Digital security issues for critical infrastructures – Focus on the Electricity Sector

by Frédéric GUYOMARD (Electricité De France R&D, Paris-Saclay Labs, France), Luigi ROMANO (Parthenope University, Italy) and Ilias GKOTSIS (Inlecom Innovation, Kifissia, Greece)

Abstract

Critical infrastructure is more susceptible to a variety of threats, such as physical and cyberattacks by terrorists, activists, or hackers, as it gets more digitalized and networked and develops interdependencies with other facilities. The continuous digital revolution and the spread of communication technology that boost connection are increasing the attack surface. This new paradigm is further exacerbated by issues related to maintenance and supply chains. The motivations behind these attacks can range from sabotage and activism to financial gain or the destabilization of operations, particularly in an international context where threat actors are numerous and diverse. An attack on critical infrastructure can inflict significant damage, leading to cascading effects on other essential services, potentially bringing cities and citizens to a standstill. Effective damage control requires a sophisticated, interconnected protection, alert, and response system. In light of these considerations, the European Commission has decided to significantly update Directive 2008/114/EC, reflecting the evolving nature of critical entities. In order to minimize cascading consequences, the new Critical Entities Resilience (CER) Directive aims to improve infrastructure security and resilience through integrated protection and response. The NIS 2 Directive, a piece of legislation aimed at achieving a high standard of cybersecurity throughout the European Union, has further reinforced this endeavour. Geopolitical factors have formed the contemporary danger landscape, which emphasizes the significance of these regulatory revisions. There are numerous potential threats that could affect energy-related critical infrastructures, including the gas and electricity sectors. These threats include but are not limited to phishing techniques, denial-of-service attacks, remote internet attacks, data breaches, theft, vandalism and sabotage. Vulnerabilities often remain due to inadequate security measures, which means that advanced persistent threats (APT) from a range of actors—including terrorists, activists, and state-sponsored organizations—need to be taken into account. The European Commission seeks to strengthen the security and resilience of Europe's critical infrastructures by facilitating coordinated response against combined physical and cyber-attacks. In the current context of evolving threats, an awareness plan is needed to ensure that critical infrastructure can withstand and recover from the increasingly sophisticated and well-coordinated attacks.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

1. Introduction to the current operating risky landscape of critical facilities

"Ransomware as a Service", is what we usually read in many news media, illustrating the observation we can find in many articles discussing dealing with the threat in industrial sectors. Unfortunately, the energy and electricity sectors are also targeted. As critical infrastructure becomes digitised and networked (interdependent) with different facilities, it becomes more vulnerable to multiple threats including physical and cyberattacks by terrorists, activists or hackers. The attack surface is increasing due to the digital transformation and because of communication systems giving more and more connectivity, but also because of maintenance and supply chain issues. The motivation is sabotage, activism, financial or operation of destabilization, in an international context where threat actors could be numerous. An attack on a critical infrastructure can inflict major damage and 'cascading effects' on other essential services, bringing cities and citizens to a standstill. Damage control requires a sophisticated interconnected protection, alert and response system. With these considerations the EC has decided to significantly update Directive 2008/114/EC [1], reflecting the evolving nature of critical infrastructure. As such, the goal of the CER Directive is to increase infrastructure security and resilience using coordinated protection and response with a view to preventing cascading effects. This effort has been enhanced with the NIS 2 Directive (Directive (EU) 2022/2555), a legislative act that aims to achieve a high common level of cybersecurity across the European Union.

1.1. Threat environment and geopolitical considerations

The Ukrainian conflict shows that the energy domain is an important target and before the beginning of the invasion many incidents were detected. Power systems and the electrical grid and components have been targeted, and the first massive attempt took place in December 2015 (Black-Energy) and December 2016 (Industroyer) followed in 2017 with Notpetya [2] The "Dragos-2023-Year-in-Review-Full-Report" discuss the Operational Technologies cybersecurity landscape with this assessment:

"The OT (Operational Technology) cyber threat landscape continued to evolve in 2023, with an increase in tracked threat groups, ransomware events, and other threat activities driven by global conflict. The adversaries involved in these activities varied widely in terms of their level of sophistication, deployed capabilities, and intended targets. On one end of the spectrum, some threat groups used advanced techniques, such as leveraging native functionality, including living off the land (LOTL) techniques, to conduct reconnaissance and intelligence operations. Conversely, some adversaries targeted low-hanging fruit such as internet-accessible devices that lacked proper hardening, thus making them easy to damage and cause operational disruptions.

