Études de l'Ifri

# CYBER ATTACKS AND ENERGY INFRASTRUCTURES

## Anticipating Risks

Gabrielle DESARNAUD

January 2017

ifri Center for Energy

The Institut français des relations internationales (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental and a non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Using an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

With offices in Paris and Brussels, Ifri stands out as one of the rare French think tanks to have positioned itself at the very heart of European debate.

The opinions expressed in this text are the responsibility of the author alone.

ISBN: 978-2-36567-724-0

**How to quote this document:**

Gabrielle Desarnaud, "Cyber Attacks and Energy Infrastructures: Anticipating Risks", *Études de l'Ifri*, Ifri, January 2017.

**Ifri**

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

Email: accueil@ifri.org

**Ifri-Bruxelles**

Rue Marie-Thérèse, 21 1000 – Bruxelles – BELGIQUE

Tel.: +32 (0)2 238 51 10 – Fax : +32 (0)2 238 51 15

Email: bruxelles@ifri.org

**Website:** Ifri.org

# Author

**Gabrielle Desarnaud** is a researcher at IFRI's Energy Center. Her work covers China's energy and climate strategies, and the issues raised by cyber security for energy infrastructures.

Previously she worked on China's energy security at the Asia Center in Beijing, looking especially at the challenges of carbon dependency. She has also researched subjects such as the reform of the gas market, and China's policy for developing renewable energies.

Gabrielle Desarnaud holds a Master's degree in International Energy from Sciences Po Paris, and a Master's degree in Sustainable Development from the University of Beijing.

# Foreword

This paper has been written on the basis of a literature review and about 20 interviews with professionals of energy and information systems security. The author would like to thank warmly all the people she met for their support, despite the sensitivity of this subject. While it was not possible to meet representatives of all actors in this field, the persons interviewed did come from a variety of energy and security companies, as well as institutions which are the most representative of the current issues at stake. The information gathered in the interviews and presented here is not attributed, in order to guarantee the utmost confidentiality of the persons who contributed to this study, without being quoted.

# Abstract

The digitisation of the energy industry is revolutionising energy production, storage, transport and consumption processes. Our energy infrastructures, which were designed several decades ago and planned to remain functional for many years to come, are now interconnected with digital equipment with which they interact on a daily basis. These developments have contributed to improve significantly the availability, effectiveness and reactivity of energy systems. But they also open up the possibility of cyber attacks which were relatively unimportant in the energy industry until 2010. The number and technicality of such attacks has increased since the Stuxnet virus was revealed to the world, although this attack on an Iranian nuclear facility remains the most sophisticated ever observed to date. And while there is now a real awareness of these threats in the energy sector, risks remain. Energy transition policies and efforts to integrate renewable energies are compounding these trends so long as cyber security is not integrated into the design of future energy systems. Regulation is trying to adapt to this situation, especially in France where the authorities are working closely with the energy companies to set up a binding regulatory framework, and to protect operators of vital importance (OVIs). This approach is also inspiring other European countries, but common measures throughout the European Union need to be taken rapidly to guarantee the security of our energy networks, which are highly interconnected.

# Table of Contents

# Introduction

The energy industry is entering a digital revolution, albeit with a certain delay compared to other sectors. Information and communication technologies (ICTs) are being gradually deployed across energy infrastructures, and are changing energy production, transformation, storage, and consumption processes. They have the twofold advantage of allowing complex data analysis to optimise the supply chain as a whole, and at the same time providing consumers with a range of more customised services.

The energy industry has strongly benefited from the efficiency gains induced by these technologies: seismic studies, oil drilling, pipeline pressure and temperature management, transmission of electricity through grids, and even trading on the European electricity exchange are henceforth carried out using ICTs. Access to real time data from plants and equipment at all stages of the value chain will considerably improve decision-making in the near future.

Some actors in the energy industry are concentrating on industrial Internet as a fully fledged separate activity: for example General Electric has set up a platform to collect and analyse data provided by sensors within industrial automation systems. Companies will therefore be able to establish statistics and create production profiles, optimising the profit margins of plants and equipment, and maximising their availability through predictive maintenance. These trends are also being accentuated by energy transition policies: the deployment of 35 million smart meters in France should help rationalise energy consumption, establish detailed consumer profiles in order to better anticipate demand, and improve investment planning for heavy infrastructures. At the same time, they should provide consumers with more detailed information so they can manage their consumption on their own and save energy. The smart grids will allow industrial and domestic infrastructures to be connected, thus providing a holistic vision of consumption at different levels of a geographical territory.

However, this enhanced digitisation also exposes the energy industry to the risks which the tertiary industry has already faced for several years. In 2007, the Idaho National Laboratory proved that a cyber attack could physically damage some components of the electricity grid. The experiment showed that a computer malware could operate the circuit breakers of a diesel generator in order to connect and disconnect it from the grid repeatedly, to the point of bursting into fire.[1] Subsequently, a number of identified cyber attacks on energy infrastructures have highlighted their potential damage under real conditions.

This study will analyse the risks faced by the energy sector and especially electricity infrastructures, in particular with regard to the energy transition. A review of the measures deployed in France and at the European level will also aim to determine the room for action still to be considered, in order to stimulate progress.

[1] M. Zeller, " Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?", Schweitzer Engineering Laboratories, 2011, available at: https://selinc.cachefly.net/.

# The Energy Industry at Risk of Cyber Attack

## Technical and human vulnerabilities

For a long time, energy systems were characterised by a certain degree of autonomy with respect to digital technologies. Decades long investment cycles have delayed the integration of these digital components into industrial sites and equipment as well as the use of mass-market computer programs and operating systems.

Until recently, the energy industry was therefore little exposed to the risk of cyber attack, since industrial sites mostly used mechanical or analogue equipment, and proprietary programs or protocols specific to each activity or installation. These could only be attacked with detailed knowledge of systems, while the lack of connections to the outside world limited the possibility of cyber spying. Even in the eventuality of someone managing to attack a system, it would have been necessary to repeat the same steps for locating and creating malicious and infiltration software, specific to each installation targeted. Until recently, the energy systems had not been much attacked compared to administrative offices or entities and so remained little protected.

Subsequently, three factors have led to the gradual integration of ICTs in the energy industry:

- the need to rationalise production with tools capable of collecting and processing large quantities of data;
- the need to share data with actors outside the sectors' industrial sites (operators, management entities, maintenance teams etc.);
- the need to make savings on software used and to facilitate the communication between management sites and industrial sites.

To meet these needs, the energy industry has gradually turned towards using turnkey operating systems and industrial control systems

(ICS), available on the market (see Annex 1).[2] These systems are less expensive than proprietary control systems, but are also better known to the general public, and thus more vulnerable to malware circulating in cyberspace. In parallel, connections and exchange of data between outside entities have multiplied: an electricity operator today needs to be able to observe the state of the network and production in real-time, and to communicate some of this information to other actors. A service provider may also require connection at a distance to carry out maintenance operations on certain plant and equipment. As a result, proprietary industrial control systems that were relatively isolated have been transformed into open architectures, using standard interconnected technologies with company networks and Internet.

The opening up of poorly protected industrial networks is not their only weakness. While the energy industry is embarking on unprecedented digitisation, its equipment has sometimes been functional for more than 30 years, while some others will remain operational for several decades. Such machinery was designed at a time when the infancy of Internet simply ruled out any concerns over cyber attacks. Protection against such attacks was simply not included in security functions. Systems were therefore programmed to be precise, stable, predictable, resistant, but not to use encryption or authentication protocols, amongst other functions. In fact, existing vulnerabilities have not necessarily been identified in all industrial facilities, as industrial managers face a certain difficulty in knowing exactly the history and configuration of all the devices and components of their installations.

However, traditional IT security solutions, such as the application of security patches when a particular vulnerability has been discovered in some software, are not easily applicable in industry. Indeed, according to one person interviewed, setting up “active defence” (such as anti-viruses) would lead to unpredictable shutdowns of 10% to 20% of machinery. The functioning of other equipment may also be altered. Applying software updates requires carrying out long tests in order to ensure that installations are restarted without any inappropriate interactions. For this reason, most software in industry is only very seldom updated, if ever, while flaws and vulnerabilities are often documented and accessible on Internet.

[2] ICS are Information Systems used to control and automate numerous industrial processes. This is a general term for different types of software, including supervisory control and data acquisition systems (SCADA). These are used a lot in the energy industry and are known to be vulnerable to cyber attacks. They are control/command systems which allow for the remote supervision and control of plant and equipment.

In the case of a nuclear power station for example, the best room for renewing equipment is during the "10 year safety visit": in other words when the station is shut down for several months once a decade allowing for extensive tests and upgrades to be conducted.[3] Many electricity and gas transmission companies still use obsolete operating systems in flow management operations, because of the difficulties involved in migrating to recent versions of software.[4] In 2015, the public body responsible for auditing government spending in Japan[5] instructed the operator of the Fukushima nuclear-power plant (Tokyo Electric Power Company-TEPCO) to upgrade some 48,000 computer stations still working with Windows XP in favour of a more secure operating system.[6] Although Microsoft had announced for several years that security patches would no longer be supplied after July 2015, TEPCO had planned to delay investment in the new software.[7] The upgrade has taken place since.

In addition, human errors are very common: the lack of training concerning external connectable devices (phones, laptops, USB flash drives), default passwords that remain unchanged on workstations or programmable logic controllers (PLCs) for practical questions or due to negligence, the lack of complex authentication systems for remote connections, etc. (Annex 2).

Up until 2010, risks incurred and protective measures to be implemented had not been examined in detail. The main trigger of concerns by industrial operators, and especially the energy industry, was the discovery of the Stuxnet virus in 2010, at the Iranian uranium enrichment site of Natanz. This event showed that the energy industry could experience attack both in its management network (offices and administrative bureaus), and in infrastructures. Given the nature of the energy industry and its vital role in any economy, these systems can be considered as a prime target.

[3] IRSN, *Visites décennales : Réévaluer la sûreté de la deuxième génération*, 2010, available at: www.irsn.fr.

[4] "Windows XP in Utilities Could Mean Big Security Problems", *The Wall Street Journal*, available at: http://blogs.wsj.com.

[5] Board of Audit of Japan, available at: www.jbaudit.go.jp.

[6] Board of Audit of Japan, the audit result of Tokyo Electric Power Co., Ltd concerning indemnities for nuclear damage: p. 100, available at: www.jbaudit.go.jp.

[7] TEPCO, Press release, 6 July 2014, available at: www.tepco.co.jp.

# Known attacks on energy infrastructures

## *Interesting precedents*

Documented attacks on the energy sector are still scarce. Some are particularly elaborate and supposedly supported with government resources, while others do not necessarily target the energy sector in particular. Some technical incidents also illustrate the damage a targeted cyber attack could cause.

### Slammer: a simplistic worm

In January 2003, the safety parameters display system of the Davis-Besse nuclear power plant in Ohio stopped for several hours due to infection by the Slammer computer worm. This safety system collects data from cooling systems, radiation sensors and other critical information within the power station to provide real-time information on the physical state of the plant. This is the system which would trigger an alarm in case of a reactor meltdown. It is interesting to note that the Slammer worm is just a small code which has no function other than sending copies of itself via internet to randomly generated IP addresses. The power station was therefore not specifically targeted but had an unsecured connection to a third-party company (which was infected by chance with Slammer, as were thousands of others). The rest of the plant's network was protected with a firewall which would have prevented contamination.[8] Moreover, a patch had already been released by Microsoft six months before the attack, which indicates the problems that industrial installations have in applying basic IT security procedures. The power station had been shut down for more than a year when the attack occurred.

