a serious impact. Its effectiveness shall be tested regularly and at least once a year. A BCP, with a scope broader than cybersecurity, may be requested by the coordinating ministries.

The corresponding detailed measures are found in section 3.5.1 of the Measures Guide [10].


2.2.8 Emergency Modes

Clearly, measures to improve cybersecurity must not reduce an ICS's safety level. It may be necessary to establish streamlined emergency procedures that enable rapid response to an industrial incident.

³Business Recovery Plan.

⁴Business Continuity Plan.

⁵Secrétariat général de la Défense et de la Sécurité nationale.



The following analogy illustrates this point. In case of a fire in a building, doors with access control open automatically. Personnel do not need to use their badge during the evacuation. This is an emergency mode.

Class 1: Emergency modes should be established and closely governed so that they do not constitute an exploitable vulnerability. They should be reflected in the risk analysis and associated procedures should be set out in the ICS security policy. In particular, the traceability of operations should be preserved.

Class 2: There are no additional measures for this class.

Class 3: Emergency modes shall be implemented and closely governed so that they do not constitute an additional system vulnerability. They shall be reflected in the risk analysis; associated procedures shall be set out in the ICS security policy. In particular, the traceability of operations shall be preserved.

The corresponding detailed measures are found in section 3.5.2 of the Measures Guide [10].

2.2.9 Alert and Crisis Management Process

An alert and crisis management process helps establish procedures for responding to incident scenarios identified by the risk analysis.

Class 1: An alert process (even minimal) should be implemented.


Class 2: A crisis management process should be implemented. It should be regularly tested to verify its effectiveness.

Class 3: An alert and crisis management process shall be defined. It shall be regularly tested, at least once a year, to verify its effectiveness. The operational chain of responsibility shall be communicated to the cyberdefence authority.

The corresponding detailed measures are found in section 3.5.3 of the Measures Guide [10].

2.2.10 Network Segmentation and Segregation

Interconnections are a significant source of vulnerabilities. Risks must be carefully evaluated before interconnecting two networks.



Networks should be segmented to the greatest extent possible. In particular, one must be vigilant concerning interconnections between an ICS and a public network (telephone, Internet), between an ICS and a corporate network, or between ICSs of different cybersecurity classes.

Class 1: The following are recommendations regarding different types of interconnection.

ICSs: Partitions using firewalls should be established between class 1 ICSs. Certified devices should be used for the interconnection.

Management Information Systems: The ICS shall be partitioned from the corporate network using a firewall. Certified devices should be used for the interconnection.

Public network: ICSs should not be exposed on the Internet unless it is imperatively justified. Where appropriate, measures should be taken to ensure that they are only accessible to authorised personnel. The risks associated with such a solution should be clearly identified.

Class 2: The following are recommendations regarding different types of interconnection.


ICSs: ICSs: Partitions using firewalls should be established between class 2 ICSs. Certified devices should be used for the interconnection. The interconnection of a class 2 ICS and a class 1 ICS should be unidirectional towards the class 1 system. Certified devices should be used for the interconnection.

Management Information Systems: Interconnection should be unidirectional from the ICS towards the corporate network. Otherwise, all data streams towards the class 2 ICS should be clearly defined and limited. Associated risks should be identified and evaluated.

The interconnection shall be implemented using cybersecurity devices such as a firewall, which should be certified.

Public network: ICSs should not be exposed on the Internet unless it is imperatively justified by an operational requirement. Where appropriate, they should not be exposed without protection and the risks associated with such a solution should be clearly identified. The interconnection should be unidirectional towards the public network. Certified devices should be used for the interconnection.

Class 3: The following are recommendations regarding different types of interconnection.



ICSs: Partitions using firewalls shall be established between class 3 ICSs. It is strongly recommended to implement the interconnection using certified devices.

The interconnection of a class 3 ICS with an ICS of a lower class shall be unidirectional towards the latter. The unidirectionality shall be guaranteed physically (e.g. with a data diode). Certified devices should be used for the interconnection.

Management Information Systems: The interconnection shall be unidirectional towards the corporate network. The unidirectionality shall be guaranteed physically (e.g. with a data diode). Certified devices should be used for the interconnection.

Public network: A class 3 ICS shall not be connected to a public network.

Note

An infrastructure with dedicated resources leased from a telecommunications operator (such as a MPLS network) is not considered a public network when resources are logically partitioned from other traffic and the operator provides service guarantees.


Note that this type of solution does not necessarily guarantee data stream confidentiality or integrity and does not in any case exempt the responsible entity from implementing appropriate measures (such as a VPN) to ensure the authenticity, integrity and confidentiality of data streams.

The corresponding detailed measures are found in section 4.2.1 of the Measures Guide [10].

2.2.11 Remote Diagnosis, Remote Maintenance and Remote Management

Class 1: Clear procedures should be defined and means of protection should be implemented to govern remote diagnosis, remote maintenance and remote management operations.

Certified products should be used for remote diagnosis, remote maintenance and remote management operations.



Class 2: Remote maintenance and remote management operations are strongly discouraged. Where appropriate, the devices used should ensure the authenticity and integrity of communications. These devices should be certified.

Class 3: Remote maintenance and remote management operations shall not be authorised.

Remote diagnosis operations may be carried out using devices that physically guarantees the impossibility of interacting with the class 3 network. Certified products should be used.

Note

When imperatively justified by operational requirements, remote maintenance and remote management may be authorised for class 3 ICSs. However, in this case, these operations should be performed from a site that is also class 3 and which should be included in the risk analysis of the ICS. In particular, the measures in section 2.2.10 concerning interconnection shall apply.

The corresponding detailed measures are found in section 4.2.4 of the Measures Guide [10].

2.2.12 Surveillance and Intrusion Detection Methods

The implementation of surveillance and intrusion detection methods increases visibility within the ICS in question and reduces the response time in the event of attack, allowing its consequences to be limited.

Class 1: A management system should be implemented for the event logs of the various devices in the network. An event management policy should be defined.

Class 2: Intrusion detection methods should be implemented on the perimeter of ICSs and at points identified as critical, in particular including:

- interconnections with the Internet (including remote maintenance);
- interconnections with the corporate network;
- specific points of connection to the outside (e.g. industrial Wi-Fi);
- PLC networks deemed sensitive.



The detection methods used should be certified.

Class 3: Intrusion detection methods shall be implemented on the perimeter of ICSs and at points identified as critical, in particular including:

- interconnections of remote management devices;
- interconnections between corporate networks and ICSs;
- specific points of connection to the outside (e.g. industrial Wi-Fi);
- secure data exchange stations and decontamination stations;
- the backbone network for industrial supervision work stations (SCADA);
- PLC networks considered sensitive.

The detection methods used should be certified.

Note

The deployment of means of detection also implies the implementation of centralisation tools and analysis tools to process the collected events.

The corresponding detailed measures are found in section 4.4 of the Measures Guide [10].

2.3 Security Approval

Approval is the process of verifying the cybersecurity level when a new ICS is placed in service. The approval file must address all measures listed in this document. The approval process essentially consists of verifying that the risk analysis for the ICS was performed correctly, that the measures it specifies have been implemented and that the residual risks are acceptable. During approval, the cyberdefence authority gives prior authorisation for entry into service and the responsible entity accepts the residual risks.

Class 1: It is recommended to address the risks identified in the risk analysis, reducing residual risk to a level the responsible entity considers acceptable.

Class 2: The responsible entity shall obtain approval for ICSs. The approval, in this case, is based on a declarative principle.

Class 3: ICSs shall be approved and require authorisation prior to entry into service. Approval shall be carried out by an external certified organisation.



