French Ministry for an ecological and solidary transition



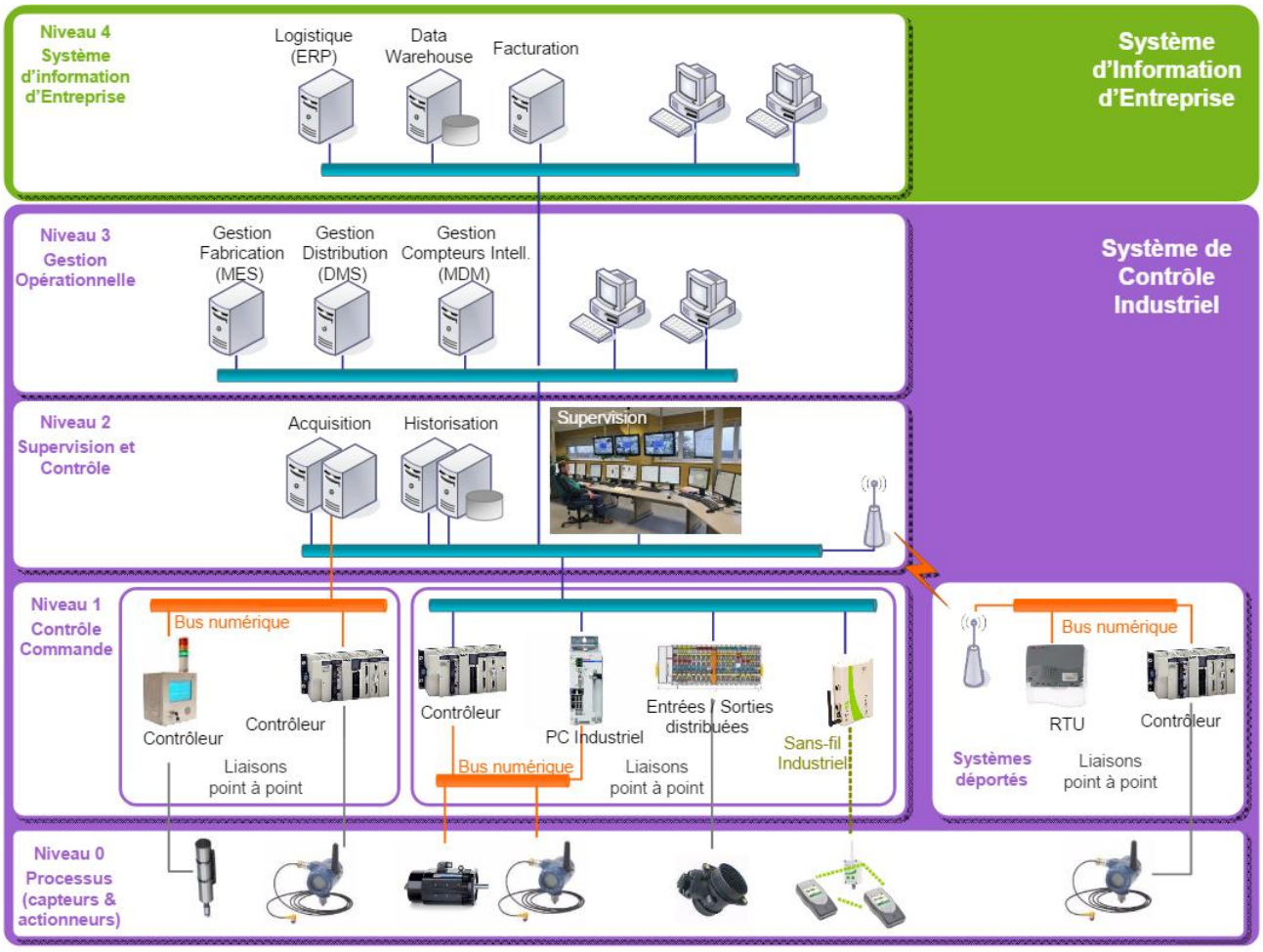
Cybersecurity in industry

ARIA
dgpr srt barpi

Table of contents

INTRODUCTION

A computer system controlling an industrial unit can be broken down schematically as follows:



This system has the particularity of being isolated, at best, by a firewall of the company's conventional IT systems (office automation, video surveillance, etc.). As shown, it generally consists of several sub-devices which are designed to:

- **control the industrial equipment**, i.e. open supply valves of a chemical reactor. Programmable Logic Controllers (PLCs), and Remote Terminal Units (RTUs) provide this functionality;
- **centralize the data and then control the industrial process in the control room with a SCADA** (System Control And Data Acquisition) generally based on a man-machine interface (MMI) and computer servers;
- **transmit information via electromagnetic waves** (Wi-Fi signal, GSM, alarm centre) or **cable networks** according to a specific protocol (Ethernet, Profibus/Profinet between several PLCs, ASi).

A malfunction within these information systems (IS) can lead to accidents. For example, the failure and unavailability of a SCADA system controlling a pipeline were partly responsible for the Bellingham accident in the United States in 1999 (ARIA No. 15621). More recently, following the Deepwater Horizon oil rig explosion in 2010 (ARIA No. 38145), articles in the American press reported several employee testimonies referring to Blue Screens of Death as a result of fatal system errors (http://www.examiner.com/article/did-bsods-on-the-deepwater-horizon-contribute-to-the-gulf-oil-disaster).

Moreover, under the sustained threat of terrorist attacks, a great deal of malicious software (malware) has recently emerged making information systems even more vulnerable. In this respect, a cyber attack on December 23, 2015, was linked to a power outage affecting nearly 1.4 million Ukrainian customers.

In order to follow the structure of an industrial control system (ICS), the events studied in this memorandum are grouped into the following categories:

- PLCs;
- sensors;
- treatment centres (SCADA);
- information transmission protocols.

Also, air-conditioning systems in control rooms can cause IS malfunctions or unavailability. A separate section is thus devoted to them specifically.

This document focuses on cybersecurity issues identified in the ARIA database. Thus, the accidents do not necessarily involve an act of malicious intent by someone inside or outside the company. Some are simply the result of a human or organisational error, although the lessons learnt could make a useful contribution to the study of computer breaches. The distinction between a malicious act and human error lies in the desire to deliberately harm an institution for ideological, financial or emotional reasons.

Programmable Logic Controllers (PLCs)

Examples of hardware:

Siemens

Allen Bradley

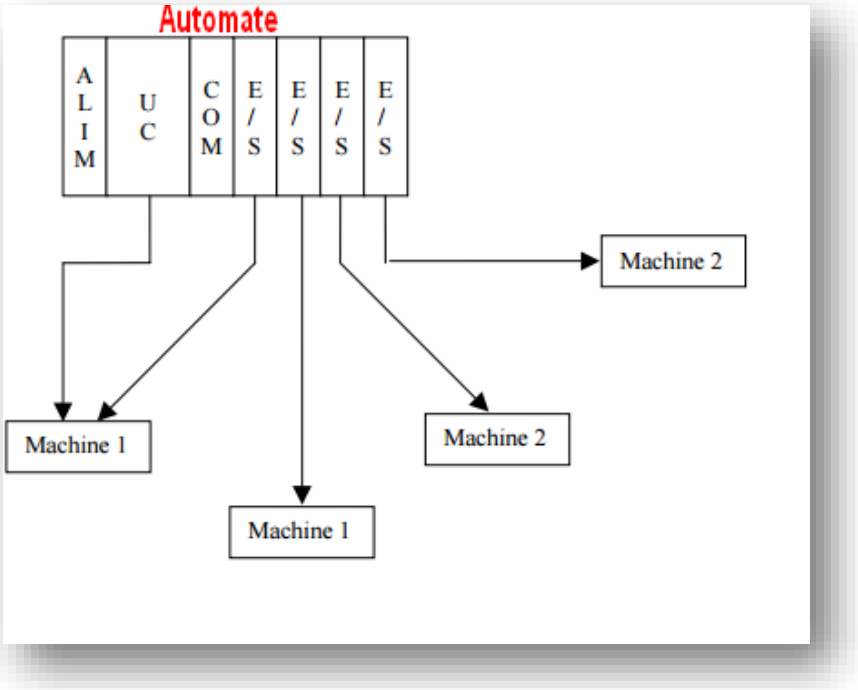
Operating principle:

An industrial PLC is an electronic component that performs two functions; one is called the operative part (OP), which operates the electric motors, pneumatic and/or hydraulic actuators of the unit, and the other is called the command part (PC) which coordinates these various actions. These components are programmed by automation specialists using specific software (programming language conforming to IEC 61131-3) or a proprietary programming device. Automation specialists connect their computer to a dedicated socket, as shown in the diagram below:

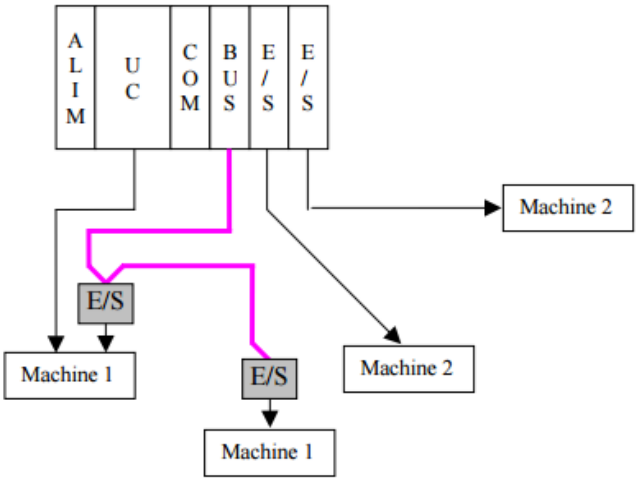
These PLCs consist of 4, 8, 16 or 32 input/output boards, which transform and adapt electrical signals from sensors or pushbuttons (inputs) to the PLC, and in the other direction, signals from the PLC to the contactors, LEDs and solenoid valves, etc.

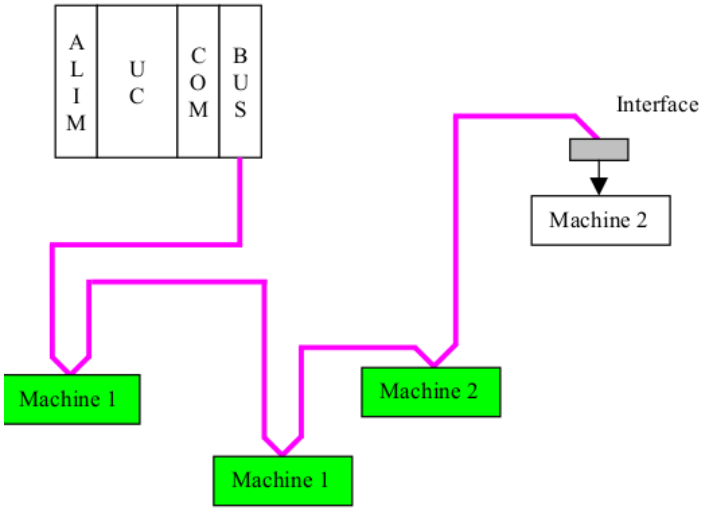
Types of possible mounting configurations:

Each input/output board is connected to a machine. This mounting configuration requires a long cable:



Little by little, technological developments have led to the installation of input/output boards closer to the sensors/machines, and to the multiplexing of the equipment through communication buses, as shown in the diagrams below:

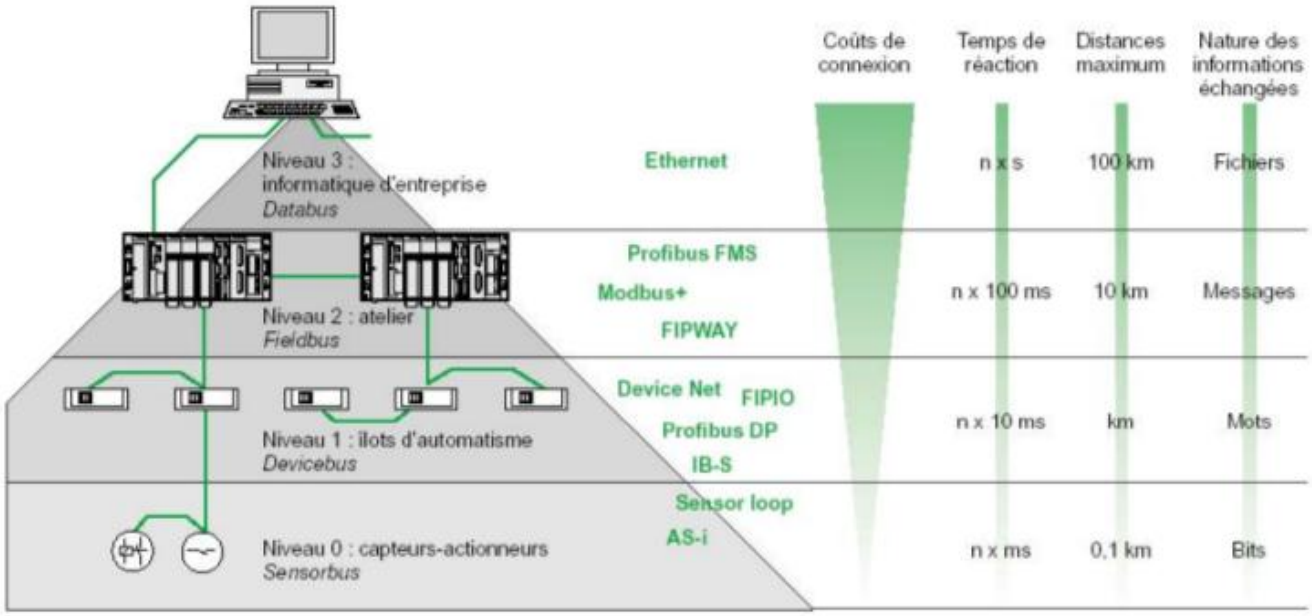




Input/output board as close to the machines as possible Multiplexing of machines

The ASi (Actuator Sensor Interface) is a field bus used to connect 31 slaves (sensors or pre-actuators) to a specific cable (two wires) carrying data and power.
This bus is completely standardised and allows the technologies of several manufacturers (interoperability) to be used. For this reason, the PLC is equipped with an ASi coupler.

The need for cells to communicate with one another (communication between PLCs) was instrumental in the development of numerous communication standards (Profibus, Fip, etc.).



The current trend is the introduction of Ethernet networks as close as possible to PLCs (e.g.: Profinet standard).

Safety:

The PLC must be able to withstand:

- External constraints of the industrial world and it undergoes numerous standardised tests (resistance to vibrations, electromagnetic compatibility, temperature, etc.);
- Power failures: the controller is designed to withstand power failures and to ensure correct operation when power is restored (cold or hot restarts);

- On/off mode: a PLC can only be started/stopped by authorised personnel. The restart is accomplished through a [programmed] initialisation procedure.

Finally, there are so-called Safety PLCs which integrate increased monitoring and redundancy functions.

The ANSSI, the National Cybersecurity Agency of France, qualifies hardware with regard to IT security. The list of certified products is available at the following address:

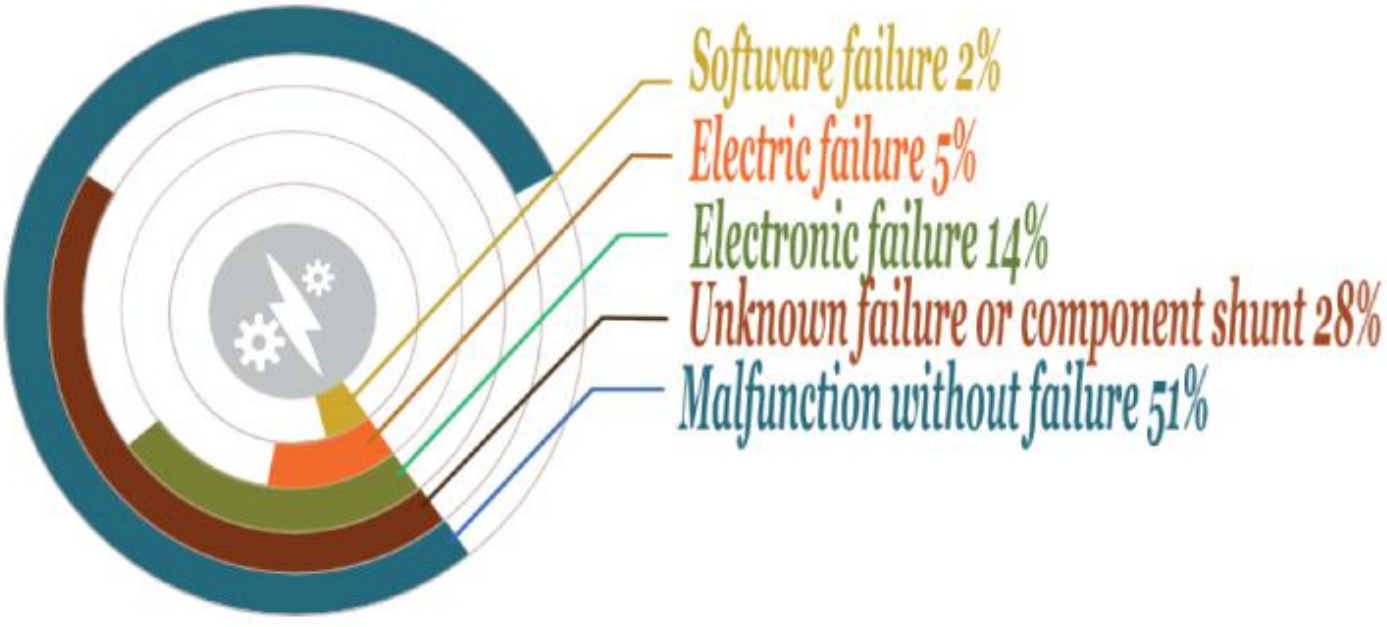
http://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/ Section: industrial equipment for PLCs.

The accidents recorded in the ARIA database:

The accident studies involving industrial automation and particularly their treatment was the subject of a BARPI study conducted in 2014. The study can be downloaded from the following address: https://www.aria.developpement-durable.gouv.fr/synthese/analyses-and-feedback/automatisms-accidentology/?lang=en.

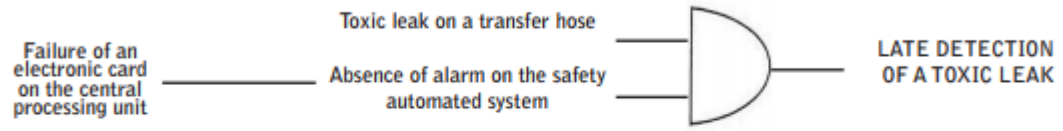
The following elements emerge from the analysis:

- An evaluation of 275 accidents involving defects in processing function components reveals the role of hardware (computer, electronic board) in 49% of accidents;
- Transmission related components within automated systems (data bus, relay) are involved in 14% of all cases;
- Component failures constitute the leading direct cause of processing function breakdowns (102 cases), which are distributed as follows:



Examples of accidents:

FAILURE OF AN ELECTRONIC CARD (ARIA 42931)
2nd May 2012



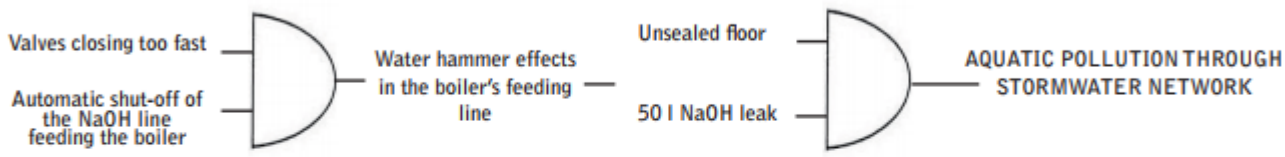
During delivery of dimethyl ether (DME) at a cosmetics plant, a transfer hose swelled around the fitting leading to the stationary installation and leaked due to incompatibility between the hose material and the product being delivered. The control operator noticed the leak and alerted the truck driver, who promptly closed the tank bottom valve and turned off the truck engine. Pressing the emergency shutoff button activated the transfer station security response, and the plant was evacuated for 20 minutes as a precautionary measure. **The accident cause focused on an inoperable gas detection device due to component defect in the electronic cards of the central processing unit (the cards had not been changed since 2001).** The sensors quickly saturated, emitting an «off-scale» signal that was interpreted as «sensor malfunction», without triggering any special action (even though the «off-scale» notification should normally activate safety procedures). **The card manufacturer had in fact identified this potential risk of malfunction back in 2008 and remedied the situation (by changing cards and updating the software). However, all potentially flawed cards at this plant had not been recalled or updated. The plant management proceeded by replacing all cards used on-site.**

OTHER RELEVANT REFERENCES Aria 3536, 7172, 10064, 21466, 27060, 32624, 39321, 43437

An analysis of the root causes of accidents also highlights the importance of **the special care required during PLC programming**. There are numerous cases involving **incomplete, inappropriate or even hazardous programming** (see ARIA 36437, 21994, 28911, etc.).

Examples of accidents:

HAZARDOUS PROGRAMMING (ARIA 28911)
21st September 2004



A 50-l soda (NaOH) leak occurred on the intake line of a boiler's demineralisation unit inside a glue factory. The deteriorated floor under the demineralisation columns facilitated the flow of washing water loaded with soda into a former storm drain system emptying into the nearby river. The pH rise caused calcium carbonate to precipitate, turning the river cloudy whitish over a long stretch. This discolouration disappeared 1 hour later. The factory operator responded by remodelling and sealing the unit floor, repairing pipes, **revising the automated control system to avoid a water hammer effect when closing valves**, and reducing the mismatch delay.

OTHER RELEVANT REFERENCES Aria 5989, 16072, 28911, 30417, 32109, 31691, 40522, 41736, 42038, 42921

PLC cyber attacks

The ARIA database does not catalogue accidents involving a cyber attack in the conventional sense of programmable logic controllers (see appendix).
However, videos can be found online showing that PLCs are sensitive to denial of service attacks (https://www.youtube.com/watch?v=Uu0bB3ptUvo) when they are not protected by a firewall. These attacks appear to cause an error code, followed by the shutdown of the system.

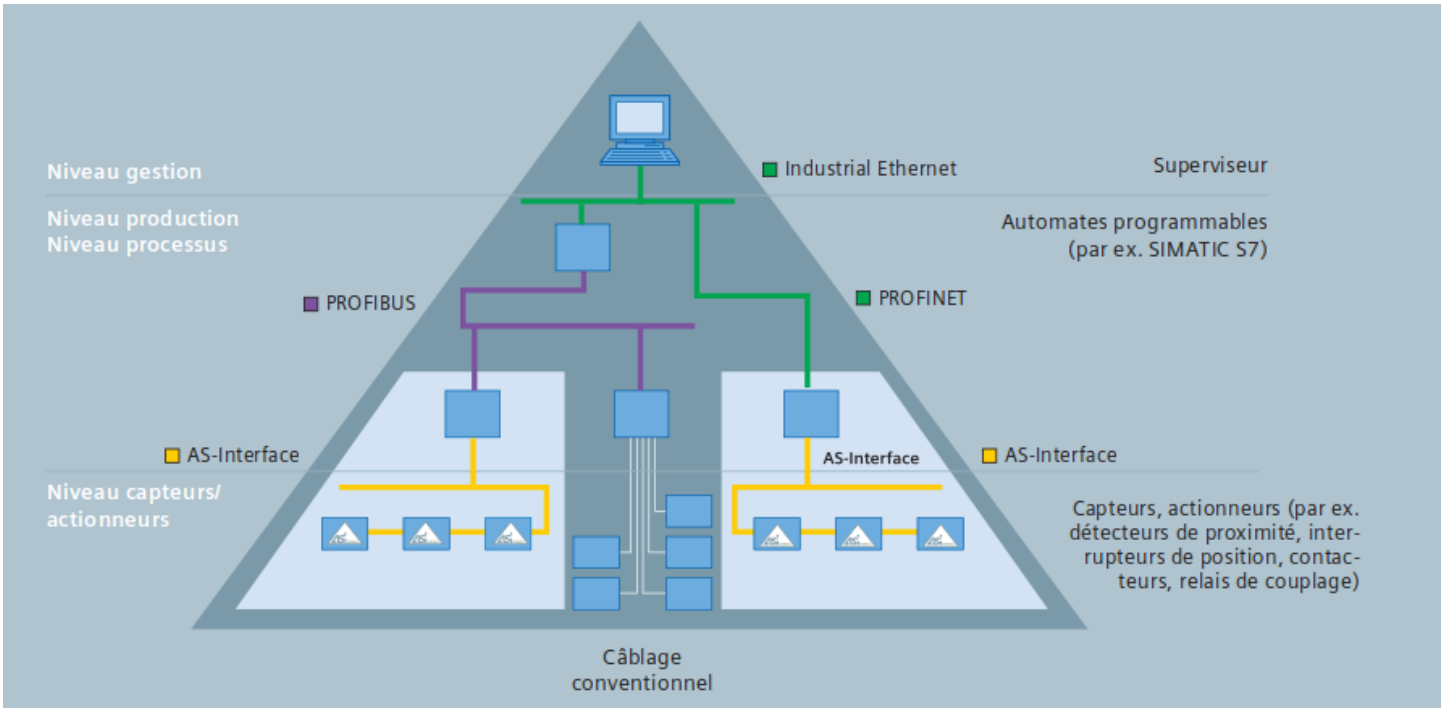
Sensors

Operating principle:

The sensor's main role is to convert the analogue value to be measured into a signal that can be understood by the control system.

