




Managing Cybersecurity for Industrial Control Systems

Cybersecurity for Industrial Control Systems



Table of Contents

1.	Context and issues surrounding industrial control system cybersecurity	9
1.1.	Industrial Control Systems - Myth and Reality	9
1.1.1.	The reality of information management systems and industrial control systems 9	
1.1.2.	Some myths about industrial control systems.....	10
1.2.	Issues surrounding ICS cybersecurity	12
1.2.1.	General information about attacks	12
1.2.2.	Human negligence	13
1.2.3.	Vulnerabilities of Industrial Control Systems	13
1.2.4.	Potential impacts on ICSs	14
2.	Deployment Method of cybersecurity	16
2.1.	Reminder of cybersecurity role	16
2.2.	Key Principles of cybersecurity.....	17
2.2.1.	Awareness-raising among personnel.....	17
2.2.2.	Assets management and risk analysis	17
2.2.3.	Prevention: the concept of Defence-In-Depth	18
2.2.4.	Monitoring and detection of incidents	19
2.2.5.	Incident handling, alert chain.....	19
2.2.6.	Monitoring of threats and vulnerabilities.....	20
2.2.7.	Disaster Recovery Plan and Business Continuity Plans (DRP/BCP) 20	
2.3.	A system-wide, structured approach.....	21
2.3.1.	Willingness at every level	21
2.3.2.	Taking account of cybersecurity in projects	21
2.3.3.	Taking account of cybersecurity in FMECA / HAZOP	23
2.3.4.	Taking account of cybersecurity in maintenance	24
2.3.5.	Taking account of cybersecurity in procurement	25
	Appendix A: Frequently encountered vulnerabilities.....	27



Appendix B: Good practices	29
Appendix C: Abbreviations and Acronyms.....	37
Appendix D: Bibliographical References	39

FOREWORD

Although until recently IT security was a scientific field limited to a handful of experts, in recent years it has become the object of increasing public awareness. The French White Paper on Defence and National Security determined in 2008 that cybersecurity was a major priority for the next fifteen years, and already highlighted the vital need to protect critically important systems.

Since the White Paper, there has indeed been an increase in awareness, although this has arisen out of necessity, in response to attacks and incidents experienced by the most developed countries. Network unavailability on a massive scale, attacks on government information systems, espionage targeting strategic companies, destabilization operations and failures of all types have unfortunately been in the news in the last three years.

Industrial Control Systems (ICSs), even when not connected to the Internet, are exposed to such threats. The *Stuxnet* worm, which appeared in 2010, provides tangible proof that our worse fears regarding attacks on sensitive plants may become a reality. In 2009 an ingenious and unwitting adolescent was able, via the Internet, to derail a tram in Poland, demonstrating the vulnerability of its signalling system. Other cases include pipeline break and water pollution. Unfortunately, examples abound.


Cybersecurity concerns are therefore just as relevant to ICSs as they are to other information systems, and probably even more so.

The issue is: just like society as a whole, industries have in many cases adopted digital technologies on an ad hoc basis and without any prior strategy, and a variety of different systems are interconnected, with the main concerns being productivity, efficiency and safety – but rarely security.

Industries possess one advantage in terms of the security of their information systems: they have a robust culture of dependability for their plants, and in most cases they possess in-house cybersecurity competences for their office systems. These two cultures must now come together and efforts must be combined in order to protect ICSs appropriately.

It is up to the General Management to take decisions in this regard, to formally appoint an cybersecurity coordinator to strengthen the security of ICSs and provide them with the necessary material, financial, organisational and human resources.

The guide on the cybersecurity of ICSs published by the French Network and Information Security Agency, ANSSI (Agence nationale de la sécurité des systèmes d'information), has been created to support companies in this endeavour. This is the first publicly available version of the guide. It is designed to evolve as standard practice changes, and in response to your



contributions and feedback.

In addition, it is a practical case study designed to illustrate scenarios posing a risk to companies and to show how these are to be dealt with.

Finally, this guide is not solely intended for ICSs; its content also applies to the following non-exhaustive list of systems: *data centres*, *smartgrids*, building management systems (BMS), centralized technical management systems (CTM), and many embedded systems.

PURPOSE OF THE GUIDE

The purpose of the guide is to assess the cybersecurity of industrial control systems. Although specific to each facility, ICSs are in most cases made up of the following components:

- Programmable Logic Controllers (PLC);
- Distributed Control Systems (DCS);
- Safety Instrumented Systems (SIS);
- Sensors and actuators (intelligent or non-intelligent);
- Fieldbus;
- Supervisory control software: SCADA;
- Manufacturing execution system (MES);
- Engineering and maintenance software;
- Embedded systems.

ICSs currently make abundant use of information technologies, but they were not designed to deal with threats that the latter present. There are now numerous examples of published ICS vulnerabilities (for example, concerning Modbus and OPC protocols).


This is why they need to be included in general discussion on the security of company information systems¹.

The purpose of this guide is not to set out an exhaustive list of recommendations or to set out all of the components of an ICS. Rather it proposes a strategy for awareness-raising and implementation of good practices to support companies in the implementation of security.

There are no ideal or "one-size-fits-all" solutions. Appendix B sets out potential good practices. Each system has its own unique characteristics and risks that need to be analysed in order to implement suitable solutions whilst limiting the impacts on the core activity of the company.

Securing a system entails costs that are often difficult to calculate. So are the resulting gains. Nevertheless, this securing process will protect company investments and production. This is why it is important to define the right objectives and adapt these to requirements. Paradoxically, "over-security" can result in effects contrary to those sought and undermine industrial

¹A company information system includes all of a company's information systems, i.e. management information systems (information systems for departments and office applications, human resource management, customer relations and integrated management) and industrial control systems.



performance.

The abbreviations and acronyms used in the document are set out in Appendix C.

1. CONTEXT AND ISSUES SURROUNDING INDUSTRIAL CONTROL SYSTEM CYBERSECURITY

1.1. Industrial Control Systems - Myth and Reality

1.1.1. The reality of information management systems and industrial control systems

Despite their increasing use of standardised "classic" or "conventional" information technologies (IT), industrial control systems (ICSs) have specific characteristics unique to the contexts within which they are used. They are distinguished from information management systems by the fact that they run physical plants (production units and chains, water and energy distribution networks, road and rail infrastructures, etc.); some of these also carry out protective functions for assets and individuals or for the environment.

	"Management" Information Systems	Industrial control Systems
Purpose of Systems	data processing	Control command of plants (physical, concrete), process regulation, data acquisition and processing
Functional constraints	business constraints and confidentiality constraints	business constraints and "real-time" constraints, dependability constraints, 24/7 availability
Culture of users	computer engineers	automation engineers, electrical and instrumentation technicians, process engineering specialists
Physical environment	climate-controlled server room, office or home	production workshops: dust, temperature, vibration, electromagnetism, proximity of hazardous materials, external environment, etc.
Geographical location	for the most part in closed premises (office or home in the case of teleworking)	in warehouses, factories, on public highways, in the countryside (pumping stations, electricity sub-stations, etc.),

	"Management" Information Systems	Industrial control Systems
		isolated locations, at sea, in the air and in space
Lifespan	approximately 5 years	more than 10 years (sometimes 30 or 40 years)
Incident management	post-incident analysis (forensic)	the large number of parameters and the complexity of the environment limits the reproducibility of the incident
Components	standard systems; systems "hardened" against cyber attacks	real-time, robust systems for the difficult conditions of industrial environments; E ² PROM systems, with no hard-disk
Diverse nature of components	component compatibility is a technical requirement (homogeneity and interoperability).	the long lifespan of plants results in an "overlying" of successive waves of technology at the same site, resulting in the phenomenon of equipment and software obsolescence.

1.1.2. Some myths about industrial control systems

There are number of myths about industrial control systems. The most commonly held are examined here.

Myth	Reality
"My industrial networks are isolated, so I'm protected".	Industrial control systems are often connected to management networks and sometimes directly to the Internet. USB sticks and maintenance laptops are also major vectors for malware propagation, even in isolated systems. The growing need to exchange data with the management information system ultimately makes

Myth	Reality
	industrial network isolation impossible.
"I use proprietary protocols and databases, so I'm protected."	Even proprietary solutions contain standard components in the interests of interoperability (with the operating system for example) and lower cost. Proprietary solutions are liable to be vulnerable since they may not have undergone any security analysis whatsoever.
"Including security mechanisms (encryption, filtering, authentication) is incompatible with the constraints of the required response times."	Components performance does no longer slow down security functions deployment. However, difficulties do exist for "real-time" systems.
"cybersecurity is not compatible with dependability."	On the contrary, cybersecurity and dependability are consistent in a number of ways, see §2.3.3.
"Dependability measures such as heterogeneous redundancy protect against attacks on availability."	This principle is less and less used because of expensive solutions. Also, the products of different manufacturers sometimes use the same technologies and sometimes incorporate the same hardware and software components. In this case their vulnerabilities would be identical.
"Cybersecurity is expensive".	Cybersecurity must be proportionate to the risks faced. It will be much less expensive if it is taken into account intelligently in the upstream phases of projects. Its cost should in theory always be less than the maximum impact of an attack, but it is true that there is no way of calculating return on investment (ROI).

Myth	Reality
<p>"An attack on the Industrial control System will always have less impact than a physical incident (theft of cables, fire, etc.) or a terrorist attack (explosion of a petroleum tank in a refinery for example).</p>	<p>An attack can create a global dysfunction in plants that is more difficult to identify and more pernicious (industrial sabotage, slow-down in production) than a physical attack and may involve a very long recovery time.</p> <p>The dysfunction caused may become an aggravating factor and bring about an industrial, human or ecological disaster (for example overriding of dangerous chemicals monitoring alarm at a SEVESO site).</p>
<p>"Cybersecurity will stop me from working the way I want to".</p>	<p>Cybersecurity must focus on critical issues.</p> <p>Its objective is not to block useful behaviours, but rather to prevent dangerous behaviours (which means these must be identified in advance). Cybersecurity sometimes requires the formal establishment of work-around measures for ordinary modes of operation (degraded modes of operation).</p>

1.2. Issues surrounding ICS cybersecurity

1.2.1. General information about attacks

A number of different types of attacks exist:

- targeted attacks: for example in furtherance of an ideology or for commercial/financial gain, undertaken by an individual or group of individuals against an organisation with a view to causing harm, by disrupting processes, or even by causing material damage. Attackers are organised individuals who possess the resources to achieve their objectives. Underground entities offer cyber-attack services via the Internet, or publish turn-key tools to carry out attacks ("*exploit kits*"²);

²Some "*exploit kits*" are officially sold as cybersecurity tools with the aim of detecting vulnerabilities during audits, for example. These "*kits*" can of course also be used by attackers.

- "challenge" attacks: the objective of which is to demonstrate the technical ability to hack into reputedly secure systems, but the effects of which, in terms of the security of assets and persons or brand image, are very real for the victims;
- certain non-targeted attacks: seeking to affect as many people as possible, can create significant damage within companies (for example, malwares and spam campaigns).

1.2.2. Human negligence

Negligence is not the result of any wilful or malicious action, but its effect can be similar to that of an attack. It can create vulnerabilities that are difficult to detect, which can be exploited by attackers or which can simply impair system availability.

For example, the involuntary modification of setting of the setpoint for regulation or modification of an alarm may have disastrous consequences for the quality of products, services provided, the environment or the health and safety of individuals.

The use of a USB stick – whether personal or not – to transfer data between isolated ICSs can cause system unavailability if the stick is infected with a malwares.

In these two very concrete cases drawn from real-life experience, the individuals involved had not intended to cause any harm. However, the impact on the ICSs was very real.

Such negligence may arise due to a lack of personnel training and information on the issues.

1.2.3. Vulnerabilities of Industrial Control Systems

Vulnerabilities may have multiple origins and it is not the purpose of this guide to enumerate them. Some examples of vulnerabilities frequently encountered in industrial systems are listed in Appendix A.

The increasing need for consolidation of company data and access to it in real time from any point on the planet, and the cutting of development and possession costs and planning constraints have precipitated the convergence of the industrial and management IT fields.

Ethernet networks are now employed in ICSs and even as fieldbuses. They offer functionalities such as a shared network infrastructure and the possibility of using IP layers (for example, for remote maintenance).

Development, maintenance and remote maintenance are currently entirely developed on generic platforms created from management IT (.Net or Java platforms, for example).

Systems standardisation and new functionalities have pushed vulnerabilities from the realm of management IT to ICSs. The systems, referred to as proprietary, often lacking in security

mechanisms, are not immune to vulnerabilities that could be exploited by motivated and organised attackers.

Whereas the field of management information systems is regularly able to correct vulnerabilities, particularly through the application of fixes published by software designers and editors, in the industrial field, due to availability and safety constraints, it is not possible to adopt the same protective measures. This difference in responsiveness when faced with public vulnerabilities is one of the main risks of industrial control systems.

Lack of training of users, cultural differences or lack of awareness of the risks associated with cybersecurity may constitute a further significant vulnerability.

1.2.4. Potential impacts on ICSs

Numerous incidents on ICSs occur each year, but few receive media attention, such as the incident with the nuclear power station in the United Kingdom linked to *Conficker*, the incident associated with the *Slammer* worm in the USA, or, in 2010, the generalised propagation of the *Stuxnet3* worm. Their impacts may be analysed along a number of different lines, which are set out below:

Material damage/bodily harm	Modifications made to the ordinary configurations of industrial systems can result in physical degradation which often has material – and also human - consequences.
Loss of turnover	Production down-time causes significant revenue loss. Changes made to manufacturing parameters lead to non-compliant products that generate major costs.
Impact on the environment	A system failure after the malicious gaining of control can result in system dysfunction (e.g. opening of pollutant containers) and cause the site and its environment to become polluted. Such an incident occurred in Australia in recent years.

³*Stuxnet* is malware that targets ICSs. It exploits multiple vulnerabilities that exist in the *Microsoft Windows* operating system and the *SCADA WinCC* software created by *Siemens*. The malware modifies the programme executed by certain industrial PLCs from the *Simatic S7* range manufactured by *Siemens*. The modifications made can lead to a slowdown in production but also to the physical destruction of the plants run by the PLC.

Data theft	Loss of trade secrets, counterfeiting, competitor advantage.
Civil / criminal liability - Image and renown	Service unavailability such as disruption to water or electricity supplies and the supply of defective products that endanger the consumer can result in legal action for damages or simply harm the image of the company (customer satisfaction and trust).

These various impacts generate financial losses associated with the loss of activity or the payment of compensation to potential victims (customers, individuals, local governments, associations, States and even the European Union) and impair the image of the company.

2. DEPLOYMENT METHOD OF CYBERSECURITY

2.1. Reminder of cybersecurity role

The objective of cybersecurity is to analyse system vulnerabilities (hardware, software, procedures, human factors) in order to implement measures to limit them and be in a position to safeguard the continuity of core business functions to an acceptable extent.

Although often seen as a constraint, well thought-out cybersecurity can, on the contrary, improve the robustness of systems and the productivity of companies.

As the General Security Guidelines (French acronym "RGS")⁴ indicates, it is built upon four pillars that are essential for the good functioning of ICSs:

- **availability:** within a context of high productivity, any degradation in availability results directly in financial losses and dissatisfied customers (delivery delays, increased production costs, production down-time, etc.);
- **integrity:** compliance in this regard certifies that the products and services provided meet customer or regulatory requirements. For Safety Instrumented Systems (SIS) that protect assets and individuals (for example, safety shutdown systems), this is imperative. Integrity concerns all ICS components, for example PLC programmes, data exchange and SCADA software databases;
- **confidentiality:** this is sometimes minimised, but the divulging of a company's information assets can have a very tangible impact on its profits and its future (loss of customers). ICSs contain sensitive parameters and data such as manufacturing formulae, quantities of substances used, system plans, maintenance plans, PLC programs and devices address lists. These can be exploited by competitors or malicious groups to direct targeted attacks or simply to collect data enabling company know-how to be copied;
- **traceability:** this is a regulatory requirement in many activity sectors (e.g. food, transport and nuclear industries). Not being able to provide proof of the traceability of operations carried out, materials used and origin of materials, and non-compliance with regulatory requirements may result in legal action being taken against a company.

⁴See the ANSSI website: <http://www.ssi.gouv.fr/res/>

2.2. Key Principles of cybersecurity

The deployment and management of cybersecurity should be organised in such a way as to safeguard systems from the consequences of security incidents. Activities may be organised according to the phases set out above. It is an ongoing process that requires continuous efforts.

2.2.1. Awareness-raising among personnel

A large proportion of incidents are linked to lack of user awareness of the risks associated with a system. Ensuring that they are aware of the rules governing "Healthy networks" will help reduce vulnerabilities and opportunities for attack⁵. Awareness-raising must be consistent since the risks are constantly evolving.

2.2.2. Assets management and risk analysis

There is no point in trying to bolt a cybersecurity strategy onto an industrial system without any prior understanding of the requirements of the core business that it serves. It is therefore important to determine:

- the business objectives (production, distribution, protection of assets and persons etc.) and the services provided;
- impacts in the event of service interruption;
- functions vital to reach objectives, and specifically:
 - their degree of involvement and criticality in service provision,
 - the systems used to provide these functions,
 - whether these systems are centralised, distributed, remotely accessible, etc.;

An inventory of physical plants, systems and critical applications is a vital prerequisite for the implementation of cybersecurity in industrial systems. This inventory is the first stage in risk analysis, and makes it possible to determine the various different levels of criticality, safety, availability and integrity that are required for the mapped items.

Any project must include a risk analysis in order to identify the sensitive elements within the system, and their requirements and security objectives when faced with the threats identified.

These objectives are then broken down into security requirements, which pertain to the system itself (intrinsic robustness), and its design, construction and operating environment. These

⁵See the ANSSI website: <http://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/>

requirements are then converted into technical, physical and organisational measures.

They are clearly formalised in a security target, and constitute a benchmark for system security.

The risk analysis principles for cybersecurity are not different from those for dependability, though if the terminology used may not be identical.

A number of risk analysis methods exist. ANSSI suggests the EBIOS⁶ method.

The conclusions of the risk analysis lead to the definition of adequate security measures, for which the effort is commensurate with the challenges and adapted to the real needs. These may be technical but also organisational.

2.2.3. Prevention: the concept of Defence-In-Depth

Defence in depth consists of protecting systems by encircling them with a number of autonomous and successive barriers. These may be technological, or linked to organisational or human procedures.

Software and embedded hardware intrinsically contain bugs and vulnerabilities. Some are known and others are discovered over time. Attack surface must be reduced.

Adopting a defence in depth strategy provides protection against threats that are not yet known, to reduce the perimeter on which a threat may be directed, or to mitigate its impact.

Networks segregation with firewalls is not sufficient. Other mechanisms must be used alongside this at different levels (e.g. physical access control, configuration hardening, antivirus protection).

On legacy systems, automatic updates may be incompatible with the availability constraints and antivirus software may disrupt the operation of business applications that are not designed for it.

Other mechanisms may be established such as operating system hardening and intrusion detection. Multiple solutions exist. It is good practice to use barriers that are suited to the system, and that do not negatively impact upon business objectives, and then to assess the residual impacts.

It may also be useful to consult white papers and manufacturer's recommendations as well as consulting the ANSSI⁷ website with regard to this area.

⁶See the ANSSI website: <http://www.ssi.gouv.fr/ebios/>

⁷See the ANSSI website: <http://www.ssi.gouv.fr>

The defence in depth strategy must include not only a preventive protection strategy but also surveillance, detection and response measures.

2.2.4. Monitoring and detection of incidents

Detecting an incident is a major action, the importance of which is often underestimated.

Within an industrial environment, it can be complicated and even impossible to set in place certain protective barriers without negatively affecting business functions. Countermeasures must include detection and system surveillance mechanisms. Their operation must be transparent so as not to disrupt any business functions.

Such measures will not prevent an incident but will enable its detection and limit its effects as far as possible.

The earlier an incident is detected, the greater the possibility of implementing measures to reduce and confine its effects, for example by:

- physically isolating systems in the case of a virus attack so as to limit propagation risks;
- stopping a systems before it is degraded if the integrity of configuration data has been compromised as a result of errors or intentional changes (this will, for example, prevent systems destruction that could be caused by propagation of a worm such as *Stuxnet*).

Finally, the collection of information from alarm and event logs is vital for subsequent analysis. In some cases these logs may provide useful information and proof within the context of a legal inquiry.

2.2.5. Incident handling, alert chain

A detection mechanism will be pointless unless accompanied by the establishment of mechanisms and procedures for incident response. It is good practice to establish:

- what to do when an incident is detected ?
- who to alert?
- which initial measures to apply ?

An escalation process must be defined in order to manage incidents at the right seniority level, and consequently to decide:

- whether an Contingency Plan (CP) should be instigated;
- whether legal action is necessary.

An ANSSI⁸ note sets out best practices in the event of intrusion into an information system.

Incident management must also include a *post incident* (forensic) analysis phase to improve the effectiveness of the cybersecurity measures initially implemented.

2.2.6. Monitoring of threats and vulnerabilities

Cybersecurity is an ongoing action that requires continuous efforts.

Keeping up to date on threat developments and vulnerabilities by identifying the incidents they give rise to and their potential effects is a fundamental defence measure.

Websites such as that of the ANSSI⁹ operations centre or manufactures' website are important sources of information on identified vulnerabilities, and on any existing corrective measures or countermeasures that can be implemented.

Firmware updates for PLC and other devices, and fixes for operating systems and applications are signalled by means of alerts and notices. RSS and Atom feeds often make information rapidly available.

It may be worthwhile contacting manufactures to find out the best way of keeping up to date. Also consider asking suppliers, contractually, to keep themselves up to date regarding vulnerabilities. The more exhaustive mapping is, the more effective monitoring will be.

2.2.7. Disaster Recovery Plan and Business Continuity Plans (DRP/BCP)

There is no such thing as total security and zero risk.

Preparing to deal with exceptional events against which all previous measures have failed will minimise impacts and allow activity to be restarted as swiftly as possible.

Company Business Continuity Plans (BCP) must therefore include industrial control systems. These include the definition of *Disaster Recovery Plan* (DRP), identifying the means and procedures needed to return to a normal situation as quickly as possible, in the event of loss or exceptional events. These should set out how to reconstruct the system following a virus attack, fire, flood or loss of data.

⁸This can be consulted on the CERT-FR website: <http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html>

⁹See the CERT-FR website: <http://www.cert.ssi.gouv.fr/>

The DRP must be regularly updated to take into account:

- infrastructure-specific changes (maintenance, integration of new components that may introduce new vulnerabilities);
- the evolution of threats.

2.3. A system-wide, structured approach

Cybersecurity is not something to be done in an emergency, or on a one-off or ad-hoc basis. It is a process that requires planning and the involvement of multiple resources and competences as well as strong commitment of the top management.

2.3.1. Willingness at every level

Setting objectives that are appropriate for the priorities involved, formulating a strategy, raising personnel awareness and providing training are all tasks that are incumbent upon the management. The process can be progressive, carried out in a number of phases over time and dealing with aspects ranging from the simplest to the most complex and from the most to the least obvious, but it must be implemented system-wide. It may draw upon existing cybersecurity standards taking into account the constraints specific to ICSs.

Industrial control systems must be included within a company information systems security policy, as it is the case with any other information system, from the outset of the project. Security issues are not specific to this field, but the implementation of solutions requires that these be tailored to suit the industrial context.

Frequently, organisations do not promote increased proximity between conventional IT and ICS environments. This is why a security implementation project for industrial control systems cannot succeed without the involvement of the top management of the company.

2.3.2. Taking account of cybersecurity in projects

System cybersecurity must be considered from the outset of the project by the end user who must express their requirements.

During the specification phase:

- define the means for conducting preventive and curative maintenance operations to enable the cybersecurity level to be maintained over time: backup modes, for example, in order to carry out updates (for example fixing PLC outputs during *firmware* updates);

- specify the location of devices to ensure their physical security;
- provide for the possibility of changing default configurations such as passwords from the HMI;
- require that software provided be not exclusively compatible with a specific version of another software platform (operating system, database management system, etc.); failing this, insist that the supplier ensure ascending compatibility with new versions of these exclusively compatible platforms;
- integrate mechanisms to facilitate re-evaluation of a system following modifications (e.g. *process* simulation, value forcing, etc.);
- require that software that is not essential to the running of system be installed on other machines (office work stations to read PDF files or fill out spreadsheets, for example).

During the design phase:

- reduce system interfaces and complexity to limit the introduction of vulnerabilities during implementation;
- select components offering the best characteristics to meet security requirements (authentication mechanisms, access right segregation, etc.);
- apply the "need to know" or "least privilege" principle to access right segregation, and uphold the principle of "access only granted if specifically authorised" for system access;
- clearly distinguish user profiles from administrator profiles;
- make provision for the management of exceptions (e.g. exceeding of value thresholds, internal component errors);
- make provision for mechanisms for standardising changes on a group of machines (for example, password changes).

During the integration phase:

- change default configurations (for example, passwords);
- delete or deactivate functions that are not used but activated by default;
- consider deleting debugging functions such as tracking used to analyse ICS behaviour.

During the test phase:

- conduct functional security tests;
- carry out limit tests and error tests for business functions and check exceptions;
- test threat scenarios (penetration tests and attempts to gain control);
- test means for carrying out of maintenance operations at cybersecurity level (e.g. deployment of fixes, analysis of event logs);
- check system performance.

These tests are carried out individually during *Factory Acceptance Testing*: (FAT) and then collectively during *Site Acceptance Testing*: (SAT).

It may be important to require that a cybersecurity audit be conducted, by an independent team, in order to check the suitability of a system for the security targets required.

Testing should conclude with an approval phase so as to:

- accept the residual risks to the plant on a fully informed basis (principle of system approval), formalised by signature of an acceptance certificate ;
- effect transfer of ownership and liability for the system.

The points listed above are far from exhaustive and will be dependent upon which solutions are envisaged for each plant. Some are built using "components off-the-shelf (COTS)", whilst others are tailored solutions that use specifically developed software, or even turnkey solutions.

Transfer of an operational system:

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

In such cases, the company with responsibility for the future operating contract must carry out an exhaustive inventory in terms of system security and of the means available to maintain it at an acceptable level. This inventory must be accepted or be negotiated with the company awarding the operating contract such that all parties are in agreement as to the cybersecurity level for the "as built" plant, and the current means that it includes to maintain an acceptable level of security. The outsourcing guide¹⁰ published by ANSSI may provide solutions to this issue.

Finally, it should be remembered that changing passwords is vital upon operational transfer.

2.3.3. Taking account of cybersecurity in FMECA / HAZOP

Incidents of cybersecurity origin may result in production down-time or industrial disasters as demonstrated in the examples in section 2.2.

The integrity of a PLC safety program, for example, is now a priority in both the cybersecurity and the safety fields. An attacker or a malware modifying a security program concerns both fields. *Stuxnet* has shown that this type of scenario is entirely plausible.

The absence of cybersecurity or insufficient cybersecurity can therefore be the potential cause of a failure mode in industrial system. Failure mode analysis is dealt with using dependability

¹⁰See the ANSSI website: <http://www.ssi.gouv.fr/externalisation>

methods such as FME(C)A¹¹ or HAZOP¹².

To cover all risks, cybersecurity and dependability must be dealt with together, using a joint approach.

For example, the potential causes of a temperature increase at a plant above its nominal threshold may be:

- a reading issue linked to the failure of a sensor:
 - physical failure of a sensor,
 - incorrect calibration of the sensor,
 - an intentional change made to the parameters of a sensor by an unauthorised person (gaining of control by a hacker, or a virus) or as a result of negligence;
- a problem associated with a cooling circuit valve:
 - mechanical failure,
 - servo-motor failure,
 - intentional forcing of the command valve value by an unauthorised person (gaining of control by a hacker, a virus) or as a result of negligence,
 - a problem with the setting of the setpoint for regulating the cooling system,
 - an input error made by an operator,
 - a change made to the setpoint by an unauthorised person.

FMECA and HAZOP type analyses are often complicated to carry out and time-consuming. Including management information system and cybersecurity competence in teams conducting these tasks will be much more effective than a stand-alone, piecemeal approach in which each individual understands their own field, but is unable to see the big picture.

2.3.4. Taking account of cybersecurity in maintenance

The cybersecurity of industrial system must be taken into account at the time the maintenance plans are designed. These plans must include the operations that are necessary in order to maintain the level of systems security in the long-term:

- defining cybersecurity-specific maintenance operations that are necessary for maintenance of operational conditions (MOC) and maintenance of secure conditions (MSC): specifically, provision must be made for integration of fixes provided by the manufacturer;

¹¹FMECA: *Failure Modes, Effects and Criticality Analysis*. Dependability and quality management risk analysis tools.

¹²HAZOP: *HAZard and OPerability study*. Risk analysis method used in the field of dependability and safety.

- including preventive business maintenance operations (for example, electrical and mechanical maintenance) in cybersecurity operations that it is not possible to carry out whilst the plant is operating.

When a production line is stopped, for example for mechanical maintenance or regulatory inspections, it may be a good time to apply fixes to PLCs running the production line in the event that vulnerabilities have been identified.

Industrial control systems maintenance cannot be separated from the maintenance plans for the plants that they command. Cybersecurity operations should be monitored in the plant maintenance management tool (CMMS¹³).

2.3.5. Taking account of cybersecurity in procurement

The security requirements of the procured system must be studied and be clearly formalised (in a security target or in the STC¹⁴) and included in calls for tenders as is the case for functional, performance, quality, environmental, and safety requirements and also regulatory compliance requirements.

These pertain to the system that is the object of the consultation and to management of the project itself (training and accreditation of installers), including operating and maintenance phases. It is therefore prudent to:

- check in tender responses that the security requirements set out in the consultation are met;
- draft clauses for device maintenance:
 - request the maintenance plans needed in order to maintain the plant in an operational and a secure condition,
 - define procedures for incident handling and provision of security fixes: who takes the initiative, who implements, by which deadline, who carries out functional testing and how, etc.;
- specify clauses governing the terms of external service provision by subcontractors:
 - specify the terms of onsite support and intervention: is remote maintenance accepted (if so, under which conditions)? can the service provider leave the site with faulty devices and their configurations? can external providers use their own tools?
 - are external providers required to have specific qualifications?
- determine the legal clauses to be included in contracts;

¹³CMMS: Computerized Maintenance Management System

¹⁴STC: Specific Technical Clauses

- define the conditions of ownership for source codes and parameters:
 - who owns the various source codes?
 - are subcontractors allowed to hold source codes offsite?
 - define the status of plant-specific settings; who will maintain these? who will perform back-up for these? who will be authorised to modify these?

For further information on our recommendations on subcontracting, consult the outsourcing guide published by ANSSI¹⁵.

¹⁵See the ANSSI website: <http://www.ssi.gouv.fr/externalisation>

APPENDIX A: FREQUENTLY ENCOUNTERED VULNERABILITIES

For IT architecture and mapping:

- no inventory of Industrial Control System assets, no inventory of hardware, no notion of technological "generations" coexisting and of their intrinsic vulnerabilities;
- no Business Continuity Plan or Disaster Recovery Plan (DRP), no risk analysis for the ICS.


For preventive technical measures:

- default passwords for service accounts, databases, applications, access in console mode (PLC, gateways, network devices), use of SNMP communities;
- passwords in plaintext in source codes, operating procedures and saved data;
- inadequate management of user access: accounts remain active when users leave the site, existence of generic accounts;
- use of accounts with "administrator" profiles for applications, when "user" profiles would suffice;
- file sharing across the network in full-access mode when read-only access would suffice;
- read (or write) access to configuration files via FTP or TFTP;
- unsecured remote administration software (*VNC*, *Dameware* etc.);
- services activated with no functional use,
- use of unsecured services / protocols: TFTP, HTTP, Telnet, SNMP v1 or v2,
- online modification of PLC programmes authorised without monitoring;
- reloading of configuration when restarting *via* USB stick or MMC¹⁶.

For long-term security maintenance:

- no back-up of data, source codes, or device configuration;
- no management policy for portable media (e.g. USB port blockage) when uncontrolled USB sticks are authorised;
- lack of supervision, lack of incident detection;
- no updating (fixes) of operating systems, applications, *firmware* (for PLCs, intelligent sensors/actuators, etc.);
- no mechanism for signature of *firmware* (possible for an attacker to distribute

¹⁶MMC: *Multi Media Card*.



corrupted update containing malware).

APPENDIX B: GOOD PRACTICES

In many cases, good practices are similar to those that apply to management information systems, although their implementation must be tailored to industrial sector constraints. They are not ranked in order of priority and their ease of deployment will depend on the plant concerned.

GP01: Control physical access to devices and to the fieldbus

Reason	Controls physical access points that could allow entry into the system.
Method	Identify who needs access to devices, why and how frequently. Install servers in controlled access premises (where possible within IT rooms). Place work station central units, industrial network devices and PLCs in locked cabinets. Protect access to the network cable and sockets.
Scope	Work stations, servers, network devices and machines, PLCs, sensors/actuators, touch screens.
Constraints	Size of system - general site protection Maintain access authorisation in case of emergency.
Ways of managing constraints	Install a door "dry contact" to generate an alarm on the SCADA system upon opening. "Break glass" type procedure

GP02: Network segregation

Reason	Limits propagation of attacks and confines vulnerabilities.
Method	Establish a flow map. Separate networks using dedicated devices or VLANs. Filter flows by means of a firewall. Trace and analyse rejected traffic.
Scope	SCADA network, PLC network, development network, etc.

Constraints	Real-time constraints on process networks.
Ways of managing constraints	Filtering is applied upstream of these networks. Physical access to the process network is limited and controlled.

GP03: Management of portable devices and media

Reason	Reduces the risk of malware attack carried on portable media (USB keys, DVDs, etc.) which are major propagation vectors.
Method	<p>Define a policy for the use of this type of media.</p> <p>Activate software restriction policies.</p> <p>Deactivate use of these media and use clean machines (see below) for data exchange between networks if needed.</p> <p>Deactivate USB ports on systems, restrict functionalities (see Industrial Control Systems Cybersecurity – A Case Study, Appendix C).</p>
Scope	Work stations, servers, programming and maintenance console, touch screens.
Constraints	It may be necessary to exchange data between networks that are not interconnected.
Ways of managing constraints	The installation of clean machines - dedicated data transfer machines - may be a way of meeting user requirements. These machines must be reinforced, regularly updated, have antivirus software installed and be under high surveillance.

GP04: Account management (logical access)

Reason	Protects against illicit access.
Method	<p>Define a management policy for user accounts and application accounts.</p> <p>Do not leave default accounts on devices, machines and applications (admin/admin).</p> <p>Favour strong passwords (see http://www.ssi.gouv.fr/mots-de-passe, -> <i>calculate the "strength" of a password</i> and the CERT-FR information note on</p>

	passwords). Remember to change passwords regularly.
Scope	Operating systems, databases, SCADA applications, PLC programmes, network devices and machines, sensors and actuators
Constraints	"Generic" accounts, often historical; "Emergency" access.
Ways of managing constraints	Trace actions performed with these <i>logins</i> to detect any diversions or abnormal behaviour. Use strict organisational procedures (logbooks) in order to determine the identity of individuals using generic accounts on a moment-by-moment basis.

GP05: Configuration hardening

Reason	Limits the area exposed to attacks.
Method	Only install necessary software. No development tools on production servers or operator work stations. Only install or activate necessary protocols and services. Who has never said "If in doubt, I tick all installation options"? Avoid default options. Systematically deactivate vulnerable and unsecured protocols and functionalities (e.g. Web server, NetBios, FTP). In particular, deactivate automatic device or topology discovery protocols (LLDP) after having verified that these are not used by applications. Deactivate remote configuration and programming modes on critical assets. On PLCs, this mode is sometimes configured by means of a physical switch on the CPU.
Scope	Operating systems, SCADA applications, PLCs, network devices, intelligent sensors/actuators, touch screens
Constraints	Impact of modifications on the functioning of applications
Ways of managing	If, ultimately, certain unsecured functionalities are needed, then an in-depth, documented analysis (for example, exception handling) must provide

constraints	justification and countermeasures must be implemented.
-------------	--

GP06: Management of event logs and alarms

Reason	Systems monitoring / Detection of intrusions / Tracing of actions and maintenance (or remote maintenance) interventions
Method	Activate traceability functions where devices and software permit this (syslog, SNMP V3, "Windows Event", text file, etc.) Select relevant events and organise event storage (volume, storage time). Centralise logs and generate alerts for certain events or event outcomes.
Scope	Operating systems databases, SCADA applications, network devices, PLCs etc.
Constraints	Issue of volume of logs generated. There is a significant amount of information to be managed.
Ways of managing constraints	Tools exist to help manage events and sort these according to predefined criteria.

GP07: Configuration management

Reason	Ensure that active versions on devices (version N) have not been maliciously modified. Ensure that differences between versions N and N-1 only relate to legitimate modifications.
Method	Compare active programmes and configurations on devices (version N executed) with a back-up version identified as a reference (version N backed-up). Identify and analyse variations between versions N and N-1 prior to the entry into service of new versions.
Scope	SCADA applications, PLC programmes, network device configuration files,

	sensors and actuators.
Constraints	Complexity and heterogeneity of ICSs.
Ways of managing constraints	Sometimes configuration management tools exist that enable variations between two versions to be rapidly identified.

GP08: Back-up and restore

Reason	Be in possession of the data needed for a full restart of a site following an attack or disaster (this includes systems data).
Method	Define a back-up policy. Which data needs to be backed up in order to meet the needs of users, reconstruct a plant following an incident or meet regulatory requirements?
Scope	Application source codes, configuration databases (users, alarm thresholds, etc.), SCADA histories, programmes, <i>firmware</i> and data (variables, words, etc.) of PLCs, configuration file <i>firmware</i> network devices (switches, VPN, routers, <i>firewalls</i> , etc.), settings parameters and <i>firmware</i> of intelligent sensors and actuators for example.
Constraints	It is not always possible to automatically back up data, particularly for sensors and actuators and for PLCs.
Ways of managing constraints	Trace modifications to the settings of sensors/actuators, control, adjustment (PID setpoint) or configuration of alarms, etc.

GP09: Documentation

Reason	Control documentation in order to have an exact representation of the ICS and avoid operating errors. Control dissemination so that only those persons requiring information receive it.
Method	Define a documentation management policy (update process, retention period,

	distribution list, storage, etc.). Documentation pertaining to an information system must not be kept on the system itself.
Scope	Technical documentation regarding plant, architectural diagrams, geographical location, addressing plan, administrator manual, maintenance manual, functional analysis, system analysis, etc.
Constraints	It can be useful to have hard copies of operating documents containing passwords (for on-call staff for example). Control of these documents may become complicated and prohibiting hard copies is not necessarily feasible.
Ways of managing constraints	Make users aware of the risks associated with documentation. Leaving documents in view on a desk or in a car boot (next to the duty computer for example) is not good practice.

GP10: Malicious code detection

Reason	To provide advance protection against virus attacks.
Method	Define an malicious code protection policy. Give priority to protecting hardware and applications in direct contact with the outside world and users.
Scope	SCADA applications, engineering stations, programming and maintenance console.
Constraints	Incompatible with certain older generation SCADA applications for example, no antivirus updating mechanism (stand-alone machines for example). Contractual issues such as loss of manufacturer's guarantee.
Ways of managing constraints	Deploy the antivirus software at least on portable machines, remote maintenance machines and engineering stations. For new plant, antivirus compatibility must be a STC requirement. Reinforce machine configurations.

GP11: Upgrade and Patch management (planning)

Reason	Preventive protection against attacks exploiting vulnerabilities published by
--------	---

	<p>manufacturers.</p> <p>Preventive protection against failures associated with bugs fixed by means of fixes.</p>
Method	<p>Define a management policy for patches (systematic, periodic or ad hoc) that is suited to the functional constraints and risks identified. For example, define priorities for deployment of patches, verify ascending compatibility, and interoperability.</p> <p>Systematically apply patches to engineering stations and portable machines.</p> <p>Periodically apply patches to operator stations.</p> <p>Apply patches during maintenance on sensitive plant.</p>
Scope	<p>Patches for operating systems, applications, firmware depending on which vulnerabilities are fixed.</p> <p>Engineering station, operator machines, servers, PLC, telecoms devices, touch screens, etc.</p>
Constraints	<p>Patches must be assessed prior to deployment.</p> <p>Some devices are not easy to stop.</p>
Ways of managing constraints	<p>Identify the vulnerabilities addressed by the patches.</p> <p>Plan updates for maintenance down-time, for example</p> <p>Monitor traffic and event logs.</p> <p>Harden configurations.</p> <p>Isolate devices.</p>

GP12: Protection of Controllers (PLC)

Reason	Protection of PLC programmes.
Method	<p>Password protect access to PLCs. Hardware allows read-only access to be configured for first level maintenance interventions.</p> <p>Protect access to source code and embedded code in CPUs.</p> <p>Deactivate remote configuration and/or programming modes when this functionality exists.</p> <p>Lock PLC cabinets. For critical ICS fit dry contact alarm to detect cabinet</p>

	opening.
Scope	Production PLCs, PLC programmes that are backed up or under development

GP13: Engineering and development stations

Reason	<p>These machines are points of vulnerability and are major vectors for contamination and gaining control.</p> <p>They are connected to the industrial network and contain device configuration, PLC programming and SCADA software, and sometimes source code versions. Some machines are portable and can be connected to other networks such as office networks.</p>
Method	<p>All of the foregoing recommendations.</p> <p>Systematically apply patches.</p> <p>Systematically activate antivirus software.</p> <p>Do not connect maintenance consoles to any networks other than SCADA networks.</p> <p>Consoles must have named users or usage must be traceable.</p> <p>Shut down desktop machines when not in use and/or disconnect them from the production network.</p>
Scope	SCADA development stations, PLC programming console, portable devices (e.g. PDA, Pocket PC) to configure intelligent sensors and actuators.

APPENDIX C: ABBREVIATIONS AND ACRONYMS

ADSL	Asymmetric Digital Subscriber Line
FMEA	Failure Mode and Effects Analysis
PLC	Programmable Logic Controller
CPU	Central Processing Unit
DoS	Denial of Service
DRP	Disaster Recovery Plan
EIA	Electrical Industry Association
ERP	Enterprise Resource Planning
RAMS	Reliability, Availability, Maintainability and Safety
FMEA	Failure Mode and Effects Analysis
FAT	Factory Acceptance Test
GSM	Global System for Mobile
BMS	Building Management System
CTM	Centralised Technical Management
HAZOP	HAZard & OPerability method
ICS	Industrial Control System
HMI	Human-Machine Interface
MES	Manufacturing Execution System
OLE	Object Linked & Embedded
OPC	OLE for Process Control

P&ID	Process & Instrumentation Diagram
PID	Proportional Integral Derivative
PLC	Programmable Logic Controller
BCP	Business Continuity Plan
BRP	Business Resumption Plan
ISSP	Information Systems Security Policy
STN	Switched Telephone Network
SAT	Site Acceptance test
SCADA	Supervisory Control And Data Acquisition
SIS	Safety Instrumented System
SIL	Safety Integrity Level
DCS	Distributed Control System
SOAP	Service Object Access Protocol
SPC	Statistical Process Control
VFD	Variable Frequency Drive
MOC	Maintening in Operational Conditions
MSC	Maintening in Security Conditions

APPENDIX D: BIBLIOGRAPHICAL REFERENCES

Good practice guides and recommendations published by ANSSI

<http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/>

“Référentiel Général de Sécurité”,

RGS v1.0: <http://www.ssi.gouv.fr/rgs>

Methodological tools proposed by ANSSI

<http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/>

see in particular the EBIOS method: <http://www.ssi.gouv.fr/ebios>

Publications by ANSSI's computer emergency response team (CERT-FR)

- Acquisition of fixes CERTA-2001-INF-004
- Recommended responses in the event of information system intrusion CERTA-2002-INF-002
- Wireless (Wi-Fi) network security CERTA-2002-REC-002
- Web applications security and "data injection" type vulnerabilities CERTA-2004-INF-001
- Passwords CERTA-2005-INF-001
- Filtering and firewalls CERTA-2006-INF-001
- Event log management CERTA-2008-INF-005

This guide was produced by Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)



with the help of ministries



and companies



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

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

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

About ANSSI

The French Network and Security Agency (ANSSI / *Agence nationale de la sécurité des systèmes d'information*) was created 7 July 2009 as an agency with national jurisdiction ("*service à compétence nationale*").

By Decree No. 2009-834 of 7 July 2009 as amended by Decree No. 2011-170 of 11 February 2011, the agency has responsibility at national level concerning the defence and security of information systems. It is attached to the Secretariat-General for National Defence and Security (*Secrétaire général de la défense et de la sécurité nationale*) under the authority of the Prime Minister. To learn more about ANSSI and its activities, please visit www.ssi.gouv.fr.

Version 1.0 - June 2012

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)