Note

To avoid the proliferation of procedures, cybersecurity approval can be integrated into the approval procedures that already exist in certain sectors.

Section 3

Classification Method

3.1 Context

This section describes the classification method for ICSs. Cybersecurity classes are determined according to a level of impact and a level of likelihood. The method is based on terms and concepts found in risk analysis methods (e.g. EBIOS¹ [7]) without constituting a comprehensive risk analysis. Figure 3.1 provides a flowchart for the method. Impacts can be easily estimated using tables. However, estimating likelihoods requires several intermediate steps.

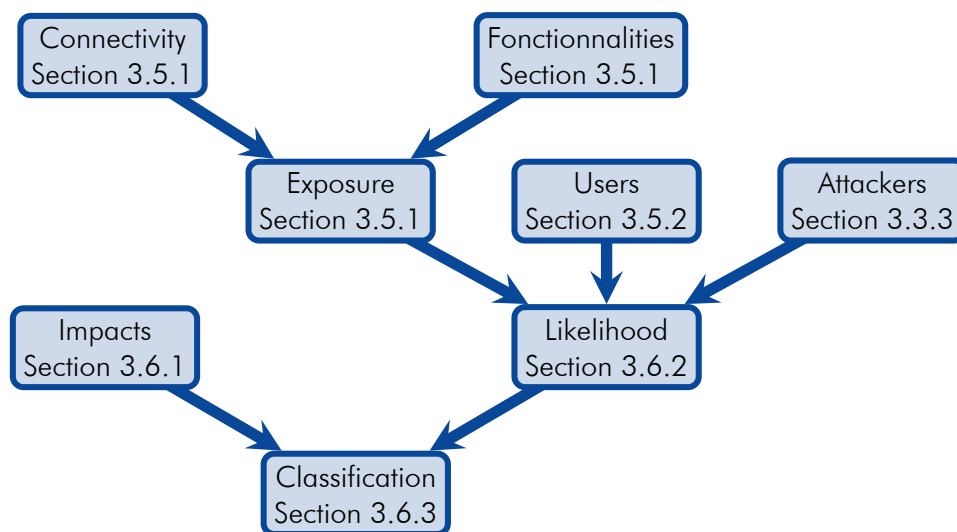



Figure 3.1: Diagram of the classification method

3.1.1 Perimeter

The perimeter must be defined so that it contains all the critical installations of a site or infrastructure (e.g. networks, transport, electricity). Conversely, it is possible to divide a site into multiple ICSs that potentially have different levels of criticality.

¹Expression des besoins et identification des objectifs de sécurité.



If the decision is made to divide an infrastructure into several ICSs, an overall risk analysis should be conducted to verify that all threats have been considered, including those that may result from the infrastructure being viewed as a whole.

Dependability analyses, which have often already been performed by responsible entities, can serve as a basis. Such analyses already define the division of systems and the processes they support.

Example

The perimeter must be defined consistently with respect to the risk and the architecture of the systems being analysed.

Therefore, it may be consistent to carry out an analysis of the technical management plant of a road tunnel (e.g. ventilation, lighting, fire prevention) independently of the rest of the systems present along the road (e.g. road signs, emergency telephones). Nevertheless, in order for this separation to be possible and consistent, the boundary between the two systems must be clearly identifiable. Otherwise, an overall analysis must be conducted.

The method can be applied iteratively:

First, it is applied to an entire infrastructure or site to identify the highest cybersecurity class that must be addressed. Then, once the functional mapping has been established, the method can be applied to smaller subsets. These subsets are sometimes called zones in the literature.

Important

Given the potential impact of certain measures presented above, it is important to precisely determine the perimeter in question. The greater the precision of the perimeter of the ICS, the more applicable measures will be limited to the absolute minimum necessary.

For example, a poorly defined perimeter could lead to the imposition of class 3 measures for a class 2 ICS.

Example

A “Seveso upper-tier” establishment will be class 3 overall. By refining how ICSs are divided, it will undoubtedly become clear only the protection systems for assets and individuals must be categorised as class 3. The production systems are most likely class 1 or 2.

3.2 Security Criteria

We will only use the two principal security criteria most often encountered in ICS, in view of their close connection with dependability: availability and integrity.

Note

In certain sectors, it is possible to add other security criteria such as confidentiality, traceability or imputability, but these are not considered in this study.

3.3 Scales

Several scales are needed to measure the impact and likelihood of an attack.

3.3.1 Consequences

To express levels of consequences, a scale of 1 to 5 was chosen: insignificant, minor, moderate, major and catastrophic. The level of consequences reflects an assessment of various impacts: human, environmental and economic. Detailed examples are provided in the following three tables; they should be adapted and refined for each sector. For example, Article L.1332-3 of the French Defence Code defines additional criteria for sectors of vital importance. Article L.511-1 of the French Environmental Code also specifies certain impacts.

	Level	Designation	Description of the consequences
Human impacts	1	Insignificant	Accident reported, no sick leave or medical treatment.
	2	Minor	Accident reported, with sick leave or medical treatment.
	3	Moderate	Permanent disability.
	4	Major	A death.
	5	Catastrophic	Multiple deaths.

	Level	Designation	Description of the consequences
Environmental impacts	1	Insignificant	Limited and temporary discharge in excess of a standard with no legal requirement to report it to the authorities.
	2	Minor	Discharge in excess of a standard with legal requirement to report it to the authorities but no consequences for the environment.
	3	Moderate	Moderate, limited pollution of the site.
	4	Major	Significant pollution or pollution outside the site. Evacuation of persons.
	5	Catastrophic	Major pollution with long-term environmental consequences outside the site.



	Level	Designation	Description of the consequences
Impacts from interruption of the service provided	1	Insignificant	Serious impacts on 1,000 people.
	2	Minor	Serious impacts on 10,000 people. Disruption of the local economy.
	3	Moderate	Serious impacts on 100,000 people. Disruption of the regional economy. Temporary loss of major infrastructure.
	4	Major	Serious impacts on 1,000,000 people. Disruption of the national economy. Temporary loss of a critical infrastructure. Permanent loss of a major infrastructure.
	5	Catastrophic	Serious impacts on 10,000,000 people. Permanent loss of a critical infrastructure.

Note

The impacts depend very heavily on the sector concerned. This is why the tables may need to be re-evaluated for specific sectors. Additional criteria specific to a sector or an organisation may be included.

3.3.2 Likelihood

Likelihood can be determined using the method described in section 3.6.2. Because of the difficulty in estimating the frequency of occurrence of an attack, this scale is not quantitative.

	Level	Designation
Likelihood	1	Very low
	2	Low
	3	Moderate
	4	Strong

3.3.3 Attacker's Level

This table is needed to evaluate likelihood. We propose to classify attackers' levels as follows.

	Level	Designation	Description/Examples
Attacker	1	Non-targeted	Virus, robots...
	2	Hobbyist	Individuals with very limited means, not necessarily intending to cause harm.
	3	Isolated Attacker	Individual or organisation with limited means, but with a certain determination (e.g. terminated employee).
	4	Private Organisation	Organisation with substantial means (e.g. terrorism, unfair business practices).
	5	State Organisation	Organisation with unlimited means and very strong determination.

Since ICSs have a very long lifetime, it seems unlikely that no determined individual with limited means would want to attack the ICS during that period. We therefore propose to set the attacker's level no lower than 3. The attacker's level should also be re-evaluated according to sector of activity. It may also be specifically specific a given organisation, but only to provide a more severe assessment than the norm for the sector.

3.4 Primary Assets

According to the definition from the EBIOS method, primary assets are the data and processes deemed important for the organisation. In this case, the primary assets are processes handled by the ICS whose alteration could result in damage to individuals, the environment or social order. The analysis of those processes (sometimes called functions or services) has often already taken place, in order to establish the dependability risk analysis, financial risk analysis, etc.

Example

For a road tunnel, primary assets include air-recycling functions, lighting management and management of rescue and fire protection systems. An attack on any of these functions may have an impact on users' safety or the smooth flow of traffic in the tunnel.

3.5 Supporting assets

Supporting assets are the components and subsystems of the system under study.

Example

For a road tunnel, supporting assets include user work stations, PLCs, servers, sensors, detectors (opacimeters, anemometers, CO meters), video cameras.

3.5.1 Typical Architectures

The attack surface of an ICS is largely a function of its architecture. To simply assess the architecture-related risks, we propose to evaluate an ICS based on two scales: its level of functionality and its external connectivity.

ICS Functionalities

The classification regarding the functionality level essentially corresponds to the layers commonly used in the model for CIM², which are as follows:

CIM 0 non-communicating sensors and actuators;

CIM 1 PLCs and analysers;

CIM 2 SCADA³;

CIM 3 MES⁴;


CIM 4 ERP⁵.

²Computer Integrated Manufacturing.

³Supervisory Control And Data Acquisition.

⁴Manufacturing Execution System.

⁵Enterprise Resource Planning.



Note that an ICS containing only CIM 0 elements is unlikely to exist. Therefore, that level has not been retained in the classification. Moreover, it appears that there are no more vulnerabilities involved in CIM 4 than CIM 3. These two levels are therefore considered jointly.

Note

It was decided to concentrate special attention on programming consoles and engineering stations, which provide significant additional tools to an attacker. Their permanent presence in the ICS is sufficient to justify a maximum level.

This yields the following levels of functionality, shown in Figure 3.2.

Functionality 1: Minimal Systems. This category contains the ICS solely containing elements classified CIM 0 and 1 (control-command systems) excluding programming consoles, namely:

- sensors/actuators;
- remote I/O;
- PLCs;
- HMIs;
- embedded systems;
- analysers.

Functionality 2: Complex systems. This category concerns ICSs containing only CIM 0, CIM 1 and CIM 2 elements (control-command systems and SCADA) excluding programming consoles and engineering workstations. Thus, we add to the previous category:

- SCADA;
- historian;
- local databases.

Functionality 3: Very complex systems. This category contains all ICSs that do not fall into the first two categories. In particular, it contains all ICSs with permanently-connected programming consoles or engineering stations, systems that are connected to an MES, and ICSs with centralised historian databases.

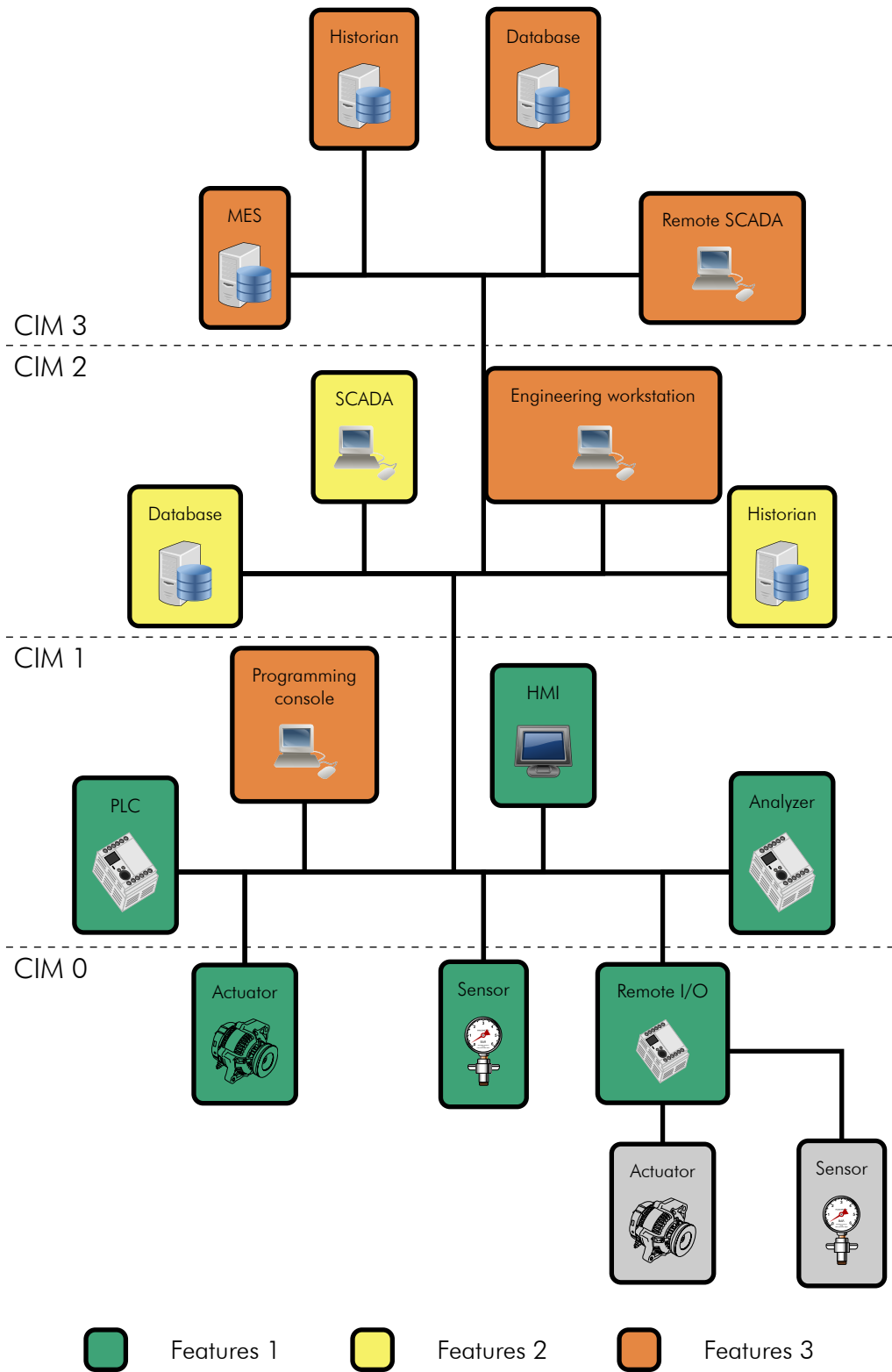


Figure 3.2: Levels of functionality.

Note

DCS^a have native elements (e.g. engineering stations) that can be optional in other systems. Except in special cases, a DCS will be considered as level 3.

^aDistributed Control System (SNCC).

Note

Historians have been divided into two different levels of functionality. Local historians are closely associated with the SCADA and sometimes integrated with it; the duration of data retention is short. A centralised historian may contain data from multiple SCADAs and the retention time is longer.

Connectivity of an ICS

Connectivity 1: Isolated ICS. This category applies to all production networks that are completely closed.

Connectivity 2: ICS connected to an MIS. This category applies to all production networks that are connected to the corporate MIS, but without permitting operations from outside the MIS.

Connectivity 3: ICS using wireless technology. This category contains all ICSs using wireless technology.

Connectivity 4: Distributed ICS with private infrastructure or permitting operations from outside. This category is for distributed systems where the different sites communicate with each other via a private infrastructure. This may be completely private or leased from a telecommunications operator.

This category also concerns all ICSs that permit operations from outside the site or from a management network (e.g. remote maintenance, remote management).

Connectivity 5: Distributed ICS with public infrastructure. This category is like the preceding one, except that a public infrastructure is used (e.g. a telecommunications operator). A typical example is a water distribution infrastructure.



The categories described above are summarised in the following diagrams. Figure 3.3 shows an ICS with connectivity 1. The ICS is completely disconnected and is located on a single closed site.

In this category, the attack surface is limited but not zero. Despite everything, entry vectors do exist, due to removable media, maintenance operators' machines or internal malicious acts.

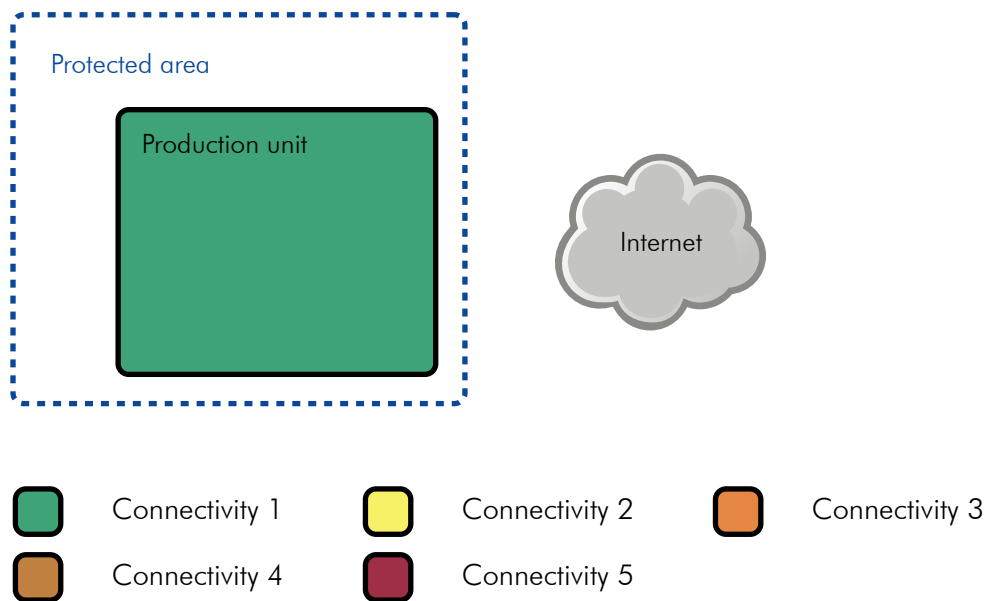


Figure 3.3: ICSs with connectivity 1.

In Figure 3.4, the ICS is connectivity 2; it is still on a single closed site, but is now connected to a management network. We make no specific assumptions about the management network, which can be connected to a public network such as the Internet or even distributed across multiple sites.

In this category, the attack surface includes everything foreseen in category 1, with the addition of attacks from the MIS.

In Figure 3.5, the ICS is connectivity 3 and uses wireless technology.

In this category, the attack surface includes all the vulnerabilities inherent in wireless systems. In particular, there can be availability attacks, which are difficult to guard against.

Figure 3.6 represents an ICS with connectivity 4 with the same nomenclature as before. The two key points are the use of a private communication infrastructure and the presence of remote maintenance systems.

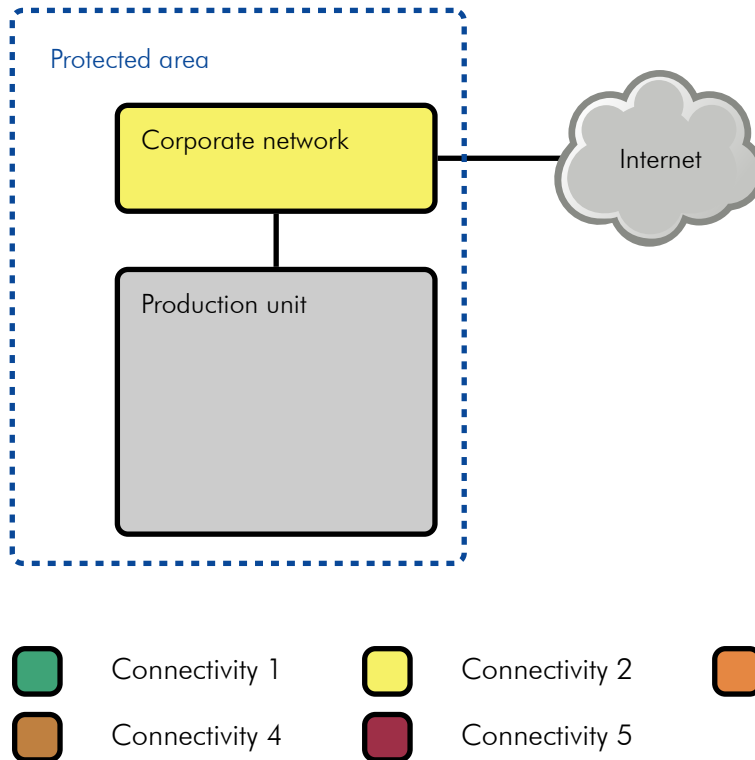


Figure 3.4: ICSs with connectivity 2.

A private network infrastructure is any network entirely under the control of the ICS's responsible entity, as well as any system provided by a telecommunications operator with a share of resources dedicated to the ICS in question, and which does not simply allow outside entities to interfere with the system. Infrastructure such as private APN⁶ or VPN⁷ of type MPLS⁸ falls into this category. In all cases, protective measures shall be taken to ensure the integrity and confidentiality of such a network. However, vulnerabilities are lower than for a public infrastructure.

In this category, the attack surface includes all preceding cases, in addition to new potential vulnerabilities related to the presence of an infrastructure that is very difficult – or even impossible – to monitor and control in its entirety, in particular from the perspective of physical access. All vulnerabilities related to remote maintenance are also present.

⁶Access Point Name.

⁷Virtual Private Network.

⁸Multiprotocol Label Switching.

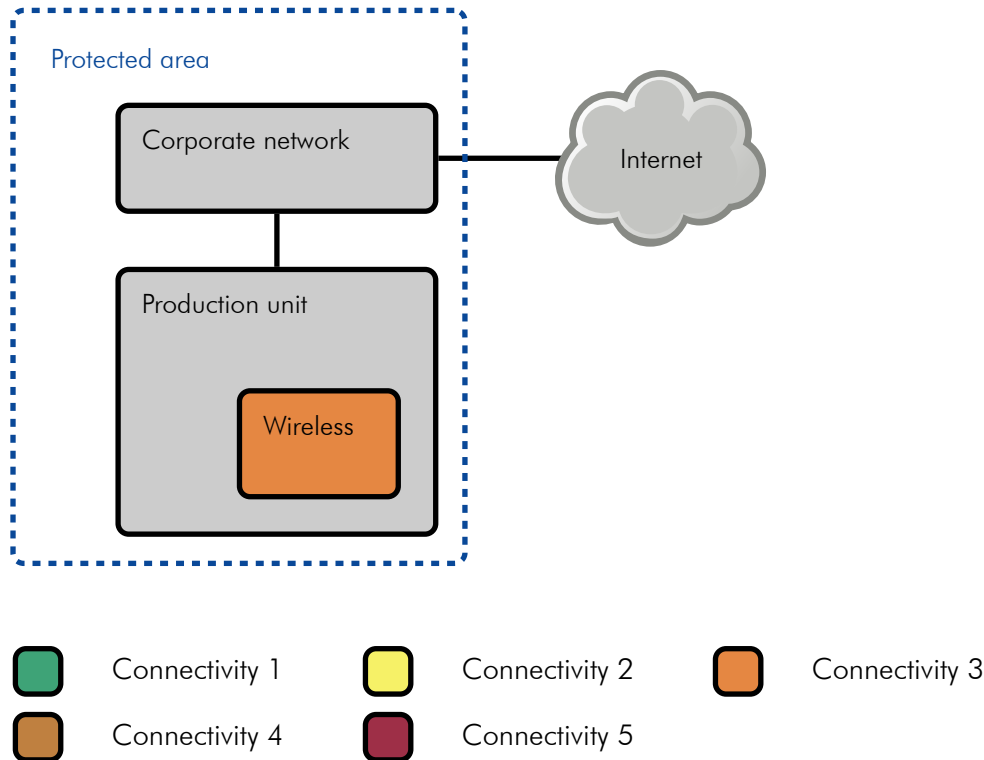


Figure 3.5: ICSs with connectivity 3.

Finally, Figure 3.7 shows an ICS with connectivity 5. In this case, connectivity between the various elements of the ICS is provided by a public infrastructure such as the Internet or the telephone network. In particular, an attacker can easily reach various access points of the ICS. This obliges the implementation of additional protective measures. Moreover, no resources are dedicated to the ICS, which can become a "collateral victim" of abnormally high network utilisation.

Exposure of the ICS

The exposure of the ICS is a combination of its levels of functionality and connectivity. We have defined five levels of exposure ranging from 1 (least exposed) to 5 (most exposed).

The exposure level is obtained from the following table.

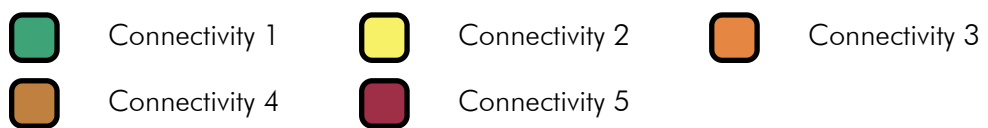
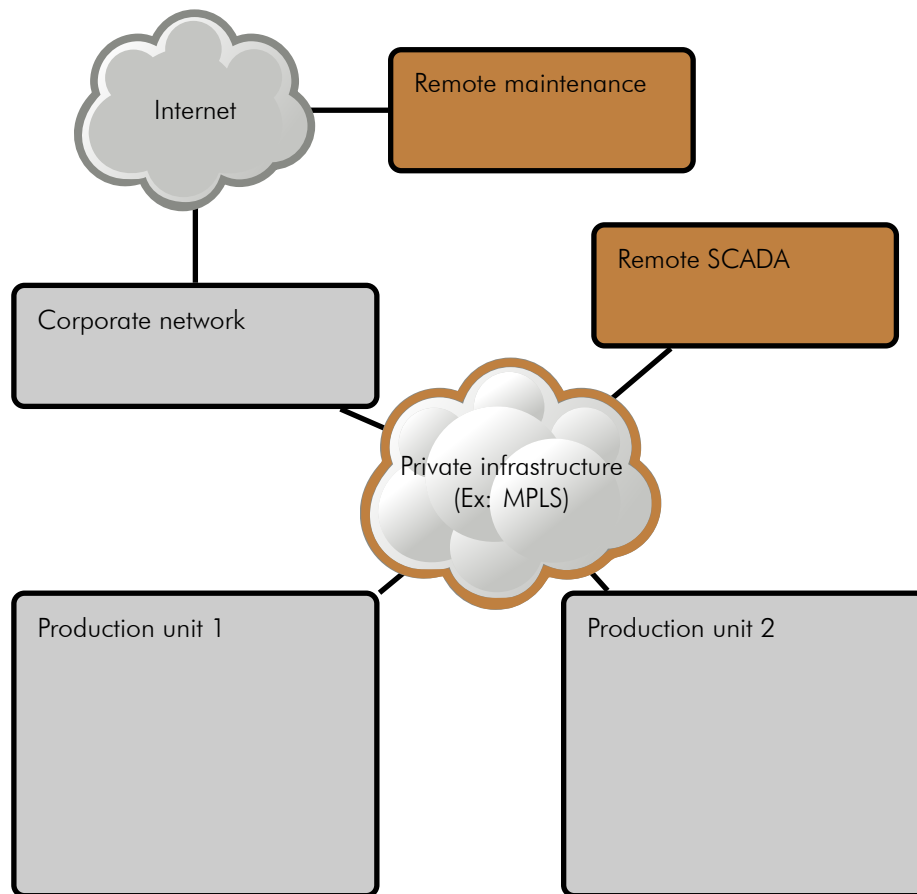


Figure 3.6: ICSs with connectivity 4.

F3	Exposure 3	Exposure 3	Exposure 4	Exposure 4	Exposure 5
F2	Exposure 2	Exposure 2	Exposure 3	Exposure 4	Exposure 5
F1	Exposure 1	Exposure 2	Exposure 3	Exposure 4	Exposure 5
Funct./Conn.	C1	C2	C3	C4	C5

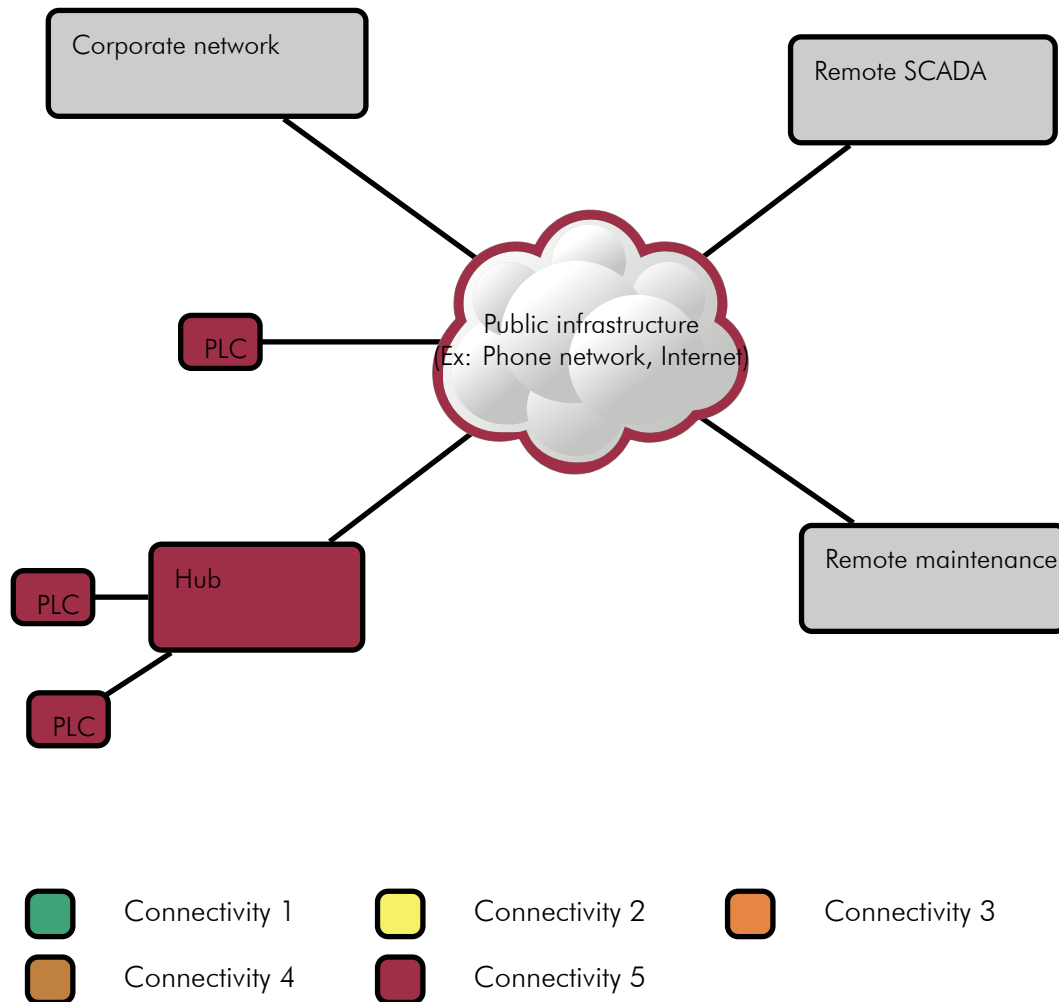


Figure 3.7: ICSs with connectivity 5.

The levels of functionality and connectivity do not vary independently. Therefore, some boxes in the preceding table may not correspond to any real ICS.

Note

Many other factors could have been considered in the analysis, but were left out for simplicity. Among these are the size of the ICS (the number of devices involved) and the heterogeneity of the devices used. These factors must be considered in a comprehensive risk analysis.

3.5.2 Accessibility of the ICS

Personnel working on an ICS are an important vulnerability vector. We have chosen to classify users into two categories. Legitimate users are all individuals with the right to interact with the ICS in a controlled manner. These users may be the operators who ensure the proper operation of the system on a daily basis, as well as the personnel responsible for its maintenance and development. Illegitimate users are all those persons who may interact with the ICS without being controlled, whether this interaction is voluntary or not.

Note

The training and awareness raising referred to for certified personnel do not necessarily have to be carried out by a training organisation; it can be internal training.

However, this training should be clearly defined by the responsible entity, which should also ensure that users have taken part.

Users 1 : authorised, certified and controlled All authorised users are certified and controlled. An unauthorised intervention is not possible.

Users 2 : authorised and certified All authorised users are certified but one or more possible operations are not tracked. An unauthorised intervention is not possible.

Users 3 : authorised There are no special requirements concerning authorised users, but an unauthorised intervention is not possible.

Users 4 : unauthorised This category includes all ICSs for which an unauthorised intervention is possible.

Example

An ICS is in category 1 if all devices are protected by a system with strict access control, logical access to devices is protected by authentication and users' actions are logged.

However, an ICS where devices are protected by access control, but certain devices do not require authentication, is in category 2.

An ICS where devices are unprotected or poorly protected, and therefore accessible to the public or personnel not concerned with system operation (e.g. uncertified cleaning staff) is in category 4.

3.6 Determining the Class

3.6.1 Estimating Impact

We recall that for each primary asset, the security criteria taken into account are integrity and availability.

Based on the established list of primary assets, the responsible entity can enumerate the feared events and estimate their impact according to the scales found in section 3.3.

The feared event with the most serious impact is used to determine the class of the ICS.

Example

The loss of availability of a tunnel's ventilation system may give rise to a human impact of 3, an environmental impact of 1 and an impact from service interruption (the tunnel is closed to traffic) of 1. The loss of integrity of that system does not give rise to more serious impacts. Therefore, the consequences are considered to be level 3.

In contrast, the loss of availability for a toxic waste treatment system in a factory gives rise to a human impact of 1, an environmental impact of 2 and an impact from service interruption of 1, while the loss of integrity of that system has a human impact of 4, an environmental impact of 3, and an impact from service interruption of 1. Therefore, the consequences are considered to be level 4.

3.6.2 Estimating Likelihood

The calculation of likelihood is based on the exposure calculated in 3.5.1. The *Users* and *Attacker* scales are then used as aggravating factors to calculate the likelihood using the following formula:

$$L = E + \left\lceil \frac{A + U - 2}{2} \right\rceil$$

where L is the likelihood, E the exposure, U the users and A the level of the attacker. The mathematical operator $\lceil . \rceil$ means to round up to an integer.

3.6.3 Classification

Feared events and threat scenarios give rise to risks. These are placed in the following table, which allows us to determine the class of an ICS. As explained above, the most serious impact (human, environmental or service interruption) is used.

5+	Class 2	Class 2	Class 3	Class 3
4	Class 2	Class 2	Class 2	Class 3
3	Class 1	Class 2	Class 2	Class 2
2	Class 1	Class 1	Class 2	Class 2
1	Class 1	Class 1	Class 1	Class 1
Impact/Likelihood	1	2	3	4+

Annex A

Simplified Case Studies

The following examples illustrate how to apply this method of ICS classification for different sectors of activity. The results given here shall in no way forecast the classification of similar real systems.

A.1 Water supply plant

The plant under consideration is a remotely managed ICS handling the water supply of an urban area with 500,000 inhabitants.

The ICS is geographically distributed over several sites (reservoirs, booster stations, pumps). Remote sites communicate with the central site via PSTN¹ lines or GPRS² connections. The ICS is composed of numerous remote management devices (RTU³) and supervision work stations (SCADA). Technicians can connect to the system from their remote location if problems occur. Therefore, the functionality level is 2 and the connectivity level is 5. According to the table provided, the exposure level is 5.

There are few users. In theory, only authorised users can access the ICS. In addition, each site has an access control system and video surveillance. The level of users is therefore 3.

Regarding attackers, it seems unlikely that foreign powers or commercial competitors would want to attack the system because the company does not do business on an international level. The level of the attacker is therefore 3.

The impact is limited to an interruption of the water supply for several hours. According to the table of service interruptions, this corresponds to a moderate impact. Therefore, the consequences are level 3.

The maximum impact is 3. Using the formula provided, we obtain a likelihood of 7. According to the classification table, the ICS is in class 2.

¹Public Switched Telephone Network

²General Packet Radio Service.

³Remote Terminal Unit.



A.2 Manufacturing industry

The site under study is a household appliance assembly line for a company essentially doing business on a national level.

As background, the company has already faced a security incident where an employee on the night shift introduced a USB key containing a virus on a supervisory work station. The production line was stopped for three days.

The ICS is limited to a single site. It includes an MES and permanently-connected engineering stations. Technicians and operators use tablets and wireless scanners to scan bar codes. Therefore, the functionality level is 3 and the connectivity level is 3. According to the table provided, the exposure level is 3.

Users are numerous, but, in theory, only authorised personnel can access machines. The level of users is therefore 3.

Regarding attackers, it seems unlikely that foreign powers or commercial competitors would want to attack the system because the company does not do business on an international level. The level of the attacker is therefore 3.

Impacts are limited to lost production, which can be inconvenient for the company but will have little impact on the local economy. We propose considering the impact as level 1.

Using the formula provided, we obtain a likelihood of 5. According to the classification table, the ICS is in class 1.


A.3 Continuous process industry

The ICS under study is a production plant for toxic chemicals. The site is covered by the Seveso Directive.

The worst scenarios are:

- introduction of malware into the ICS;
- an intrusion into the ICS.

This malicious action may be carried out by an individual on site, remotely via the MIS or via a compromised work station on the ICS.



The scenario results in either the loss of one or more operator HMIs (e.g. black or frozen screens, erroneous information displayed) or commands being sent with the intention of causing malfunction.

This incident would be detected by one of the following:

- a control operator;
- alarm signals (e.g. threshold exceeded);
- the securing of the units concerned by the Safety Instrumented System (completely isolated from the control system) in response to detection of abnormal operating conditions or manual operator action.

This would result in downtime for some units, typically lasting one to three days, in order to diagnose the problem and restore configurations. The system could operate temporarily in degraded mode until the problem is fully corrected.

There is no human impact resulting from this scenario. The environmental impact is estimated at 2. The impact on the service provided can range from 1 to 3 depending on the time elapsed before return to service. The impact is chosen to be level 3.

The ICS has centralised historians, engineering stations or programming consoles that are permanently connected. The industrial networks are connected to the site's MIS. Wireless networks are not yet deployed on the industrial perimeter. The functionality level is therefore estimated to be 3; the connectivity level is estimated to be 2. Using the table provided, the exposure is therefore level 3.

As this site is covered by the Seveso Directive, users are all certified and controlled, and the corresponding level is 1.

This sensitive industrial site is likely to attract the attention of "hacktivists," so the attacker level is 4.

Using the formula provided, the level of likelihood is 5. Combined with the impact of level 3, we consider this ICS to be class 2.

Note

If the Safety Instrumented System (for assets and individuals) were not isolated from the production unit control system, we could envision a virus or takeover of the ICS that disrupts the safety functions. In that case, rather than just service interruptions, major human impact could potentially result (level 4). According to the table, the ICS would then be in class 3.

A.4 Railway switch automation

In a railway transport network, a computerised railway switch control system allows management of track assignments and remote control of switches and signalling devices.


The system is composed of the following elements:

- a computerised interlock module (i.e. a PLC) connected to the switches on the railway tracks (i.e. an actuator). The module contains configurable routing maps that are formally validated in advance;
- configuration work stations on a private network dedicated to the transport system. Devices in this network is located in private physical locations, and is therefore protected against undesired access. The configuration work stations are used for diagnostics and to configure routing maps;
- a maintenance work station, outside the network, that is physically connected to the module to set up a new map when necessary. This connection is used only on specific occasions.

We can immediately identify two feared events:

- an accident, if the control system implements an invalid map and sends dangerous commands to the switches;
- loss of service for the line (or at least a portion of it), if the control system stops working or sets up restrictive routing configurations.

The impact is therefore level 5, since a dangerous system malfunction could cause an accident with multiple fatalities.



In view of the devices, the functionality is level 2. The telecommunications network used by the control system is distributed but private. Therefore, the connectivity is level 4. The exposure level is thus 4.

Users using the control system are certified maintainers. Their interventions are controlled in accordance with the requirements for dependability. Therefore, the user level is 1.

We choose a maximum threat level because the system can cause fatal accidents and is therefore likely to attract the attention of malicious individuals. Additionally, the scenario of causing a train derailment is regularly cited in cyberattack scenarios. The attacker level is therefore 5.

In conclusion, the likelihood is greater than 4 and the system is class 3.

Acronyms

ANSSI Agence nationale de la sécurité des systèmes d'information.	5
APN Access Point Name.	32
BCP Business Continuity Plan.	14
BMS Building Management System.	6
BRP Business Recovery Plan.	14
CIM Computer Integrated Manufacturing.	27
DCS Distributed Control System (SNCC).	30
EBIOS Expression des besoins et identification des objectifs de sécurité.	21, 26
ERP Enterprise Resource Planning.	27
FAT Factory Acceptance Test.	13
GPRS General Packet Radio Service.	39
ICS Industrial Control System.	5, 6, 9, 39
IT Information Technology.	5, 6
LPM Loi de programmation militaire.	5
MES Manufacturing Execution System.	27
MIS Management Information System.	7
MPLS Multiprotocol Label Switching.	17, 32
PLC Programmable Logic Controller.	27, 28
PSTN Public Switched Telephone Network.	39
RTU Remote Terminal Unit.	39
SAT Site Acceptance Test.	13
SCADA Supervisory Control And Data Acquisition.	19, 27, 39
SGDSN Secrétariat général de la Défense et de la Sécurité nationale.	14
VPN Virtual Private Network.	32

Glossary

- Asset** Any resource that has value to the organisation and is necessary to achieve its objectives [4]. In particular, we distinguish between primary assets and supporting assets.
French: bien. 26, 27
- Primary Asset** Data or process deemed important for the organisation. We can assess its sensitivity but not its vulnerabilities.
French: bien essentiel. 26
- Supporting Asset** Asset that provides support for primary assets. Typical examples are information systems, organisations and premises. We can assess its vulnerabilities but not its sensitivity. *Examples:* systems integrator, production unit, automation engineer, Ethernet network, operating system.
French: bien support.
27
- Attack** An attempt to compromise an information system, carried out with a malicious objective. The intention may be to steal data (e.g. military, diplomatic or industrial secrets, personal banking data) or to destroy, damage or alter the normal operation of information systems (including ICSs).
French: Attaque. 10, 14, 23, 28
- Attack Surface** All vulnerable resources of a system, exposed to attacks from external sources of threats via various interfaces between the system and its environment.
French: Surface d'attaque. 27, 31, 32
- Availability** Property allowing the expected service to be performed in the desired time and in conformity with the expected conditions of use.
French: disponibilité. 23, 37
- Building Management System** Building Management System ICS that manages all technical installations in a building (e.g. electricity, climate control, ventilation, elevators, access control, video surveillance). *French: Gestion technique de bâtiment.* 6
- Compromise Access** Compromise Access, certain or probable, to data or protected media by one or more unauthorised individuals [3].
French: compromission.
For an information system, see *Intrusion.* 11

Confidentiality	Private aspect of data or of a process, to which access is restricted solely to certain individuals in view of requirements of the service, or to authorised entities or processes [3]. <i>French: Confidentialité.</i>	17, 23, 32
Consequences	Quantification of the severity of a risk or feared event. <i>Examples: See 3.3.</i> <i>French: Gravité.</i>	23
Control	Control Means of addressing a data security risk. A control's nature and the level of detail of its description can be highly variable. <i>French: Mesure de sécurité.</i>	10
Control-Command System	Automated system that handles the operation and protection of an industrial process. Control-command systems are frequently composed of sensors, actuators and PLCs. <i>French: Système de contrôle-commande.</i>	6
Controller	Programmable Logic Controller. <i>French: Automate programmable industriel.</i>	19, 27
Cyberdefence	All technical and non-technical measures allowing a State to defend information systems deemed essential. <i>French: cyberdéfense.</i>	6
Cyberdefence authority	Cyberdefence authority National authority responsible for the defence of information systems. In the framework of guidelines established by the Prime Minister, it sets down measures that the State implements to respond to crises affecting or threatening the security of information systems for public authorities and operators of vital importance [1]. <i>French: autorité de cyberdéfense.</i>	6, 11, 15, 19
Cybersecurity	A desired condition for an information system, allowing it to withstand events of malicious origin that are likely to compromise the availability, integrity or confidentiality of data stored, processed or transferred or the services provided by the system. <i>French: cybersécurité.</i>	7
Data Diode	Data diode Partitioning device designed to allow the circulation of information in a single direction. The unidirectionality is ensured using physical techniques. <i>French: diode.</i>	17
Decontamination station	Decontamination station Work station allowing verification that removable media is virus-free before it is used on the plant. <i>French: Station blanche or station de dépollution.</i>	19

Dependability The study of a system's failures and faults in order to ensure its ability to accomplish its functions, under defined conditions and for a given period of time.

In particular, dependability addresses the properties of Reliability, Availability, Maintainability and Safety (RAMS). In this context, dependability concerns people and assets.

Failure Modes, Effects and Criticality Analysis (FMECA) is a methodology frequently used in this domain.

French: Sûreté de fonctionnement. 7

Engineering Station Computer devices with software packages for configuring, designing, programming, or administrating industrial devices such as PLCs and SCADAs. This device is connected to the industrial network and made available to different teams (e.g. maintenance, engineering, support).

French: Station d'ingénierie 28

Feared Event Feared event Generic scenario representing a situation feared by the organisation. It is expressed by a conjuncture of threats likely to be the cause of the event, a primary asset, a security criterion, the sensitivity concerned and the potential impacts. *Example:* a malevolent individual (e.g. journalist, competitor) manages to obtain the organisation's estimated budget, deemed confidential, and publishes the information in the media. *French:* Événement redouté. 37, 38

Firewall Firewall Device that implements the partitioning policy between multiple networks by filtering the data streams between them.

French: Pare-feu. 16

Flaw Vulnerability in a computer system that allows an attacker to compromise its normal operation, confidentiality or the integrity of the data it contains.

French: Faille. 13

Historian Database containing logs of alarms and process values collected by the supervision software (SCADA). These historians are often local or centralised.

French: Historique. 30

Centralised Historian Historian centralising data from multiple supervisor consoles (SCADA). Data retention time is often long, but with a coarser granularity than in the local historian.

Management can use this historian for data analysis, statistics, etc. concerning the entire production unit. *French:* Historique centralisé.....

30

Local Historian	Historian located near the industrial devices for which it records data. Data retention time is often limited, but with a very fine granularity. This historian allows operators to perform detailed analyses when production incidents occur. <i>French: Historique local</i>	30
Human-Machine Interface	Human Machine Interface allowing an intervener to interact with and control the operation of an ICS. <i>French: Pupitre.</i>	28
Impact	Direct or indirect consequences on the organisation and/or its environment of not addressing sensitivities. <i>Examples:</i> On the organisation's activity; on individuals' safety; financial, legal, image or environmental issues. <i>French: Impact.</i>	21, 23, 25, 37, 38
Imputability	Ability to attribute legal responsibility for an action to a natural or legal person. <i>French: Imputabilité.</i>	23
Information Security Risk	Scenario, with an associated level, representing the conjuncture of a feared event and one or more threat scenarios. Its level corresponds to an estimate of its consequences and likelihood. <i>French: Risque.</i>	37
Information System	Set of human and material resources designed to develop, process, store, transfer, display or delete information [3]. <i>French: système d'information.</i>	7
Distributed Information System	Distributed information system Information system or ICS interconnecting multiple sites. A system falls into this category when it is not possible to set up a closed perimeter with access control around the entire system. This applies in particular to the cables and optical fibres for the network supporting the system. <i>French: Système d'information distribué.</i>	30
Industrial Control System	Set of human and material resources designed to control or operate a group of sensors and actuators. <i>French: Système automatisé de contrôle des procédés industriels (Système industriel).</i>	6
Management Information System	Information system including services and applications designed for management purposes (e.g. office applications, human resources, customer service). <i>French: Système d'information de gestion.</i>	7
Integrity	Property of protecting the accuracy and completeness of assets. <i>French: Intégrité.</i>	17, 23, 32, 37

Intrusion	Takeover, certain or probable, of an information system or one of its components by one or more unauthorised individuals. <i>French: Intrusion.</i>	18, 19
Intrusion Test	Security test for an information system generally consisting of simulating the behaviour of a malicious individual or programme. <i>French: Test d'intrusion.</i>	13
Likelihood	Estimate of the possibility that a threat scenario or a risk will occur. It represents the estimated level of possibility. <i>Example: See section 3.3.</i> <i>French: Vraisemblance.</i>	21, 23, 25, 26, 38
Programming Console	Work station containing tools that allow programming, configuring and administering an industrial PLC. <i>French: console de programmation.</i>	28
Remote Diagnosis	Remote diagnosis The action of remotely (implying from outside the information systems of the responsible entity) carrying out diagnostics on a technical plant. This does not include modifying configurations (read-only). <i>French: Télédiagnostic.</i>	17, 18
Remote Maintenance	The action of remotely (implying from outside the information systems of the responsible entity) carrying out maintenance tasks on a technical plant. In particular, this implies being able to modify configurations or programmes (read/write). <i>French: Télémaintenance.</i>	17, 18
Remote Management	The action of remotely (implying from outside the information systems of the responsible entity) taking control of geographically distributed technical plant (read/write). <i>French: Télégestion.</i>	17, 18
Responsible Entity	Natural or legal person that has legal responsibility for the implementation of appropriate cybersecurity measures for the system concerned. <i>French: Entité responsable.</i>	7
Secure data exchange station	Secure data exchange station Secure device allowing data exchange with removable media. It is usually a dedicated work station implementing security mechanisms to limit the potential spread of viruses, verify the authenticity of data, etc. <i>French: Sas.</i>	19

Security Approval Declaration by the approval authority, in light of the approval file, that the information system in question is considered capable of fulfilling its objectives in conformity with the security objectives that were set, and that the residual security risks are accepted and controlled.

The security approval remains valid as long as the information system operates under the conditions approved by that authority.

French: Homologation de sécurité. 19

Security Criterion Characteristic of a primary asset allowing assessment of its various sensitivities. *Examples:* availability, integrity, confidentiality, traceability.

French: critère de sécurité. 23

Security Incident One or more undesirable or unexpected events related to information security, with a high probability of compromising the operations linked to the organisation's activity and endangering data security. *French:* incident de sécurité [5]. 10, 11, 14, 15

Sensitivity A precise and unambiguous definition of the level of a primary asset's operational requirements for a given security criterion (e.g. availability, confidentiality, integrity).

Examples: must be available during the day, must be known to the project group.

French: besoin de sécurité. 9

Threat Potential cause of an undesirable incident, which may harm a system or organisation [5].

Examples: Theft of media or documents, corruption of software, passive listening. *French:* Menace. 5, 7, 13, 22

Threat Scenario Scenario, with an associated level, describing methods of attack. It represents the conjuncture of the sources likely to be the cause of threats, a supporting asset, a security criterion, threats and the exploitable vulnerabilities that make it possible. Its level corresponds to the estimate of its likelihood.

Examples: Theft of media or documents because of the ease of entry into offices; corruption of software due to users' naivety.

French: Scénario de menace. 14, 15, 38

Traceability Property allowing identification of the source of a primary asset and reconstruction of its path from its production through to its use.

French: Traçabilité. 15, 23

User User Any person who intervenes on an information system. This includes personnel responsible for operation of the system but also integrators and maintenance personnel.

French: Intervenant. 12, 36



Certified User Certified user Any user on an information system who received specific training regarding his role for the installation concerned and awareness of information system security. The training must have been officially recorded by the system's responsible entity. *French:* Intervenant habilité. . . . 12, 36

Vulnerability Characteristic of a supporting asset that can constitute a weakness or flaw concerning information system security. Examples: credulity of personnel, ease of entering a site, possibility to create or modify system commands. *French:* Vulnérabilité. 11, 13–15, 28, 32

Bibliography

- [1] Décret n° 2011-170. février 2011.
- [2] Secrétariat de la Défense et de la Sécurité nationale. Guide pour réaliser un plan de continuité d'activité. June 2013.
- [3] Secrétariat général de la défense nationale. Instruction générale interministérielle sur la protection du secret de la défense nationale. August 2003.
- [4] ISO. ISO27001: Information Security Management System (ISMS) standard. 2005.
- [5] ISO. ISO27000: Information security management systems — Overview and vocabulary. 2013.
- [6] Agence nationale de la sécurité des systèmes d'information. Guide d'élaboration de politiques de sécurité des systèmes d'information. 2004.
- [7] Agence nationale de la sécurité des systèmes d'information. EBIOS-2010 - Expression des besoins et identification des objets de sécurité. 2010.
- [8] Agence nationale de la sécurité des systèmes d'information. Maîtriser la ssi pour les systèmes industriels. June 2012.
- [9] Agence nationale de la sécurité des systèmes d'information. 40 essential measures for a healthy network. January 2013.
- [10] Agence nationale de la sécurité des systèmes d'information. Cybersecurity for industrial control systems: Detailed Measures. 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

Licence « information publique librement réutilisable » (LIP V1 2010.04.02)

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](mailto:communication@ssi.gouv.fr)