Threat groups continued to use publicly disclosed vulnerabilities and discover and develop their own capabilities. The identified vulnerabilities have the potential to result in loss/denial of view, denial/manipulation of control, theft of operational information, and loss of productivity and revenue."

In general, a non-exhaustive threat list that could affect the energy CIs (electricity and gas ones) include:

- Remote/Internet attacks
- Denial of service
- Botnets
- Data breaches
- Unauthorized physical access
- Vandalism and Sabotage

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

- Theft (usually copper or other materials that can be sold)
- Third party interference
- Pandemics
- Landslide (especially for gas CIs)
- Flood
- Fire
- Lighting
- Corrosion

1.2. Vulnerabilities: lack of sufficient security controls

To evaluate the risk level, it is necessary to consider advanced persistent threats (APT) that could be planned or carried out by terrorists, activists, or even state actors. Attacks could be carried out using specialised digital tools — malware, hacking, intrusion, or any attempt to penetrate the systems; or due to physical threats, including drones for spying or carrying bombs. The two types of attacks — digital and physical could be combined, taking advantage of a disaster situation, natural or not. Despite security efforts in certain sectors, attackers continue to exploit the same technical weaknesses to gain access to networks. Exploiting 'day-zero' and 'day-one' vulnerabilities remains a prime entry point for attackers, who all too often still have benefited from poor administrative practices, delays in applying patches and the absence of encryption mechanisms. Many CVEs are published, and the severity scores must be considered to estimate the urgency of remediation action. See the "Dragos ICS Report 2023" [4].

To fulfil a link with the PRAETORIAN European project[1], the strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project provides a multidimensional (economical, technological, policy, societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which will include digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision-making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures.

From the ENISA 2023 report[2] we learn that in 2022, following the invasion of Ukraine, Industroyer2 was discovered targeting energy substations. This is a variant of Industroyer malware that was used by the Sandworm APT group to cut power in Ukraine in 2016367. Another malware strain detected was INCONTROLLER (aka PIPEDREAM) which was built to manipulate and disrupt industrial processes368.

In May 2023, novel malware targeting OT and ICS was discovered and tracked as COSMICENERGY. The purpose of this malware was to disrupt electric power through interactions with devices, such as remote terminal units (RTUs), used in electric transmission and distribution operations in Europe370.

Further code analysis of the malware and its components showed it lacks maturity, contains errors and is far from having a full-fledged attack capability like Industroyer2 or CRASHOVERRIDE. It was concluded that COSMICENERGY is not an immediate threat and that is likely part of a training exercise or for use in detection development371. However, these incidents show that industrial protocols are susceptible to attacks and serve as a wake-up call for the critical infrastructure sector,

[1] https://praetorian-h2020.eu/
[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

emphasising the need for continuous vigilance and proactive measures to safeguard operational technology and industrial control systems.

1.3. Impact and consequences on the Energy Sector

Malware and threats against data or availability via supply chain processes have consequences on the critical entities' essential functions (for example XZ backdoor attack [5]. But hybrid threat could produce stronger consequences because of the opportunity to use some temporary weaknesses, completed with prepositioned point on the digital domain. The "ENISA threat landscape 2023" document clearly the link with the geopolitical context: "*Cyber threat actors and their modus operandi are inevitably influenced by geopolitical events. A sizeable number of operations have been monitored, during the reporting period, where the actions of some cybercriminals, state-nexus threat groups and hacktivists have their roots in geopolitical developments. In general, at least state-nexus groups and hacktivists, regardless of motivation or agenda, can be triggered into action by these events.*"

Plant management and engineering activities are directly linked to industrial IT and provide sensitive services for the company. What's more, the centralisation of these activities requires particular attention in terms of IT security. Guaranteeing availability and integrity is therefore of paramount importance.

The threat is constantly evolving, and attacks can have major consequences. They can cause a deterioration in system performance (e.g. increased response times) or lead to a loss of integrity (e.g. modification of data, modification of application functions). They can also lead to information leakage, data loss and even the loss of critical services. For a company, there may be impacts on its operations, financial impacts, and impacts on intellectual assets (loss of knowledge, theft of know-how or innovative capabilities). In some cases, damage to critical systems can have a strong human or environmental impact. Another significant issue concerns the brand image, possible interference and destabilisation of companies and states. For example, the media coverage of the various energy sectors often puts these activities in the spotlight. The stakes are high, and the security measures to be implemented at the level of a complete system must ensure the right level of protection, for reasons of operational safety and availability, as well as efficiency.

1.4. Relationship with Resilience: Governance

In 2023, major regulatory changes for critical infrastructure asset owners, led organisations to spend more time and resources preparing for a cyber security event. This included updates for US pipeline operators in North America with TSA Pipeline-2021-02D (SD-02D). In Europe, it was the Networks and Information Systems Directive (NIS2); in Australia, the Critical Infrastructure Security SOCI Act; and the Kingdom of Saudi Arabia's Essential Cyber Security Controls (ECC) ECC. One of the most significant changes was not aimed at critical infrastructures, but at listed companies in the United States: the new cybersecurity risk management rules of the Securities and Exchange Commission (SEC). These rules apply to many IoT asset owners, including investor-owned utilities and manufacturing companies.

To support the resilience needs, regulatory framework and compliance in the Power Sector have been established. The US Cybersecurity and Infrastructure Security Agency and the EU NISv2 (DIR 2022/2555) establish cybersecurity requirements for operators of essential services, including power companies. The NERC (North American Electric Reliability Corporation) and IEC (International Electrotechnical Commission) are also providing strong recommendation with NERC CIP and IEC 62443 standards. Another major document is the "NIST Releases Version 2.0 of Landmark

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Cybersecurity Framework [6] where after the magic 'Identify, Protect, Detect, Respond, Recover', the Governance is becoming central and everywhere.

2. Attack Scenarios - examples

The Cybersecurity Innovation Cluster for EPES (CyberEPES, **https://cyberseas.eu/cyberepes-the-cybersecurity-innovation-cluster-for-epes/**) produced a repository of attack scenarios, which were shared among the projects of the cluster for a more accurate validation of the solutions developed individually by projects.

The following list provides the most significant and common attacks that the energy CIs face, both cyber and physical, along with some past incidents:

Cyber Threats:

1. **Ransomware Attacks**
    - **Description**: Malicious software that encrypts data and demands ransom for the decryption key.
    - **Example**: Colonial Pipeline Attack (2021) - A ransomware attack by the DarkSide group led to a significant fuel supply disruption across the East Coast of the United States.
2. **Phishing and Social Engineering**
    - **Description**: Techniques used to trick individuals into divulging confidential information.
    - **Example**: Ukraine Power Grid Attack (2015) - Hackers used phishing emails to gain access to the control systems of Ukrainian power companies, causing widespread outages.
3. **Advanced Persistent Threats (APTs)**
    - **Description**: Prolonged and targeted cyberattacks aimed at stealing information or disrupting operations.
    - **Example**: Dragonfly (Energetic Bear) - A group believed to be linked to the Russian government, targeting energy companies in the U.S. and Europe.
4. **Malware and Viruses**
    - **Description**: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
    - **Example**: Stuxnet (2010) - A sophisticated computer worm that targeted Iran's nuclear facilities.
5. **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**
    - **Description**: Attempts to make a machine or network resource unavailable to its intended users by overwhelming it with traffic.
    - **Example**: Attack on the Ukrainian Power Grid (2016) - A DDoS attack coincided with a physical intrusion and cyberattack, disrupting power distribution.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Physical Threats:

1. **Terrorist Attacks**
    - **Description**: Deliberate acts of violence aimed at causing disruption or damage.
    - **Example**: Metcalf Sniper Attack (2013) - Unknown gunmen attacked a substation in California, causing extensive damage and raising concerns about the vulnerability of physical infrastructure.
2. **Natural Disasters**
    - **Description**: Events such as earthquakes, hurricanes, and floods that can cause extensive damage to infrastructure.
    - **Example**: Hurricane Maria (2017) - Devastated Puerto Rico's power grid, leading to prolonged outages.
3. **Physical Sabotage**
    - **Description**: Intentional damage or disruption caused by individuals or groups.
    - **Example**: Vandalism of power transmission lines and substations.
4. **Insider Threats**
    - **Description**: Threats posed by individuals within the organization who may cause harm intentionally or unintentionally.
    - **Example**: Malicious insiders exploiting their access to disrupt operations or steal sensitive information.
5. **Theft and Vandalism**
    - **Description**: Theft of valuable materials (e.g., copper) and vandalism causing operational disruptions.
    - **Example**: Copper theft from electrical infrastructure leading to power outages and safety hazards.

Other realistic objectives such as disrupting the transmission of electricity or even creating a blackout, impacting the safety of people working on the electricity network or causing an explosion at a source substation are usually considered. It could also consist in using malicious code or ransomware to disturb but also to ask for money when the command-and-control system is paralysed. Taking control of driving systems with no objective other than recreation or the desire to make a name for oneself. For instance, the management of the electricity frequency is very important on a grid, and having wrong information about that sensitive feature is critical due to integrity needs.

Expanding on the above usual attacks, the following two scenarios provide combined cyberphysical incidents that energy infrastructures could face:

<u>Coordinated Attack on a Power Grid</u>

Scenario Description *(based on the Ukrainian Power Grid Attack (2015) combined with physical substation sabotage)*:

A sophisticated attacker launches a cyber-physical attack targeting a national power grid to cause widespread blackouts and infrastructure disruption.

Cyber Incident:

- The attackers use spear-phishing emails to infiltrate the IT systems of the power company.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

- They deploy malware to gain access to the Supervisory Control and Data Acquisition (SCADA) systems.
- The malware manipulates the control systems, causing critical components to fail or operate outside safe parameters.

Physical Incident:

- Simultaneously, a team of attackers physically sabotages several key substations and transmission lines.
- They use explosives or gunfire to damage transformers and disable physical security systems, making recovery efforts more challenging.

Impact:

- Widespread power outages are affecting millions of people.
- Extended downtime due to the combination of physical damage and cyber manipulation.
- Economic losses, public safety concerns, and a significant impact on daily life.

Attack on Oil and Gas Infrastructure

(based on the Colonial Pipeline ransomware attack (2021) combined with physical sabotage)

Scenario Description:

An attacker targets an oil and gas company to disrupt production and cause environmental damage.

Cyber Incident:

- The attackers breach the company's network through a vulnerable internet-facing application. They plant malware to take control of the pipeline's control systems.
- The malware sends false data to operators, leading to incorrect valve operations and pressure levels.

Physical Incident:

- The attackers coordinate with a physical team that places explosives along critical points of the pipeline. They time the explosions to coincide with the cyber-induced pressure build-up, causing a massive rupture and oil spill.

Impact:

- Significant disruption in oil and gas supply.
- Environmental disaster due to the oil spill.
- High costs for repairs, cleanup, and legal liabilities.
- Public outcry and damage to the company's reputation.

These scenarios underscore the need for integrated security strategies that address both cyber and physical threats to critical infrastructure.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

3. Regulations – Network Code, CER Directives, others

Regulatory Framework and Compliance in the Power Sector

Regulatory Body	Relevant Standards	Description
NERC (North American Electric Reliability Corporation)	NERC CIP (Critical Infrastructure Protection)	NERC CIP standards define security requirements for the bulk power system in North America. They address the protection of critical assets, cybersecurity incident reporting, and the security of the power grid.
FERC (Federal Energy Regulatory Commission)	Various	FERC oversees the interstate transmission of electricity, oil, and natural gas. They have regulatory authority over the wholesale power market and enforce compliance with NERC CIP standards.
IEC (International Electrotechnical Commission)	IEC 62443	IEC 62443 is a global standard for the security of industrial automation and control systems (IACS). It provides guidelines and requirements for securing ICS, which are applicable to power sector organizations worldwide.
CISA (Cybersecurity and Infrastructure Security Agency)	Various	CISA provides guidance and resources to enhance critical infrastructure cybersecurity. They offer tools and recommendations to help power companies improve their cybersecurity posture.
EU's NIS Directive (Network and Information Systems Directive)	NIS Regulations	The NIS 2 Directives in the European Union establishes cybersecurity requirements for operators of essential services, including power companies. It mandates the reporting of incidents and the adoption of adequate security measures.
Industry-Specific Regulatory Bodies	Industry-Specific Standards	Some countries or regions have their own industry-specific regulatory bodies and standards for the power sector. These standards can vary by location and may include additional requirements beyond global standards.
Critical Entities Resilience Directive (CER)	CER regulations	CER directive lays down obligations on EU Member States to take specific measures, to ensure that essential services are provided. The Directive creates an overarching framework that addresses the resilience of critical entities in respect of all hazards, whether natural or man-made, accidental or intentional.
Regulation (EU) 2019/941 **on risk-preparedness in the electricity sector**		Aims to ensure that Member States are well-prepared to deal with electricity crises. Requires the establishment of a framework for assessing and managing risks related to electricity security.
Regulation (EU) 2017/1938 **concerning**		Although primarily focused on gas, it includes measures relevant to the electricity sector due to the interdependence of energy sources.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

measures to safeguard the security of gas supply		Ensures a coordinated response to energy supply disruptions.
Regulation (EU) 2022/868 on cybersecurity of critical infrastructure		Focuses on enhancing cybersecurity across critical infrastructures, including the electricity sector. Mandates specific security measures and incident reporting requirements for operators.
Cyber resilience act		Supervises connected products and the services on which they depend
ISO	ISO 27402 ISO 27404	Cybersecurity – IoT security and privacy – Device baseline requirements and certification scheme
RED-DA		Delegated Regulation (EU) 2022/30 and cybersecurity compliance
ETSI	EN 303645	Cybersecurity for the consumer Internet of Things: basic requirements
NISTIR	8425	Profile of the IoT core baseline for consumer IoT products
IEC	62443	Safety of industrial automation and control systems

"These regulatory bodies and standards play a crucial role in shaping the compliance requirements for power sector organizations. Compliance with these standards is essential to ensuring the security and reliability of critical infrastructure and protecting against cybersecurity threats".

4. The Energy Dataspace, emerging issues and introduction to cloud

4.1. Rationale for a European Energy Dataspace

In today's interconnected world, existing systems are required to meet increasing data-sharing demands. The rapid growth of data-centric applications, which highlight the true value of data, has also impacted smart grids and energy supply chains. Specifically focusing on energy exchange, current data exchange methods show limitations, especially when multiple stakeholders, such as Transmission System Operators (TSOs) and Distribution System Operators (DSOs), need to collaborate and share sensitive information. The development of 'Common European Dataspaces' is a strategic response to these challenges, creating an environment where data can be exchanged securely and efficiently while respecting privacy and data sovereignty. The European Common Data Spaces in the energy sector brings about several important benefits and enables utilities and governments to develop new services for citizens and uncover new revenue streams. It is a transformative paradigm in the energy sector, uniting stakeholders—energy providers, consumers, grid operators, and regulators—under a shared digital context. This unification is not only about connecting dots but about creating a secure exchange of data that bridges the traditional silos, fostering a seamless flow of information and insights across the energy landscape. Such integration and interoperability are fundamental for the sector's efficient resource management and distribution, ensuring that energy reaches where it is needed most when it is needed. Several research initiatives are contributing to building a European Energy Data Space. Among these, the CyberSEAS project[3] targets the crucial objective of securing it, by delivering robust security measures in the realm of data

[3] https://cyberseas.eu/

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

sharing and exchange. CyberSEAS is dedicated to advancing applications of enabling technologies that are crucial for facilitating privacy-preserving data exchange and sharing among various utility operators. By focusing on these technologies, the project aims to establish a secure framework that ensures data confidentiality and integrity across different entities within the utility sector, enhancing trust and collaboration among stakeholders.

4.2. Privacy-Preserving and Sovereign Data Exchange

In the dataspace paradigm, data exchange is enabled through connectors, which can be deployed on-premises or in a cloud environment, primarily using helm charts and Kubernetes clusters. Establishing a data marketplace requires, among other things, a shared vocabulary, which enables participants to comprehend a shared language. This common understanding is essential for facilitating machine-to-machine (M2M) communication and simplifying the creation of privacy-preserving policies. From a technical perspective, it is also essential to guarantee the minimum requirements needed for stakeholders' computing nodes, verify the level of security provided (e.g., Trusted Execution Environment support [7]), and confirm their geographical locations. Stakeholders can publish descriptions of their data offerings on a data broker, while developers can provide applications that utilize this data to create added-value services. All transactions between different connectors are recorded by a clearing house, to ensure the accurate processing of payments and data exchanges. Examples of policy enforcement in dataspaces include restrictions on the duration of data usage, the rights to view and utilize data, and the conditions under which data may be shared or processed. For instance, policies might dictate that certain data can only be accessed for a limited time, or specify that data must not be transferred to unauthorized parties. Additionally, policies can enforce data anonymization or de-identification before it is shared to protect privacy. These rules ensure that all data handling within the dataspace adheres to agreed-upon ethical and legal standards, fostering a secure and trusted environment for all participants.

5. Gaps Identification

The regulatory framework and the technological advancements provide an improvement and upgrade of the risk and security management systems that are implemented on CI, but also some serious gaps in the new challenges of security and safety of CI, the convergence of them, the new types of hazards like the Hybrid ones, and the not so satisfying implementation of advanced scientific solutions.

The typical current practices of security management (physical and cyber) for the electricity sector, do include but are not limited to:

1. Operational monitoring in a control room
2. Procedures and guidelines in case of events
3. Preparation and training to manage all identified credible critical events
4. Communication channels with public authorities (police, fire brigades), mainly oral communication via phone
5. Use of meteorological forecast and local measurement stations to cover the effects of weather, temperature, wind direction
6. Additional possible surveillance systems e.g.:
    a. Fiber-optic
    b. Viber-acoustic
    c. Cameras (optic, IR)
    d. Drones combined with optic/thermal cameras, lidar, etc

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

e. Local access control of plants and facilities
f. Satellite surveillance (SAR) for geo hazards
g. Operational room covers emergency in operation, health (occupational safety) and security
h. There is not a dedicated security system as such, but security issues are integrated into overall operation, often taken from different additional systems (other than the operational system)
i. Emergency, maintenance and repair operative local teams receive alarms by UMTs, email, etc.

Some of the observations and potential gaps in security contain the following issues:

1. Cybersecurity efforts are often fragmented across different regulations and sectors, leading to inconsistent implementation and vulnerabilities
2. The regulations may not fully address advanced persistent threats (APTs) and sophisticated cyber attacks targeting critical infrastructure
3. There are challenges in ensuring interoperability and coordinated responses between different Member States, especially during transnational crises
4. Physical security standards for protecting critical infrastructure may not always be up-to-date with evolving threats
5. The supply chain for critical infrastructure components, including technology and equipment, often involves third parties that may not meet stringent security requirements
6. Effective coordination mechanisms for incident response and recovery at the EU level need further development and testing
7. There is a need for more comprehensive training programs to ensure that personnel are prepared to handle security and resilience challenges effectively
8. Keeping regulations up-to-date with technological advancements and emerging threats requires ongoing effort and coordination
9. Current security systems are not real-time integrated with operational system
10. Lack of common operational picture, e.g. the remote control room information versus local authority and responder knowledge, while there is also a lack of spatially visualized information also
11. No real-time, overall security assessment (e.g. risk assessment with KPIs provided and impact analysis, including cascading effects)

6. Conclusion

The energy sector is critical in Europe to provide essential services to citizens. It's also critical for all the other critical sectors and critical entities (see the CER Directive). Electricity is so sensitive that we can't imagine the consequences of a disruption or a blackout due to combined physical and digital attacks on the network or on power plants. The threat level has risen considerably in recent years, as can be seen from the attacks on hospitals and the malicious activity recorded on the Internet by international C-SIRTs. The strong development of the Internet of Things (IoT) is also increasing the threat landscape because offering more access points and possible uncontrolled connection systems. New Directives appeared such as NISv2 and Cyber Resilience Act but the measures to be deployed to protect, monitor, alert and react have a cost that must be understood, integrated, and planned during all the lifetime of the installations, from the design to the end of life of the different digital and electronic components. For all the reasons we developed in this white paper, the risk consideration and the risk analysis are the basis of a global defence. Regarding that, the ECCC (European

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Cybersecurity Competence Centre) has been created to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community.

The setup of a secure European Energy Data Space is a key priority. Important results have already been achieved, but the sector still has to face specific privacy and security challenges. For instance, integration and exchange of data among energy stakeholders require robust privacy-preserving mechanisms to prevent unauthorized access and to ensure integrity and confidentiality. This is essential for enabling operational security and trust within and across the energy supply chain.

We are witnessing an amazing increase in the number and in the variety of energy services, which are being deployed on virtually any type of platform of the so called "Computing Continuum", i.e. the infrastructure integrating the Internet of Things (IoT), the edge, and the cloud. This mandates that effective security measures be developed and applied throughout the data lifecycle, to ensure that data is always handled securely and in all locations. Stringent confidentiality and integrity requirements must be satisfied not only for data "in transfer" (e.g., during network exchanges) and "at rest" (e.g., stored on a disk) but also "in use" (e.g., loaded in RAM or the CPU for computation). While securing data in transfer and at rest is relatively straightforward, protecting data in use remains a significant challenge. This difficulty arises because data must be safeguarded from attacks by privileged users (e.g., system administrators or cloud providers) and software (e.g., the operating system or the hypervisor).

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

References

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992

[2] https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

[3] CyberSEAS — Cyber Securing Energy dAta Services, 2024.

[4] https://www.dragos.com/ot-cybersecurity-year-in-review/

[5] https://www.synopsys.com/blogs/software-security/xz-utils-backdoor-supply-chain-attack.html

[6] https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[7] Luigi Coppolino, Roberto Nardone, Alfredo Petruolo, and Luigi Romano. Securing firmware with tee technology. In New Trends in Intelligent Software Methodologies, Tools and Techniques: Proceedings of the 22nd International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT 23), volume 371, page 149. IOS Press, 2023.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Consortium:

Engineering – Ingegneria Informatica SPA (ENG), Italy
Deutsches Zentrum für Luft und Raumfahrt EV (DLR), Germany
GFT Italia SRL (GFT), Italy
Inov instituto de engenharia de sistemas e computadores inovacao (INOV), Portugal
Inlecom commercial pathways company limited by guarantee (ICP), Ireland
SINTEF AS (SIN), Norway
Steinbeis EU-VRI GMBH (EU-VRi), Germany
Stowarzyszenie Polska Platforma bezpieczenstwa wewnetrznego (PPHS), Poland
Laurea – Ammattikorkeakoulou oy (LAU), Finland
Innov - Acts Limited (INNOV), Cyprus
Norks Regnesentral (NRS), Norway
European Organisation for Security (EOS), Belgium
Katholieke Universiteit Leuven (KUL), Belgium
Fstechnology SPA (FST), Italy
Athens International Airport S.A (AIA), Greece
Fundacion de la Comunidad Valenciana para la investigacion, promocion y estudios comerciales de Valenciaport (FV), Spain
Orange Romania (ORO), Romania
Electricité de France (EDF), France
Leonardo Societa per Azioni (LDO), Italy

Contact:

Project Coordinator: Emilia Gugliandolo (ENG)

Whitepaper Contact: Frédéric GUYOMARD (EDF)

Dissemination Manager: Elodie Reuge (EOS)

Funded by the European Union

*Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.