### Stuxnet: a brutal awakening

Stuxnet has been the most advanced attack on nuclear infrastructure so far. The first version of this extremely sophisticated malware was launched in 2005. Using several "zero-day"[9] vulnerabilities, Stuxnet was designed to attack the uranium enrichment site at Natanz in Iran. The worm was probably passed into the industrial network of the factory via an infected USB flash drive. The malware infected the PLCs that run the spinning

[8] B. Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", *Strategic Insights*, Vol. 10, No. 1, 2011, p. 15-25, disponible sur : http://large.stanford.edu.

[9] This refers to vulnerabilities of a programme which are still unknown and for which there is no security patch released. These vulnerabilities can be sold for several hundreds of thousands of euros (to companies or governments) and are also traded on the black market.

machines and modified the rotation speed of centrifuges in a repeated way. This compromised the enrichment process and caused damage to the centrifuges, spinning at enormous speed and suddenly slamming on their brakes. About 1,000 centrifuges were damaged at the site before the worm was discovered in 2010. To escape detection, Stuxnet recorded the measures of operations during normal operating phases, and played these back repeatedly to the control interface when the computer worm was taking control. This way, even though on site engineers could notice that the speed of rotation had somehow changed, no alarm would be triggered. This program was specifically designed to attack the Iranians' systems and only activated itself when encountering the very precise configuration of the site under attack, such as the exact number and layout of the centrifuges. The attackers thus carried out extensive reconnaissance of the installations beforehand and surely reconstructed parts of the equipment identically in order to test the program before infecting the Iranian factory.[10] Though it is difficult to attribute the origin of the attack with certainty[11], several enquiries have revealed that its creation was supported by the American and Israeli governments.[12] The primary intention was to slow down Tehran's nuclear programme, possibly to gain time to complete diplomatic negotiations.

### Shamoon: limited spread thanks to adequate protection

In August 2012, a malware called Shamoon destroyed about 30,000 computers of the Saudi Aramco oil company. Part of the programme was configured to destroy the master boot record of hard drives, preventing them from restarting.[13] The primary aim of this attack seems to have been sabotage, possibly with the wish to interrupt some of the company's industrial activities. In fact, the programme did not contain any functions designed to control or attack the industrial system, even though it could have destroyed computers linked to the operation of production or maintenance of machines. Saudi Aramco seems to have had reasonably reliable security systems in place for the attack to be restricted to the firm's management network, without being able to spread into the separate and protected operational network. According to the company, this incident

[10] D. E. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran", *The New York Times*, June 2012, available at: www.nytimes.com.

[11] For more information on the attribution of Stuxnet, see G. Desarnaud, "Le secteur énergétique exposé à la cyber-menace", *Édito Énergie*, Ifri, 12 July 2016, available at: www.ifri.org.

[12] D. E. Sanger, *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*, New York, Broadway Books, 2012.

[13] The first partition of the hard disk which allows the operating system to be loaded.

had no impact on oil activities, even though running operations (invoicing, settling contracts, etc.) had to be carried out manually, as new hard drives were installed. [14]

## Energetic Bear: the importance of securing the supply chain

In 2014, some 250 energy companies in the United States and Western Europe were infected by a virus similar to Stuxnet, called Energetic Bear. This malware had probably been operating since 2011, and had mainly infected electricity producers, electricity and oil distribution operators as well as equipment manufacturers. In particular it allowed attackers to take control of industrial equipment. The group responsible for the virus was reported to have first infected three manufacturers of industrial control systems which would then have transmitted the virus to their energy customers during upgrading or maintenance operations.[15]

## BlackEnergy: vulnerable electric grids

In December 2015, an attack on the Ukrainian power grid deprived some 200,000 residents of electricity for several hours. A phishing campaign likely introduced a malware into electricity operators' ICS in order to take remote control over the distribution of electricity. Acquiring passwords beforehand facilitated access to the internal network, allowing the attackers to activate circuit breakers in about 30 electricity substations, and to cut off current. The transfer of electricity to lines still operating overloaded other parts of the network. In parallel, two control centres blacked out, as their backup power system had been reprogrammed by attackers not to be triggered in the event of overall power failure.[16] A module similar to Shamoon seems finally to have damaged hard drives, preventing the rebooting of operating systems. Several weeks after the incident, a certain number of electricity substations were still being operated manually, even though such infrastructures are usually fully controlled remotely.[17]

[14] Symantec, *Targeted Attacks Against the Energy Sector – Security Response*, 2014.

[15] Symantec, *Dragonfly: Cyberespionage Attacks Against Energy Suppliers – Symantec Security Response*, 2014.

[16] Uninterruptible power supply (UPS).

[17] SANS-ICS, E.-I., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016.

## Documented Attacks and Incidents Affecting Energy Infrastructures

| Year | Target | Name of the attack | Consequences | Objective | Attackers |
|---|---|---|---|---|---|
| **1982** | Explosion of a gas pipeline in Siberia (Russia) | | Malware introduced into the SCADA managing the pipeline, the explosion was equivalent to 3 tonnes of TNT. | Sabotage | External |
| **1992** | Ignalina nuclear-power station, (Lithuania) | | A technician at the Ignalina nuclear-power station introduced a virus into the control system of one of the two RBMK reactors (Chernobyl type). | Sabotage | Internal |
| **1992** | Emergency warning system at Chevron, (USA) | | An employee dismissed by Chevron activated the emergency warning system of the company by hacking the computers in charge of the system. The intrusion was only discovered when an accident took place at the Chevron refinery in Richmond, during which thousands of people living nearby were exposed to toxic substances for about 10 hours. | Sabotage | Internal |
| **1999** | Gazprom, (Russia) | | Takeover of the distribution panel controlling gas flows through pipelines. | Sabotage | Internal |
| **1999** | Gas pipeline in Bellingham (USA) | | This accident was linked to the development of a database for the SCADA system operating the pipelines of the Olympic Pipe Line company. The accident was partly responsible for the spillage of oil causing three deaths and several injuries. | Accident/ human error | Internal |
| **2001** | Electricity operator California, (USA) | | The attackers had access to one of the internal networks of the California Independent System operator. The attack only affected the PLC network of the company before being discovered. | Sabotage | External/ China? |
| **2003** | Davis-Besse Nuclear-power, (USA) | Slammer | Shutdown of the parameter display system for four hours due to a worm, with no espionage or sabotage functionality. | Not targeted | External |
| **2008** | Hatch power plant, (USA) | | The updating of the computer management system of the operator led to an error in the control system of the reactor, causing an unintentional shutdown for 48 hours. | Incident/ human error | Third-party |
| **2010** | Natanz, (Iran) | Stuxnet | Several years of infiltrating the uranium enrichment at Natanz, damaging more than 900 uranium enrichment centrifuges. | Sabotage | External/ State-sponsored/ USA, Israel? |
| **2011** | Oil and gas industries | Night Dragon | Extracting confidential information about oil and gas projects. | Espionage | External |
| **2011** | Energy industries | Duqu | Parts of code nearly identical to Stuxnet, designed only for industrial espionage, without any destructive function. | Espionage | External |
| **2011** | Areva, (France) | | Theft of non-critical company data. Infiltration over two years. | Espionage | External |
| **2012** | Companies and institutions linked to | Flame | Widespread in the Middle East and North Africa, operated for at least two years. Designed for espionage and data analysis. Discovered after Iran's Ministry of Oil and the | Espionage/ data theft | External |

| | | | | | |
|---|---|---|---|---|---|
| | energy | | Iranian National Oil Company had reported theft and the erasure of some important data from their systems. | | |
| **2012** | Saudi Aramco, (Saudi Arabia) | Shamoon | 30,000 hard disks destroyed and to be replaced, no impact on the operational network. | Sabotage | External |
| **2013** | Bowman Avenue Dam, (USA) | | Attackers had taken remote control of a small dam near New York, with no consequences. | Reconnaissance | External/ Iran? |
| **2014** | Energy companies | Energetic Bear | 250 companies in the USA and Western Europe were infected. | Espionage/ potential sabotage | External |
| **2014** | Petrol stations | Operation Petrol | The *Anonymous* group of *hacktivists* announced its attack on oil companies and petrol stations (denial of service, data theft). There is little information about what was done or not. | Sabotage/ data theft | Anonymous |
| **2014** | Korea Hydro and Nuclear Power (KHNP), (South Korea) | | Theft of plans and manuals of two reactors, electricity circuits, measures of radiation exposure in the zone, and data on more than 10,000 employees. Following pressure on the government by activists to close down three reactors. | Blackmail | External |
| **2015** | Electricity operators, (Ukraine) | Black Energy | 30 electricity substations disconnected from the grid, eight provinces without electricity for several hours, more than 200,000 people affected, ICS physically damaged, substations manually operated for several weeks after the event. | Sabotage | External/ State-sponsored, Russia? |

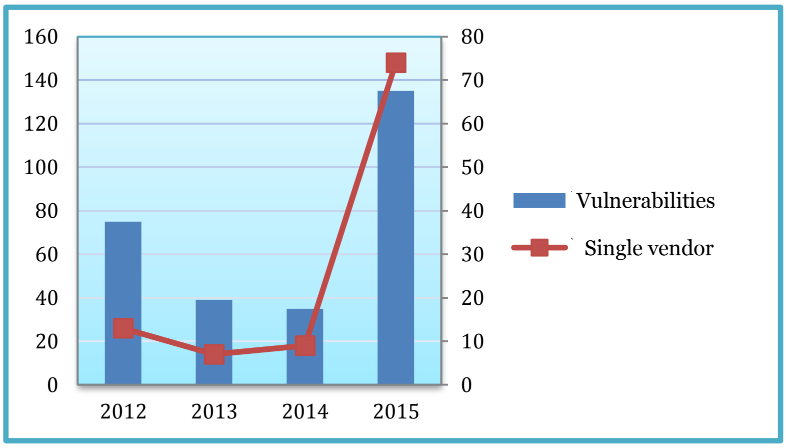
*Non-exhaustive list. Source: B. Miller, and D. C. Rowe, Symantec, ICS-CER, NERC.*

## The energy sector as a prime target

The discovery of Stuxnet in 2010 created a shockwave throughout the energy industry. The attack acted as a projector on unknown vulnerabilities, revealing the political as much as the financial dimensions of cyber attacks targeting the energy industry.

Since then, there has been an increase in attacks on the energy sector, as well as discoveries of vulnerabilities in industrial systems. As the table below shows, these attacks rose by 380% between 2014 in 2015, much more than the discovery of vulnerabilities associated to plug-ins or cell phone operating systems. The know-how of hackers in this area is improving, whereas there are very few cyber security experts for industrial systems at present. The discovery of vulnerabilities in ICSs delivered by a single vendor is also increasing, placing risks on all their corporate clients.

### Discovery of Industrial Vulnerabilities in the World (2012-2015)



### Discovery of Vulnerabilities by Type (2014- 2015)

| | |
|---|---|
| **"Zero day" vulnerabilities** | + 125 % |
| **Browsers** | + 37 % |
| **Plug-ins** | + 102 % |
| **Internet** | + 2 % |
| **Cell phones** | + 214 % |
| **Industrial** | + 380 % |

*Source: Symantec,* Threat Landscape Evolution and Internet Security Threat Report*, 2016.*

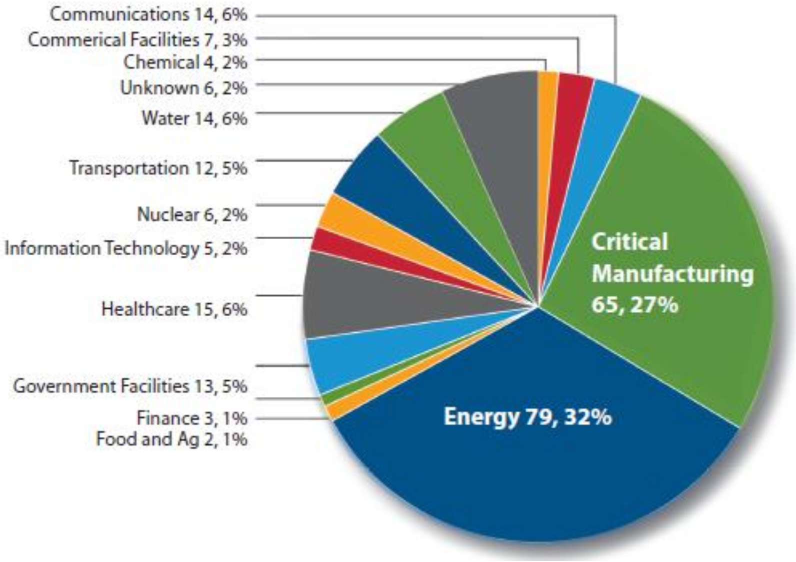
In 2014, the American authorities were solicited for 245 attacks on industrial systems in the United States[18], most of which occurred in the energy sector, and half of which can be considered as advanced persistent threats.[19] These are on average discovered 200 days after they have effectively infiltrated a companies or factory network.[20]

[18] US fiscal year, October 2013 to September 2014.

[19] Advanced Persistent Threat: a type of IT attack mobilising significant financial and technical means, which may last several years. The target is generally defined and studied beforehand (US Department of Homeland Security, 2015).

[20] Mandiant, *M-Trends Report 2015: A View from the Front Lines*. *Premier Outlook* (Vol. 4). 2014, available at: https://login.proxy.bib.uottawa.ca.

**Incidents Reported by sector in the United States, 2014 (Total 245)**



"Critical Manufacturing" refers to equipment manufacturers, some of which supply ICSs and PLCs to the energy sector.

*Source: US Department of Homeland Security, ICS-CERT Monitor 2014*

Interviews with companies operating in the energy sector have revealed that they are confronted by cyber attacks on a daily basis. Institutions linked to the energy industry are not spared: the US Department of Energy reportedly suffered 150 "successful" attacks between 2010 and 2014, targeting systems in which critical information about the electric grid and certain nuclear power plants could be found.[21]

## Financial and geopolitical motives

Three types of attack can be identified to date:

- attacks which aim to interrupt the availability of a system or a service;
- attacks on confidentiality which aim to acquire information and monitor an activity, often for financial gain;
- attacks on the integrity of the system aiming to change or disrupt information or processes (removing critical software, modifying the behaviour of certain types of machinery, causing SCADA to send false commands, etc.).[22]

[21] "Records: Energy Department Struck by Cyber Attacks", *USA Today*, September 2015, available at: www.usatoday.com et https://assets.documentcloud.org.

[22] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014.

The type of attack can sometimes reveal the profile of the attacker. Attacks on confidentiality for example are often carried out by criminal gangs seeking to exploit the theft of data in certain markets, and may even be sponsored by competitors.

## *Risks of sabotage: political and geopolitical factors*

Cyber attacks generally have financial or espionage motives: the financial sector remains the most targeted to date. However the energy industry also faces attempts at sabotage, sometimes for geopolitical reasons. For the two most devastating attacks known (Stuxnet in 2010 and BlackEnergy in 2015), the capacity mobilised and the investigations conducted in the field suggests that these attacks were supported by States rather than activist groups or independent criminal actors.

In the Iranian case, apart from the reproduction of part of the original installation, the analysis of the program itself surprised experts in its ingenuity and complexity. The malware was developed for this specific installation, which is rare because it requires highly developed IT and automation engineering skills. Very few people have developed competencies in both fields at the moment. The BlackEnergy program which targeted Ukrainian operators was also the result of several months of work by a team backed with considerable finance.

Faced with such attacks, experts are formal: it is no longer a question of knowing if attacks will breach the targeted companies' industrial system, but when.

Given the consequences of using such IT resources against energy infrastructures, this type of attack could be considered as an act of war, which thus discourages ill-intentioned States from acting. However, the difficulty of attributing a cyber attack also protects the assailant and allows hackers to perpetrate devastating actions without overt engagement. The use of false flags, which is very frequent as malware used progressively become public and can inspire other individuals, complicates the identification process. It limits the capacity of open retaliation, or even the formation of coalitions denouncing the actions of the sponsor. But it can certainly lead to diplomatic tensions and a game of cyber dissuasion which would reshuffle geopolitical cards. Experts in information systems security agree that several States have the means to carry out large-scale attacks against European energy systems. However, some experts believe that the costs (in diplomatic, economic or commercial terms) of such sabotage are greater than the benefits which the attacking State could obtain. It remains possible that a terrorist entity could link up with a group of hackers to carry out such attacks. However, one expert in IT security interviewed for this report stressed that nothing at present suggests that such manoeuvres are being prepared.

Certain activists could also constitute a threat even if they do not seem at present to have the technical means to attack critical infrastructures. In 2014, *Anonymous* launched Operation Petrol, which aimed to attack oil companies and denounce the use of the US dollar in the oil trade. While the announcement of the attack by the group of "hacktivists" did indeed make a lot of noise, it does not seem to have been very successful. Three years earlier, the US Department of Homeland Security demonstrated that the group did not have the capability of attacking industrial control systems.[23] According to certain experts this is still *a priori* the case.

## Financial motives: data theft and espionage

Financial motivations may encourage an attack on the control system of an energy infrastructure. Nevertheless, there are several obstacles limiting the profitability of such a choice compared to what can be done by simply targeting a company's management network: industrial systems remain quite unknown to hackers, and controlling the effects of an attack on installations requires precise technical knowledge in IT but also in automation. In comparison, ransomware bring billions of euros each year through traditional IT resources, with no need of aiming at critical infrastructure. Which is why the financial sector still pays the highest price of targeted cyber attacks.[24]

Finally, industrial espionage also comes into play, even though it is complicated to copy plant and equipment configuration by introducing espionage software. The resources used should be particularly significant, while technical documents about targeted plant and equipment are often stored on companies' corporate networks. These are easier to attack using conventional means. The attack on Korea Hydro Nuclear Power in 2014 illustrates this well. The attackers were not aiming at industrial espionage, but were able to obtain the plans and manuals of two reactors from the company's office network. Obtaining the configurations of the reactors by infiltrating spyware would have been much more complex. The Stuxnet

[23] Department of Homeland Security Bulletin: *Anonymous Hacktivist Threat to Industrial Control Systems (ICS)*, October 2011, https://publicintelligence.net.

[24] PwC, *Global Economic Crime Survey 2016*, available at: www.securityweek.com, Symantec, *Internet Security Threat Report 2016*, available at: https://resource.elq.symantec.com.

attack, however, shows that a certain degree of detection is possible in this way, given sufficient resources.

A certain number of documented attacks on energy companies illustrate the reasons for which this sector is a lucrative, as well as geopolitical target. While some incidents are never reported or discovered, an increase in attacks against energy infrastructures has been observed in the past 6 years. The rising digitisation of the energy industry has exposed new vulnerabilities, and anticipating risks has become crucial in order to develop robust protection systems.

# Vulnerabilities in Power Grids

## Risks to our present and future energy systems

### *The power grid: at the heart of critical infrastructures*

It is in the electricity supply chain that the consequences of a cyber attack would be greatest. Flows in the electric grid are instantaneous, which rules out any possibility for reacting manually to stem the consequences of a large-scale attack. The integration of Europe's electricity grids makes them more resilient, but also exposes each country to the instabilities of its neighbours. The incident that faced the European grid in 2006 is quite representative of what a cyber attack might provoke. The disconnection without any warning of a high-voltage line in Germany deprived 15 million Europeans of electricity for several hours, even causing the Spain-Morocco interconnection to trip.[25] Even though it is important to keep in mind that it was the consequence of a communication error between dispatchers, and that European networks have evolved considerably since 2006, it illustrates the implications which a cyber attack on the European electricity systems could have, in a scenario similar to what happened in Ukraine, but at a continental scale.

The first consequences of an attack on the electricity grid would be financial. For example, considering that an undelivered megawatt hour (MWh) costs  RTE (the French transmission system operator) an average €26,000,[26] then the disconnection of a 10 MW consumption area for two hours is worth about half a million euros. At a State level, in 2015 the Lloyd's insurance market simulated the costs of a cyber attack on several electricity generators in the United States. The subsequent shutdown of the

[25] Union for the Coordination of Transmission of Electricity UCTE, *Final Report, System Disturbance on 4 November 2006*, available at: www.entsoe.eu.

[26] The cost of a power cut from more than 3 minutes: see Programmation *pluriannuelle de l'énergie*, available at: www.developpement-durable.gouv.fr.

network in 15 states would lead to a total cost to the US economy of between $243 billion and $1 trillion.[27]

As a supplier of essential services, the electricity sector is a key actor in raising awareness about cyber risk. If the supply of electricity is interrupted for several days, other critical infrastructures (health, transport, communications, financial transactions…) will only be able to operate until their emergency diesel reserves have run out. The risks of collapse in other economic sectors are many, including: the breakdown of the cold chain in food warehouses; telecommunications reduced to a strict minimum (in the armed forces, government services, etc.); water processing and distribution services in danger, etc. All this not counting the damages suffered by the energy industry itself, which is dependent on the supply of electricity, if only to maintain cooling systems in nuclear power stations, or to provide petrol to back up generators. In 2011, an official report by the Office of Technology Assessment (a research organisation reporting to the German Bundestag) analysed the impact of an extended electricity blackout on German society. The authors show that within a few days, the supply of food and water could no longer be assured, and would take several weeks or even months in some cases to return to normal, once electricity has been restored.[28]

## *The present risks to electricity grids*

### Sensitive points in the transmission network

While the whole electricity value chain is vulnerable, the transmission network is the most critical part. Its well functioning ensures the stability of the whole electricity grid, and its dispersed infrastructure is difficult to protect.

The consequences of a cyber attack on the electricity grid would be quite similar to physical events such as extreme weather, and for which operators are prepared thanks to recovery plans. However the specificity of a cyber attack lies in the possibility to target several of the grid's nerve centres simultaneously. The consequences could be difficult to control and would limit the possibility of physical intervention by maintenance teams, which are properly dimensioned to address relatively localised problems, but not large enough to respond to a large scale, widespread attack. One person interviewed confirmed that it would be possible for a co-ordinated

[27] Lloyds and University of Cambridge, *Business Blackout – The Insurance Implications of a Cyber-attack on the US Power Grid*, 2015.

[28] Office of Technology Assessment at the German Bundestag, *What Happens during a Black-Out*, technology assessment studies series, available at : www.tab-beim-bundestag.de.

team to attack several electricity substations, if they had knowledge of a certain number of parameters beforehand.

In cases of physical sabotage, there has to be at least one assailant dealing with each targeted site. But a cyber attack could theoretically use just a few points of entry to spread a virus to the rest of the infrastructure. A team of OpenSource Security[29] has indeed been able to create a worm capable of reproducing itself from PLC to PLC, without having to pass through a computer.[30] Even if PLCs from different substations are not interconnected, all it takes is a human error for the virus to spread, like the use of an infected USB flash drive at several electricity substations during maintenance operations. It is also possible to program a virus to launch a simultaneous attack on all PLCs once infected. The designers of *PLC Blaster* estimate that this type of threat will develop strongly in the years ahead.[31]

Regional or national operators' ICS may also be targeted and could lead to more substantial consequences than attacks on substations.[32] A multitude of sensors collect data concerning the state of the grid in real time and transmit them to operators' SCADA managing electricity transport and distribution. When the control and command systems are operating, it is always possible to make adjustments and limit imbalances in case the electricity power cuts in certain zones, or in the face of localised cyber attacks. However, if the main system commanding the transmission or distribution network is attacked, as was the case in Ukraine, the operator loses the overall vision of what is happening in the grid, and the ability to conduct operations properly. Over a very short period of time, these can be maintained relatively normally. But risks of error with important consequences for the equilibrium of the grid increase with time. Under a very unlikely, though possible scenario according to several sources, in which large parts of the European electricity grid are affected,

[29] Open Source Security is a German network security company, which carries out intrusion tests for governments and companies. Its teams constantly seek new vulnerabilities which they reveal with care, once remedial security action has been found. The creation of PLC Blaster was presented at the Black Hat Asia 2016 conference in Singapore, using a vulnerability of some PLCs that had already been patched by Siemens.

[30] R. Spenneberg, M. Brüggemann and H. Schwartke, *PLC-Blaster: A Worm Living Solely in the PLC*, 2016, available at: www.blackhat.com.

[31] Securityweek, "PLC Worms Can Pose Serious Threat to Industrial Networks", 2016, www.securityweek.com.

[32] SCADA may be found in local installations (such as electricity substations) and are supervised by the same type of program, at a large level. In France, there are several regional SCADA, but according to the configuration of the electric grid and the number of operators, only one national SCADA may be responsible for all operations.

only the British Isles would escape damage, because of the direct current (DC) lines which isolate them from the European network's instabilities.

## Full protection is impossible

In France, numerous measures for the physical protection of installations have been put in place, providing an effective defence against the potential consequences of a cyber attack on the electricity grid.

In case of a direct attack on the SCADA of an electricity substation, manual intervention may limit effects to the local level. Part of this infrastructure is not indispensable to the stability of the network, and can be disconnected without damage (leaving aside financial and "reputational" costs). Components of substations which may have been damaged by a cyber attack can be replaced relatively easily.

In France, regional control systems which supervise the operation of field infrastructures are all backed by another SCADA located at another site, usually used to meet maintenance needs. More than 70 other driving tools may be used in the event of the simultaneous failure or malfunction of a regional SCADA and its backup.

Critical information systems, in other words systems which are indispensable to the proper operation of the network, are subject to legal security requirements in France, as set out in the Military programming law of 2013 (*Loi de programmation militaire*, LPM). Points of vital importance (PVIs), in other words particularly important sites to the grid such as certain major substations, must comply with significant physical protection obligations since 2006.[33]

However, it remains impossible to perfectly protect electricity installations even with these protection measures in place, just as it is impossible to prevent all physical sabotage by highly motivated persons. Certain infrastructures such as substations, spread throughout the territory and often in isolated areas, are particularly difficult to protect. Security professionals are confronted to a massive digitisation of the industry, while these digital components used are continuously acquiring new functionalities, which may potentially contain yet undiscovered weaknesses. In this context, it is particularly difficult for them to anticipate to possible scale and consequences of a cyber attack. And the deployment of a number of connected objects accompanying the energy transition will

[33] Decree No 2006-212 of 23 February 2006, relating to the security of activities of vital importance.

increase the number of entry points into the network and therefore the available surface for attack.

## *Digitisation and the energy transition: anticipating risks*

### The vulnerabilities arising in an evolving electricity grid

Energy transition policies have led to the deployment of renewable energy technologies throughout the world. These however require new solutions for integration, storage as well as supply and demand management. Smart grids and meters are essential elements of this new energy system which is set to be more effective, resilient and less polluting.

Aspects of cyber security must therefore be anticipated as of now, in order to design the security and resilience of the energy system as it evolves. However, renewable energy projects do not integrate cyber security measures, even though these installations are more and more subject to attacks.[34] Using a cyber attack to knock out a wind farm would not at present have a significant impact on the grid balance, and would not present a real danger to the environment or to people. The simultaneous disconnection of several installations however risks creating important problems in the future.

The electricity grid of tomorrow will be made up of a multitude of individual producers,[35] as well as new actors such as power aggregators. The latter are intermediaries between the electricity system and its users (households, collective dwellings, industry, etc.), whose function is to optimise operations of several decentralised producers together. Some already took control over important functions, such as partial load shedding or the starting up of emergency generators.[36] In order to pilot these “virtual power stations”, aggregators also use control and command systems, such as those currently employed to manage the transmission and distribution of electricity. These are commercial off-the-shelf software, less expensive than proprietary systems but better known from the public, and better accessible to malicious persons. Apart from risks weighing on the stability of the network, it is important to anticipate direct physical danger to individual producers owning equipment at home (such as batteries).

[34] For more information see: www.windpowerengineering.com.

[35] Massachusetts Institute of Technology, *The Future of the Electric Grid*, 2011, available at: http://energy.mit.edu.

[36] Commission de Régulation de l’Énergie, available at: www.smartgrids-cre.fr.

## Smart meters

As essential enabler of the energy transition, smart meters raise questions of security and data protection. At the Black Hat Europe 2014 conference, two IT security professionals[37] did indeed demonstrate that it was possible to hack certain Spanish meters, even though ingoing and outgoing communications were encrypted.[38] Within a few months, they discovered that it was possible to send false consumption reports to the operator, or even use their communication channels to modify the behaviour of other connected meters. These actions on several thousand meters at the same time could destabilise the distribution network, even creating power cuts in important zones.

In France, Enedis has paid particular attention to the cyber security of its Linky meters, as 35 million units are set to be deployed across France by 2021. Emphasis has been put especially on protecting consumer data, which was a sticking point in the meters' acceptance. Enedis made sure that its product could not be manipulated: the exchange of data with a highly secured concentrator is encrypted and goes directly through the electric and the telephone network, avoiding the vulnerabilities of internet. Data are sent to Enedis data centres, which are strictly isolated. The concentrator that retrieves data and sends information back to the smart meters via the data centre is equipped with a "security module", i.e. a tamper-proof hardware which enables private encryption keys to be generated and stocked for use in transferring data. Other measures have been put in place, which strictly comply with ANSSI's recommendations.

However, while resistance to all types of intrusion was tested beforehand, experts agree in saying that the existence of vulnerabilities cannot be ruled out, as is the case for any other connected objects with digital functions. Others state that with sufficient motivation, technical knowledge and financial means, hackers will achieve their goals no matter what the level of protection of our energy systems is. Resilience is therefore an essential aspect of cyber security.

Smart grids and meters have the particularity of increasing singularly the number of entry points into a network in which data is exchanged. As far as the meters are all configured in the same way and so may have the

[37] J. Vazquez Vidal and A. Garcia Illera, known for also having demonstrated that it was possible to hack a car or certain urban transport systems. See their presentation at the Black Hat Europe 2014 conference, "Lights Off! The Darkness of the Smart Meters", available at: www.youtube.com.

[38] "Popular Electricity Smart Meters in Spain Can Be Hacked, Researchers Say", *Reuters*, 2014, available at: http://uk.reuters.com.

same flaws, they increase considerably the available surface for attack.[39] Considered as essential to the creation of smart cities, the development of the "Internet of things", still in its infancy, will also reinforce this trend. The interaction of little protected private electronic devices (cell phones, electrical appliances) with components of the electric grid will make the needs in cyber security policies and expertise even more pressing.

Yet, the cyber security of energy infrastructures and its role in the security of supply are not subject to any specific provisions in France, neither in the Energy Transition Law, nor in the "section concerning the security of supply, the development of infrastructures and the flexibility of the electricity system" of the project of Multi-annual Energy Plan. The technical aspects are certainly dealt with by the ANSSI, which supports the energy industry in securing its facilities. But a strategic analysis of the impacts of cyber risks on the structure of tomorrow's energy system has not yet been carried out.

## The case of nuclear energy: should we be alarmist?

The nuclear industry has developed a safety culture because of the high level of physical risks it faces. It therefore has a habit of applying drastic measures which can be transposed to cyber security issues. Moreover, numerous long-standing mechanisms of physical protection remain a considerable obstacle to cyber attacks.

First of all, equipment and their communication processes are duplicated in many ways: the Ethernet network is duplicated, redundancy is ensured for on-site equipment, and safety functions are also secured by supplementary equipment deployed on remote sites. Sensors monitoring the state of critical equipment in reactors send information through four independent cables, and information retrieved must be identical in three cases out of four to be considered as reliable. The only information leaving the nuclear power station for a third party is data about voltage and power, which is exchanged with the electricity transmission operator every five seconds in order to adjust production as a function of demand. The network of the power station does not allow any other kind of information to be received from the outside.

[39] T. McLarty and T. J. Ridge (Eds), "Securing the U.S. Electric Grid", Washington D.C., The Center for the Study of the Presidency and Congress, 2014, available at: www.thepresidency.org.

In case a cyber attack manages to cut the electricity supply of the power station (required for operating the security systems), bullying – i.e. operation during which the plant supplies itself with electricity – can be successful in 80% of cases. Alternatively, each unit can rely on several independent generators, and one backup generator which can be allocated to different units. It is therefore also very difficult to attack the emergency power systems. These emergency measures have been particularly reinforced since the Fukushima catastrophe. Indeed, the European commission launched an unprecedented campaign between 2011 and 2012 to test the resistance of all European nuclear reactors, which led to a report aimed at reinforcing safety procedures in certain sites.[40]

The report clearly showed that all French nuclear power plants (and most in Europe) were equipped with a backup command centre before 2012. If one ICS breaks down, a second system located off-site and configured differently is available. Access to sites is also especially controlled. Moreover, the majority of the French nuclear fleet (reactors of 900 MW and 1,300 MW) was built before the digitisation of the energy sector, and still uses analogue equipment (apart from some supervisory functions). This makes it much more difficult for power stations to be corrupted by malware. The Grand Carénage programme which sets aside €51 billion of investment by 2025 to modernise the fleet does not intend to switch most critical functions into digital format.[41]

These measures were originally designed to keep control over operations in the case of fire, radiation or any other physical incident. They also limit not only the possibility of introducing malware into the most critical parts of nuclear power plants, but also the scope of action for any attack.

The progressive digitisation of France's nuclear energy nevertheless raises certain questions. Only four reactors (the N4 model) and the EPR have modern control systems.[42] However, their design has led EDF to review some equipment, especially at the Chooz reactor. [43] In 2009, the nuclear safety authorities of France, the United Kingdom and Finland published a common position expressing their reserves about the digital

[40]. European commission, *Technical Summary on the Implementation of Comprehensive Risk and Safety Assessments of Nuclear Power Plants in the European Union*, Corrigendum du document SWD (2012) 287 (2012), Bruxelles, 22 August 2013, available at: http://eur-lex.europa.eu.

[41] EDF, grand Carénage: key facts available at: www.edf.fr.

[42]. These systems act as solutions for bringing together means of surveillance and action. The digitised system allows information from some 12,000 sensors which control the state of the equipment permanently, to be passed on in real time.

[43]. V. Nouyrigat, « EPR – Les 4 erreurs de la filière française », *Science & Vie*, No. 1113, June 2010, p. 94.

command system in the EPRs, stressing that "the EPR design, as originally proposed by the licensees and the manufacturer, AREVA, doesn't comply with the independence principle, as there is a very high degree of complex interconnectivity between the control and safety systems".[44] France's Institute for Radiological protection and Nuclear Safety (Institut de Radioprotection et de Sûreté Nucléaire) stated in the same year that "this move towards greater complexity raised fundamental questions and that future designs should not continue to evolve in this direction.[45]

The control system of the EPR at Olkiluoto in Finland was finally duplicated by an ancillary system which is independent of computer technology.[46] The United Kingdom has gone even further in its demands for the Hinkley Point project and has duplicated all sorts of processes, in addition to the vital functions of the two units. Some experts consider that these measures are understandable, but risk increasing the complexity of the system without necessarily improving its resilience. The architecture of command and control system in the EPR at Flamanville has also been reviewed to reinforce the independence of the safety processes relative to IT.[47]

Digitisation is therefore also affecting the nuclear power industry and partly raises questions about its safety model. The drastic security procedures nevertheless make a cyber attack and damages on physical equipment very complex to perpetrate. The nuclear energy industry remains highly controlled and has a strong awareness of the issues at stake, at least in France, and tries to proactively adapt itself to the regulations which have been put in place.

[44] *Joint Regulatory Position Statement on the EPR Pressurised Water Reactor*, ASN, STUK, HSE, 2009, available at: www.asn.fr.

[45] Institut de radioprotection et de sûreté nucléaire (IRSN), Synthèse du rapport de l'IRSN portant sur l'architecture du contrôle-commande du réacteur EPR de Flamanville 3 et les plateformes associées, 2009, available at: www.irsn.fr.

[46] Non Computerised Safety System (NCSS).

[47] Autorité de sûreté nucléaire (ASN), "L'ASN lève ses réserves sur le contrôle commande de l'EPR Flamanville 3", 2012, available at: www.asn.fr.

# Cyber Security for Energy Infrastructures: the French and European Responses

There are many ways to protect (to a certain extent) energy systems from cyber attacks. The Stuxnet and BlackEnergy attacks do in fact demonstrate that a number of measures could have helped detecting them during their preparation.

"Defence in depth"[48] is one of the principles that best ensures the protection of information systems, the aim being to superimpose various defences so that the attacker encounters a new security layer after overcoming each obstacle. Applying basic security principles, like separating management and operational information systems, installing firewalls, changing default passwords of PLCs and connected objects when possible and imposing drastic "hygiene" procedures (prohibiting connexions of unverified devices like phones, testing new equipment before installing it, etc.), could significantly reduce risks. In industry, cyber security is "80% organisation and 20% technique" one person interviewed recalled. It is also the guarantee of dissuading the least effective hackers at the lowest cost.

Training employees is also crucial: most of the time hackers count on human error to breach networks security. One person working in industrial security did in fact state during an interview that the easiest way introduce a malware into an industrial plant was to drop flash drives at the company's car park. An imprudent employee would certainly pick it up and use it on site shortly after.

Such measures are within reach of companies which however sometimes find it difficult to identify priority actions to be carried out. That is why France and some neighbouring countries have chosen to regulate companies, and essentially those providing essential services such as energy delivery, to support their upgrading.

[48] ANSSI, Maîtriser la SSI pour les systèmes industriels, 2012, available at: www.ssi.gouv.fr.

# The French vision: using regulation

## *An innovative approach*

In 2009, the French Network and Information Security Agency (ANSSI, Agence nationale de la sécurité des systèmes d'information) was created to provide the country with means for fighting cyber risks, and is now one of the most extensive in Europe (with about 500 employees). Its powers were extended in 2011 when the national digital security strategy was launched (Stratégie nationale de cybersécurité).[49] The Military Programming Law (LPM, Loi de programmation militaire)[50] then adopted in 2013 set out the first legal milestones for a cyber security policy in France. In particular, it fixes the rules for some 200 operators of vital importance (OVIs) identified by a decree[51] relating to the security of activities of vital importance in 2006: i.e. companies, factories, operators and institutions "whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation".[52] These operators are subject to strict obligations in terms of security of their information systems, which are backed up by fines (€150,000) for breach of regulations.

In August 2016, France[53] was the first country to issue sectoral orders for OVIs (in hydrocarbons,[54] gas, [55] and electricity[56] for the energy sector). These included a list of measures to be implemented by companies, in order to protect their information systems, including:

- providing the ANSSI with a list of their critical information systems;
- Implementing a security policy for information systems which sets out the means to be adopted to protect the critical information systems. This policy must include an accreditation procedure for the information

[49] Stratégie nationale pour la sécurité du numérique, 2011, available at: www.ssi.gouv.fr.

[50] Loi n° 2013-1168 of the 18 December 2013 concerning military programming for 2014 to 2019 and including various measures concerning the defence of national security (2013). See article "Chapitre IV : Dispositions relatives à la protection des infrastructures vitales contre la cyber-menace", Article 22, available at: www.legifrance.gouv.fr.

[51] Décret n° 2006-212 du 23 February 2006, concerning the security of activities of vital importance, available at: www.legifrance.gouv.fr;

[52] Article L1332-6-1 of the defence code.

[53] ANSSI, "Cybersécurité des OIV : publication d'une nouvelle vague d'arrêtés sectoriels", 2016, available at: www.ssi.gouv.fr.

[54] Decree of 11 August 2013 (*Arrêté du 11 août 2016*) fixing the rules for security and the methods for declaring information systems of vital importance and security incidents relative to the subsector of activities of vital importance, "Approvisionnement en hydrocarbures", 2016, available at: www.legifrance.gouv.fr.

[55] *Ibid.*

[56] *Ibid.*

system within three years.

- Mapping existing systems: a certain number of industrial installations have been in place for several decades and operators often ignore the exact position and configuration of each set of equipment or network. A company such as RTE owns and supervises about 2,500 electricity substations throughout the country,[57] and must have a very precise view of the systems deployed. If RTE has for long conducted inventories of its assets, this is not the case for many companies. The results must be communicated to the ANSSI.
- Notifying the ANSSI without delay of any cyber security incident. Not only it will give the ANSSI the opportunity to technically support the attacked institution, but it will also ensure cyber forensics to be made in order to detect and prevent similar attacks.
- Other practices are henceforth imposed, such as the obligation to plan the installation of new versions of software or updates in order to avoid preserving obsolete versions.

Ministerial decrees provide for exception clauses to take into account existing equipment for which updates or the application of security patches are impossible.[58] These will be reassessed by the ANSSI in cooperation with industry, in order to adapt them to technological changes and to encourage investment in safer machinery.

The ANSSI also started certifying industrial equipment[59] to help companies clearly identify the most secured options on the market. Only one PLC passed the certification process at the moment, and according to experts it will take some time for a large variety of certified products to be made available. Siemens, whose one of the vulnerable PLCs was exploited by Stuxnet to breach in Natanz enrichment plant, restructured part of its activity subsequently, in order to provide "secure by design" products. Schneider Electric is seeking similarly to make cyber security a competitive advantage, and French regulations have led the company to hope that a dynamic market for industrial cyber security will develop.

The French approach strongly involves energy companies (as other OVIs for the regulations concerning them) in the process of formulating

[57] RTE, *Memo 2014*, available at: www.rte-france.com.

[58] "When justified for technical and operational reasons, the operator may decide [...] not to install a version offered by the supplier or manufacturer of the resource in question or not to install a measure for correcting security. In this case, the operator implements technical and operational measures set out by this procedure to reduce risks."

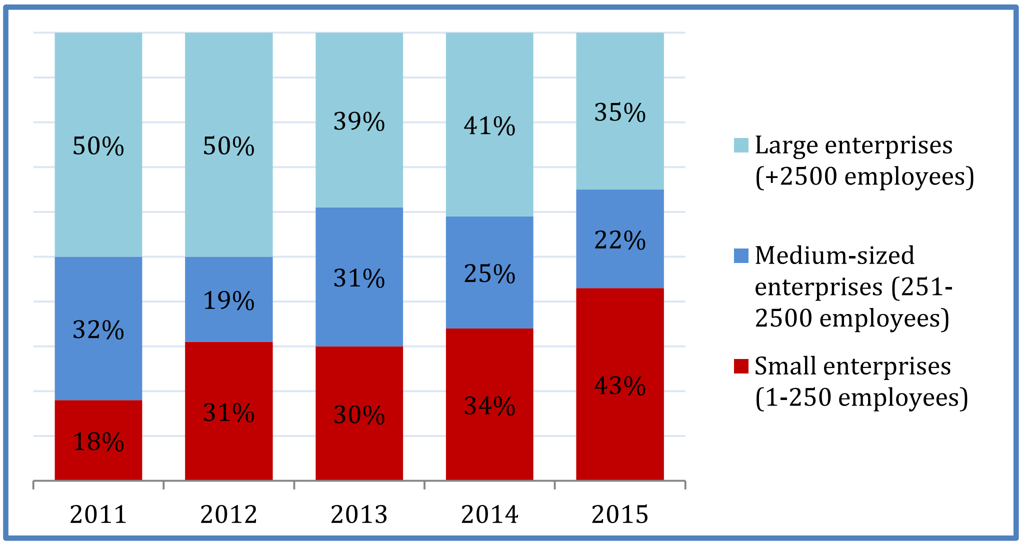
[59] ANSSI, Certification of first level security of information products and technologies, 2014, available at: www.ssi.gouv.fr.

these ministerial decrees in order to provide adapted responses to their specific needs. This way of proceeding helped build mutual trust between French authorities and OVIs, who seem in the end to accept quite well these regulations, and who recognise the interests they have in referring to clear measures.

## Obstacles to overcome

The ambitious legislation adopted by France nevertheless raises some difficulties. Most small actors, even among the OVIs, do not necessarily have the resources to designate a person in charge of industrial systems security, to carry out audits and to set up ambitious security policies. Yet recent analysis by information security companies shows that SMEs have been subject to increasing attacks over the past years.

**Phishing Attacks by Company Size Worldwide (2011-2015)**



*Source: Based on Symantec.*

While cyber risks are now well identified within the energy industry, security measures are not always a spending priority. In 2015, a Chatham House report referred to the lack of sensitivity to the problem from critical infrastructure operators in Europe.[60]

According to one person interviewed, the market for industrial cyber security solutions is still little consolidated and existing solutions are scarce, making them hardly affordable for small companies. Certified

[60] C. Baylon, R. Brunt and D. Livingstone, "Cyber Security at Civil Nuclear Facilities", *Chatham House Report*, 2015.

equipment provided by equipment manufacturers are still few, and require the replacement of existing ones, which involves considerable cost.

Moreover, the sectoral decrees specify that operators should install probes analysing files and protocols,[61] in order to improve the detection of events likely to impact security. If this stage is indispensable to analysing suspect information flows within the network, like the flows generated by the attack on Ukrainian operators during the tracking phase, it nevertheless raises questions for industries. In fact, it involves inserting totally digital devices throughout old infrastructures, with a shorter lifespan than that of equipment to be monitored. Such objects require more frequent replacement in an environment where reducing comings and goings is an integral part of security.

Despite a certain evolution in the understanding of the issues at stake, the energy industry should make important efforts to adapt itself to legislation. The French regulatory framework holds out the possibility that certified solutions for OVIs will indeed emerge and slowly replace equipment which is hard to protect. Yet protection will not be optimal as long as the whole value chain is secured, at least at the European level.

# Organizing cyber security in the European Union: an essential step

## *The necessity of a synchronized and comprehensive upgrading*

At the European level, legislation is gradually incorporating the requirements of cyber security. In the autumn of 2016, the European Commission published the Winter Package[62], an important piece of legislation which, for the first time, introduced obligations concerning cyber security for the electricity sector into European regulations. The proposal for a Regulation on Risk Preparedness in the Electricity Sector and Repealing stipulates that Member States have different risk

[61] Probes are systems for detecting intrusion, which aim at making surveillance of events occurring in the network or machine automatic. They signal to the administrator of the system any trace of abnormal activities in the system or in the machines under surveillance.

[62] The Clean Energy for all Europeans Package of Proposals is a set of legislative measures (directives, regulations and their annexes) presented by the European Commission on 30 November 2016. It aims to maintain the competitiveness of the EU in energy markets. For further information see: http://ec.europa.eu.

management practices.[63] These are not coordinated and are essentially geared to national contexts with little concern for cross-border situations. The draft regulation on the Internal Market for Electricity therefore states that measures to ensure data protection and cyber security should be dictated by a network code developed at European level.[64] The preliminary version of the Network Code on Operational Security prepared by Entso-E[65] has been validated by the Member States and is awaiting approval by the European Parliament and the Council before coming into force. This network code obliges electricity transmission operators to establish cyber attack scenarios and to evaluate means of prevention. These new regulations also complement Europe's main legal progress in cyber security, namely the Network and Information Security Directive (NIS), adopted on 6 June 2016.[66] It henceforth obliges Member States to designate a national authority in charge of cyber security issues. The draft directive created an upgrading effect when it was published in 2013, when more than half of the European countries had no competent institution in this field. Since 2013 however, almost all countries have introduced measures to meet the requirements of the Directive before its entry into force. Nevertheless, there are still significant discrepancies between the cyber security rules, legal instruments and operational capacities of the Member States (Annex 4). This situation weakens all the European infrastructures, which are closely interconnected.

The NIS Directive therefore lays down common security bases for information systems, thus avoiding the creation of weak links that would undermine all the measures taken by the most mature countries on the issue. The Directive also focuses on 'operators of essential services', which at European level include actors whose activities extend to several Member States. These include:

- suppliers of electricity and gas;
- electricity and gas transmission operators;
- refineries and processing plants;

[63] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on Risk-preparedness in the Electricity Sector and Repealing", Directive 2005/89/EC, available at: https://ec.europa.eu.

[64] Article 55, "Proposal for a Regulation of the European Parliament and of the Council on the Internal Market for Electricity", 2016/0379 (COD), available at: http://eur-lex.europa.eu.

[65] Article 26, "Network Code on Operational Security, Commission Regulation, Establishing a Guideline on Electricity Transmission System Operation", available at: www.entsoe.eu.

[66] Proposal for a Directive by the European Parliament and the Council concerning measures aimed at ensuring a high level of common security for networks and information in the Union, NIS Directive, available at: http://eur-lex.europa.eu.

- gas and oil producers;
- operators in the electricity and gas markets;
- operators of gas and oil pipelines and storage (including LNG).

Until now, Member States could voluntarily provide the European institutions with a list of operators deemed to be essential EU operators in their territory. But this only led to a very small number of declarations.

The Directive also requires Member States to develop national cyber security strategies. In 2015, only 19 States had developed action plans, which are sometimes incomplete and often static, whereas the speed of change in this area requires constant adaptation.[67] The Directive also requires each State to create a Computer Emergency Response Team (CERT), and the notification by critical operators of incidents to national authorities.

The European Commission supports the upgrading of less advanced Member States on these questions through a financing program for the inter-operability of infrastructures and digitised services (the Connecting Europe Facility, CEF).[68] With a budget of €60 million over seven years, the CEF is intended to purchase equipment, provide training and support institutional capacity building. A public-private partnership was also established between the European Commission and the European Cyber Security Organisation whose aim is to stimulate applied research in cyber security. The EU is providing €450 million to this end, and is seeking private sector investment of €1 billion.[69]

The EU also intends to reinforce cooperation between Member States by setting up exchange networks: the first network is made up of all the national CERTs and aims to share technical detailed information.[70] The second network links the European commission and national institutions. The aims of these measures are to encourage the dissemination of information in order to create a common culture on cyber security. But this is not easy to develop.

[67] BSA, EU Security Scoreboard, 2015, available at: http://cybersecurity.bsa.org. In this regard France revised its own strategy in 2015.

[68] The Connecting Europe Facility: this is an instrument for financing trans-European infrastructures in the years 2014-2020. For more information see: https://ec.europa.eu.

[69] European Commission, *Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tackle Cyber-Threats*, 5 July 2016, available at: http://europa.eu.

[70] Organised by ENISA, the European Union Agency for Network and Information Security.

## Difficulties in harmonisation

Several countries including France have campaigned to ease the constraints of the Directive proposal by the European Commission,[71] notably regarding sensitive information sharing with other EU countries. France and Germany cooperate almost on a daily basis and have set up a similar cyber security framework, but the principle of a binding agreement on mandatory information sharing between all Member States has not been included in the functioning of the exchange networks.

Similarly, certification procedures are being introduced in the most advanced countries in terms of cyber security legislation, but they raise questions about harmonisation which the European Commission hopes to tackle by creating a common certification framework. In the longer term, this measure would require creating a European certification agency, employing between 30,000 and 60,000 people to meet all EU certification needs, which is hardly conceivable. The alternative would be to have industrial equipment and products certified by national bodies. This however raises diplomatic questions within the EU. Some countries do not have the means to accomplish such tasks and should entrust existing large-scale European laboratories (probably German, such as the BSI, or French) to comply with an EU certification standard. These in turn should be audited by the client Member States. Yet, these laboratories use synergies with their military research to develop cyber security solutions, which makes audits by other state organisations very sensitive.

The harmonisation of standards is also a crucial question at the European level, and at the international level over the longer term.

Adopting common standards and a certification recognition framework would stimulate regular updating of regulatory frameworks within the EU, thus preventing them from remaining static once adopted. This is also a means of ensuring that all European energy installations are protected by minimum safety standards, even within less advanced countries. In this context, the agreement of the Senior Officials Group Information Systems Security (SOG-IS) could act as a basic framework.[72] The SOG-IS brings together national authorities for the safety of information systems in 10 countries, its aim being to coordinate the standardisation of protection profiles. Developing a system of international standards will be easier if the EU is already in agreement over its common

[71] European Commission, "Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union", 2013.

[72] Senior Officials Group Information Systems Security, available at: www.sogis.org.

framework. Concerning international standards, the European Commission has set up a working group which is collaborating with the United States (which has some of the most advanced standards concerning cyber security within the electricity and nuclear industries).[73] The aim here is to analyse and generalise good practices. The formulation of international standards and recognised equivalences is strongly supported by the industry, which fears having to reveal the manufacture of its equipment to foreign certification bodies. Discussions between Europe and China every two years also address this point, but the idea of formulating European norms is not very well received by the latter, as China fears that such norms could become import barriers to its goods. Such standards are still far from being established within Europe, despite the involvement of the European Network and Information Security Agency (ENISA).[74]

A study by the European Parliament stresses that while significant progress has been made on the question of cyber security in Europe, efforts lack coordination. This entails the risk of having a variety of measures which leave flaws in protection in place. According to this report, one of the measures which should be adopted as a priority relates to the creation of a sectoral cyber security institution as the main reference framework for the energy industry in Europe. But this assumes that Member States will accept the principle of regular and compulsory sharing of information.[75]

## *Similarities and divergences in approaches*

### Germany

Germany's cyber security strategy was adopted in 2011, a few days after France's. It similarly stresses the need to protect vital national infrastructures as a priority.[76] The German law on cyber security (the IT Security Act) was finally adopted in 2015 and coincides strongly with the European NIS Directive. As in France, this law obliges operators of critical infrastructures to ensure the protection of their information systems, to carry out security audits every two years, to notify the Federal Office Information Security (BSI) of any incident, and to appoint a contact person

[73] Including the North-American Electrical Reliability Corporation (NERC) for nuclear power, and the NIST which is applied in the electricity sector.

[74] Created in 2004, the ENISA or AERSI supports Member States in strengthening their technical capacities, formulates practical reference guides and participates in resolving problems faced by Member States in terms of network security and information systems.

[75] European Parliament, Directorate General for Internal Policies, Cyber Security Strategy for the Energy Sector, 2016, available at: www.europarl.europa.eu.

[76] *Cyber Security Strategy for Germany*, Federal Ministry of the Interior, 2011, www.bsi.bund.de.

for the BSI within each critical company.[77] Again, non-compliance with the law may lead to fines.[78] The Ordinance adopted in April 2016 sets out criteria which allow identifying vital infrastructures[79]: their number is known to be higher than in France (2,000), although the full list remains confidential. However, the German approach makes no distinction between critical operators' activities in different sectors.

The law discussed in the Bundestag since 2013 has been strongly criticised by German industries, arguing that it is both vague and strict, risking weakening their competitiveness.[80] By contrast, two well established public-private partnerships are operating in Germany. UP KRITIS brings together operators of critical infrastructures, trade associations and public institutions, with the aim of sharing risks analyses and developing common structures to respond to incidents. The Alliance for cyber security was established between BSI and Bitkom (the German IT trade association), in order to create a platform allowing the 1,200 participating institutions to share sensitive information.[81]

As far as the cyber security of critical infrastructure is concerned, the German approach is thus very similar in its guidelines to the French one, although the legislative arsenal concerning essential services operators is less precise at the moment.[82] Reluctance within the industry remains stronger than in France, while collaboration between the private and public sectors is easier and backed by well-established partnerships, fuelled by the government's "Industry 4.0" strategy.[83]

[77] Bundesamt für Sicherheit in der Informationstechnik.

[78] "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)", *German Federal Law Gazette*, 2015, No. 31, p. 1324, available at: www.bgbl.de.

[79] The regulation determining critical infrastructures according to the BSI law: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIGesetz (BSI-Kritisverordnung – BSI-KritisV), 22 April 2016, available at: www.gesetze-im-internet.de.

[80] Council on Foreign Relations, Germany's Cybersecurity Law: Mostly Harmless, But Heavily Contested, 2015, http://blogs.cfr.org.

[81] ENISA, CIIP Governance in the European Union Member States, January 2016, available at: www.enisa.europa.eu.

[82] IT safety standards specific to operators of nuclear power stations, which existed before the passing of the IT Security Act.

[83] D. Kohler and J.-D. Weisz, *Industrie 4.0 : Les défis de la transformation numérique du modèle industriel allemand*, Paris, La Documentation française, 2016.

## The United Kingdom

The United Kingdom (UK) also adopted a cyber security strategy in 2011, which identifies the risk of cyber attack as one of its priorities.[84] In the same year, the government launched the National Cyber Security Programme with a budget of £860 million, in order to meet the objectives of its cyber security strategy. The strategy was updated at the end of 2016 to cover the period 2016-2021, and emphasizes especially the creation of a training programme to meet the growing needs in cyber security experts over the coming years. The budget has also been increased to £1.9 billion for the five-year period.[85]

That said, the British approach uses little regulation to advance the security of information systems, even for critical infrastructure. The latter are indeed considered as infrastructures to be protected in priority but are not subject to any specific legislation. According to a Chatham House researcher, the private ownership of major energy assets in the UK energy sector, as well as cultural factors, make it easier to engage in public-private partnerships to encourage good practices rather than regulating.[86] This trend is also to be observed in the institutional structure responsible for cyber security questions: a multitude of offices and institutions is sharing power.[87] This tends to limit the visibility of their actions, even though their financial means are important. The national CERT was only established in 2014, and no national cyber security authority existed when the NIS Directive was adopted. The National Cyber Security Centre (NCSC), which was founded in the autumn of 2016 with the aim of "manag[ing the] operational response to cyber security incidents"[88], finally endorses the role of national authority and single point of contact imposed by the European Directive. This was a belated decision given the level of maturity of the UK concerning cyber security.[89] The Cyber Security Information Sharing Partnership (CiSP) was set up in 2013, bringing together more than 750 organisations and acts as a platform for sharing critical information on cyber attacks, based on a model similar to Germany's

[84] The UK Cyber Security Strategy, November 2011, available at: www.gov.uk.

[85] *UK Cyber Security Strategy: Statement on the Final Annual Report*, 14 avril 2016, available at: www.gov.uk.

[86] M. Carr, "Public–Private Partnerships in National Cyber-Security Strategies", *International Affairs*, Vol. 92, No. 1, 2016, p. 43-62, available at: www.chathamhouse.org.

[87] Government Communications Headquarters (GCHQ) has most powers and funding. The National Crime Agency, National Cyber Crime Unit (NCCU) as well as the Cyber Security Operation Centre (CSOC) are housed at GCHQ, and work alongside the Communications Electronics Security Group (CESG).

[88] *National Security Strategy and Strategic Defence and Security Review 2015*, HM Government, 2015, p. 41.

[89] UK National Cyber Security Strategy 2016-2021, available at: www.gov.uk.

Alliance cyber security body. However, Alex Dewdney, director of cyber security at CESG, reported at an international conference in March 2016 that the government's approach had not been fully satisfactory and that adopting a more interventionist approach in the future might be considered.[90]

Institutions in charge of cyber security in France, Germany and in the UK cooperate on a permanent basis. This partly explains the similarities in the information sharing institutions and collaboration practices, as well as in the regulatory approach in France and Germany. The NIS Directive will help narrow the gaps between Member States policies, even though it remains unlikely that all countries will be able to set up similar capacities to those in more mature countries. Some countries like Sweden and Greece have not yet adopted a national cyber security strategy, despite the existence of initiatives to protect energy infrastructures.[91]

[90] "UK government to change tack on cyber security", Computer weekly, RSAC16, March 2016, available at: www.computerweekly.com.

[91] To follow the progress of national cyber security strategies in Europe, see: www.enisa.europa.eu.

# Conclusion

Our energy systems are experiencing crucial digital changes and it is difficult to imagine exactly where it will lead. Along with heavy, aged infrastructures, all sorts of ephemeral and interconnected components are revolutionising energy professions. But they are also bringing their share of risks which the current industrial environment has difficulty dealing with. While the energy industry has been taking cyber security into account for hardly five years, the speed of digitisation and the impossibility of anticipating the nature of new technologies will constantly challenge efforts being made. Experts agree that risks exist, that they can be contained, but that preventing all cyber attacks is impossible. This follows from the nature of digital technologies which in their essence are more vulnerable than analogue and mechanical systems. But it also follows from their permanent upgrading and evolution, which open up new weaknesses that must be detected, analysed and corrected. A particular approach in the energy industry estimates in fact that maintaining analogue systems to ensure the most critical processes is indispensable.

Regulatory developments may perhaps permit this digital revolution to be achieved, without compromising the safety of energy infrastructures. Measures taken in France, Germany, the United Kingdom and followed by the EU hold out the hope for greater awareness, a better coordination of actions, and targeted investments in the most reliable equipment. This is also a way in France to stimulate research and innovation in the field of cyber security, and motivate the adoption of common standards which will prevail in the European energy industry. In this respect, France’s energy actors are relatively mature concerning cyber security issues, and are inclined to cooperate with national authorities. They are also organised into a community of interest, which can constitute an excellent driver for France's cyber security industry.

# Bibliography

Agence Nationale de la Sécurité des Systèmes d'Information, (ANSSI), Stratégie de la France, 2011.

ANSSI. *Maîtriser la SSI pour les systèmes industriels*, 2012. www.ssi.gouv.fr.

ANSSI, Certification de sécurité de premier niveau des produits des technologies de l'information, 2014, www.ssi.gouv.fr.

Baylon C., Brunt R., et Livingstone, D., « Cyber Security at Civil Nuclear Facilities », *Chatham House Report*, 2015.

Connecting Europe Facility, instrument de financement des infrastructures transeuropéennes pour la période 2014-2020 : https://ec.europa.eu.

Council of the European Union, Report of the Ad Hoc Group on Nuclear Security, www.consilium.europa.eu.

ENISA, Incident reporting and security regulation, www.enisa.europa.eu.

ENISA, Smart Grid Security www.enisa.europa.eu.

ENISA, Good Practice Guide for Incident Management, 2010, www.enisa.europa.eu.

European Commission, Proposal for a new regulation on risk preparedness in the electricity sector, 2016, http://ec.europa.eu.

European Commission, Technical summary on the implementation of comprehensive risk and safety assessments of nuclear power plants in the European Union Accompanying the document Communication From The Commission To The Council And The European Parliament on the comprehensive risk and safety assessments ("stress tests") of nuclear power plants in the European Union and related activities : http://eur-lex.europa.eu.

European Parliament, Directorate General for Internal Policies, Cyber Security Strategy for the Energy Sector, 2016, www.europarl.europa.eu.

Gluschke, G., Cyber Security Challenges in the Energy Context, (2016).

Hausermann, L., «  SENTRYO – Cybersécurité industrielle, que doit-on craindre ? », www.cxp.fr.

Industrial Ethernet Book, Using ANSI/ISA-99 standards to improve control system security, www.iebmedia.com.

Introducing The Activities Of Control System Security Center (Cssc): www.css-center.or.jp.

Kesler, B., « The Vulnerability of Nuclear Facilities to Cyber Attack », *Strategic Insights*, *10*(1), 2011, p. 15-25, http://large.stanford.edu.

Miller, B., A Survey of SCADA and Critical Infrastructure Incidents., 2012, http://citeseerx.ist.psu.edu.

MIT, The Future of the Electric Grid, 2011, http://energy.mit.edu.

National Cybersecurity and Communications Intergration Center – US Department of Homeland Security, 2015 ICS-CERT Monitor.

Nicolas, M. et Machado, C., « Cyber Security Governance: Securing the European Union's Cyber Domain », 2015.

Nouyrigat, V., « EPR – Les 4 erreurs de la filière française », *Science&Vie*, juin 2010, p. 94.

Office of technology assessment at the German Bundestag, « What Happens During a Black-out », *Technology Assessment Studies Series*, www.tab-beim-bundestag.de.

Programmation Pluriannuelle de l'Énergie, www.developpement-durable.gouv.fr.

Rid, T. et Buchanan, B., « Attributing Cyber Attacks », *Journal of Strategic Studies*, 2014.

Sanger, E. D., *Confront and Conceal*, New York, Broadway Books, 2012.

SANS-ICS, E.-I., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016.

Singer, P.W. et Friedman, A., *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014.

Trend Micro, « Who's Really Attacking your ICS Equipment? », 2013, www.trendmicro.com.

Union for the Coordination of Transmission of Electricity UCTE, *Final report, System Disturbance on 4 November 2006*, www.entsoe.eu.

Wired. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, www.wired.com.

# Annexes

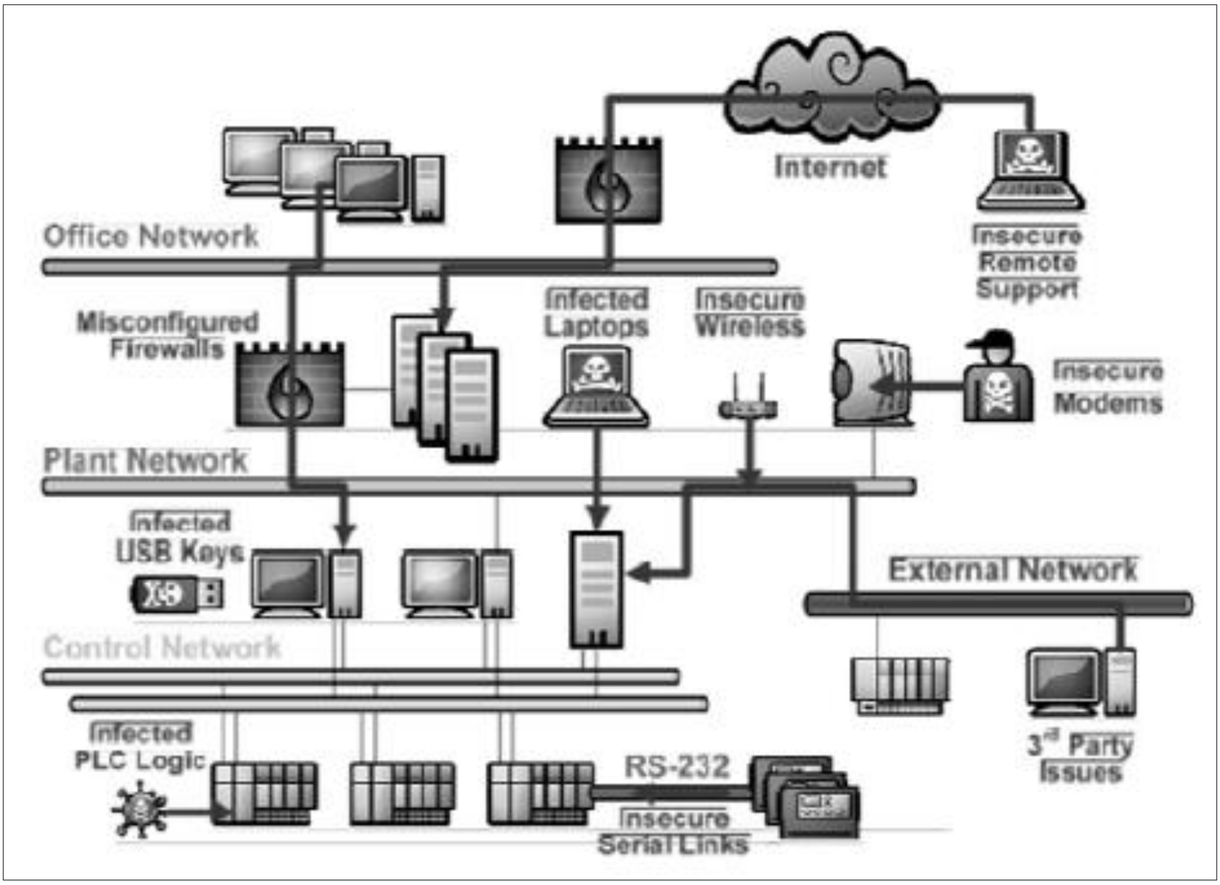
## Annex 1: Industrial information systems

An industrial information system is a digital system monitoring and controlling physical installations. It is often referred to by the acronym ICS (industrial control system). IISs are made up of four main categories of components:

- Components ensuring interaction with the physical world: sensors (temperature, aperture, humidity, light, etc.), and actuators (pumps, cylinders, motors, indicators, etc.), interconnected by a specific network.
- Components piloting the actuators according to the information provided by sensors. They may be distributed (DCS: Distributed Control System) or autonomous such as programmable logic controllers (PLCs) which are deployed locally, or remotely (remote terminal units, RTUs). Today these distinctions are tending to fade. Components of the new generation (PACs or programmable automation controllers) can carry out a wider range of functions than traditional components and are linked with an IP-address to IT networks piloting production.
- Supervision and control components allow entire processes to be visualised and piloted thanks to a human machine interface (HMI). These are often referred to as SCADA (Supervisory Control And Data Acquisition). They are linked to firms' production management systems, such as servers and workstations that function with mass-market operating systems (mainly Windows and Linux).
- Increasingly, industrial systems are digitised and interconnected to company management systems.

*Source: based on Clusif 2014, Cybersécurité des systèmes industriels.*

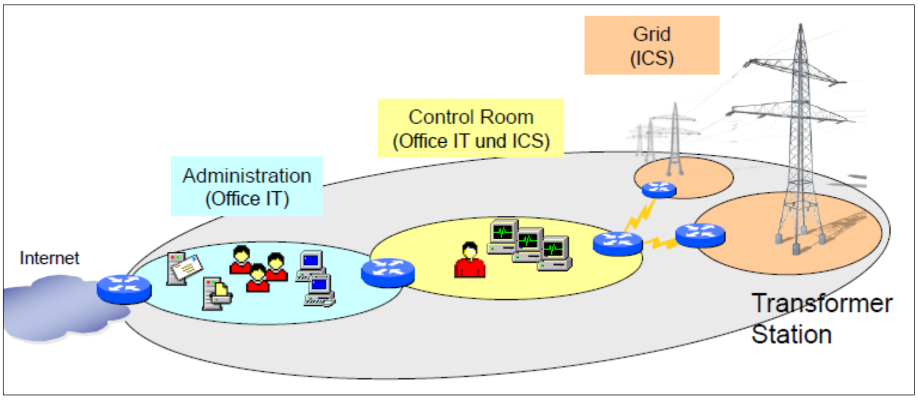
# Annexe 2: Vulnerabilities and points of entry into industrial control systems

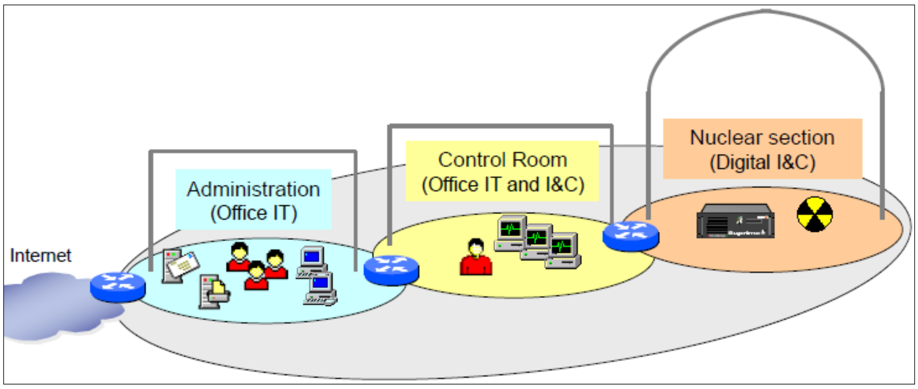


*Source: Nokia*

# Annex 3: Architectures of energy infrastructures networks

## Architectures of an electric grid and a nuclear power plant network





*Source: Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, NISS / NATO ENSE CoE.*

# Annex 4: The scorecard for cyber security in the EU, 2015 *(Source: BSA | The Software Alliance)*

✓ Yes ✗ No ◑ Partial

| QUESTION | Austria | Belgium | Bulgaria | Croatia | Cyprus | Czech Republic | Denmark | Estonia | Finland | France | Germany | Greece | Hungary | Ireland | Italy | Latvia | Lithuania | Luxembourg | Malta | Netherlands | Poland | Portugal | Romania | Slovakia | Slovenia | Spain | Sweden | United Kingdom |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **LEGAL FOUNDATIONS** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Is there a national cybersecurity strategy in place? | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | Draft | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ |
| What year was the national cybersecurity strategy adopted? | 2013 | 2012 | – | – | 2013 | 2011 | – | 2014 | 2013 | 2011 | 2011 | – | 2013 | – | 2014 | 2014 | 2011 | 2013 | – | 2013 | 2013 | – | 2013 | 2008 | – | 2013 | – | 2011 |
| Is there a critical infrastructure protection (CIP) strategy or plan in place? | ✓ | ◑ | ◑ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ◑ | ✗ | ✓ | ✗ | ◑ | ✗ | ◑ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Is there legislation/policy that requires the establishment of a written information security plan? | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ◑ | ✓ | ◑ | ✗ | ✗ | ◑ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ◑ | ◑ | ✗ | ✗ | ✗ | ◑ | ✗ | ✗ | ✓ | ◑ |
| Is there legislation/policy that requires an inventory of "systems" and the classification of data? | ✓ | ✓ | ✓ | ✓ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ◑ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels? | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Is there legislation/policy that requires (at least) an annual cybersecurity audit? | ✓ | ✗ | ✗ | ✗ | ✗ | ◑ | ✗ | ✓ | ✓ | ✗ | Draft | ✗ | ✗ | ✗ | ✗ | ✓ | ◑ | ◑ | ◑ | ◑ | ✗ | ◑ | ✗ | ✗ | ◑ | ◑ | ✗ | ✗ |
| Is there legislation/policy that requires a public report on cybersecurity capacity for the government? | ◑ | ✗ | ✗ | ◑ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | Draft | ✗ | ✓ | ✗ | ✓ | ✗ | ◑ | ✗ | ✗ | ✓ | ✗ | ◑ | ✗ | ◑ | ✗ | ✗ | ✗ | ◑ |
| Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)? | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Is there legislation/policy that requires mandatory reporting of cybersecurity incidents? | ✗ | ◑ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ◑ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)? | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements? | ✓ | ◑ | N/A | N/A | N/A | ◑ | ✓ | ✓ | ✓ | ◑ | ✓ | ✓ | ✓ | N/A | ✓ | ◑ | ◑ | ◑ | N/A | ✓ | ◑ | N/A | ◑ | ✗ | N/A | ✓ | ✓ | ◑ |
| **OPERATIONAL ENTITIES** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)? | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| What year was the computer emergency response team (CERT) established? | 2008 | 2008 | 2008 | 2009 | – | 2011 | 2009 | 2008 | 2014 | 2008 | 2012 | 2009 | 2013 | – | 2014 | 2006 | 2006 | 2011 | 2002 | 2012 | 2008 | 2008 | 2011 | 2009 | 2010 | 2008 | 2003 | 2014 |
| Is there a national competent authority for network and information security (NIS)? | ◑ | ✓ | ✓ | ✓ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ◑ | ✓ | ◑ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Is there an incident reporting platform for collecting cybersecurity incident data? | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Are national cybersecurity exercises conducted? | ✓ | ✓ | ✓ | ◑ | ◑ | ◑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ◑ | ✓ | ✓ | ✓ | ◑ | ◑ | ◑ | ✓ | ◑ | ◑ | ◑ | ✓ | ◑ | ◑ | ✓ | ✓ |
| Is there a national incident management structure (NIMS) for responding to cybersecurity incidents? | ✓ | ✗ | ◑ | ✗ | ✗ | ✓ | ◑ | ◑ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ◑ | ◑ | ✗ | ✓ | ✓ | ◑ | ◑ | ✗ | ✗ | ✓ | ◑ | ✓ |
| **PUBLIC PRIVATE PARTNERSHIPS** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Is there a defined public private partnership (PPP) for cybersecurity? | ✓ | ◑ | ◑ | ◑ | ◑ | ✗ | ✗ | ◑ | ◑ | ✗ | ✓ | ✗ | ◑ | ✗ | ◑ | ✗ | ✗ | ✗ | ◑ | ✓ | ✗ | ◑ | ✗ | ✗ | ✗ | ✓ | ◑ | ✓ |
| Is industry organised (i.e. business or industry cybersecurity councils)? | ✓ | ✓ | ◑ | ✗ | ✗ | ✗ | ✓ | ◑ | ✓ | ✗ | ✓ | ✗ | ◑ | ✓ | ◑ | ✗ | ◑ | ✗ | ✗ | ✓ | ◑ | ✗ | ◑ | ◑ | ◑ | ✓ | ◑ | ✓ |
| Are new public private partnerships in planning or underway (if so, which focus area)? | ✓ | – | ✗ | ✗ | ✗ | ◑ | ✗ | ✗ | ✗ | ◑ | ✓ | ✗ | ✗ | ✗ | ◑ | ◑ | ◑ | ◑ | ✗ | – | ✗ | ✗ | ✓ | ✗ | ✗ | – | ✗ | – |
| **SECTOR SPECIFIC CYBERSECURITY PLANS** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Is there a joint public private sector plan that addresses cybersecurity? | ✓ | ✗ | ✗ | ◑ | ◑ | ✗ | ✗ | ✗ | ◑ | ✓ | ✗ | ✗ | ◑ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ |
| Have sector specific security priorities been defined? | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ◑ | ✗ | ◑ |
| Have any sector cybersecurity risk assessments been conducted? | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **EDUCATION** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age? | ✓ | ◑ | ◑ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ◑ | ✗ | ✓ | ◑ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ |

ifri institut français des relations internationales