Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

FLASH ARIA
February 2019

BARPI
DGPR SRT

Industrial cybersecurity: scope and past accidents

More and more plants and factories are being automated and the amount of information being transmitted over telecommunication networks is increasing. The general consensus is that there is a risk. However, is it possible to delineate this risk and evaluate its consequences — particularly its environmental consequences — by analysing the events logged in ARIA's database?

The term cybersecurity is a neologism that designates all the tools, procedures, security mechanisms, training, best practices, and technologies used to protect a plant's cyber environment. This environment primarily consists of a plant's connected computer and alert networks, but also includes its employees, contractors, applications and their updates, telecommunication networks (GSM, PSTN, fibre optics, Wi-Fi, etc.), automatic control chains (from server to actuator) and all the information sent and/or stored using various exchange or encryption protocols.

ARIA's database is populated with events relating to technological incidents. Although it does not provide detailed statistics about the occurrence of computer attacks, the events in it can be used to highlight a number of disruptions or root causes in an industrial site's cyber environment.

ARIA 50755 – 15/09/2017 – Montoir-de-Bretagne
Accident alert system failure

While an LNG terminal at a Seveso-classified plant was being restarted, natural gas began leaking out at around 6:00 am after a high-pressure pump was turned on. A technician gave the alert and the pump was shut off manually. The pump was then restarted. At around 6:20 am, gas once again began leaking and formed a cloud of flammable gas. The operator activated its internal emergency plan and alerted neighbouring companies using its **telephone warning system**. However, a problem prevented the message being sent out. **A computer glitch or technician error is believed to be the cause.** In addition, **the walkie-talkie communication channels used to manage the event were overloaded.**

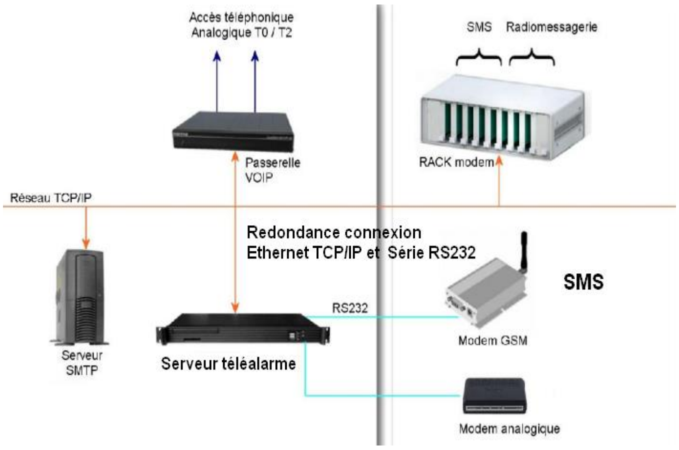
Since the event, **automatic control systems** are checked to ensure overpressure does not occur if the various valves (lineup) are closed or opened. **Telephone lines have also been added** to reduce the time needed to send alert messages via the warning system. Lastly, the technician tasked with operating the remote alarm received refresher training.

Vocabulary of cybersecurity experts:
Threat, vulnerability, and countermeasure

A **threat** is an action that may result in harm or damage.

A **vulnerability**, also referred to as a breach or weakness, is the level of exposure to a threat in a specific context.

A **countermeasure** is a range of preventative actions taken. **Generally, countermeasures are not just technical solutions. They also include user training and awareness** and clearly defined rules.



Operating principle of a remote alarm © DR

ARIA 51131 – 08/02/2018 – Europe
Wastewater treatment plant hit by cryptocurrency malware mining attack

Cryptocurrency mining malware was detected on servers connected to the network of a wastewater treatment plant in Europe. This was the first public discovery of such an attack targeting the network of a critical infrastructure operator.

The malware, which slowed down the network's human-machine interfaces (HMI), was discovered during routine monitoring of the plant's network. Cryptocurrency mining attacks characteristically increase consumption of machine computing cycles and decrease available network bandwidth, slowing down the response times of facility-management tools (HMI/SCADA). According to the media, cryptocurrency mining malware is designed to secretly operate in the background on a computer or peripheral device and disable the tools used to protect them.

ARIA 42931 – 02/05/2012 – FOLKLING
Sensor failure caused by old printed circuit board

A flexible conduit being used to offload methoxymethane (DME) from a truck at a Seveso-classified cosmetics plant began swelling at the connection with the stationary facility. Incompatibility between the material of the flexible conduit and DME was found to be the cause. A technician noticed the leak and alerted the driver, who closed the tank's bottom valve and cut off the truck's engine. The emergency stop button was pressed, placing the unloading station in a safe state. As a precautionary measure, the plant was evacuated for 20 minutes. No injuries or environmental damage were reported.

The accident revealed **a sensor fault. The gas detector fitted at the unloading area failed to work due to a hardware failure affecting the processing unit's printed circuit boards (which dated back to 2001)**. As a result, the sensors were quickly overloaded and sent an 'out of scale' signal. This signal was processed as a sensor fault not requiring any special action when in fact it should activate security procedures.

The manufacturer of the printed circuit boards had identified the risk of failure back in 2008 and corrected the problem **by replacing the boards and updating the software**. However, not all the boards in question were recalled or updated. The operator of the chemical plant subsequently replaced all the boards at an estimated cost of €10,000. It also replaced the gas sensor in the semiconductor unloading area by an infrared sensor.

ARIA 5989 – 01/12/1994 – RIBECOURT-DRESLINSOURT
Incorrectly programmed PLC

An ammonia leak at a Seveso-classified fertiliser plant injured three workers, subsequently killing one of them.

An analysis into the causes of the accident highlighted poor planning of work (particularly when stoping the power inverters) and problems in programming the PLCs used to control a valve.

For further information, click the image to read the detailed accident description:

ARIA

Fuite d'ammoniac
dans une usine de
fabrication d'engrais
Le 1er décembre 1994
Ribecourt-Dreslincourt (60)
France

Chimie
Ammoniac / engrais
Fuite de matière dangereuse
Contrôle / Organisation
Opération manuelle
Victime
Travaux / consignation

LES INSTALLATIONS CONCERNÉES

Le site

Page 1

The accidents analysed in this flash highlight a number of key points that should be kept in mind when protecting a plant's cyber environment:

- ✓ **Telecommunication network/Remote alarm or emergency alert system:**
  - Is the system correctly sized (e.g., number of telephone lines)?
  - Are technicians (security company) adequately trained in using it? Is it regularly tested? Is the list of people to contact regularly checked and updated (fax numbers, etc.)?
- ✓ **Virus attacks:**
  - Does the company implement a user awareness policy?
  - Does it apply cyber threat intelligence (website of the French National Cybersecurity Agency [ANSSI], company cybersecurity officer)?
- ✓ **Computer hardware updates:**
  - Are they regularly scheduled? Are they covered by a risk analysis? What tools are used to ensure that updates are not potentially dangerous?
- ✓ **PLC programming:**
  - Are contractors audited and authorised to carry out the necessary work (programming quality/understanding of the industrial process and facilities involved)?

To learn more about industrial cybersecurity and preventing cyberattacks, download the following BARPI study:

https://www.aria.developpement-durable.gouv.fr/wp-content/uploads/2017/08/2017-08-02_SY_cybers%C3%A9curit%C3%A9_JFM_finale.pdf

If you have comments or suggestions or want to report an accident or incident, contact us at barpi@developpement-durable.gouv.fr
Accident summaries logged in the ARIA database are available at www.aria.developpement-durable.gouv.fr