Connection to the Industrial Control System:

As mentioned above, the sensors were previously connected directly to a bus, in parallel. Now, the current trend is multiplexing with the ASi standard as indicated in this excerpt from a documentation published by the manufacturer Siemens:



The accidents recorded in the ARIA database:

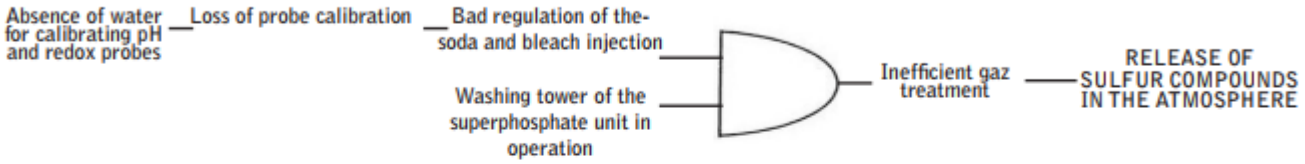
In 2012, BARPI conducted an accident analysis of sensors. The study can be downloaded from the following address: https://www.aria.developpement-durable.gouv.fr/synthese/analyses-and-feedback/accident-analysis-of-industrial-automation-sensors/?lang=en.

Among the lessons drawn from this analysis, we should note that:

- Accidents involving sensors represent only a small portion of ARIA base accidents (3% of total entries), while those caused by critical sensor failure account for less than 2%;
- The sensors' influence on accident occurrence rates is more marked outside the normal operating phases of industrial installations: restart, stop or shutdown;
- More than half of all sensor-related accidents are due to a malfunction, as two-thirds of all identifiable causes stem from either human error or improper organisation: e.g. lack of maintenance, poor connections, and shoddy cleaning...;
- For those sectors most heavily equipped with sensors, false detections lie at the origin of over 20% of all accidents involving failure. False detections tend to arise from either measurement drift or faulty calibration;
- Despite being less widespread than temperature and pressure sensors, level controls are involved in more than 20% of all accidents analysed, regardless of sector of activity. Their mechanisms appear to make them prone to jamming and clogging.

Examples of accidents:

CHEMICAL INDUSTRY - CALIBRATION (ARIA 33707)
September 3, 2007



Around 7:30 pm, the atmospheric discharges of a fertilizer manufacturing plant intoxicated three employees at a neighbouring facility, all of whom were hospitalised suffering from headaches. The next day, new odours were notified as of 6:50 am by the neighbouring plant. The superphosphate unit was shut down at 8 am, and this step eliminated the foul-smelling emissions. The unit's odour treatment installation was verified, the three Venturi tubes were drained and the pH and redox probes were replaced as a precaution. The unit's restart did not trigger any new detection of foul odours. **Erroneous pH and redox probe settings from the previous afternoon led to this accident. A leak on the washing machine's recirculation pipe, which was supplying water to the pH/redox probe measurement bowl, prompted a maintenance service call and the loss of probe calibration subsequent to an absence of water in the measurement container.** The failure of these probes to regulate soda and bleach injection into the washing tower lowered the efficiency of the gas treatment system installed on the superphosphate unit that had been loaded chiefly with sulphur compounds.

OTHER RELEVANT REFERENCES :

Poorly-calibrated sensor	Aria 733, 2137, 11107, 32470, 33487 34256
Measurement drift	Aria 10905, 11665, 30178, 34319 37175
False detection	Aria 2684 , 4908 , 25057, 29767 , 31490 31734, 33310 , 33626 , 33838

Sensor cyber attacks

The ARIA database does not catalogue accidents involving cyber attacks in the conventional sense of sensors.

The attacks rather seem to concern wireless sensors that convey information via electromagnetic waves. The encryption of the information conveyed, therefore, deserves special attention (http://www.lemondeinformatique.fr/actualites/lire-les-capteurs-industriels-vulnerables-a-des-attaques-par-ondes-radio-54532.html).

In the case of a wireless sensor, one should also study how information transits between the control centre and the sensor. Does the SCADA system send a query to the sensor after a certain period, or is it the sensor that sends its telemetry? This latency in information processing must be consistent with the possible need for real-time information.

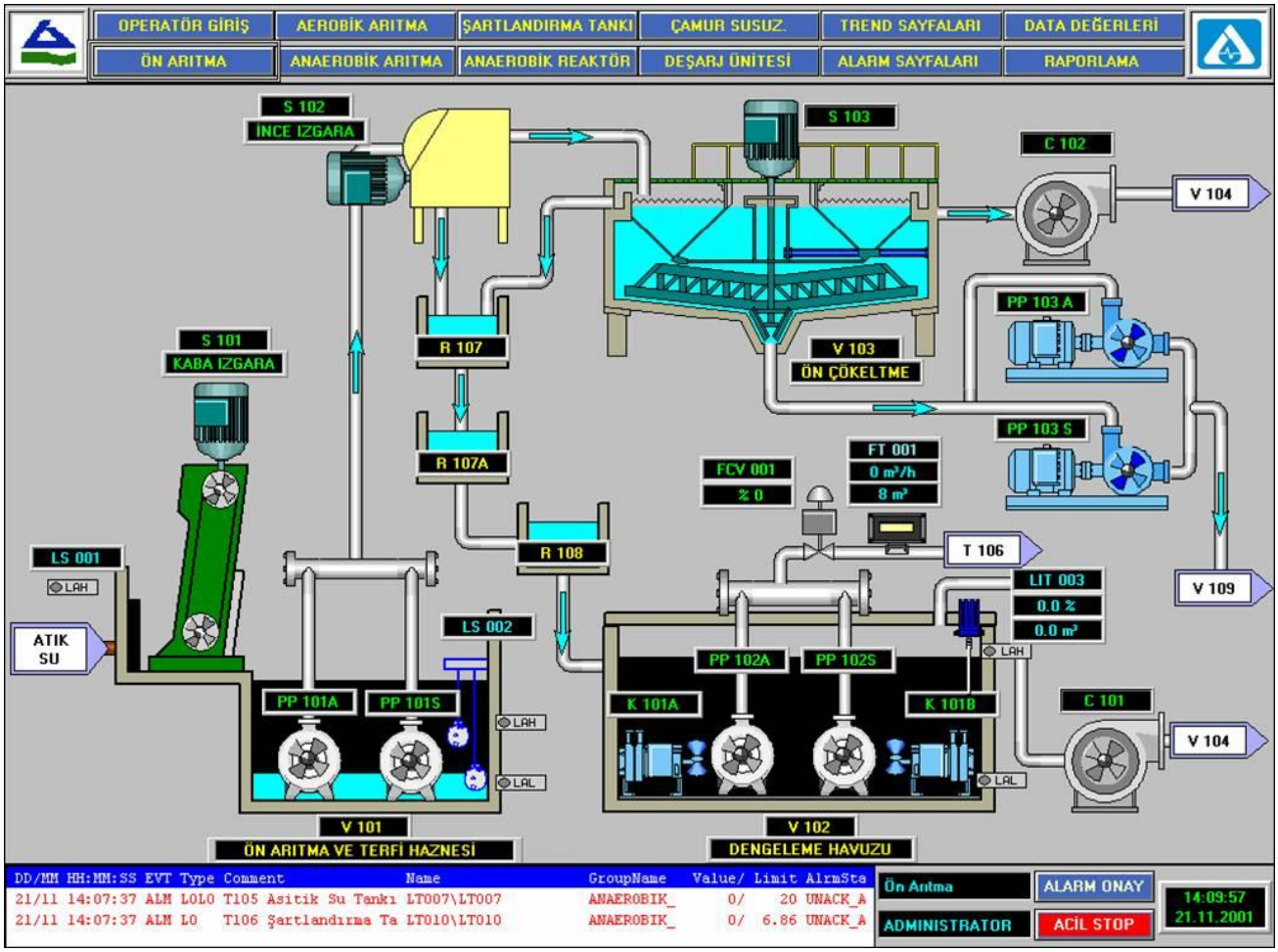
System Control And Data Acquisition (SCADA) systems

Definition:

A Supervisory Control And Data Acquisition system (SCADA) **manages and processes** a large number of telemetry data in real time. It also remotely **monitors** technical facilities. It is, so to speak, the industrial control system's brain. The system **alerts** operators in the control room via alarms if the physical parameters of the industrial process are exceeded.

Among other things, a SCADA system includes controllers, a database, I/O management software and a man-machine interface (MMI). The information regarding the SCADA device is centralised on a CPU, which allows the operator to control all or part of an installation's actuators, which are often (plant, distribution network, etc.). Field monitoring is performed by remote terminals (*RTU- Remote Terminal Units - refer to the diagram on page 2*) or by programmable logic controllers.

Example of an MMI:



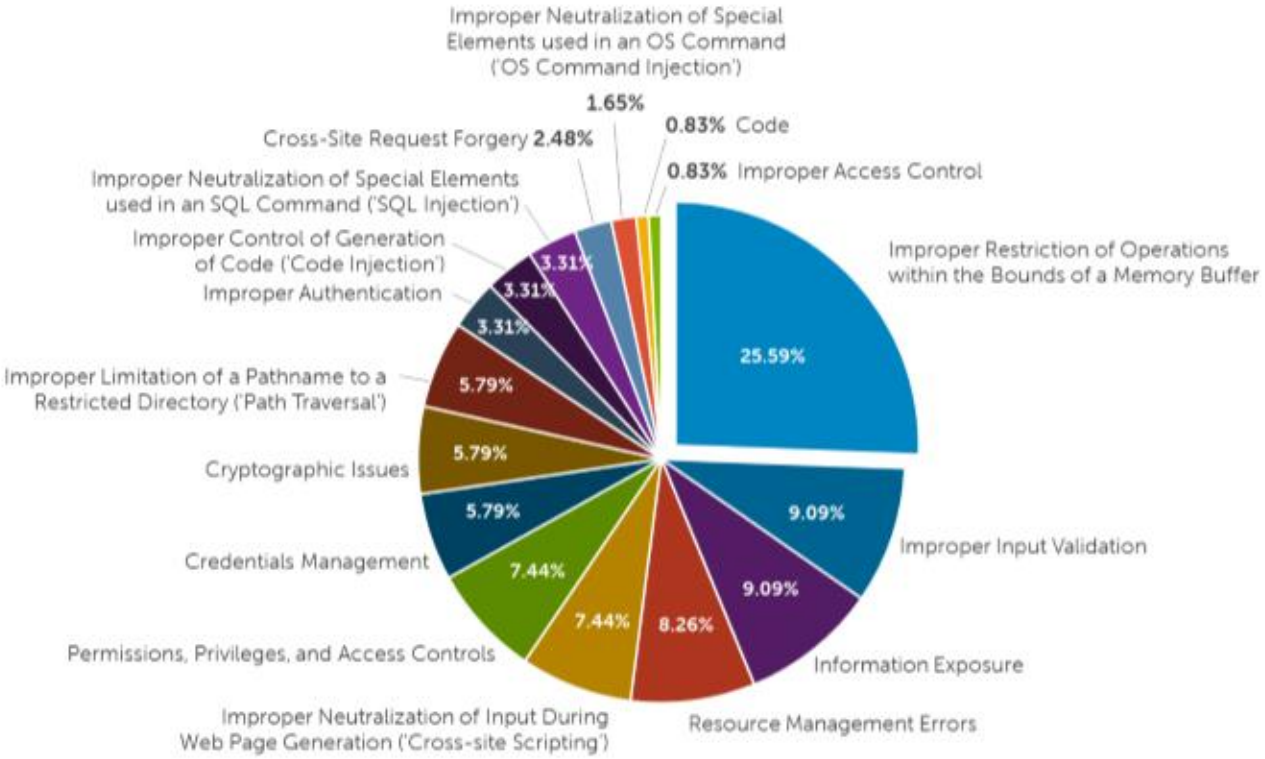
Accident analysis:

Apart from the Bellingham accident in the United States (ARIA 15621), the ARIA database does not list an accident in which the word “SCADA” is explicitly mentioned in the accident summary. These systems have undoubtedly been involved in more events, but analysis of the root cause has unfortunately not been conducted in the area of IT security.

Nevertheless, some lessons can be drawn more broadly on the ergonomics of MMI. Refer to the accident analysis of the treatment part published in 2014 by BARPI in which the following is noted: “If ergonomic defects primarily concern perception errors due to important parameters not visible to the operator, they are also the source of errors, interpretation and decision and sometimes even execution.”

Computer attacks:

As SCADA systems consist of computer servers, they are susceptible to the cyber attacks described in the appendices of this document. In January 2012, for example, the US computer hardware manufacturer, Dell, observed more than 91,000 attacks against SCADA systems, and then more than 163,000 a year later, and more than 675,000 attacks in January 2014. The group states that the majority of these attacks targeted installations in Finland, the United Kingdom and the United States, “one likely factor is that SCADA systems are more common in these regions and more likely to be connected to the Internet”. For example, by 2014, nearly 70,000 attacks targeted SCADA systems across the United Kingdom. These figures are based on the hardware that the manufacturer has installed on these customers' premises to guard against possible attacks. The distribution of the various attacks observed is as follows:



In more than 25% of cases, attacks involve searching for and exploiting buffer memory overflows. Moreover, in more than 9% of the cases, the vulnerabilities targeted concern the validation of the input data. This is without counting SQL injection in more than 3% of cases, or even the injection of code, (3%). This situation highlights the importance of ensuring proper software programming.

Then there are also the vulnerabilities attributed to the implementation of the systems concerned, or to their operation: encryption vulnerabilities, username management, or access and rights control (7.44%).

Dell recommends that its clients do the following:

- ensure that SCADA systems and their software are up-to-date;
- check that the network only accepts “trusted” IP address connections;
- block USB ports and Bluetooth interfaces when they are not needed;
- share information about cyber attacks.

Communication protocols

A wide variety of communication protocols is used in industrial control systems (see diagram on page 5). A keyword search, “Profibus, Profinet, ASI, etc.”, highlighted an event involving the Ethernet protocol at a plastics processing plant in France. Control parameters were stored in memory on a server following micro-disconnection of the Ethernet link, leading to the release of chlorine:

No. 43639 - 03/04/2013 - FRANCE - 57 - MORHANGE

C22.21 - Manufacture of plastic plates, sheets, tubes and profiles

At around 2:10 pm, overheating occurred in a plastics processing plant in a mixer containing 400 kg of PVC. Chlorine was detected by the staff, who then evacuated the premises. The installations were taken out of service. Chlorine measurements were conducted and turned out to be negative. Firefighters, assisted by employees wearing respiratory protection, drained the mixer. Intervention operations ended at 4:15 pm; the gendarmerie went to the scene. The mixer

is managed by a central processing unit (CPU), itself connected to a server which allows for the programming, tracking and recording of the production parameters. Each of the 3 mixers has its own CPU, although the server is common to all. A brownout of the Ethernet link occurred between the incriminated mixer's CPU and the server, generating a “memory effect” toward the server which indicated normal production values, even after the actual shutdown. The latter did not automatically switch off the mixer. Even without a link to the server, the CPU was able to manage the mix to completion. Following joint analysis with the supplier, the reason for the CPU failure or the brownout could not be determined; the cable showed no signs of deterioration. The operator plans to equip the mixer with an additional safety loop, independent from the CPU and the server, allowing for the automatic evacuation of the mixture to the cooling tank should a given temperature be exceeded. The mixer will be switched off and an alarm will sound within 15 seconds. It plans to insert this same loop into the server program. The PLC program will also be modified to add a monitoring parameter that takes the duration of the mixture into account and allows it to be shut down in case it is exceeded. These modifications were carried out from early July and the return of the mixture to service depends on positive operating tests. Finally, the operator plans to undertake additional actions, such as replacing all “sensitive” cables (digital and analogue connections). It will check the possibility to modify the PLC program, jointly with the supplier, in order to prevent values from freezing in the event of an Ethernet link outage. It will also verify the correct operation of the program in the event of various connection breaks and the possibility of integrating additional safety loops for these cases. All actions defined for this mixer will be extended to the other two.

Air conditioning systems

Two events involving air conditioning systems and affecting computer processing centres are listed in the ARIA database:

No. 43506 -19/02/2013 - FRANCE - 33 - SAINT-MEDARD-EN-JALLES

084.11 - General public administration

A safety valve “ruptured” around 11:30 on an air-conditioner undergoing maintenance in the computer room of the administrative building of a technical study centre. All of the chlorofluorocarbon refrigerant in the installation was released into the atmosphere, the pressurised jet damaged the asbestos-containing flocking and dispersed it into the air. The resulting fog triggered the automatic fire detection and extinguishing system. The 100 employees had to evacuate the building. Inoperable since a refrigerant leak observed several months earlier, the air conditioner was repaired by a specialised company. The fire detection system was returned to normal service. Additional fire extinguishers were installed in the room, as the cylinders of the extinguishing system could only be replaced 2 weeks later. As long as the air conditioning system remains out of service (replacement of the valve), the server centre's operation remains fragile due to the presence of just one refrigeration unit which does not have electrical back-up.

No. 5132 - 30/03/1994 - FRANCE - 92 - COURBEVOIE

D35.30 - Steam and air conditioning production and distribution

An explosion occurred at 1:30 am inside an urban heating plant (500 MW, 6,000 m3), with the energy dissipated into the ground estimated at the equivalent of a 50 kg charge of TNT. Operational since 1987, this heating unit comprised 5 boilers (2 coal-fired, 2 fuelled by a coal/gas mix, and 1 gas-powered). During the previous shift, several attempts to start up one of the mixed fuel boilers failed. Unable to restart the equipment and with the gas inlet pressure gauges indicating zero pressure, the foreman of the night shift ordered the opening of both valves a quarter turn towards shutting off the gas inlet on the main circuit. Since the indicated pressure remained at zero, the shift foreman asked the boiler technician to open a blowout preventer and then a butterfly control valve to feed the mixed fuel boiler with gas. This operation resulted in a major gas leak. A gas boiler underwent emergency shutdown, and 2 technicians had exited the unit to cut the general gas supply at the regulator station, 110 m from the building, when the explosion occurred.

One of the 5 employees was killed on the spot. A 10-year old girl, living 40 m from the plant died 4 days later as a result of her injuries; 59 other neighbours were also injured. The installation was destroyed. A total of 600 personnel from local businesses had to be laid off temporarily and 250 residents were displaced from their homes. While awaiting hook-ups to neighbouring utility lines, some 140,000 users and 2.2 million m^2 of office space had no heating or hot water service. Total damage was valued at 544 M francs (or 83 million euros). Investigation results indicated that 3,750 nm3 of gas were probably released beforethe gas utility company was able to cut the supply line 30 min after the explosion. The defective pressure gauges might have been damaged by a pressure surge occurring sometime prior to the accident. The orders issued by the night shift foreman fell under the exclusive responsibility of the maintenance crew; in case of emergency, plant technicians should have requested intervention from the gas company. The blowout preventer had not been designed for handling within a pressurised environment. Moreover, the butterfly valve upstream of the blowout preventer may have been adjusted by the boiler operator while the device was in the intermediate position, where it was no longer sealed since the flanges were slightly spaced. The gas cloud ignited upon contact with the coal-fired boiler, which was operating at the time of the accident. No scenario involving a leak and gas explosion had ever been assessed in any of the site's previous safety reports. The risks related to coal dust had not been addressed either. Dust particle behaviour was also likely to have contributed to the force of this explosion. On May 5, 2004, the Versailles Appellate Court magistrate ruled that the case had no grounds for prosecution.

Points for evaluating the IT security of a plant

In conclusion, several lessons appear to emerge from this analysis and the accident study. The main items worth consideration during an audit of an IT system in a plant relate to:

- **The company's organisation:**
  - Is there a security manager? Does he/she have cybersecurity skills? If not, who handles these aspects? Is there coordination between these two individuals?
  - Is there a rule for closing the computer accounts of outgoing employees?
  - Is there a policy regarding the allocation of user rights based on two main principles?: Assign only access rights that are strictly necessary, and only use access rights that are strictly necessary (in other words, a person with administrator rights on a computer system must log onto another account, with reduced rights, when not performing administrative duties);
  - How are passwords managed? Is there a local management policy? Is it regularly checked, even for passwords of theoretically unconnected systems?
  - Are the technical cabinets containing the PLCs secured?
  - Is access to the computer server room restricted? Are backup procedures in place? Is the level of the programs managing PLCs stipulated (backup of SCADA system servers)? …).

- **IT security:**
  - Is the IT system independent from that related to the management/remote surveillance of the company? Is the nature of the protection (firewall) and the individuals with access to it stipulated? Does the operator have a conceptual diagram of its network with the various protocols used (Ethernet, Profibus)? Does the diagram cover the entire chain of the company's various computer networks (office automation, remote alarm, etc.) within SCADA up to the sensor, passing via VPN and VNC access?
  - What happens if the Ethernet connection is lost? Is the network redundant?
  - Are the communication protocols within the network secure (no transmission of information via HTTP, FTP, Telnet, etc.)?
  - Are TCP/IP traffic analysis probes installed? What is the frequency and nature of the checks? What happens when an abnormality is detected?
  - Does the manufacturer know the ANSSI and its guides (such as the computer hygiene guide)? Are they applied in full (password, personnel cybersecurity awareness)? Does it use ANSSI-certified hardware? Why?

The ANSSI guides can be downloaded from the Internet free of charge, at the following address:
http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

  - Does the operator use a Simple Network Management Protocol (SNMP) system to update all the hardware in its inventory? Is it up to date? How does it ensure that updates are not potentially dangerous? How are file sources identified?
  - Is the operating system used always updated by the manufacturer (Windows 2000, NT, XP)?
  - Has the company's IT system been audited by a specialised company? Have the non-conformities been corrected? Is the last audit report available? Check which part of the system has been audited (the SCADA system, the remote transmission modules, the routers or switches, etc.);
  - Certain input/output modules at PLC level accept SD cards (e.g. Siemens ET200S). How are these cards managed internally?
  - Is software installed that allows the system to be controlled remotely? Has their security been assessed?
  - Is maintenance or monitoring performed using software downloaded from the Google Playstore or the Apple market? Is the risk associated with their use assessed?
  - Are changes on the network or at PLC level managed? Is risk analysis performed?

- Is a fallback phase defined for the industrial processes used on the site? If IT goes down, is the operator able to control the processes in progress on its site? Can its installations be controlled manually?

- **Information sharing / IT monitoring**:
  - Are events considered anomalous recorded? Are they reported to the ANSSI and the Classified Facilities Inspection authorities as soon as they are likely to lead to an accidental risk scenario?

The form for transmitting information to the ANSSI in the event of an accident can be downloaded from the following address:
https://www.ssi.gouv.fr/uploads/2016/04/formulaire-declaration-incident-lpm_anssi.pdf

  - How does the operator monitor cybersecurity (monitoring on specialised websites, which ones?), monitoring of IT security loopholes and updates of PLC components, particularly their firmware (internal operating software)?)

- **The reliability of the measuring instruments:**
  - Do they rely solely on sensors connected to the ICS? Are there physical measurement means independent of the ICS (more difficult to hack)?
  - Are the sensors properly maintained (risk of dirt/corrosion)? By whom?
  - Are the manufacturer's calibration recommendations followed? Are deviations from the manufacturer's recommendations justified?
  - Are the sensors correctly positioned (level sensor)?
  - Are physical measurement surveys planned? Are survey histories maintained?
  - What happens in the event of measurement offset?
  - Are security issues associated with remote data transmission via wireless sensors taken into account? Is there a risk of transmission jamming?

- **Information confidentiality:**
  - Does the company have a data protection policy (data processing, industrial processes, etc.)?
  - Is information about the resistance of pressurised equipment (max. service pressure, bursting pressure, valve calibration pressure) freely available on the Internet?
  - Is information available on the Internet likely to facilitate a hacker's understanding of the company's industrial process?

- **Subcontracting:**
  - On which parts of the ICS can a subcontractor intervene?
  - Is the subcontractor audited and authorised to perform the interventions it has to carry out (quality of the programming/knowledge of the industrial processes and installations)?
  - Can the subcontractor intervene quickly in the event of an accident if a PLC needs to be reprogrammed?
  - Is the hardware used (laptop PC) for programming PLCs reliable (updating of the operating system, anti-virus protection, etc.)? Good practice dictates that foreign PCs are not admitted (PCs “confined to the site” are used for updates).
  - Does the provider have all the information (passwords) concerning the industrial control system or only those required for its task?
  - Is the operator able to intervene on its network or does it systematically call on an external service provider?

- **Air conditioning system:**
  - Is a malfunction of the air conditioning system considered? Does the operator have a back-up system?
  - Are the maintenance and regulatory monitoring of chilling units, subject to pressurised equipment regulations, performed correctly?
  - When auditing urban heating plants that provide “cooling” to other companies, the consequences for these establishments must be investigated, particularly data centres (cloud computing).

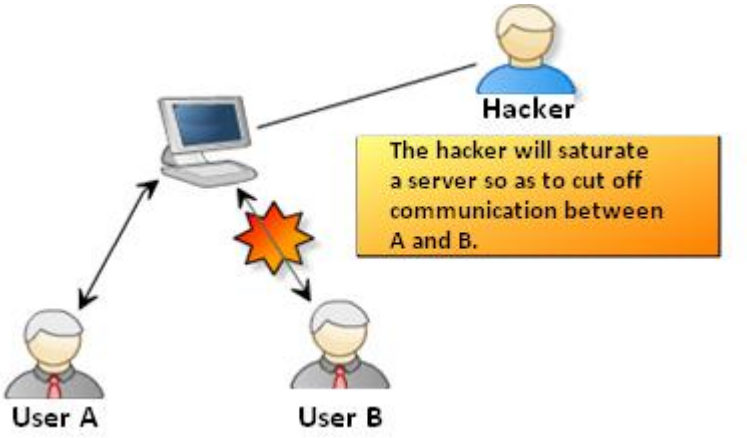
- **Reliability of communications:**
  - Is there redundancy in the Internet connection with various telephone operators?
  - Are the connection nodes or optical zone shared access points remotely located from the subscriber connection nodes (RTCs)? Is their access secured?


Appendices

THE VARIOUS CYBER ATTACK TECHNIQUES

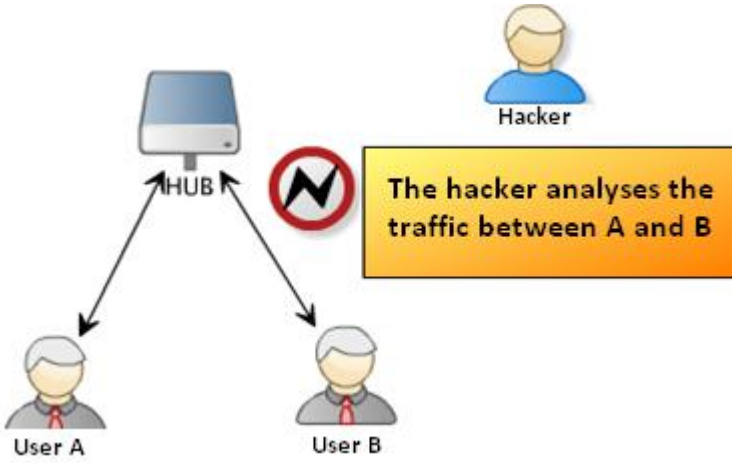
The most common attacks, as mentioned below, can be unique or combined to form “chained exploits”. Hackers are generally skilled and do not act randomly. The objectives behind the cyber attacks are varied: malicious act inside or outside the company, terrorism, industrial espionage, digital warfare to paralyse one's enemy at low cost, and blackmail, etc.

- **Denial of service**: the victim is unable to communicate (e-mails, file server, website unavailable, etc.). Flooding of a server with computer queries may be the cause.



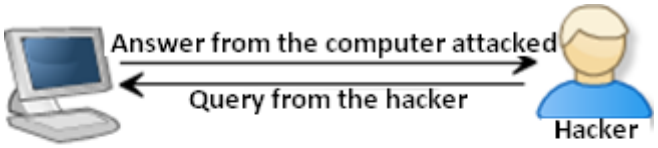
The hacker's objectives: economic blackmail (pay me to stop),
paralyze a website, springboard to launch another attack technique.
Means of protection: maintain software patches up to date on one's operating system.

- **Sniffing**: the hacker analyses the data traffic between 2 computers to discover sensitive data (usernames and passwords, secure Wi-Fi network password)



The hacker's objectives: penetrate a system to steal data
or steal someone's digital identity.
Means of protection: preferably use a switch rather than a hub;
use encrypted protocols for sensitive information such as passwords.

- **Scanning**: a device (scanner) scans the machine's communication ports to determine which ones are open or closed. This technique determines the operating system of the attacked machine and the applications associated with each port. A system administrator can use this method within the scope of his/her duties. One must, therefore, be able to differentiate a hacker from an authorised individual.



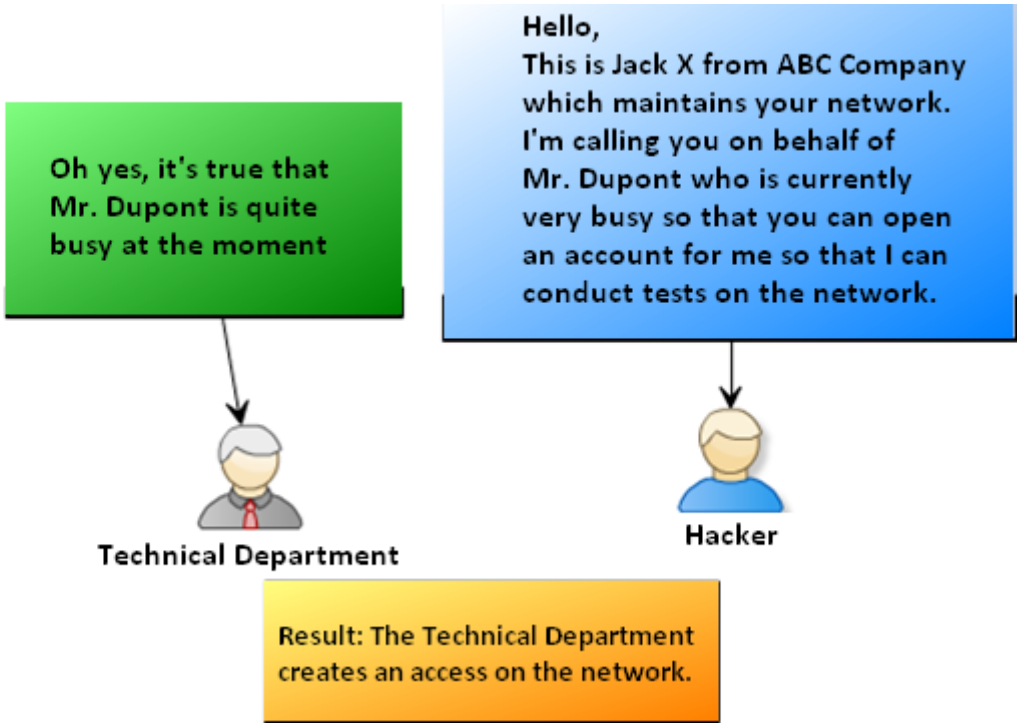
Based on the answer from the computer to certain types of queries, the hacker is able to determine the system's security vulnerabilities.

The hacker's objective: identify potential targets to subsequently launch a denial-of-service attack.
Means of protection: carry out regular inventories of the open ports on one's machine; use a firewall or intrusion detectors.

How do I know which ports are open on my computer?

There are various ways to do this, the easiest way is to call up the command prompt. The command is ***netstat -an***. Open ports are indicated by "listening".

- **Social engineering**: this is the art of manipulating people through information found on social networks ("Facebook", "Classmates", etc.). It does not require any special computer knowledge.



The hacker's objectives: breach of trust, trying to guess a password (date and place of birth) in the hope of subsequently usurping the victim's identity (e-mail account).
The victim is sometimes exposed to intense stress (urgent request) so that he/she discloses information or performs actions that he/she would never have given out or performed under normal conditions.
Means of protection: common sense and appropriate organisation within the company to deal with this type of situation.

- **Cracking of passwords**, hackers use several techniques to accomplish this:
  - dictionary attacks: this method tests all the words in a dictionary since many users use existing words as passwords;
  - hybrid attacks: this method tries combinations of words and numbers, e.g. "envelope01";

- brute force attacks: all combinations of digits and letters are tested. The attack always succeeds, the time required to determine the password is more or less long depending on the password and the means available to the hacker;
- an Internet watch makes it possible to know the passwords assigned by default when equipment is delivered. These passwords are not always replaced during the operational phase. This nevertheless requires an understanding of the premises to know the type of hardware the manufacturer uses (see the section on physical identity theft);
- keylogger type software makes it possible to record the information that a user types on his/her keyboard.

The hacker's objectives: take control of a system (administrator rights), data theft, take control of an e-mail account, etc.
Means of protection: use mnemonic passwords, use two-factor identification (type in the password and then an SMS with a code is sent to the mobile phone of the user)
Note: for e-mail and all communication: use data encryption software.

- **Computer identity theft**:
  - IP or MAC spoofing of the computer they want to attack. This data is sometimes freely available on the Internet via specialised search engines (the shodan.io site is the "Google" of connected objects);
  - take someone's e-mail address;
  - use Phishing: such as sending an e-mail featuring the style guide of a bank.

The hacker's objectives: obtain information, download malware to someone, etc.
Means of protection: Be wary of messages received and don't hesitate to contact the sender by telephone or other means to confirm the request.

- **Physical identity theft**:
  - an RFID scanner is used to copy access badges to secure buildings. Such equipment is available off the shelf from Amazon for around 60 euros (see bibliography).

The hacker's objectives: install infected hardware such as a USB thumb drive or keylogger software in the premises. Find passwords (post-it notes on screens or under keyboards). Find a PC with an open session to be able to send an e-mail, search through the trash.
Means of protection: Security guard services. Video surveillance with strict management of internal and external personnel. Policy regarding the destruction of confidential documents.

- **Runtime or buffer overflow errors**: a particular string of characters must be introduced in order to initiate or cause a runtime error (SQL or javascript flaws for databases).

The hacker's objective: take control of a website or a computer system.
Means of protection: This technique uses the defects or abnormal programming of software (bugs).
It is important to keep abreast of the security flaws surrounding your computer system.
Note: the most well-known security vulnerabilities are listed here: http://www.cert.ssi.gouv.fr/site/index.html

- **Ransomware (e.g. Locky) attacks following identity theft (e.g. through fake invoices): the user receives an e-mail with an MS Word file containing malicious macros that will encrypt the contents of the machine's hard drive, thus making it unusable.** Normal operation is resumed only following payment of a sum of money. This threat is fairly widespread in France (see the ANSSI alert bulletin of March 2016, No. CERTFR-2016-ALE-001).
  For example, the computer controlling a marine current power plant in the Finistère department (France) was hacked in this manner (ARIA 48048). The marine current power plant did not produce electricity for two weeks.

The hacker's objective: make money.
Means of protection: Deactivate Microsoft Office or Libre Office suite macros by default.
Update your antivirus software.

Certain **attacks** do not require **extensive IT knowledge**, but simply **Internet monitoring** (a social engineering attack or exploitation of security vulnerabilities, for example).

A FEW NEWSWORTHY CYBER ATTACKS

1- Stuxnet

General information: This computer virus was first identified in 2010. Its aim was to attack the Iranian nuclear program. The software altered the speed of motors on centrifuges designed to physically separate the isotopes from uranium to produce a highly-enriched nuclear fuel. The virus may have damaged 1,000 centrifuges.

Method of attack: The virus attacks Windows systems using gaps their security and targets systems using SCADA software. The virus is introduced using a USB thumb drive. It then infects other computers on the network. Once in the system, it uses the default passwords to make queries. The worm's complexity is unusual for malware: the attack requires **knowledge of industrial processes** and computer science (**weaknesses in the Windows system)**.

2- Computer attacks at a steel plant in Germany

General information: A German blast furnace was damaged in 2014 because it has not been secured in time.

Method of attack: using a **social engineering attack**, the pirates first infiltrated the computer system of a company's administrative department, and from there they entered the production department. The attack **caused several components to fail** which **prevented the controlled shutdown of the blast furnace**, thereby resulting in damage. According to the report published by the German governmental agency (see reference in the appendix), the hackers had "highly advanced" technical capabilities. They were also **highly knowledgeable of the industrial production processes**.

3- Dragonfly

General information: In 2014, a group of hackers, known as "Dragonfly" penetrated the computer systems of major companies in the energy sector (electricity, gas, pipeline operators, industrial equipment suppliers). According to the antivirus software editor, Symantec, the majority of the victims were located in the United States, Spain, France, Italy and Germany). This is **the second proven case of hacking of SCADA systems**, following the Stuxnet virus. However, the purpose of this cyber attack would appear to be **industrial espionage**.

Method of attack: The Dragonfly group uses mass e-mail campaigns, sending out infected attachments (PDFs) targeting organisations and individuals (executives and senior managers of industrial service providers). This direct mail campaign is further reinforced by phishing. The victim is then redirected to a website to download malware.

Once the target computer is infected, a backdoor device (a Havex type remote access tool) is installed on the computer to take control of it. The Outlook Address Book data and VPN configuration files are also extracted. This data is then written to a file in encrypted format before being sent to the hacker.

The cyber hacking group is thus able to reach the target computer in stages (from the supplier to the manufacturer).

Among the companies that spread the infection are:

- The German company, MB Connect Line (controls for wind turbines and biogas plants);
- The Belgian company, eWon (VPN access).

4- BlackEnergy

General information: In late 2015, more than one million Ukrainian customers were deprived of electrical power. According to several IT security experts, **malware** allegedly infected the network of the electricity supplier, Prykarpattya Oblenergo, in the west of the country. This event perhaps constitutes the largest "blackout" of a computer system of a public utility system. BlackEnergy also infected Ukrainian mining and railway systems.

Method of attack: The malware appears to have spread using a simple macro contained in a spreadsheet. To confuse recipients, the e-mail appeared to have been sent by a government agency and contained a message encouraging them to open the infected document.

BlackEnergy is able to create a backdoor on the computer in order to control it remotely. The malware also includes an access module to the manufacturer's supervisory control and data acquisition systems (SCADA).

The majority of attacks investigated seem to depend on an employee of a company downloading the spy software. The vigilance of individuals reading the e-mails would be the best weapon against the spread of this kind of threat.
However, hackers use social engineering techniques to be very convincing with their request. They are thus able to pass themselves off as a mere supplier and send an invoice in the form of an infected PDF or Excel file. The only barrier is thus the anti-virus software installed on the receiver's workstation. However, the anti-virus database must have the characteristics of the malware, which is hard to keep up-to-date in the case of new polymorphic viruses.
Another common characteristic of the attacks studied is the hackers' knowledge of industrial processes and installations. The attack targets systems that are at the heart of sometimes complex industrial processes. This suggests that these attacks are perpetrated by people with a highly-developed IT and industrial culture.
Also, an "air gap" (no IS interconnection) is not a guarantee against an attack, because they can often easily get around it if an internal support is available (installation of a Wi-Fi thumb drive, for example).

Foreign websites and good practices guides:

Europe

United Kingdom:

https://www.cert.gov.uk/

Sweden:

https://www.msb.se/en/Prevention/Information-security/Publications/

Guide to Increased Security in Industrial Control Systems, with recommendations:

https://www.msb.se/RibData/Filer/pdf/26118.pdf

Germany:

https://www.bsi.bund.de/DE/Home/home_node.html

Spain:

https://www.osi.es/

Outside Europe:

United States:

https://www.us-cert.gov/

China:

http://www.itsec.gov.cn/

TECHNOLOGICAL ACCIDENTS ONLINE

Safety and transparency are two legitimate requirements of our society. Therefore, since June 2001, the website www.aria.developpement-durable.gouv.fr hosted by the French Ministry for an ecological and solidary transition has been offering to both professionals and the general public lessons drawn from analyses of technological accidents. The main sections of the website are available in both French and English.

Under the general sections, the interested user can, for example, inquire for the governmental action programmes, access large excerpts of the ARIA database, discover the presentation of the European scale of industrial accidents, become familiar with the "dangerous substances index" used to complete the "communication on the spot" in case of accident or incident.

The accident description, which serves as the raw input for any method of feedback, represents a significant share of the site's resources : when known, event sequencing, consequences, origins, circumstances, proven or presumed causes, actions taken and lessons learnt are compiled.

Over 250 detailed and illustrated technical reports present accidents selected for their particular interest. Numerous analyses, sorted by technical topic or activities, are also available. The section dedicated to technical recommendations develops various topics : fine chemistry, pyrotechnics, surface treatment, silos, tyre depots, hot work permits, waste treatment, material handling, etc. A multicriteria search engine enables getting information about accidents occurring in France or abroad.

The website www.aria.developpement-durable.gouv.fr is continually growing. Currently, more than 50 000 accidents are online, and new theme-based analyses will be regularly added.

The events summaries can be downloaded at :

www.aria.developpement-durable.gouv.fr

Bureau d'analyse des risques et pollutions industriels
5 place Jules Ferry
69006 Lyon
FRANCE
Téléphone : +33 (0)4 26 28 62 00

Service des risques technologiques
Direction générale de la Prévention des risques
Ministère de l'Environnement, de l'Énergie et de la Mer
Tour Sequoia
92055 La Défense cedex
FRANCE
Téléphone : +33 (0)1 40 81 21 22

Coordination :
Annie NORMAND, Christian VEIDIG
Writer :
Jean-Francois MICHEL

Date of writing : juillet 2016

Translation:
OEC - Office Européen de Communication

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE