INCIDENTI DATABASE ARIA

1)Gas leaks in an LNG terminal

**N° 50755** -  **04/12/2017** -  **FRANCE - 44 - MONTOIR-DE-BRETAGNE**

*D35.21 - Manufacture of gas*

Pollution 

Humain 

Environnement 

Economique 

An LNG terminal that was being restarted following a one-week shutdown began leaking at around 6:00 a.m. after a high-pressure pump was turned on. A technician gave the alert and the pump was shut off manually. The pump was restarted. However, gas once again began leaking at around 6:20 a.m. and formed a cloud of flammable gas. The facilities were shut down and their power supplies were cut off. The operator believed that a pocket of gas in a low-pressure circuit of liquefied gas caused excess pressure and opened the valves. The circuit was purged and another attempt to restart the terminal was made. Another leak formed at 8:40 a.m. The operator implemented its internal emergency plan and alerted neighbouring companies via its telephone warning system. An investigation is being conducted to find the cause of the excess pressure (opening of the valves on the low-pressure network).

**Mechanical malfunction of a valve**

An analysis found that a discharge valve on a pump had remained open, causing gas to migrate to the low-pressure network and creating the excess pressure.

None of the valves at the terminal were serviced or tested.

**Communication issues during implementation of the internal emergency plan**

An error, caused either by a computer glitch or human failing, occurred when the telephone warning system was used to send the alert message to neighbouring sites. In addition, walkie-talkie communication channels used to manage the event were overloaded.

**Action taken by the inspection authorities for classified facilities**

The inspection authorities for classified facilities asked the operator for an analysis of the accident to identify the event’s causes and consequences. A model of the dispersion of the gas cloud in the environment will also have to be developed. The inspection authorities drew the operator’s attention to the fact that the repetition of incidents in 2017 point to the need for a comprehensive look at the safety of its facilities and more particularly its safety management system (SMS).

**Measures taken by the operator**

After the event, the operator implemented the following actions:

* leak testing of the discharge valves on the other high-pressure (HP) pumps;
* the test results are recorded in a software program (CMMS);
* pumps may not be restarted if leaks are detected on two valves;
* the automatic control system has been modified to check for the absence of excess pressure if the various valves (lineup) are opened/closed;
* telephone lines have been added to reduce the time required to send alert messages via the telephone warning system;
* the technician has received training in operating the remote alarm system.

51131

**N° 51131** -  **08/02/2018** -  **- 00 – NC** *E37.00 - Sewerage*

Pollution 

Humain 

Environnement 

Economique 

Cryptocurrency mining malware is detected on servers connected to a network of a wastewater treatment plant in Europe. This is the first documented cryptocurrency malware attack to hit a network of a critical infrastructure operator. The HMIs (human-machine interface) are thus slowed down.

The attack is discovered as part of routine network monitoring since an attack of this type increases CPU consumption and decreases the bandwidth available on the network, which reduces the response times of the tools (HMI/SCADA) used to monitor the installations. According to press reports, cryptocurrency malware is designed to operate in stealth mode on a computer or device while disabling its tools to protect it.

Release of methoxymethane during a delivery to a cosmetics factory

**N° 42931** -  **02/05/2012** -  **FRANCE - 57 - FOLKLING**

*C20.42 - Manufacture of perfumes and toilet preparations*

Pollution 

Humain 

Environnement 

Economique 

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.

Ammonia leak in a fertilizer factory

**N° 5989** -  **01/12/1994** -  **FRANCE - 60 - RIBECOURT-DRESLINCOURT**

*C20.15 - Manufacture of fertilizers and nitrogen compounds*

Pollution 

Humain 

Environnement 

Economique 

[ARIA 5989\_AMMONIA LEAK IN A FERTILIZER FACTORY.pdf](ARIA%205989_AMMONIA%20LEAK%20IN%20A%20FERTILIZER%20FACTORY.pdf)

50842

**N° 50842** -  **01/08/2017** -  **NC - 00 - NC**

YYY - Activity not determined

Pollution 

Humain 

Environnement 

Economique 

Computer security experts report a cyberattack on a factory. A group of anonymous hackers introduced malware called "Triton" or "Trisis" into the site's industrial control system (SCI/ICS/SCADA) at a workstation. According to press reports, the software has been around since August 2017. It targets systems based on the proprietary Triconex protocol (non-free and non-publicly documented code).

During the attack, controllers of the safety instrumented system entered a failed security state, automatically stopping the industrial process and prompting the operator to open an investigation.

Several viruses capable of disrupting an industrial process have been discovered in the past: Stuxnet (sabotage of a nuclear power plant), Havex (espionage in the energy sector), Blackenergy and Crashoverride (hacker of an electricity grid in Ukraine).

58778

**N° 58778** -  **24/02/2022** -  **FRANCE - 62 - COUPELLE-VIEILLE**

D35.11 - Production of electricity

Pollution 

Humain 

Environnement 

Economique 

A cyberattack on the satellite linking the remote control and the SCADA (Supervisory Control and Data Acquisition) system of the wind turbines leads to the loss of monitoring and remote control of the wind farm. The wind turbines concerned remain in service and produce electrical energy. They operate in automatic security mode. The operator shall implement daily visual checks of wind turbines.

The loss of communication corresponds to the Russian invasion of Ukraine. The outage is due to a cyberattack.

While the satellite connection is restored, the operator deploys temporary technical solutions such as the use of the 4G network. When ordering the replacement hardware damaged by piracy, it encounters delivery difficulties due to the very high demand, as 30,000 units were affected in Europe (ARIA 58714). The faulty router is removed from the affected sites.

The maintainer plans to set up a larger spare parts storage in a context of global tension in the supply of equipment with semiconductors.

56854

**N° 56854** -  **09/05/2020** -  **FRANCE - 22 - LAMBALLE-ARMOR**

E38.21 - Treatment and disposal of non-hazardous waste

Pollution 

Humain 

Environnement 

Economique 

Around 5 a.m. on a Saturday and the day after a public holiday, the computer network of a biogas company is the victim of a cyberattack by ransomware. The alert is given by the employees following the loss of display of the supervision screen, without stopping the operation of the process. The production team secures the various processes, disconnecting all network cables. A business continuity plan is put in place and process management is carried out in manual and human mode. A communication is made to staff equipped with laptops about the prohibition to connect to the internal network. Two days later, each process is reconnected via network cables directly to the PLCs.

Due to the health crisis linked to Covid-19, teleworking has been deployed and is encouraging the multiplication of computer attacks.

Following the event, the operator implements the following measures:

1. a firewall at the heart of the network on datacenters and sensitive sites;
2. PC control;
3. an organization of network infrastructure teams;
4. security audits;
5. Bulk server recovery tests (1 time/month)
6. the establishment of external control center 7/7 and 24/24h against cyberattacks;
7. a firewall at the heart of the network on the group's 20 strategic sites;
8. user awareness of computer hygiene.

53738

**N° 53738** -  **09/06/2019** -  **FRANCE - 41 - NAVEIL**

D35.21 - Manufacture of gas

Pollution 

Humain 

Environnement 

Economique 

**Characteristics of the facilities:**

1. Automatic operation
2. injection rate in the network: 100-150 Nm³/h
3. Network pressure before injection: 6 bar

At approximately 4 a.m., a biogas (methane) leak occurred on a polyethylene pipeline (HDPE, 6 bar, DN160) between a biogas storage site and an injection site in the natural gas distribution network, in the facility's wire mesh enclosure. A motorist, seeing a "cloud of smoke", contacts the firefighters. A crater just over 1 m in diameter is visible on the ground. Gas technicians cut off the gas supply. Firefighters secure the site. A security perimeter is installed. Road traffic is cut off for 2h35. The installation is at a standstill for a week.

## Overpressure and failure of PLCs (cybersecurity)

The leak is believed to be due to an overpressure of gas that caused the rupture of the underground pipeline serving the injection station. A malfunction of a pressure regulator (20/6 bar) is suspected. This would have caused a sudden increase in pressure and the immediate safety of the injection station generating water hammer in the polyethylene network at a fitting. The volume of biomethane released is estimated at more than 3,500 Nm³. Safeguards integrated into the automation controlling a valve also did not work. This failure is investigated by the operator (PLC failure, actuator?). A lack of communication with the remote site supervising the facilities due to an Internet network cut also compromised the sending of SMS alarms to the operator. As a result, the remotely controllable valves could not be closed until the emergency stop button was activated on site.

## Compliance with pressure equipment regulations

Following the occurrence, the inspection of classified installations verifies the conformity of the fleet of pressure equipment operated. Several regulatory non-conformities are noted: lack of a list of equipment subject to monitoring in service, lack of control program for piping, as well as declarations and commissioning controls not made.

The operator is considering replacing the damaged pipe with stainless steel piping.

56510

**N° 56510** -  **15/12/2020** -  **FRANCE - 27 - VAL-DE-REUIL**

C21.10 - Manufacture of basic pharmaceutical products

Pollution 

Humain 

Environnement 

Economique 

During the night, a pharmaceutical factory is the victim of a cyberattack. Production management and access controls become inoperable. Specific protocols are implemented. The reactions in progress continue thanks to the emergency generators, no start of new synthesis reaction is carried out. Administrative staff are furloughed.

The site had just announced that it would participate in the industrial manufacture of a vaccine against Covid-19.

Following the attack, the operator reinforces its control system and carries out a manual (day and night) a manual check-in of the agents present.

57057

**N° 57057** -  **31/03/2021** -  **FRANCE - 81 - SOUAL**

C20.42 - Manufacture of perfumes and toilet preparations

Pollution 

Humain 

Environnement 

Economique 

Around 4 a.m., the computer network of a cosmetics company is the victim of a cyberattack. The production site is shut down and the 600 employees are informed not to come to work. Remediation is conducted, the virus is contained and the network architecture is modified to prevent any further attacks.

Following the event, the group filed a complaint against X.

This computer attack affects several production sites of the group which are also at a standstill (ARIA 57278).

58868

**N° 58868** -  **01/04/2022** -  **FRANCE - 14 - ONDEFONTAINE**

D35.11 - Production of electricity

Pollution 

Humain 

Environnement 

Economique 

Around 11:30 am, a loss of monitoring of wind turbines by the manufacturer in charge of their maintenance occurs on a wind farm. Remote control of machines is no longer possible. The wind farm operator verifies the proper functioning of its remote management tools and finds that they are operational. The operator informs the stakeholders and sets up a reinforced monitoring mode as well as a mode of regular transmission of monitoring information with the turbine manufacturer. Around 6:30 p.m., communication was restored.

This is a cyberattack.

The main lesson focuses on the effectiveness of the remote management tools that the operator has put in place on its side, thus enabling it to maintain operational control of its wind farm. The operator shall ask the manufacturer for a root cause analysis in order to determine whether or not a strengthening of the security of remote management tools is necessary.

58714

**N° 58714** -  **24/02/2022** -  **FRANCE - - NC**

D35.11 - Production of electricity

Pollution 

Humain 

Environnement 

Economique 

More than fifty wind farms in France and others in Europe are affected by a cyberattack, affecting 30,000 wind turbines. This is the loss of communication of remote control with the SCADA (Supervisory Control and Data Acquisition) system of wind turbines. Wind turbines continue to generate electricity and operate in automatic safety mode. Operators are implementing daily park monitoring visits and increased weather alertness. A park is stopped because of the impossibility of making these visits.

Remote supervision was interrupted due to the cyberattack on the satellite link. It is related to Russia's invasion of Ukraine because the satellites are probably used for communications of the Ukrainian army.

Some parks have local wired control and regularly transmit information to the remote control center. 4G solutions are deployed a few days after the loss of satellite communication but the supply of routers is delayed and white areas persist. Operators switch to another satellite. A month after the incident, all parks have resumed remote communication.

Operators and maintainers want to implement long-term solutions for back-up satellite communication.

58623

**N° 58623** -  **29/01/2022** -  **GERMANY - 00 - NC**

G46.71 - Wholesale of solid, liquid and gaseous fuels and related products

Pollution 

Humain 

Environnement 

Economique 

Several companies supplying oil companies are victims of a ransomware cyberattack. The IT systems of 11 sites of a company in Germany are affected and contingency plans are triggered. Land-based procurement activities are severely disrupted. The tanks managed by the company are no longer able to replenish the trucks used to deliver fuel to the various petrol stations, this process being generally automated. The port of Hamburg and at least six oil terminals in the Netherlands and Belgium were also attacked.

The oil barge unloading management software was reportedly hacked.

60468

**N° 60468** -  **26/03/2023** -  **FRANCE - 53 - CHANGE**

E38.21 - Treatment and disposal of non-hazardous waste

Pollution 

Humain 

Environnement 

Economique 

One Sunday, a waste recovery site is the victim of a cyberattack on its sorting center part. An intrusion attempt is detected and the operator takes precautionary measures, including isolating servers and restricting access to the Internet. The activity is not impacted. A complaint is filed. The cyberattack impacts another site of the same group (ARIA 60545).

60545

**N° 60545** -  **26/03/2023** -  **FRANCE - 82 - MONTECH**

E38.21 - Treatment and disposal of non-hazardous waste

Pollution 

Humain 

Environnement 

Economique 

On a Sunday, a waste treatment site is the victim of a cyberattack. An intrusion attempt is detected. The operator shall take precautionary measures, including isolating servers and restricting access to the Internet. Neither industrial activity nor safety equipment is impacted. A complaint is filed. The cyberattack impacts another site of the same group (ARIA 60468).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CSI | Date | Location | Industrial sector | Attacker type | System infected | Main impact |
| [1](#CSI1) | 2017 | France | PC | ACC | OT | IC-01 |
| [2](#CSI2) | 2018 | EU | WW | INT-EXT | IT | IC-06 |
| [3](#CSI3) | 1994 | France | CM | ACC | OT | IC-01 |
| [4](#CSI4) | 2022 | France | EP | INT-EXT | IT | IC-06 |
| [5](#CSI5) | 2020 | France | EP | INT-EXT | IT | IC-04 |
| [6](#CSI6) | 2019 | France | EP | INT-EXT | OT | IC-01 |
| [7](#CSI7) | 2020 | France | CM | INT-EXT | IT | IC-06 |
| [8](#CSI8) | 2021 | France | CM | INT-EXT | IT | IC-03 |
| [9](#CSI9) | 2022 | France | EP | INT-EXT | IT | IC-06 |
| [10](#CSI10) | 2022 | France | EP | INT-EXT | IT | IC-06 |
| [11](#CSI11) | 2022 | Germany | CM | INT-EXT | IT | IC-03 |
| [12](#CSI12) | 2023 | France | WR\* | INT-EXT | IT | IC-06 |
| [13](#CSI13) | 2023 | France | WR\* | INT-EXT | IT | IC-06 |

\*WR = waste recovery