ENERGY NETWORKS AND SMART GRIDS

Cyber security for the energy sector

WG3 I Sectoral Demand

NOVEMBER 2018

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg3_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

This document will be continuously updated based on developments within the sector and ECSO members' input.

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

This report presents a synthesis of recent studies, analysis and initiatives related to cyber security in the energy sector. It relies mostly on relevant related literature and aims at providing a picture of the current situation while highlighting specific gaps of the energy sector.

The report is not meant to be exhaustive but rather to present a common vision and understanding of the main cyber security related challenges as it pertains to the energy sector and specifically the electricity sub-sector (ECSO membership does not currently cover the oil and gas sub-sectors). It is comprised of four main chapters (landscape, user engagement, sector specificities, market study) and has been elaborated by ECSO's sub-working group 3.2 on Energy Networks and Smart Grids, with input from key external stakeholders during workshops organised by ECSO. Future activities foreseen for this sub working group include the continuous liaison with energy stakeholders and the report will be updated as and when needed (and to include oil and gas), based on inputs from ECSO members and the outcomes of stakeholder engagement workshops.

2 Landscape

Evolution of the energy sector

The ultimate goal of energy infrastructures is to provide an uninterrupted supply of energy as the functioning of society relies completely on energy. Therefore, it is crucial for energy operators to ensure the safety and security of the whole interconnected energy chain, from generation to supply. Major recent changes in the energy sector which implies new cyber security challenges could be summarised as follows:

Energy model

Over the last decade, energy infrastructures, in particular electricity infrastructures, have undergone profound changes, characterised by the transition from a system where generation, based on fossil fuel, adapts to user consumption, to a system which has to manage different kinds of users connected to it – generators, consumers and those that do both.

Digitalisation of energy infrastructures

Another evolution is the massive digitalisation of the whole infrastructure to optimise and to remotely supervise and monitor an increasingly complex infrastructure. Moreover, to cope with the global growth of energy demands and climate change, there is an increasing need for efficient and optimised use of energy. To save energy, demand-response services are proposed to users to optimise their consumption, for example by reducing or shifting their electricity usage during peak periods. These services rely on interconnected smart devices, such as sensors and actuators, widely deployed in households to measure energy use and reduce energy equipment consumption to prevent overload. It is predicted that these smart devices, or Internet of Things, will total several billion in the coming years. The benefits of this transformation are envisioned to be a more economical, sustainable and reliable supply of energy.

Increase of threats

In the meantime, energy infrastructures are increasingly exposed to cyber threats. The attack surface is increasing due to the massive use of ICT (Information and Communication Technologies) and of new data interfaces such as new and connection-oriented meters, collectors, and other smart devices which offer new points of entry to attackers. In addition, energy systems present targets with potentially high impacts for attackers, e.g. major supply disruption or acquiring sensitive information. Cyber-attacks can also be motivated by the increasing amount of private sensitive customer data available to service providers, utilities, and third-party partners. In a study published by ENISA in August 2016 assessing the cost of cyber security incidents affecting critical information infrastructures [4], the energy sector appears as one of the 3 most impacted sectors having the highest incident costs (the 2 other sectors are finance and ICT). According to this study, the specific threats per sector are analysed in the table below.

Nr.	Attack / Threat	Number of studies per sector									
		Public Administration	Energy	Health	Financial	ICTs	Transport	Water	Aerospace	Food	Chemistry
1	Malware	7	10	7	9	9	7	1	1	1	1
2	DoS/DDoS	10	8	8	11	11	8	1	1	1	–
3	Cyber Espionage	2	3	3	3	2	1	1	1	–	1
4	Web-Based Attacks	5	7	4	7	7	6	–	1	1	–
5	Insider Threat	7	4	6	8	7	3	–	1	1	–
6	Hacktivism	3	3	3	5	4	–	–	1	1	1
7	Malicious Code	5	6	5	7	7	6	–	–	–	–
8	Phishing	6	4	4	6	6	4	1	–	–	–
9	Web Application Attacks	5	2	4	4	4	2	1	–	–	–
10	Ransomware	3	1	3	2	2	1	1	–	–	–
11	Botnets	1	2	2	2	2	2	–	–	–	–
12	Critical Vulnerabilities	1	1	1	–	–	1	1	–	–	–

Table 1 : Attack/Threat types per CII sector (Source: [4])

A recent study on cyberattacks targeting energy systems [12] confirms the increasing of cyberattacks against energy infrastructures. This study lists cyberattacks and incidents that have impacted energy infrastructures (see Table **2**).

Year	Target	Name of attack	Consequences	Objective	Attackers
1982	Gas pipeline explosion in Siberia (Russia)		Malicious software introduced into the SCADA management of pipeline; explosion equivalent to 3 tons of TNT	Sabotage	External
1992	Ignalina nuclear power plant (Lithuania)		A technician at the Ignalina nuclear power plant introduced a virus into the control system of one of the two RMBK reactors (Chernobyl type)	Sabotage	Internal
1992	Chevron emergency alert system (US)		An employee laid off by Chevron deactivated the company's incident alert system by hacking into the computers in charge of the system. The intrusion was only discovered when an emergency occurred at a Chevron refinery	Sabotage	Internal

			in Richmond which exposed thousands of people living in proximity to toxic substance for several hours		
1999	Gazprom (Russia)		Takeover of the (switchboard)/distribution board controlling the gas flows of the pipelines	Sabotage	Internal
1999	Bellingham gas pipeline (US)		Incident linked to the development of a database for the SCADA system operating the gas pipelines of the company Olympic Pipe Line. Incident partly responsible for a resulting diesel leak which caused 3 deaths and 8 injuries	Incident/human error	Internal
2001	California electricity operator (US)		Attackers gained access to one of the internal networks of the operator California Independent System. The attack was discovered before it reached the PLC network controlled by the company	Sabotage	External/China ?
2003	David-Besse nuclear station (US)	Slammer	4-hour shutdown of safety display system due to worm without espionage or sabotage features	Non-targeted	External
2008	Hatch power plant (US)		An update performed on a computer in the operator's management system misled the reactor control system, resulting in an unintentional shutdown of the reactor for 48 hours	Incident/human error	Third party company
2010	Natanz (Iran)	Stuxnet	Several years of infiltration into the Natanz uranium enrichment complex; damage to over 900 uranium enrichment centrifuges	Sabotage	External/State/ USA, Israel?
2011	Oil & gas industry	Night Dragon	Extraction of confidential information linked to oil & gas projects	Espionage	External
2011	Energy industry	Duqu	Part of code almost identical to Stuxnet, designed solely for industrial espionage without containing a destructive function	Espionage	External
2011	Areva (France)		Data theft, non-critical according to the company. The infiltration evidently lasted two years	Espionage	External

2012	Energy-related companies and institutions	Flame	Spread through the Middle East and North Africa, operated for at least two years. Designed for espionage and data analysis. Discovered after the Ministry of Iranian oil and the national Iranian oil company reported the theft and erasure of certain important data in their systems	Espionage/data theft	External
2012	Saudi Aramco (Saudi Arabia)	Shamoon	30000 destroyed hard disks to be replaced, operational network unaffected	Sabotage	External
2013	Bowman Avenue Dam (US)		Attackers took control remotely of a small dam close to New York, without consequences	Reconnaissance	External/Iran?
2014	Energy companies	Energetic Bear	250 companies in the US and Western Europe infected	Espionage/possibly sabotage	External
2014	Petrol stations	Operational Petrol	The hacktivist group Anonymous announced its attack on oil companies and petrol stations (denial of service, data theft). Little feedback however on what could or couldn't have been done	Sabotage/data theft	Anonymous
2014	Korea Hydro and Nuclear Power (KHNP) (South Korea)		Plans and manuals of the two reactors, electrical circuits, radiation exposure measures in the area, and data on 10000 employees stolen. Due to pressure by activists on the government to shut down three reactors.	Blackmail	External
2015	Electricity operators (Ukraine)	Black Energy	Thirty or so substations disconnected from the network, 8 provinces without electricity for several hours, more than 200000 people affected, controls systems physically damaged, (diminished operations)/degraded mode operation for several weeks after attack	Sabotage	External/State, Russia?

Table 2: List of cyberattacks and incidents that impacted energy infrastructures (translated from [12])

Cyber security regulation and other initiatives for the energy sector

In the last few years, legislations and policies related to cyber security for different sectors have been defined at European and national levels as a consequence of the recent changes observed in different domains, including energy. The main cyber security regulations are:

- The Directive on Security of Network and Information Systems (NIS Directive) [10]: it was adopted by the European Parliament on 6 July 2016. It is a major component of the European cyber security strategy aimed at strengthening Europe's cyber resilience and cooperation across different sectors. The implementation of the NIS Directive in EU countries has been in effect since May 2018. One major challenge is to ensure the alignment of NIS Directive implementations among EU Member States.
- The General Data Protection Regulation (GDPR): it was adopted in 2016 and defines requirements for the protection of personal data. The GDPR regulation has been in effect in EU Member States since May 2018.
- Regulation (EU) No 994/2010: the gas supply regulation aims at ensuring the security of gas supply. Member States shall establish at a national level a Preventive Action Plan and an Emergency Plan.
- The EU Cybersecurity package, including the Cyber Act, as presented in the joint communication to the EU Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" in September 2017 [13], covers many aspects such as: a reinforced and permanent mandate of ENISA, a EU cybersecurity certification framework, a cybersecurity competence network with a European Cybersecurity Research and Competence Centre, developing Information Sharing and Analysis Centres (ISACs), etc. Furthermore, the Cybersecurity Package acknowledges the importance of specificities of different sectors and refers to sector-specific requirements.
- Cybersecurity Network Code**:** in the context of the EU Clean Energy package (released on November 30th, 2016, and currently under negotiation), the Cybersecurity Network Code proposes cybersecurity technical rules for electricity aiming at going beyond the NIS Directive obligations by addressing energy sector specificities (could be an energy specific legislation). While final results are expected by end 2018, the 2nd intermediary report [14], set up by the Smart Grids Task Force-Expert Group 2, was published in July 2018. The main components proposed in the 2nd draft for the Network Code on cybersecurity are:
    - Early warning system in Europe for the energy sector
    - Cross-border and cross-organizational risk management in the EU
    - Minimum Security Requirements for critical infrastructure components
    - Minimum Protection Level for energy system operators
    - European Energy Cybersecurity Maturity Framework for Operators of Essential Services
    - Supply Chain Risk Management for Operators of Essential Services
- National security strategies and legislations [11]: beyond the definition of cyber security strategies in European countries, national legislations related to cyber security for critical infrastructure operators have been defined (e.g. Loi de Programmation Militaire (LPM) in France).
- Other initiatives have been initiated by the European Commission to strengthen existing cyber security policies and legislations. For example, the Energy Expert Cyber Security Platform

(EECSP) - Expert Group has been mandated by DG Energy to prepare an energy cyber security strategy to be considered by the European Commission to complement the implementation of the NIS Directive [2]. After examination of the existing policy/legislation and identification of the specific challenges of the energy sector (39 gaps identified in existing legislations), the expert group came up with a set of recommendations presented in as strategic priorities linked to the strategic areas and areas of actions [2].

Strategic Priorities		**Strategic Areas**	**Areas of Actions**
I	Set-up an effective threat and risk management system	European threat and risk landscape and treatment.	1) Identification of operators of essential services for the energy sector at EU level. 2) Risk analysis and treatment. 3) Framework of rules for a regional cooperation. 4) EU framework for vulnerabilities disclosure for the energy sector
		Identification of operators of essential services	
		Best practice and information exchange	
		Foster international collaboration.	
II	Set-up an effective cyber response framework	Cyber response framework	5) Define and implement cyber response framework and coordination. 6) Implement and strengthen the regional cooperation for emergency handling.
		Crisis management	
III	Continuously improve cyber resilience	European cyber security maturity framework	7) Establish a European cyber security maturity framework for energy. 8) Establish a cPPP for supply chain integrity 9) Foster European and international collaboration.
		Supply chain integrity framework for components	
		Best practice and information exchange	
		Awareness campaign from top level EU institutions	
IV	Build-up the required capacity and competences	Capacity & competence build-up	10) Capacity and competence build-up.

Table 3: Overview table on strategic priorities, areas and recommended actions (Source: [2])

3 User Engagement

The engagement of all stakeholders involved in the functioning of energy infrastructures is necessary to define the energy sector demands, mainly:

- Energy operators, including all energy business units (generators, TSO, DSO, Supplier, aggregators, market operators)
- Industrial equipment suppliers providing the maintenance during the lifespan of the equipment;
- Authorities/regulators
- Organisations/associations representing energy sectors
- Consumers and prosumers as end users of the grids
- Consumers associations

ECSO sub working group 3.2 has already engaged with a number of key stakeholders within the energy sector, through face to face workshops held at ECSO, where discussions were used to elicit key needs & requirements from these stakeholders as well as to validate the content of this report. These workshops were attended by, inter alia, the European Commission's DG Connect and DG Energy, the EE-ISAC, associations such as ENTSO-E, ENTSO-G, and CENTRICA, as well as utilities not yet part of the ECSO membership such as Alliander, Iberdrola, and Dansk Energi.

4 Sector Specificities

There are different ways to differentiate energy sub-sectors. For example, the NIS Directive distinguishes between 3 energy subsectors: electricity, oil, and gas [10]. The EECSP - Expert Group report, identifies four energy sub-sectors: electricity, oil, gas, and nuclear energy [2]. The ENISA Report on Cyber Security Information Sharing in the Energy Sector considers four subsectors: electricity, oil and gas, nuclear energy and alternative fuels [1].

In this document, we propose to consider common requirements for all energy subsectors, in addition to those specific to the electricity subsector. ECSO membership does not currently cover the oil and gas sub sectors but the report could be updated with these later.

Common energy specifics include:

- Critical infrastructures
- Massive digitalisation
- Importance of safety
- Importance for the European society and potential economic impact [2]
- Potential national or cross-border impact related to the 'weakest link problem' [2]
- Prospects of respective level to address the challenges [2]
- Real-time and dependence on availability requirements: reaction time in case of incident ranges from milliseconds (e.g. nuclear energy and electricity) to days in other subsectors [2]

4.1 Electricity

Smart grids specifics and requirements

Smart Grids are the digitalisation of electricity infrastructure and the transition from a closed, centralised, analogue infrastructure to an open, largely decentralised, digital infrastructure. This new scheme is based on a highly interconnected ICT infrastructure, allowing the monitoring of the different components of the electric system. While smart grids take substantial advantage of this new ICT infrastructure, they become at the same time more vulnerable as they are now exposed to communication networks and computer application cyber-attacks which could cause serious damage to the electricity network, as well as impact the integrity and confidentiality of customers' data.

The main security challenges specific to smart grids are:

- High level of complexity and very high volume of interconnected component deployed at country/continent scale. There is a need for security solutions preventing cascading effects, especially when a large volume of components is compromised.
- Energy systems usually have a very long lifetime, sometimes remaining in the field for decades. Security solutions should take into account resource constrained legacy systems and should be extensible and evolving to integrate new components and new security requirements.

- Privacy concerns have arisen, such as the possibility of creating behavioural profiles of customers if their energy consumption is transmitted into the Smart Grid especially in small time intervals.
- Attack surface is increasing over time due to new data interfaces such as new and connection-oriented meters, collectors, and other smart devices (IoT technologies) which cause new entry points for attackers. Thus, all components of the Smart Grid, from smart meters to power plants, or relays, including software components, could be targets for cyber-attacks, as well as the SCADA systems used to monitor these software components. These components could be compromised either because they are exposed to the Internet, or because physical security can be bypassed. There is a need for new security approaches detecting and preventing threats with severe impacts (e.g. blackouts).
- A Smart Grid is a system where electricity is traded as a commodity on international marketplaces. Mechanisms of trading marketplaces should be resilient.
- The use of protection techniques (hardware and software) must consider constraints of smart grid processes (e.g. real time, limited resources, etc.) to operate efficiently.
- It is crucial to devise means to defend against denial-of-service attacks that do not disrupt the Smart Grid.
- The Smart Grid architecture and governance must be such that compromised components are detected and isolated in a way that minimises the impact on the rest of the infrastructure.
- Disaster recovery techniques are required in case of major disruption.
- Safety components are of major importance in smart grids operation. Thus, it is necessary to identify and control interdependencies between safety and security.

Distributed Energy Resources (DER) specifics and requirements

Distributed Energy Resources (DER) are expected to occupy in the smart grid landscape an increasingly important part of the global energy generation through a large number of energy sources on various scales (solar panels, small wind turbines, energy storage, etc.), highly dispersed across the whole grid. DER therefore represent an important part of the whole electricity generation due to their massive integration in the grid. An attack targeting a large number of renewable energy sources (e.g. windfarm) could have a severe impact on the grid and thus on electricity supply.

The main security challenges specific to DER are:

- Highly distributed and resource constrained systems which implies the need for distributed security schemes operating with limited resources.
- Limited or not connected systems (due to their difficulty in reaching location), such as offshore wind farms, which implies the need for autonomous security solutions and secure remote supervision.
- DER infrastructures encompass new components (e.g. power storage systems) crucial for the maintenance of the equilibrium of the whole grid, and operating through different models (e.g. Virtual Power Plants). More generally, they use technology which is still rapidly evolving and which needs rapidly evolving cyber security solutions.

Centralised electricity generation specifics and requirements

Centralised electricity generation plants can have a significantly long lifespan and are now introducing the use of new ICT technologies. The combination of these two generations of technologies has to be considered while conceiving and developing security solutions. In particular, legacy systems have constrained resources and sometimes rely on old software that cannot always be changed. Moreover, as safety is a major requirement of these infrastructures, security solutions have on the one hand to mitigate security threats which can have an impact on safety, and on the other hand to manage potential interdependencies between security systems and safety systems. Finally, due to the use of new technologies such as IoT, privacy issues have to be addressed and solutions proposed.

The main security challenges of « centralised electricity generation » are:

- Energy systems usually have a very long lifetime, sometimes remaining in the field for decades. Security solutions should take into account resource constrained legacy systems together with new technologies (IoT, etc.). New security solutions should fit both generations of technologies and be extendable and evolve to integrate new components and new security requirements.
- Evolving threats should be detected and isolated as they could have disastrous impacts on generation plants.
- Safety components are of major importance in smart grids operation. Thus, it is necessary to identify and control interdependencies between safety and security.
- Privacy concerns have arisen due to the increasing use of industrial IoT technologies in power plants.
- Strong need for advanced physical access control schemes (distinguishing between the access rights of internal employees and of external personnel, e.g. for maintenance).
- Strong need for the early detection and isolation of compromised components and more generally of threats.

5 Market Study

The energy sector represents a major market at European and international levels. According to EU Reference Scenario 2016 [5], energy related investment expenditures on the supply side (power plans, power grids) should reach 500 billion euro, for the period 2016-2020, and more than 400 billion euro for the period 2046-2050. Investment expenditures in demand sectors (industry, tertiary and residential) is increasing and should be higher than 1 000 billion € for the 2041-2045 period (and the following 5 years period).

At international level, according to the International Energy Agency [6], the world's energy needs continue to grow and the Agency 2016's main scenario expects a 30% rise in global energy demand to 2040. The World Energy Outlook 2016 states that a cumulative $44 trillion in investment is needed in global energy supply.

Due to the increase of attacks on energy infrastructures, with potential serious damage, cyber security investments in this sector are expected to increase significantly [7]. The overall trend is confirmed by different reports. According to Energy and Resources Digest [8], Europe's cyber security market should see compound annual growth of 7.2% from 2014 to 2019, while marketsandmarkets [9] estimates that the cyber security market will grow from USD 122.45 Billion in 2016 to USD 202.36 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 10.6% during the forecast period.

According to the EECSP- expert group report [2], the main energy market change is related to new players involved in the energy scheme. These new players are the consumers becoming energy producers, the aggregators and third parties managing demand and supply, in addition to utility planners and operators using demand-response to ensure the balancing of supply and demand on the grids. Demand-response affects in the meantime the cost of electricity in wholesale markets, and thus of retail rates. The energy market is also changing with new energy supply options, through dynamic pricing and new market players such as aggregators controlling new flexible loads (e.g. electric vehicle charging, demand response). The main changes in the energy market are due in particular to more interactions between market players through ICT technologies and to the role of consumers as suppliers which affect the energy cost.

References

[1] ENISA, ”Report on Cyber Security Information Sharing in the Energy Sector”, November 2016, available at: https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

[2] Energy Expert Cyber Security Platform, ” Cyber Security in the Energy Sector”, February 2017, available at: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

[3] ENISA, ” ENISA Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends”, January 2017, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[4] ENISA, ” The cost of incidents affecting CIIs, Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII)”, August 2016, available at: https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

[5] European Commission, Reference Scenario Energy, https://ec.europa.eu/energy/en/news/reference-scenario-energy

[6] International Energy Agency, www.iea.org/newsroom/news/2016/november/world-energy-outlook-2016.html

[7] Forbes, http://www.forbes.com/sites/michaelkrancer/2015/11/04/the-biggest-cybersecurity-threat-the-energysector/#197a1c760ba6

[8] Energy and Resources Digest, Why 2016 Will Be the Year of Cybersecurity, https://dev.energyandresourcesdigest.com/invest-cybersecurity-2016-hack-cibr/

[9] http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

[10] NIS Directive, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

[11] ENISA, ”National cyber security strategies”, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[12] Gabrielle Desarnaud, “Cyberattaques et système énergétiques, faire face au risque“, IFRI, January 2017.

[13] Joint communication to the EU parliament and the council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", September 13, 2017, available at : https://eur-lex.europa.eu/legal-conent/EN/TXT/?qid=1505316068800&uri=JOIN:2017:450:FIN

[14] Smart Grids Task Force-Expert Group 2-Cybersecurity, 2nd Interim Report "Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity", July 2018, available at: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU