RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERSECURITY OF INDUSTRIAL CONTROL SYSTEMS - CLASSIFICATION METHOD

ANSSI GUIDELINES

ANSSI-PA-107-EN
04/12/2025

TARGETED AUDIENCE:

Developers | Administrators | IT security managers | IT managers | Users

Information

Warning

This document, written by ANSSI, the French National Cybersecurity Agency, is titled **"Cybersecurity of Industrial Control Systems - classification Method"**. It is freely available at cyber.gouv.fr/en.

It is an original creation from ANSSI and it is placed under the "Open Licence v2.0" published by the Etalab mission.

According to the Open Licence v2.0, this document can be freely reused, subject to mentionning its paternity (source and date of last update). Reuse means the right to communicate, distribute, redistribute, publish, transmit, reproduce, copy, adapt, modify, extract, transform and use, including for commercial purposes

The recommendations are provided as is and are related to threats known at the publication time. Considering the information systems diversity, ANSSI cannot guarantee direct application of these recommendations on targeted information systems. Applying the following recommendations shall be, at first, validated by IT administrators and/or IT security managers.

This document is a courtesy translation of the initial French document **"Titre non défini"**, available at cyber.gouv.fr. In case of conflicts between these two documents, the latter is considered as the only reference.

Document changelog:

VERSION	DATE	CHANGELOG
1.0	01/01/2014	Initial Version
2.0	04/12/2025	Redesign of the document

Contents

1
Introduction

1.1 Guide objectives

Industrial systems based on *Operational Technology* (OT) are used to operate and monitor processes that have a direct physical effect and can therefore pose a risk to people, property or the environment.

Some industrial systems use *Information Technology* (IT) but have not been designed to address the threats it involves. Moreover, the security solutions used in business computing are not always suited to the operation of industrial systems.

In theory, OT should be secured at the design stage and sometimes requires tailor-made solutions. In practice, there are many vulnerabilities specific to the components of an industrial system (e.g. protocol stacks on PLCs or servers). For this reason, it is essential to integrate these elements into the overall approach to the security of corporate information systems.

The purpose of this guide is to propose a method for defining a security baseline suitable for industrial systems. This method is based on dividing the industrial scope and its classification into four levels. For each of the levels, called classes, the detailed measures guide [6] proposes a set of measures proportionate to the security baseline.

Warning

This guide focuses exclusively on the cybersecurity of industrial systems. The definition of an organisation's global IT security strategy is not included here. It is therefore up to each responsible entity to integrate the industrial systems and their specific constraints into their information system security policy (ISSP).

Information

This is an update to the requirements developed by the ANSSI-led working group on industrial system cybersecurity. This update takes into account feedback from the previous guide and the limitations imposed by the presence of three cybersecurity classes and includes equivalence with IEC 62443 [9].

1.2 Organisation of the guide

Each industrial system has its own specific features and risks which need to be analysed in order to deploy appropriate security solutions that limit the impact on the company's business. This process of securing the system safeguards the company's investments and production. This is why it is important to define the correct objectives and adapt them to the relevant needs, as described in chapter 5 of this guide.

The ANSSI's methods and recommendations for protecting industrial systems are presented in two documents. This document contains the structural elements of the classification methodology. The approach to securing industrial systems is presented in chapter 3, the cybersecurity classes are presented in chapter 4 and the classification method changes are presented in chapter 5. A case study proposing the application of the previous chapters is presented in chapter 6. The detailed measures guide [6] - only available in French - contains all of the specific technical and organisational recommendations to be applied according to the identified classes.

The work presented in this guide establishes links with ISA/IEC 62443 [9], used in the field of industrial systems.

1.3 Glossary

FMECA
: Failure Modes, Effects and Criticality Analysis. This is a quality management and operational safety tool.

PLC
: Programmable Logic Controller. This is a piece of equipment with a set of inputs/outputs, to which sensors and actuators are connected and which executes a program cyclically in order to manage an industrial process.

Conduit
: Logical grouping of communication channels with shared security requirements connecting two or more zones (IEC 62443 definition [9]).

ERP
: Enterprise Resource Planning. Computer system for managing the planning process, production monitoring, stock management, etc.

CMMS
: Computerised Maintenance Management System. Industrial maintenance software for managing equipment maintenance operations (preventive or corrective), inventory management, etc.

IT
: Information Technology. This acronym is used in the document to refer to the "management" computing that drives corporate information systems. In the case of industrial systems, IT is used in levels 3.5, 4 and 5 of the Purdue model [1].

MES

Manufacturing Execution System. Computer system enabling the acquisition of production data, resource management, quality control, maintenance management, product and batch routing, product traceability, etc.

OT

Operational Technology. This acronym is used in the document to refer to the technology used from level 0 to level 3 of the Purdue model [1] to control and operate physical systems (e.g. in the fields of energy transport, transport of people or goods, manufacturing industry, building management systems or water purification).

Maintenance station

Component enabling interaction with the control system (SCADA) and all of the PLCs for the purpose of carrying out maintenance operations and, if necessary, modifying the configuration of the PLCs.

SCADA

Supervisory Control And Data Acquisition. Set of IT resources enabling operators and technicians to implement functional supervision and control, either remotely or locally, of the technical installations on one or more sites.

Information

Outside Europe, the term SCADA refers to a comprehensive system for controlling an industrial facility, including PLCs, sensors and actuators.

SIS

Safety Instrumented System. This is an automated component that performs functional safety functions to protect people and property, based on the principles of reliability, availability, maintainability and safety (RAMS). These functions stem from operational safety requirements and should not be confused with cybersecurity.

SL

Security Level. According to the definition in IEC 62443, the SL is an indicator identifying a set of measures which contribute to reducing the level of risks relating to a system (SUC), a safety zone or a conduit.

IT security

Information Technology Security. All of the technical and non-technical means of protection enabling an information system to ensure the availability, integrity and confidentiality of the data, processed or transmitted, and of the related services that these systems provide or make accessible.

Engineering station

This equipment enables, among other functions, the programming of the control system (SCADA) and programmable logic controllers (PLC).

SUC

System Under Consideration. System under consideration. As defined in IEC 62443, this is a set of industrial system assets required to provide a complete automation solution, including any relevant elements of the network infrastructure.

Zone

As defined in IEC 62443, a zone is a group of subsystems or components sharing the same security requirements. It is therefore a set of logical or physical assets that represent the division of a system under consideration (SUC) on the basis of their common security requirements, their criticality level (e.g. high financial impact or impact on health, safety or the environment), their functionalities and their logical and physical relationships (including their location).

2
Context and Challenges of Industrial System Cybersecurity

Industrial systems are facing constantly evolving threats driven by geopolitical events and the evolution of cyber crime. Securing these systems is a major challenge given the growing scope and inherent risk of the physical processes that they control. It is important to understand the context in which industrial systems evolve in order to understand the challenges of securing them.

Objective

To present an overview of the threats targeting industrial systems and their potential impact.

2.1 Misconceptions and realities of industrial systems

2.1.1 Realities of corporate systems and industrial systems

Although they increasingly use of standardised technologies derived from business or management IT, industrial systems have their own specific characteristics for the contexts in which they are used. They differ from corporate information systems in that they manage physical systems (production units and lines, water and energy distribution units, road and rail infrastructure, etc.). Some also provide protection for people, property and the environment.

	Corporate systems	Industrial systems
System objectives	Process data	Control physical systems, regulate processes and gather and process data
Functional aspects	Business constraints, confidentiality and privacy constraints and system load constraints Business constraints and “real-time”, functional security and high availability (24/7) constraints	
Technical personnel	Computer scientists	Automation engineers, instrumentation specialists, electrical technicians and process engineering specialists
Physical environment	Air-conditioned server room, office or even home	Production workshops: dust, temperature, vibrations, electromagnetism, nearby harmful products , external environment, etc.
Geographic - location	Mostly in enclosed environments (office, home in the case of teleworking)	In warehouses, factories, on public roads, in the countryside (pumping stations, electricity substations, etc.), in isolated locations, at sea, in the air and in space
Service life	About 5 years	More than 10 years (sometimes 30 or 40 years)
Incident - management	Post-incident analysis	The multitude of parameters and the complexity of the environment make it more difficult to reproduce the incident
Components	Standard systems, systems ”hardened” against cyber attacks	“Real-time” systems that can withstand the harsh conditions of industrial environments
Heterogeneity of components	Component compatibility is a technical requirement (homogeneity and interoperability)	The long service life of equipment results in the “superposition” of successive technological waves at the same site, leading to hardware and software obsolescence

Table 1 – Duality of corporate systems and industrial systems

2.1.2 Misconceptions surrounding industrial system cybersecurity

There are a number of misconceptions about industrial systems. The most commonly accepted are reviewed below.

Misconceptions	Realities
"Industrial networks are isolated; they are protected."	Industrial information systems are often connected to the management networks and sometimes directly to the Internet. USB flash drives and maintenance consoles are also major drivers of the spread of viruses, including on isolated systems. The growing need for data feedback to the corporate system will eventually render the air-gapped isolation of industrial networks a utopian concept.
"The protocols and databases used are proprietary, which is a guarantee of protection".	Proprietary solutions are just as attractive to attackers as open standards, and are not inherently more difficult to hack. They may contain vulnerabilities or may not have even undergone any security analysis. Moreover, even proprietary solutions include standard components for reasons of interoperability (with the operating system, for example) and lower cost.
"The integration of security mechanisms (encryption, filtering, authentication) is incompatible with the required time constraints ."	Component performance is no longer a hindrance to the deployment of security functions. On the other hand, there are difficulties: "real-time" systems or management of certificate durations (risk of production interruption in the event of expiry).
"IT security is incompatible with operational safety."	On the contrary, IT security and operational safety share many commonalities. See chapter 3.
"Operational safety measures such as heterogeneous redundancy protect against availability attacks".	This principle is being applied increasingly less as it is very expensive. In addition, products from different manufacturers sometimes rely on the same technologies and incorporate the same hardware and software components. In this case, they contain identical vulnerabilities.
"IT security is expensive".	IT security must be proportionate to that at stake. It will cost less if given appropriate consideration in the early stages of projects. The cost is generally lower than all of the costs associated with a cyber attack, such as the loss of turnover, the cost of rebuilding the information system or the loss of markets.

Misconceptions	Realities
"An attack on the industrial system will always have less impact than a physical incident (theft of cables, fire, etc.) or a terrorist attack (explosion of an oil storage tank in a refinery, for example)."	A cyber attack can cause direct damage to industrial facilities. An attack can cause a global malfunction of facilities that is harder to identify and more harmful (industrial sabotage, slowdown in production) than a physical attack that could result in a very long recovery time. The malfunctions caused may become an aggravating factor and result in an industrial, human or ecological disaster.
"IT security will make work less efficient".	IT security must focus on the critical issues. Its purpose is not to block useful behaviours, but to prevent dangerous behaviours (which requires identifying them beforehand). IT security sometimes requires formalisation of measures to bypass nominal operating modes (degraded operating modes).

Table 2 – Misconceptions surrounding industrial systems

2.2 Cybersecurity issues facing industrial systems

2.2.1 Threats and objectives of attackers

Industrial systems are increasingly being targeted by attackers. Availability problems (ranging from a simple slowdown to the interruption of service) may have serious human and financial consequences. In addition, targeted attacks may lead to accidents.

Developments in technology and, in particular, the advent of Industry 4.0, are driving industrial systems integrating operational technologies to interconnect with corporate information systems, and even with the Internet. This interconnection contributes to an increased attack surface in industrial control systems, which were designed to operate in isolation.

Attack campaigns aimed at espionage are a constant threat over time. A number of state-sponsored attacker groups have the technical capability to target industrial control systems. Campaigns aimed at obtaining industrial data or conducting reconnaissance on industrial networks (such as the size and organisation of the network) have been observed [11]. Pre-positioning and destabilisation through cyber sabotage, affecting electrical networks and production units in particular, are serious threats that generally arise in the context of international tension. Several states have reportedly already implemented pre-positioning measures on electrical grids.

The transition to Industry 4.0 presents several cybersecurity risks:

- the use of unsecured or poorly secured protocols gives attackers the opportunity to modify and inject traffic or to retrieve login credentials circulating in clear text on the network;

- the increase in the volume of information that can be transported over networks can make it difficult to control acceptable values, thereby enabling *buffer overflow* or distributed denial-of-service (DDoS) attacks;
- wireless technologies used without protective measures expose industrial systems to more availability issues (signal interference) than wired infrastructure and allow them to be compromised (e.g. injection of malicious traffic, frame modification);
- ”historic” equipment and protocols that were physically isolated (*air gapped*) are now accessible through other equipment connected to the corporate network (IT), either directly or via communication gateways;
- greater automation of actions related to industrial processes can lead to increased risks in the event of poor decision-making without human oversight (which can occur in a scenario in which data from outside the industrial information system is directly injected into the information system to control part of the process) and, in the longer term, a loss of control and governance of this same industrial process by the business teams.

Major cyber attacks on industrial systems have been carried out by specifically exploiting the OT protocols or solutions of the victim entity, demonstrating a significant reconnaissance phase applied to the chosen target's information system. The most visible attacks on industrial systems have been motivated by sabotage intentions. However, motives such as espionage and data theft are becoming increasingly common.

Cybercriminal groups and ransomware pose an additional threat to industrial systems. The critical need for business continuity in industrial systems is seen by attackers as an advantage in obtaining ransom payments. The ANSSI is aware of several French entities that have been targeted in this way in recent years [11].

In addition, internal malicious activity can be considered a limited threat, but it can have a significant impact on the functioning of industrial systems. The technical skills of employees who are familiar with the operation of the industrial systems they are responsible for can then be exploited for malicious purposes.

In order to respond to these threats as effectively as possible, operators must adhere to best practices for securing their corporate and industrial information systems to ensure the continuity of their operations, but also to increase their compliance with applicable laws. Safeguarding industrial systems against cyber attacks must therefore be a top priority for economic stakeholders.

2.2.2 Human negligence

Negligence is not the result of malicious action, but its effects can be similar to those of an attack (for example, an employee deliberately disregarding security instructions to “make their work easier”). It can create vulnerabilities that are difficult to identify, which could be exploited by attackers or simply affect system availability. For example, unintentional changes to control settings or alert modifications can have disastrous consequences for the quality of products and services delivered, the environment and human health and safety. For instance, using a USB flash drive – whether personal or otherwise – to transfer data between isolated industrial systems can lead to system unavailability if it holds malicious code.
This negligence may be due to a lack of staff training and information on IT security issues.

2.2.3 Vulnerabilities of industrial information systems

Vulnerabilities can have multiple causes, and the aim of this guide is not to list them all.
The growing need to consolidate company data, access it in real time from anywhere in the world, reduce development and ownership costs and meet tight deadlines has accelerated the convergence of industrial IT and corporate IT.

Development, maintenance and remote maintenance tools are now fully developed using generic components derived from corporate IT.
System standardisation and new functionalities have transferred the vulnerabilities of the corporate IT world to industrial systems. Proprietary systems, which often lack security mechanisms, are not immune to vulnerabilities that can be exploited by motivated, organised attackers.
While the corporate IT world manages to regularly fix vulnerabilities, namely by applying patches published by manufacturers and software publishers, the industrial world is unable to adopt the same level of protection under the same conditions (responsiveness, qualification procedures, roll-back processes, etc.) due to its functional security constraints. This difference in responsiveness to public vulnerabilities is one of the main risks facing industrial information systems.
Other major sources of vulnerability include a lack of training for personnel, cultural differences and a lack of awareness of the risks associated with IT security.

Information

Industrial systems required to meet a high level of functional security (e.g. SIL4 level according to IEC 61508 [10]) follow development and validation processes (in accordance with IEC 24772 [12]), which reduce the impact of certain cyber attacks.

2.2.4 Potential impacts on industrial systems

There are numerous incidents involving industrial systems every year. Most receive little media coverage, with only a few attracting greater attention. Such was the case, for example, with incidents targeting nuclear power plants in the United Kingdom (associated with the Conficker worm) and the United States (associated with the Slammer worm), the widespread propagation of the Stuxnet [1] worm in 2010 and the Triton *malware* that targeted *Schneider Electric* SIS equipment in 2017. Their impact can be analysed from a number of angles, as shown in table 3.

1. Stuxnet is a malicious code targeting industrial systems. It exploits multiple vulnerabilities in the *Microsoft Windows* operating system and the SIEMENS *WinCC* SCADA software package. The malicious code modifies the program executed by certain industrial PLCs in the SIEMENS *Simatic S7* product range. The modifications made can lead to a slowdown in production, but also to the physical destruction of the installations controlled by the PLC.

Property damage/bodily injury	Modifying the nominal configurations of installations can cause physical damage, most often with material consequences, but sometimes also with human consequences.
Loss of turnover	The interruption of production generates significant losses of earnings. Modifying manufacturing parameters, leading to non-compliant products, can result in significant losses.
Environmental impact	System failure following a malicious takeover can cause equipment malfunction (opening of valves containing pollutants) and lead to pollution of the site and its environment.
Data theft	Loss of manufacturing secrets, counterfeiting, competitive advantage, hacktivist threats with damage to reputation through the disclosure of sensitive information.
Criminal/civil liability - Image and notoriety	Service unavailability, such as power or water outages, as well as the supply of defective products that endanger consumers, can result in lawsuits for damages or simply be detrimental to the company's image (customer satisfaction and trust).

Table 3 – Potential impacts on industrial systems

3
IT Security Approach Applied to Industrial Systems

The IT security approach must be tailored to its implementation context. For industrial systems, it should align with the specific characteristics of the sector in order to ensure that IT security is taken into account without compromising operational safety.

Objective

To present an IT security approach tailored to industrial systems.

3.1 IT security deployment method

Sometimes perceived solely as a constraint, IT security does in fact help to improve the robustness of equipment and business productivity. Deploying IT security in industrial systems involves considering the threats (organisational, hardware and software aspects) and putting in place mechanisms and procedures (human aspects) as part of security policies to ensure the continuity of business functions at an acceptable level.

The deployment of IT security can be organised around the following themes:

- **Awareness**: A significant proportion of incidents are linked to a lack of awareness of the risks associated with the system. Raising awareness of "digital hygiene" [2] rules significantly reduces vulnerabilities and the risk of attacks. This awareness raising must be ongoing because the risks and the people involved are constantly changing.
- **Mapping**: An inventory, extracted from the mapping, will specify the critical hardware, systems and applications. This is an essential prerequisite for establishing secure information systems in industrial installations. This inventory, the first step in the risk analysis process, will enable the various levels of criticality, functional safety, availability or integrity expected to be defined for the mapped elements.

Information

A five-step mapping guide is available on the ANSSI website [3].

- **Risk analysis**: Each project must include a risk analysis to identify the critical elements of the system, feared events and security objectives in the face of identified threats. These objectives are then broken down into security requirements, which relate to the system itself (intrinsic robustness) and its design, construction and operating environment. These requirements are then translated into technical, physical and organisational measures.

Information

A guide to developing a risk analysis in five workshops (EBIOS method **Risk Manager**) is available on the ANSSI website [5].

- **Defense In Depth**: Defense In Depth involves protecting systems by surrounding them with several protective barriers, independent of each other, so that the failure of one can be compensated for by another. They may be technological or linked to organisational procedures. Adopting a Defense-In-Depth approach means protecting against threats that are not yet known, reducing the perimeter within which a threat occurs or mitigating its impact. The Defense-In-Depth strategy must incorporate not only preventive measures, but also surveillance, detection and response measures.
- **Incident detection**: In an industrial environment, deploying certain protective measures may be difficult (or even infeasible) without disrupting operations. Countermeasures should include mechanisms for monitoring systems and detecting incidents. Gathering information from alert and event logs is essential for detecting attacks and for subsequent analysis in the event of an incident. Properly configured, these logs can provide useful information, and even evidence in a criminal investigation.

Warning

These measures will not prevent an incident, but they will help detect it, limit its impact as much as possible and identify a threat.

Information

For more information, please refer to the industrial systems detection doctrine [4].

- **Incident response, alert chain**: A detection system is only sensible if it is combined with the implementation of a plan and procedures for handling incidents. When a security incident is detected, the right actions need to be taken. An escalation process must be defined to manage incidents at the right level of responsibility and make the appropriate decisions on whether to trigger an incident response plan (IRP), a business continuity plan (BCP) and then a disaster recovery plan (DRP), and whether legal action is required. Incident management must also include a post-incident analysis phase for the purpose of improving the effectiveness of the IT security measures initially deployed.

Information

The ANSSI has published three guides to help companies implement and manage remediation measures [13].

- **Business continuity plan (BCP) and disaster recovery plan (DRP)**: Preparing for feared events helps to mitigate their impact and minimise recovery time. The company's BCP and DRP must integrate industrial systems by identifying the resources and procedures needed to maintain and resume nominal business in the event of an incident.

Information

The BCP and DRP must be adapted to the constraints imposed by the industrial systems. They must be updated and tested during periods of operational maintenance so as not to risk disrupting the system during production.

- **Threat and vulnerability watch**: Keeping abreast of evolving threats and vulnerabilities and their potential impact is a fundamental defence measure. Firmware updates for industrial equipment and patches for operating systems and applications are the subject of security alerts and notices available on the CERT-FR [2] website. Vulnerabilities specific to industrial systems currently fall under the SCADA category.

Information

Suppliers of industrial equipment regularly publish security bulletins, via their own communication channels, providing precise information on the implementation of patches specific to their equipment.

3.2 A global IT/OT approach

IT security cannot be properly addressed on an emergency, ad hoc or isolated basis. It is a process that needs to be planned, and requires multiple resources and skills, as well as strong commitment at the highest level of the hierarchy.

3.2.1 Commitment at all levels

In industrial systems, the worlds of IT and OT coexist, each with their own specific characteristics and constraints. Nevertheless, the IT security approach must be comprehensive. It can be based on the security standards of existing information systems, taking into account constraints specific to industrial systems. Like all information systems, industrial information systems must be integrated into the company's security policies right from the start of the project.

2. https://www.cert.ssi.gouv.fr/

Warning

Although many security issues are common to both IT and OT, implementing OT solutions requires them to be tailored to the industrial context and its constraints.

Projects to deploy security on industrial systems cannot succeed without the involvement of management at the highest level of the company.

3.2.2 Consideration of IT security in projects

The security of the system must be considered from the outset of the project by the owner of the equipment (or the operator in the case of a delegated public service, for example), who must indicate its cybersecurity requirements. For the various phases of a project, a number of recommendations are set out in the ANSSI guide on detailed measures for the cybersecurity of industrial systems [6].

Information

The earlier cybersecurity is taken into account in a project and integrated as an initial component of the business need, the less costly it will be to the project.

4
Industrial Information System Classes

Not all industrial systems are equally critical. While some perform functions where the slightest failure could result in the loss of human life, others on the same site may, at most, cause discomfort to those involved. Efforts to secure them should therefore be tailored to the potential impacts of an attack. To achieve this, it has been suggested that cybersecurity classes be defined based on systems' criticality levels, with associated recommendations.

Objective

To define four cybersecurity classes for industrial systems, followed by the method for determining the class of an industrial system based on its maximum potential impact.

4.1 Cybersecurity classes for industrial systems

It is suggested that industrial systems be classified into four categories indicating their security needs. Such needs are directly linked to the maximum impact that a major malfunction may have.

Cybersecurity class

A cybersecurity class is defined according to the severity of the consequences for the Nation in terms of the impact on the population, the economy and the environment. The maximum impact anticipated is the sum of the most pessimistic theoretical consequences that may result from an act of IT sabotage. This corresponds to the feared events found in the (functional safety) security reference standards used in the industrial sector, limited to those that are the direct or indirect consequence of a cyber attack. For example, purely electromechanical containment enclosures and safety controllers help to reduce the anticipated impact of cyber attacks. The class is determined before countermeasures or provisional measures are put in place to limit the consequences.

4.1.1 Presentation of the classification

The classification method uses terms and concepts found in the initial steps of the risk analysis methods. For example, the EBIOS RM method [**?**], workshop 1 "Scope and security basis" involves

identifying the feared events and the severity of their impact. In the rest of the chapter, tables are provided for estimating impacts. The industrial classification is determined on the basis of these impacts.

This classification can be applied to a site as a whole, a more specific part of the site or an industrial system spread across several sites. This will be detailed in the perimeter description in section 4.2.1. Each responsible entity is responsible for defining the specific perimeter of the industrial system in question.

Version 1.0 of this guide proposed three classes based on impact and likelihood. Likelihood is the subjective probability of occurrence determined on the basis of empirical formulas involving the threat (internal and external) and the industrial system's exposure. However, with this previous method, systems were too often defined as class 3.
One of the reasons was a feedback loop caused by likelihood-based reasoning: as the architecture of the industrial system incorporated IT security measures, the likelihood of an attack decreased, which in turn lowered the system's classification. To avoid this feedback loop from recurring, it was common practice to keep the likelihood consistent (even though it varies depending on context). However, for an industrial system whose functions do not change, it is preferable to keep the class consistent so that the appropriate security measure reference standard can be clearly determined. On the other hand, there is excessive fluctuation in likelihood over time, while the classification proposed here aims to determine long-term security mechanisms.

There is no direct equivalence between the four classes defined in this guide and the security levels (*SL*) for standard IEC 62443 [9]. This standard determines security levels according to the level of threat (opportunistic, criminal or state-related), while cybersecurity classes correspond to the criticality of the impacts. However, the impacts of cyber attacks are considered latent threats, and the detailed measures for each class are linked to the requirements of standard IEC 62443. Class 1 or 2 measures focus on resilience, i.e. the ability to overcome a breakdown or cyber attack and to restore and restart the systems, while class 3 or 4 measures focus on the need to survive an attack for the most critical systems.

Information

The security policy applied on an industrial site is based on a risk analysis subject to regular updates to take account of the threat assessment. In fact, the risk of occurrence of a feared event (R) depends on the severity of its impact (G) and its likelihood (V): $R = I \times V$. Likelihood is updated according to the current risk analysis based on the threat (political and geopolitical contexts and perception of the cyber threat) and exposure (attack surface, uncorrected vulnerabilities, etc.).
Therefore, from a security policy perspective, likelihood, which is not taken into account in this classification, remains a key criterion in the risk analysis, especially if it involves attack scenarios.

Warning

With an appropriate security policy, it should be possible to swiftly (within a few hours) switch from a nominal situation to an alert situation with reinforced checks

when the threat assessment and degree of exposure of the industrial information system so require.

4.1.2 Definition of cybersecurity classes

Defined by the ANSSI, the four cybersecurity classes for operational systems used to control and operate industrial processes are as follows:

Class 1: These are industrial systems for which the impact of an attack would be low.

Class 2: These are industrial systems for which the impact of an attack would be moderate. There is no state control for these systems, but the responsible entity must be able to prove that appropriate measures have been implemented in the event of an inspection or incident.

Class 3: These are industrial systems for which the impact of an attack would be high. The detailed security measures are reinforced in this class, and it is recommended that a qualified body check the compliance of these industrial systems.

Class 4: These are industrial systems for which the impact of an attack would be catastrophic. The detailed security measures are strongest in this class, and it is recommended that a qualified body check the compliance of these industrial systems.

Each new class reinforces the measures of the lower class(es), with some exceptions.

Warning

Any functional or technical modifications to an industrial system, excluding measures specifically related to security itself, require a review of the cybersecurity class estimate.

4.2 Determination of the class

4.2.1 Perimeter

A perimeter must be chosen containing all of the critical systems of a site or infrastructure (networks, transport, electricity, etc.). Conversely, it is possible to divide a site into multiple industrial systems with the potential for varying levels of criticality. The choice of perimeter must be consistent based on the risk and architecture of the systems being analysed.

Warning

If it is decided to split an infrastructure into multiple industrial systems, a global risk analysis must be carried out to ensure that all threats have been taken into account, including those that could result from the infrastructure as a whole.

Functional safety analyses, which have often already been conducted by the responsible entities, can serve as a basis for work. The breakdown of systems and the processes that they support have already been defined. However, they should be updated, taking into account the common methods used in cyber attacks in particular. Due to its non-physical nature, a cyber attack on one piece of equipment can easily be replicated across all equipment with the same vulnerability because, for example, they share the same software component. This means that two physically redundant systems must be considered as being attacked at the same time, unlike functional redundancy.

The method is applied sequentially:

- It is initially applied to an entire infrastructure or site in order to identify the highest class level that must be met.
- Then, once the functional architecture has been established, the method is applied to smaller subsets. These subsets are sometimes referred to as ”zones” in the literature and in standard IEC 62443 [9] in particular.

Given the potential impact of certain measures, it is important to determine the exact perimeter of the project. For example, a poorly defined perimeter could result in class 3 measures being imposed on class 2 industrial systems.

Information

For example, an upper-tier SEVESO site will generally be class 3 (or even 4). By refining the classification of industrial systems, it will undoubtedly become apparent that only systems for the protection of property and people should be classified as class 3. Some production systems may only be class 2.

4.2.2 Criticality assessment

When assessing the criticality of an industrial system, only two security criteria are primarily considered – namely availability and integrity – which are closely linked to operational safety. Depending on the sector, it will be possible to add other security criteria, such as confidentiality, traceability and accountability, but these are not taken into account in this guide.

The class applied to the industrial system is determined by the greatest impact of the worst feared event. The severity of an impact is assessed on the basis of a four-level impact scale (ei): minor, moderate, major and catastrophic. Multiple scales are needed to measure the severity of the impact of a feared event (er). The impacts considered are human, environmental, macroeconomic and possibly economic. The levels are provided in the tables 4, 5, 6, and 7.

Information

The decision to have an even number of severity levels means a position must be taken, avoiding the trap of the “safe zone” of indecision in the middle.

The choice of class, which can be intuitively understood on the basis of the maximum level of impact of the feared events, is formally written as follows:

$$\text{Class} = \max_{\forall ei, \forall er} \text{Level}_{ei}(er)$$

Where ei is an impact level scale from among all proposed impact scales, and er is a feared event from among all of the events considered in the risk study. The $\text{Level}_{ei}(er)$ is determined using the impact scale ei, based on the assessed impact of event er.

In some industrial sectors, security or operational safety analyses are used to demonstrate independence from feared events. This means that a physical attack on an industrial system can be considered independent of attacks on other systems of the same type from a certain distance. These assumptions are no longer valid in the event of a cyber attack on networked systems with identical interfaces: an attack on one of them is generally considered an attack on all of the systems at the same time by way of the same operational scenario. This is illustrated by the case study in section 6.4.

Warning

The impacts must take into account the common methods used in cyber attacks: in the case of distributed industrial systems with standardised interfaces, the impact of an attack from a computer network is the impact resulting from the attack on all equivalent systems, which are equally vulnerable. **This leads to a significantly stronger class for small systems, which are largely spread across the country**. This point is illustrated in section 6.4.

4.3 Severity scales

The tables below show the severity scales for human, environmental and unavailability impacts for the community.

Information

Depending on the business sector, it is possible to add an extra scale for the impacts on turnover for the company.

The scale of economic impact is left to the discretion of the owner or operator of the system. It may reflect the economic context of the industrial system. The consequences must be described in figures (in euros, dollars,

- physical loss, replacement, repair or destruction of equipment;
- lost earnings;
- economic sanctions.

Impacts are largely dependent on the sector involved. The scales therefore need to be adapted and specified for each business sector. For sectors of vital importance, Article L1332-3 of the French Defence Code (see document [7]) provides a definition of additional criteria. A sector deemed

strategic may have greater economic impact. In addition, Article L511-1 of the French Environment Code (see document [8]) also specifies impacts. Lastly, if an FMECA analysis has been conducted, use of the severity scales identified therein is recommended.

Warning

Adapting impact severity scales to the specific sector must not significantly reduce the levels outlined here. This would lead to an underestimation of the class and consequently the security measures to be implemented.

Severity	Qualificative	Human consequences
1 cline1-3 2	Minor Moderate	Reported accident with time off work or medical treatment. Permanent disability.
3	Major	One death.
4	Catastrophic	Several deaths.

Table 4 – Severity of human impacts

Severity	Qualificative	Environmental consequences
1	Minor	Exceeding a discharge standard, which must be reported to the authorities, but with no environmental impact.
2	Moderate	Moderate pollution limited to the site.
3	Major	Significant pollution or pollution outside the site. Evacuation of people.
4	Catastrophic	Major pollution with lasting environmental consequences outside the site.

Table 5 – Severity of environmental impacts

Severity	Qualificative	Macroeconomic consequences
1	Minor	Significant impact on 10,000 people. Disruption to the local economy.
2	Moderate	Significant impact on 100,000 people. Disruption to the regional economy. Temporary loss of major infrastructure.
3	Major	Significant impact on 1,000,000 people. Disruption to the national economy. Temporary loss of critical infrastructure. Permanent loss of major infrastructure.
4	Catastrophic	Significant impact on 10,000,000 people. Permanent loss of critical infrastructure.

Table 6 – Severity of macroeconomic impacts resulting from service unavailability

Severity	Qualificative	Economic consequences
1	Minor	Impact less than ***XX,XXX*** euros.
2	Moderate	Economic impacts of at least ***XXX,XXX*** euros.
3	Major	Economic impacts of at least ***X,XXX,XXX*** euros.
4	Catastrophic	Economic impacts of at least ***XX,XXX,XXX*** euros or resulting in the cessation of activity.

Table 7 – Severity of economic impacts for the industrial system owner

5
Classification Method

Various elements must be considered in this classification method. To facilitate its implementation, the classification process and procedures are detailed below.

Objective

This chapter presents the method used to classify an industrial information system in order to determine its cybersecurity class and define a baseline for security measures. This method relies on a preliminary study to identify the feared events, among other things.

This classification method is aligned with the EBIOS RM method to enable risk to be controlled throughout the industrial system. Given that the classification method is autonomous, other methods for identifying feared events may be used.

As a reminder, the EBIOS RM workshops are as follows:

1. **Workshop 1** - Scope and security baseline
   - Steps:
     a. define the scope of the study;
     b. define the business and technical perimeter of the studied object and the supporting assets;
     c. identify the feared events and assess their level of severity;
     e. determine the security baseline and assess its compliance.
   - Outputs:
     a. framework elements: objectives of the study, roles and responsibilities, timeframe;
     b. business and technical perimeter: tasks, business assets, supporting assets, etc;
     c. feared events and their level of severity;
     d. security baseline: list of applicable requirements, implementation status, gap identification and justification.
2. **Workshop 2** - Risk origins (RO)/target objectives (TO)
3. **Workshop 3** - Strategic scenarios
4. **Workshop 4** - Operational scenarios
5. **Workshop 5** - Risk treatment

Information

The activities involved in the classification method are part of Workshop 1 in the EBIOS RM method.

"as defined in"

This term means that the referenced EBIOS RM activity can be carried out without modification as part of the classification method.

"using"

This term means that additional instructions must be taken into account when performing the EBIOS RM activity as part of the classification method.

The activities to be carried out as part of the classification method are the following:

1. **Activity 1.** Defining the framework of the study using EBIOS RM - Workshop 1.a and Workshop 1.b (section 5.1).
2. **Activity 2.** Establishing zones within the perimeter (section 5.3).
3. **Activity 3.** Identifying the feared events (section 4.3), using EBIOS RM – Workshop 1.c, and determining the classes.

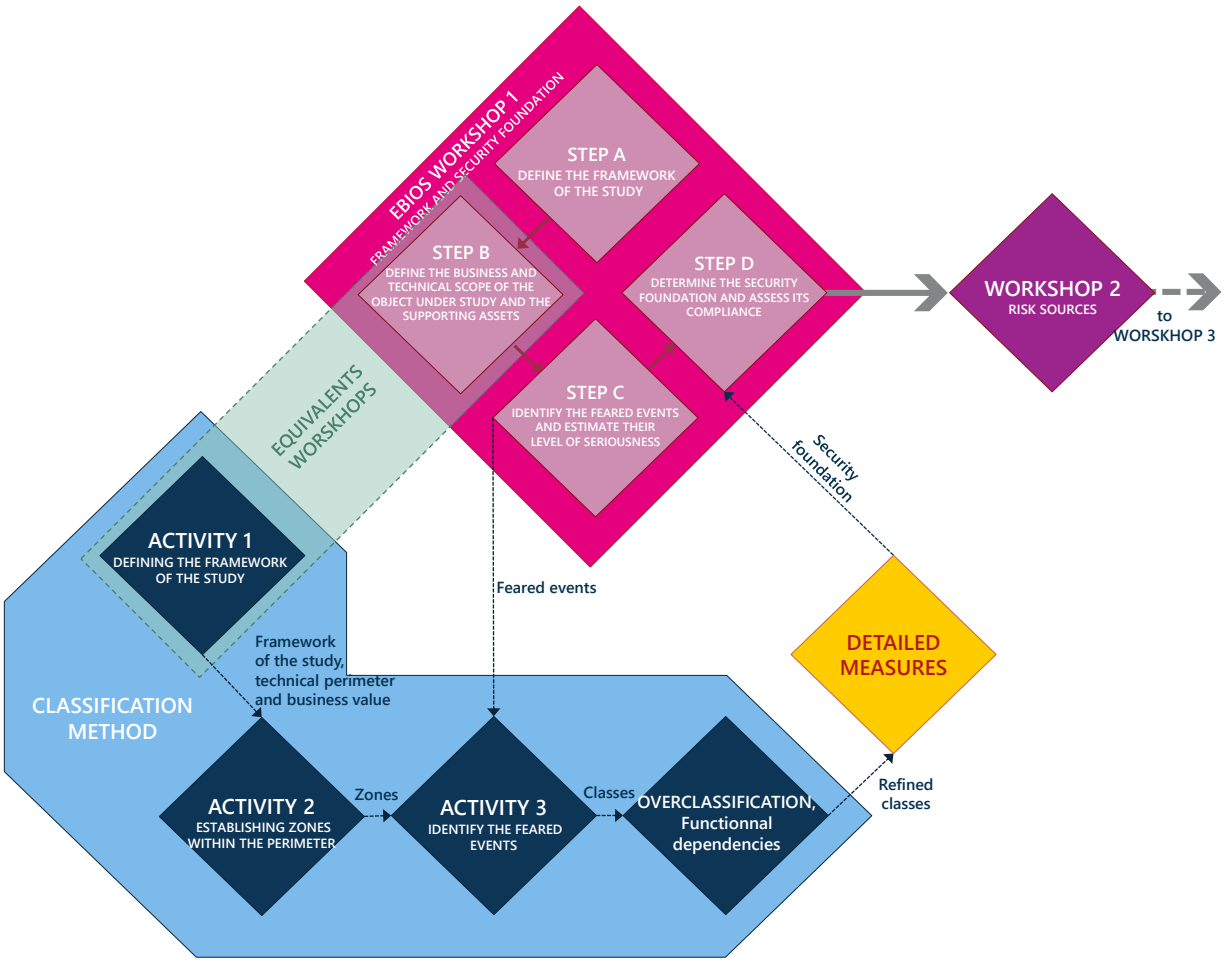

Figure 1 – Classification method associated with the EBIOS RM approach

5.1 Activity 1 - Defining the framework of the study

5.1.1 Objective

The objective of this activity is to identify the perimeter of the information system of industrial equipment, and to break it down into zones for which the severity of impacts will be assessed in the next activity involved in this method.

Information

For example, IEC 62443 [9] proposes defining a perimeter known as the System Under Consideration (SUC), which is described in section 3-2 of the regulatory requirements. An SUC consists of one or more zones and the corresponding conduits (see the definition of zones and conduits according to IEC 62443 in the glossary in this guide in section 1.3).

5.1.2 Reference to EBIOS RM

This activity is based on EBIOS RM - Workshop 1.a and Workshop 1.b. First, carry out the activities as suggested in EBIOS RM. Additional information specific to industrial systems is given in section 5.1.4.

5.1.3 Output data

This activity produces the following outputs:

- framework of the study;
- perimeter of the study;
- tasks and business assets.

5.1.4 Procedure

5.1.4.1 Define the objectives and assumptions

- Present the main objective of the study, i.e. to establish the security baseline for the industrial system, as well as the secondary objectives. Secondary objectives may include, for example, setting up a cyber risk management process within the organisation, issuing an authorisation to commission an information system or identifying the security level required to achieve regulatory compliance.
- Based on the defined objective, determine the appropriate level of detail and the workshops to be conducted.
- State the assumptions and constraints that must be considered in the analysis.

5.1.4.2 Define the business and technical perimeter

Next, identify the missions, business assets and supporting assets associated with the object of the study.
The questions that may be asked include:

- What is the purpose of the industrial system? What are its main missions, objectives and overall purpose?
- What are the key functions and types of information that enable the industrial system studied to fulfil its missions?
- What digital services (applications, networks, organisational structures, human resources, facilities, etc.) support these functions or process this information?

Warning

Be sure to respect the level of detail chosen for the study, in particular when identifying missions and business assets.

Start by listing **all of the missions** of the industrial system: its core objectives and overarching purpose. Depending on the level of detail of the study, the missions may be specific to the industrial

system, but are more often those of the broader organisation that it serves.
For example:

- what the system produces (paper production, electricity generation, etc.);
- the service that it provides (passenger transport, electricity transmission, safety of goods and people, etc.).

In the same manner, then list all of the business assets associated with the industrial system, i.e. the information or functions considered important to the study and in need of protection. Business assets represent information assets vital to the organisation, which a risk source may seek to attack in order to achieve its own goals (e.g. the protection of people and property, steam production, maintaining the fluid transport network load level, etc.).

The aim is to identify the business assets associated with the industrial system. Unlike EBIOS RM, which does not aim for exhaustiveness and limits the number of business assets to those identified as essential or sensitive, this classification method requires all functions and information in the industrial system to be identified, while respecting the chosen level of detail for the study.

As a general guideline, an industrial system corresponds to one mission and three to five business assets, such as production, supervision, the safety of people and property, etc.

- At this stage, identify the associated equipment (technical perimeter) for each business asset. To do this, you may identify control loops and relevant data for each business asset.
- Map the data flow through your information systems, particularly the systems (on-site or outsourced) that process or store the data. These systems are part of the technical perimeter of the industrial system.

Warning

In the case of a geographically distributed system, ensure that the perimeter includes all sites and infrastructure involved in the industrial process.

5.2 Activity 2 - Establishing zones within the perimeter

5.2.1 Objective

The objective of this activity is to create coherent zones within the previously identified technical perimeter of your organisation. This zoning is not necessarily based on the business assets previously identified.

Information

For example, IEC 62443 [9] specifies the characteristics of zones and conduits in section 3-2 of the regulatory requirements.

5.2.2 Reference to EBIOS RM

This activity is not based on the EBIOS RM method.

5.2.3 Output data

This activity produces the following outputs:

- the criteria used to create the zones;
- the division of the perimeter into zones.

5.2.4 Procedure

Establish the criteria used to define the zones. To do this, identify the industrial system's missions as well as its characteristics.

For example, to define these criteria, the following questions may be asked:

- What does the industrial system produce?
- How does the industrial system affect the industrial process?
- What functions are performed by the industrial system?
- Where will the industrial system be located?
- What populations are involved in the industrial system?
- Which functions are essential to the smooth running of the industrial process?
- Is there an existing (natural or organisational) division of the perimeter?
  Divisions may be the result of:
  - the functional security classification level (e.g. the SIL [3] level) of the equipment (safety PLC or safety relay);
  - usage (e.g. by type of product manufactured by the industrial system);
  - the existing network architecture;
  - the manufacturer (e.g. a set of systems delivered and maintained by the same supplier);
  - the geographical location, particularly in the case of geographically distributed systems;
  - the population managing the systems (e.g. machines under the responsibility of a particular trade group or service provider).

To finish, identify the populations managing the plant's resources, especially:

- those responsible for configuring PLCs (business-side administration) and industrial applications (typically handled by the engineering team);
- those responsible for keeping the plant's IT equipment in operational and secure condition (workstations, servers, network equipment, etc.).

At this point, a set of criteria for establishing zones should emerge. Refine these criteria to obtain zones composed of homogeneous resources administered by the same group.

3. Safety Integrity Level. Safety level of a product or system (defined in IEC 61508).

5.3 Activity 3 – Identifying the feared events and determining their class

5.3.1 Objective

The objective of this activity is to identify the feared events affecting the industrial system, and to determine the class applicable to the zones.

5.3.2 Reference to EBIOS RM

This activity uses EBIOS RM – Workshop 1.c: Identify the feared events and assess their level of severity.
In an EBIOS RM analysis, the degree of harm or impact of feared events is estimated using a severity scale that allows them to be ranked. This is not the case in the classification method. The evaluation of the impact level of feared events should allow such events to be compared between two industrial systems.

5.3.3 Output data

This activity produces the following outputs:

- the feared events and their severity;
- the level of digital involvement for each feared event;
- the class of each zone.

5.3.4 Procedure

In the classification method, feared events are associated with business assets and reflect the harmful effects of a deterioration in service quality or performance to which the business asset must conform.

To identify the feared events, you may, for each business asset identified in the previous activity, consider:

- the feared events taken directly from your organisation's operational safety studies and quality processes. These feared events generally originate from accidental rather than malicious sources;
- the harmful effects of a loss of availability of the business asset (e.g. production halted or service not delivered);
- the harmful effects of a loss of integrity of the business asset (e.g. non-compliant product or process malfunction);
- the harmful effects of a loss of confidentiality (e.g. disclosure of proprietary expertise that creates a competitive advantage);

- the harmful effects of a loss of traceability (e.g. missing batch number for a product);
- the harmful effects of degraded service quality or performance to which the business asset must conform.

Information

- A feared event is described using a short phrase or a scenario that makes it easy to understand the harm associated with compromising the corresponding business asset.
- For feared events affecting availability, it is recommended that the threshold beyond which the stated severity level is reached (e.g. service unavailable for more than two hours or inability to transmit data flows greater than 1 Mbps) be specified. This approach also allows you to incorporate the concept of degraded operation into your risk assessment.
- At this stage, feared events are identified from the organisation's perspective, without reference to any attack scenario. Their severity is estimated independently of the attacker's ability to carry them out.

Next, the severity of each feared event must be assessed using the method proposed in section 4.1.

Information

It is important to ensure that the economic impact scale is clearly defined and adapted to your organisation's context in accordance with table 7. This scale must be adapted to your activity and entity.

For each feared event, identify the level of digital involvement. The questions that may be asked include:

- Can this event be triggered by or from IT or industrial IT equipment, such as a PLC?
- Can this event be facilitated by the use of IT or industrial IT equipment, such as a PLC?

For each zone, identify the feared event with the highest level of severity. This level of severity corresponds to the zone's class.

Likelihood is integrated through the strategic scenarios defined by the EBIOS RM method in accordance with section 5.4 and the case study provided in Appendix B.

Information

If you wish to group zones together, the class of a group of zones is equal to the highest class among them.

5.3.5 Raising the classification

Depending on how the perimeter was initially defined, it may be possible to raise a zone's classification.

For each zone, consider whether raising the classification is appropriate, in particular:

- In the case of geographically distributed facilities, the impact of an event on a single site may be low. However, if the event occurs simultaneously across multiple sites, the overall impact may be significant. In such cases, raising the classification of each site to reflect the maximum impact of the event across all sites, as described in section 6.4.1, is recommended.
- If two zones of different classes cannot be separated at the recommended level (see the detailed security measures guide [6]), raising the classification to the higher class (e.g. in the case of safety instrumented systems (SIS) and standard PLCs that cannot be separated) is recommended.

5.3.6 Functional dependencies

A functional dependency arises when communication needs to be established between two zones. This applies when, to perform a function, one zone depends on data originating from another zone.
The security of the interconnection is ensured in two scenarios:

- If communication is established between two zones of the same class, the associated risk can be considered acceptable.
- Otherwise, the interconnection must be secured as described in the detailed measures guide.

Information

An equivalent principle is described in section 3-2 of IEC 62443 [9]:

- In a zone, a device interconnected to one or more devices inherits the highest security level (SL) from the connected device(s).
- A conduit between two or more distinct zones inherits the highest security level (SL) of the connected zones.

5.4 Conducting an EBIOS RM analysis using the classification method

The following elements help align the two methods:

- Contributing to the security baseline

  Once the classes have been determined, all corresponding applicable measures (see detailed security measures guide [6]) must be included in the EBIOS RM security baseline.

- Operational scenarios

  During Workshops 3 and 4, you define risk scenarios based on “Risk Origin (RO)” and “Target Objective (TO)” pairs. If you wish to perform a simplified risk analysis, these usual modes of operation may be considered partially covered by the security baseline, allowing you to focus on scenarios that exploit specific characteristics of the industrial system studied.

6
Case Study

The previous version of the classification method was put into practice using the case study of a road tunnel. As part of the update of this method, a new case study on a water sanitation network has been included in this guide to illustrate chapters 4 and 5.

Objective

This chapter is a case study aiming to contextualise the classification method by applying it to the context of securing a wastewater and rainwater sanitation network managed by the fictional entity Assaineaux. To keep the chapter concise, the results of certain EBIOS RM workshops have been deliberately omitted.

6.1 Context

6.1.1 Overview of Assaineaux

The sanitation network is operated by a local authority, which created a semi-public company named Assaineaux for this purpose.

The existing sanitation network is currently being renovated. In this context, the company wishes to secure the industrial information system of the various sites that it operates.

6.1.2 Organisation of the sanitation network

The sanitation network is a fictitious system consisting of several wastewater and rainwater treatment plants (WWTP) and rain gauges. These sites are geographically distributed over a 20-kilometre perimeter and collect wastewater and rainwater from a population of approximately 100,000 inhabitants. This system is supervised locally, but also from a remote control station. For the purposes of this study, the control station is not redundant on another site. Figure 2 shows the architecture of this network.

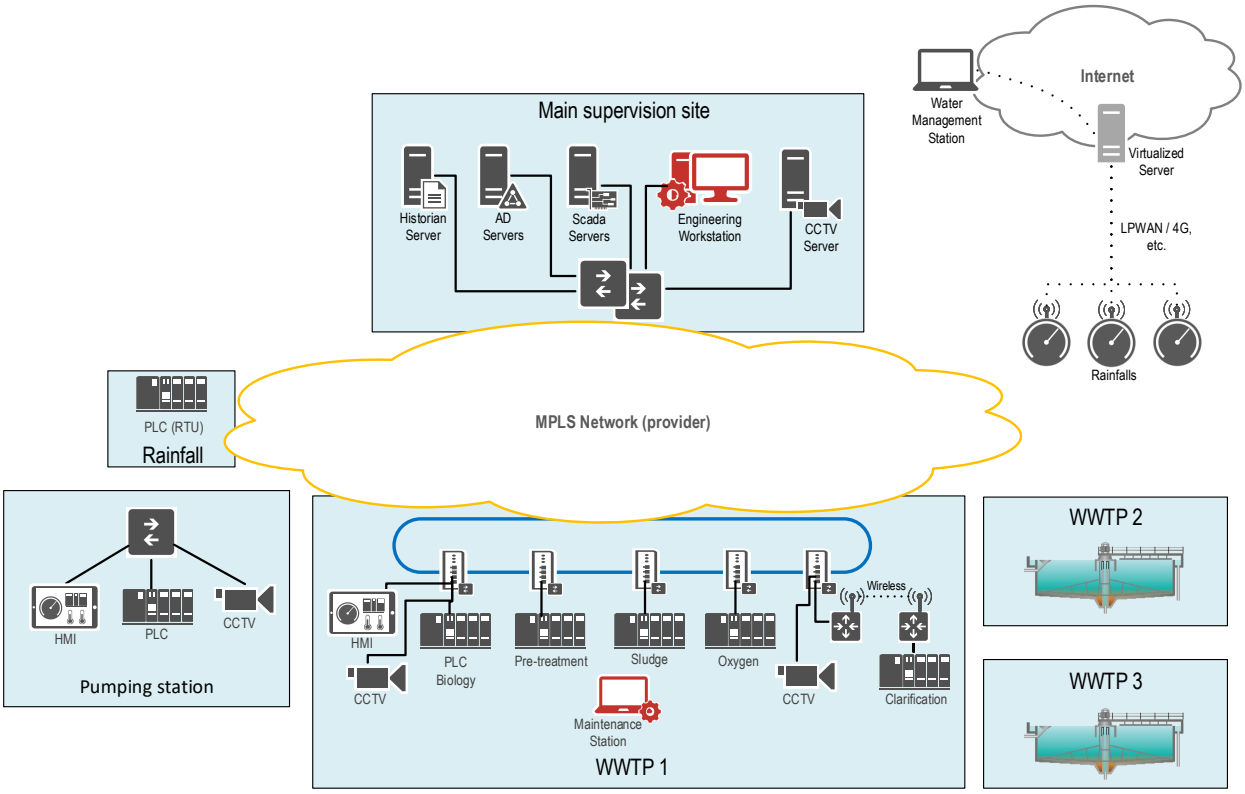

Figure 2 – Sanitation network architecture - 1 technical approach before classification

6.1.3 Definition of the perimeter of the wastewater network

To begin this study, an inventory of the various areas of the sanitation network should be carried out in accordance with section 5.3 (Workshops 1.a and 1.b). These elements have been established on the basis of the questions presented in subsection 5.2.4.

The areas correspond to the following functions:

- **pumping**: this is an active water pumping system to allow continued gravity-fed water flow when the collection point is below the treatment plant;
- **pretreatment**: this is the plant's first treatment. This process protects structures (e.g. pipes and downstream machinery) from the arrival of materials or bulky matter (degritting, degreasing, etc.);
- **oxygenation** (biological treatment): this is a process of producing air in water to enable the development of bacterial biomass. These aerobic bacteria break down organic compounds that can contaminate the water (resulting in secondary sludge);
- **clarification** (clarifier or secondary decanter): this is the final stage of treatment. The aim is to extract the sludge from the micro-organisms in the treated water in order to produce a clarified effluent that complies with discharge standards;
- **sludge recovery**: after the clarification stage, the sludge is then recycled for various applications such as spreading, composting, methanisation or incineration (after drying);

- **deodorisation** (air treatment): this is a system for reducing odours emitted by the treatment plant (not covered in this guide, as specified in section) 6.2.1);
- **rain gauge**: during heavy rainfall, it allows discharge into a storage basin or storm overflow. Rain gauges are also installed to transmit only rainfall information to the local authority, which is linked to them via a cloud service to which the rain gauges are connected (system not covered in this guide, as explained in section 6.2.1);
- **supervision**: supervision involves the management of treatment plants, sanitation network structures and rain gauges;
- **video surveillance**: this is a system consisting of a central station and a number of cameras used to monitor any intrusions on sanitation network sites.

6.2 Integration of elements from Workshop 1 - EBIOS RM

The scope of the study was defined in section 6.1.3. Following the method presented in chapter 5, the risk analyses and the application of Workshop 1 in the EBIOS RM method made it possible to identify, in particular, the feared events, the business assets and the supporting assets. These elements are described in this section.

6.2.1 Business assets

The business assets used in this study are as follows:

- pumping of water from low points to high points;
- water treatment (pretreatment/primary treatment);
- sludge treatment (drying and incineration of sludge and grease).

Information

The business assets *waste recovery*, *transport* (collection and transfer of rainwater to the natural environment, etc.) and *deodorisation* (air treatment) are not used here for the sake of simplifying [4] the study and, in some cases, because no information system is present, and the equipment is predominantly physical (collectors, buses, etc.).

6.2.2 Business asset supporting assets

From a technical perspective, each function may involve a greater or lesser number of components. Without taking into account the possible pooling of certain equipment (including PLCs and HMI consoles), the list of functions and associated components is summarised in table 8.

4. Unavailability or malicious intent regarding these elements has no impact on the feared events.

Business assets	Business asset functions	Supporting assets
Pumping water from low points to high points	**Pumping**	PLC Local HMI Pump and level measurement probe
Water treatment	**Pretreatment**	PLC Local HMI Particle suction pump, bridge scraper motor, level sensor, solenoid valves, flow meter, etc.
	Oxygenation	PLC Local HMI Reagent injectors, air compressor or blower, solenoid valves, agitator, level sensor, measuring sensor O_2 surface turbine, buffer tank, pressure gauge (which controls compressor startup when the pressure falls below a defined threshold), etc.
	Clarification	PLC Local HMI Bridge scraper motor Sludge recirculation and discharge pumps, etc.
	Video surveillance of the site	Video surveillance management server (VMS) Cameras Video surveillance console Recorder
	Monitoring	Control/command system servers Control/command operator station
Sludge treatment	**Sludge recovery**	PLC Local HMI Pumps, flow meter, level sensor, gear motor, compressed air, pressure sensor, solenoid valve, agitator, etc.

Table 8 – Business asset functions

6.2.3 Feared events

As part of the operational safety study, Assaineaux conducted various analyses, including:

- functional analysis and modelling;
- a preliminary risk analysis (PRA) or hazard analysis (HA);
- a failure mode, effects and criticality analysis (FMECA);
- a fault tree.

These various analyses, in particular the fault tree and the system FMECA (or functional FMECA), led to the emergence of functional failure modes: malfunction, loss of function, incorrect function, failure to stop function, etc. They therefore made it possible to identify and characterise the criticality of feared events linked to system function failures.

On the basis of the operational safety analysis, supplemented by Workshop 1.c in the EBIOS RM method, it is possible to draw up a list of feared events grouped together in table 9.

Business assets	Feared events
[Business asset 1] Pumping water from low points to high points	**[ER1]** Destruction of physical assets
[Business asset 2] Water treatment	**[ER1]** Destruction of physical assets
	[ER2] Destruction of biological micro-organisms
	[ER3] Service delivery disruption
	[ER4] Equipment sabotage using ransomware
[Business asset 3] Sludge treatment	**[ER1]** Destruction of physical assets

Table 9 – List of feared events associated with business assets

6.3 Classification

Information

Sufficient oxygen levels in the natural environment (streams, rivers, seas, etc.) must be ensured to maintain aquatic life. Released organic matter feeds micro-organisms. These micro-organisms consume oxygen to grow and break down this pollution, thereby reducing the level of oxygen present in the natural environment. In order to control the environmental risks caused by wastewater, several parameters are monitored:

- chemical oxygen demand (COD). Oxygen-consuming substances are measured. This measurement is used to determine the effect of an effluent on the receiving environment;
- biochemical oxygen demand (BOD). This is the breakdown of organic pollutants by micro-organisms. This measurement is used to determine the effect of an effluent on the natural environment;
- suspended solids (SS). Too many SS can clog up fish gills.

Pumping: A fault in this unit may result in total or partial flooding of the facilities or significant damage to downstream equipment (pump failure or loss of the downstream solenoid valve). Based on the severity scales presented in section 4.3, the result is the following levels:

Human impact: 1 Environmental impact: 2 Macroeconomic impact: 1

Pretreatment:
A fault in this system may have the following consequences:

- a risk of overflow leading to clogged drains;
- toxic biogas emissions at the grease receiving station;
- health risks, contaminated drinking water with nearby water collection points (water production);
- pollution of the natural environment when discharged into the effluent;
- a bad reputation for the local authority;
- a risk of damage to downstream equipment if the water contains too much sand or grease;
- impairment of the biological treatment function.

Human impact: 1 Environmental impact: 2 Macroeconomic impact: 1

Oxygenation: A fault in this unit may result in non-compliance of the discharged water (risk of pollution) due to the degradation of the biological treatment unit (failure of a component in the oxygenation unit).

Human impact: 1 Environmental impact: 2 Macroeconomic impact: 1

Clarification: A fault in this unit may result in non-compliance of the discharged water (risk of pollution) due to the deterioration of the biological treatment unit (failure of a component in the clarification unit or obstruction of the drain by floating elements).

Human impact: 1 Environmental impact: 2 Macroeconomic impact: 1

Information

The discharge of untreated wastewater can pose health risks to both humans and animals if there is a water table nearby. In this study, no wastewater treatment plants or collectors are located near a water table or a borehole for drinking water production.

Video surveillance: The video surveillance system does not interfere with the industrial process or with operators' decisions regarding the control of the facility and is used to detect intrusions into the sanitation network sites. However, an intruder could damage the biomass or even cause a power outage at the site involved.

Human impact: 1 Environmental impact: 2 Macroeconomic impact: 2

Monitoring:
The events that would no longer be visible at the monitoring centre in the event of a failure are:

- alerts for blower or compressor faults;
- alerts for bridge brush, agitator or sensor faults;
- alerts for bridge scraper faults and torque threshold applied to the bridge scraper motor;
- alerts for low tank levels;
- alerts for excessive flow;
- alerts for pump faults;
- visualisation and action on the operation of the various treatment units (status of pumps, solenoid valves, tank levels, flow rates, turbidity level [5], etc.).

The impact of a failure at the central monitoring site is greater if it is combined with a failure on a functional unit. Otherwise, the process remains operational. In addition, some sites are equipped with local monitoring. This results in the elements below.

Human impact: 1 Environmental impact: 1 Macroeconomic impact: 1

Sludge recovery:
A fault in this system may have the following consequences:

- a delay in waste incineration;
- injured or poisoned operators;
- negative reputation for the metropolitan authority (or local authority);
- an inability to determine the quality of exhaust fumes.

Human impact: 2 Environmental impact: 2 Macroeconomic impact: 1

Information

The company's economic criterion was not included in this case study.

Referring to chapter 4 and taking into account the criteria mentioned in section 4.3, the following elements have been selected (in accordance with activity 3 5.3):

Functions	Human impact	Environmental impact	Macroeconomic impact
Pumping	1	**2**	1
Pretreatment	1	**2**	1
Oxygenation	1	**2**	1
Clarification	1	**2**	1
Video surveillance	1	**2**	1

5. Turbidity is one of the parameters that indicate water quality. It refers to the clouding of water caused by suspended matter.

Monitoring	1	1	1
Sludge recovery	**2**	**2**	1

Table 10 – Impacts by function

Taking the above into account, the breakdown of classes is shown in table 11. This classification of functions will be used for the remainder of the analysis.

Classes	**Functions**
Class 1	Monitoring
Class 2	Video surveillance, Pumping, Pretreatment, Oxygenation, Clarification and Sludge recovery
Class 3	None
Class 4	None

Table 11 – Classification of functions

6.4 Refinement and grouping of classes

6.4.1 Consideration of the perimeter (raising the classification)

As specified in section 4.2.1, the perimeter must be chosen so as to contain all of the critical systems of a site or infrastructure. Therefore, **all treatment plants must be included** in this case study. The population served is therefore larger than with a single treatment plant (which raises the classification for the perimeter in question). In fact, when all of the treatment plants managed by the local authority are included, the population to be considered is the entire population served (more than 100,000 inhabitants). The environmental impact for water pollution is therefore 3, and the macroeconomic impact is 2, as specified in table 12.

Information

The “Video Surveillance” function is not affected by this reassessment because an attack on all sites would not directly cause a feared event. Intrusions would have to occur at the same time on all sites in the sanitation network. This is a security measure to protect a system of significant business asset to the entity.

Functions	**Human impact**	**Environmental impact**	**Macroeconomic impact**
Pumping	1	**3**	2
Pretreatment	1	**3**	2
Oxygenation	1	**3**	2
Clarification	1	**3**	2
Video surveillance	1	2	2
Monitoring	1	1	1
Sludge recovery	**2**	**2**	1

Table 12 – Impacts by function after raising the classification

Taking into account the perimeter of all wastewater treatment plants, the distribution of classes is presented in the following table:

Classes	Functions
Class 1	Monitoring
Class 2	Sludge recovery and Video surveillance
Class 3	Pumping, Pretreatment, Oxygenation and Clarification
Class 4	None

Table 13 – Classification of functions with the entire perimeter

6.4.2 Functional dependencies of classes

In addition to the standalone classification of functions, and as outlined in section 5.3.6, the analysis should be supplemented by an examination of the relationships between these functions (the functional dependencies in this study are presented in Appendix A).

The analysis of functional dependencies therefore requires the “Monitoring” and “Sludge recovery” functions to be reclassified as class 3 in accordance with figure 4 presented in Appendix A. A summary is provided in the table below:

Classes	Functions
Classe 1	None
Class 2	Video surveillance
Class 3	Monitoring, Pumping, Pretreatment, Oxygenation, Clarification and Sludge recovery
Class 4	None

Table 14 – Classification of functions with functional dependencies

6.5 Integration of the threat

6.5.1 Strategic scenarios - Workshop 3

Following the method presented in chapter 5, the application of Workshop 2 in the EBIOS RM method enabled a pair (RO/TO) to be identified and characterised. The analyses performed as part of Workshop 3 in the EBIOS RM method, based on RO/TO pairs, enabled the following strategic scenarios to be developed:

- service disruption;
- loss of operating data.

6.5.2 Operational scenarios - workshop 4

Following the analysis of operational scenarios (Workshop 4 in the EBIOS RM method) and risk treatment (Workshop 5 in the EBIOS RM method) presented in Appendix B, the measures to be applied can be specified according to the business assets and supporting assets concerned (see table 8).
The operational risk scenarios **R1**, **R2**, **R3**, and **R4** of the "Service disruption" strategic scenario present a high risk.
These scenarios are linked to the feared events **ER1** and **ER2** in accordance with table 9.
These feared events are associated with the business assets **Business asset1**, **Business asset 2** and **Business asset 3**.

Information

Since these business assets depend on supporting assets, it is essential to implement appropriate safeguards to reduce the risk of malicious acts. The detailed measures are described in the case study in the detailed measures guide [6]. An initial step could involve the physical separation of the video surveillance network in order to make this network completely independent from those of the treatment plants.

Appendix A
Functional dependencies

The relationships between the functions can be summarised as in figure 3. All relationships are bidirectional with the business supervision centre or the security command post. There are also inter-site communications between functions (variables not issued by the monitoring centre or for transmitting local statuses).

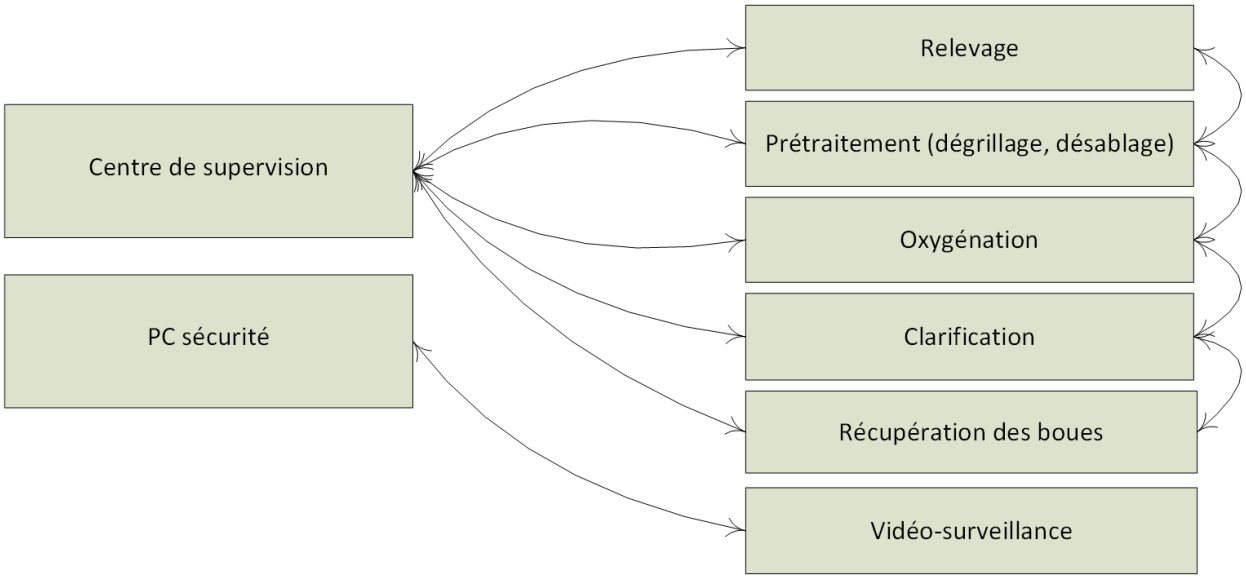

Figure 3 – Case study - Functional dependency graph

The central monitoring site communicates with all functions. Functional dependencies require a higher level of function classification “Supervision” and “Sludge recovery”.

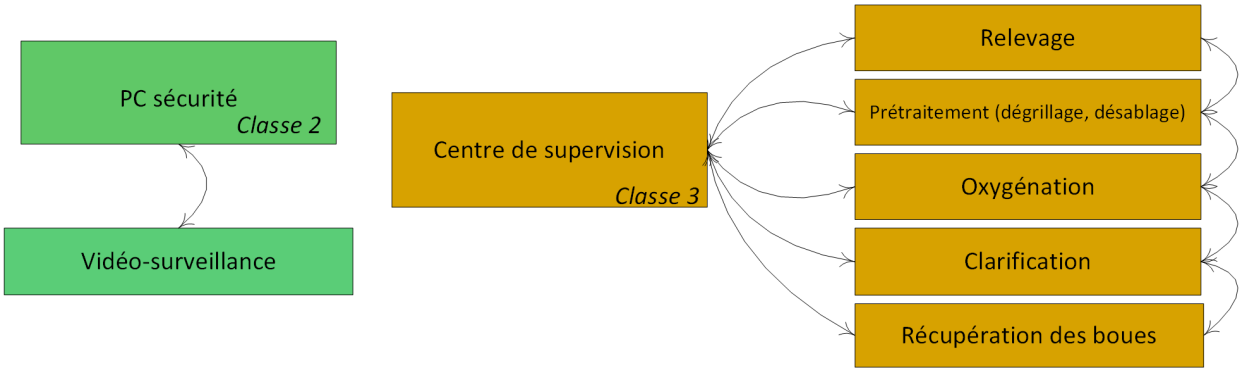

Figure 4 – Case study - Graph after analysis of functional dependencies

Appendix B
Risk Study

This chapter presents the risk management process according to the various operational scenarios that can lead to each of the feared events listed in section 6.2.3.

B.1 Risk mapping for the "service disruption" strategic scenario

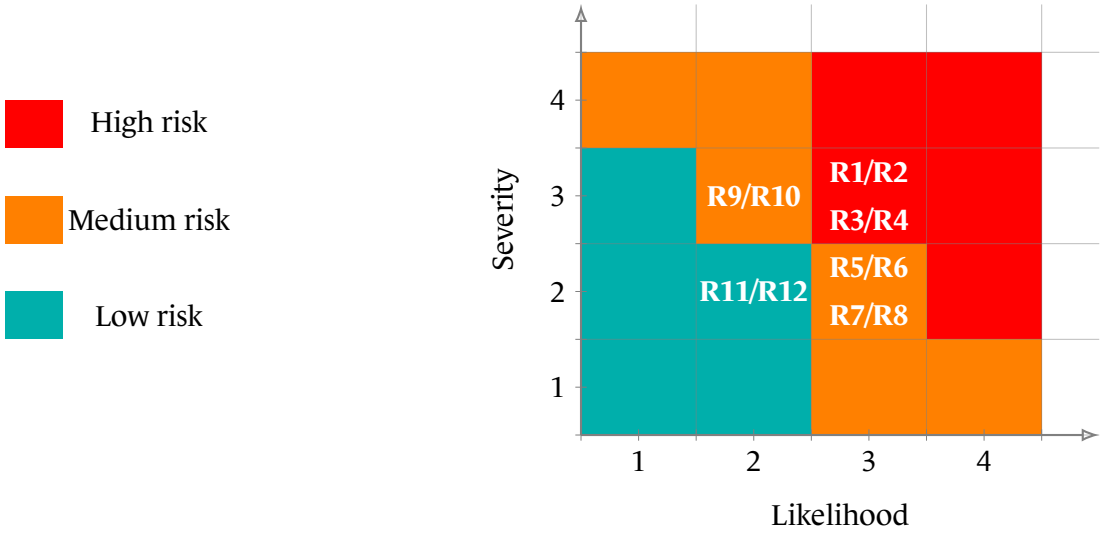

Figure 5 – "Service disruption" mapping

The operational scenarios are as follows:
R1: Legitimate account compromised resulting in the destruction of equipment
R2: Exploitation of vulnerabilities resulting in the destruction of equipment.
R3: Legitimate account compromised resulting in the destruction of biomass.
R4: Exploitation of vulnerabilities resulting in the destruction of biomass.
R5: Legitimate account compromised resulting in service disruption (via ransomware encryption).
R6: Exploitation of vulnerabilities resulting in service disruption (via ransomware encryption).
R7: Legitimate account compromised resulting in service disruption (via equipment sabotage).
R8: Exploitation of vulnerabilities resulting in service disruption (via equipment sabotage). **R9**: Propagation of an attack via a third party resulting in the destruction of hardware.
R10: Propagation of an attack via a third party resulting in the destruction of biomass.
R11: Propagation of an attack via a third party resulting in service disruption (via ransomware encryption).
R12: Propagation of an attack via a third party resulting in service disruption (via equipment sab-

otage).

B.2 Risk mapping for the "loss of operational data"

strategic scenario

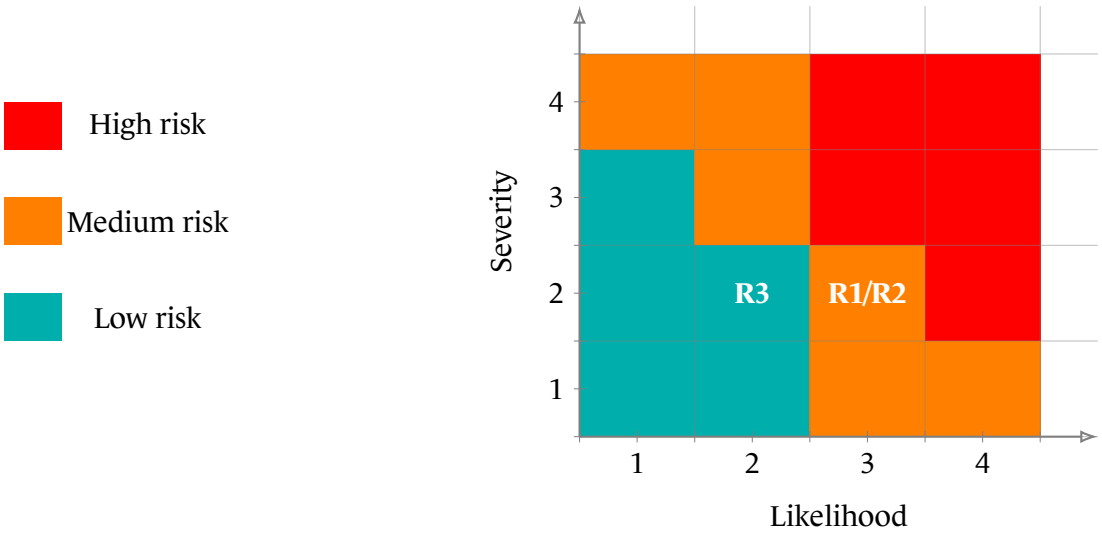

Figure 6 – "Loss of operational data" mapping

The operational scenarios are as follows:
R1: Legitimate account compromised resulting in the loss of operational data.
R2: Exploitation of vulnerabilities resulting in the loss of operational data.
R3: Propagation of an attack via a third party resulting in the loss of operational data.

Bibliography

[1] *Purdue Reference Model (ISA95)*.
Website, PERA, june 1990.
https://www.pera.net.

[2] *Guideline for a healthy information system*.
Guide ANSSI-GP-042-EN v2.0, ANSSI, september 2017.

[3] *Mapping the information system*.
Guide ANSSI-PA-046-EN v1.0, ANSSI, july 2019.
https://cyber.gouv.fr/en/publications/mapping-information-system.

[4] *Doctrine de détection pour les systèmes industriels*.
Guide ANSSI-PA-084 v1.0, ANSSI, décember 2020.
Only available in French.
https://cyber.gouv.fr/doctrine-detection-si-indus.

[5] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.5, ANSSI, march 2024.
Only available in French.
https://cyber.gouv.fr/ebios-rm.

[6] *La cybersécurité des systèmes industriels - Mesures détaillées*.
Guide Version 2.0, ANSSI, december 2025.
Only available in French.
https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels.

[7] *Service public de la diffusion du droit*.
Code, Legifrance.
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006901449.

[8] *Service public de la diffusion du droit*.
Code, Legifrance.
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043978078.

[9] *ISA/IEC 62443 : Series of standards ISA/IEC 62443, « Security technologies for industrial automation and control systems »*.
Standards, ISA, july 2009 to 2024; depending on the parts.
This document is the result of joint efforts between the IEC and the ISA.
https://www.boutique.afnor.org/en-gb/resultats?Keywords=IEC+62443
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[10] *IEC 61508 : Functional safety of electrical/electronic/programmable electronic safety-related systems.*
Standards, IEC, 2010.
https://www.boutique.afnor.org/en-gb/standard/iec-6150812010/functional-safety-of-electrical-electronic-programmable-electronic-safetyre/xs121824/244493.

[11] *Cyber attacks and remediation : Managing the remediation*.
Guides, ANSSI, december 2023.
https://cyber.gouv.fr/en/publications/cyber-attacks-and-remediation-managing-remediation.

[12] *Cyber threat overview 2024*.
Report, ANSSI, march 2024.
https://cyber.gouv.fr/en/publications/cyber-threat-overview-2024.

[13] *IEC 24772 : Programming languages. Avoiding vulnerabilities in programming languages*.
Standards, IEC, october 2024.
https://www.boutique.afnor.org/en-gb/standard/bs-iso-iec-2477212024/programming-languages-avoiding-vulnerabilities-in-programming-languages-lan/eu188126/427410.

Version 2.0 - 04/12/2025- ANSSI-PA-107-EN
Licence ouverte / Open Licence (Étalab - v2.0)
ISBN : 978-2-11-167186-7 (papier)
ISBN : 978-2-11-167187-4 (numérique)
Dépôt légal : mars 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité