



EPES and Smart Grids: practical tools and methods to fight against cyber and privacy attacks

*Insights and recommendations
from research and innovations
projects and entities*



Acknowledgements

Cyberwatching.eu is grateful to the projects and individual experts that have contributed to the series of webinars of the project clusters on the topic of the Energy sector, and to the recommendations provided in this document. More details and contact details can be found in section 5.



Disclaimer

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under Grant Agreement no.740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Contents

1	Introduction	4
2	Cybersecurity and privacy in the Energy Sector	5
3	Insights and recommendations from R&I projects	6
3.1	DEFEND: Data Governance for Supporting GDPR	6
3.2	EnergyShield: Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures.....	6
3.3	SDN-microSENSE: SDN – microgrid reSilient Electrical eNergy SystEm.....	7
3.4	SealedGRID: A Secure Interconnection of Technologies for Smart GRID Applications	8
4	Conclusion.....	10
5	Contributing Projects	11
	How to reach us.....	12

1 Introduction

One of the goals of the Cyberwatching.eu¹ project is to identify ways to cluster active projects with similar aims for their mutual benefit, identifying possible opportunities for lightweight synergies and supporting them with targeted support activities, such as joint webinars and outreach activities.

To achieve this objective, in the past weeks Cyberwatching.eu has organised two virtual meetings with two different groups of projects, with the specific aim of helping them improve their market capabilities.

The clusters have been created according to the similarity of projects in their Marketing Readiness Level (MRL) at this point of their execution.

The meetings included some key speakers, such as Georgios Lyssandredis and Ada Matei, from the Common Competence Centre at DG RTD², who presented the Horizon Results Platform; Michel Drescher, from Oxford University³, who showcased the new project radar and asked projects to test the new features; and Nicholas Ferguson, Cyberwatching.eu coordinator, who introduced the marketplace and the new Horizon Results Booster⁴ service.

During the second part of the meetings, Marina Ramírez, from AEI Ciberseguridad⁵, explained which are the commonalities of the projects joining the meetings and opened the debate.

In the first virtual meeting, which took place on 9 July 2020, some starting points for collaboration emerged. One of the identified collaborative activities for the research and innovation project was the organisation of webinars focussing on different sectors. The energy sector is one of the first three sectors that were identified during the meeting. The theme was proposed by SealedGRID⁶, which is oriented towards digital infrastructure and government and public authorities in the energy sector.

Based on experience with their platforms, use cases and demonstrators, the projects identified several interesting challenges. In this report, four (4) research and innovation (R&I) projects related to cybersecurity and privacy collaborated with Cyberwatching.eu to provide a consolidated overview of the most significant barriers in the area of cybersecurity and privacy concerning cybersecurity and privacy in the energy sector. Also, the projects laid down concrete recommendations and showcased their solutions on these matters.

¹ <https://cyberwatching.eu/>

² https://knowledge4policy.ec.europa.eu/organisation/dg-rtd-dg-research-innovation_en

³ <https://www.ox.ac.uk/>

⁴ <https://www.horizonresultsbooster.eu/>

⁵ <https://www.aeiciberseguridad.es/>

⁶ <https://www.cyberwatching.eu/projects/1156/sealedgrid>

2 Cybersecurity and privacy in the Energy Sector

The electrical power and energy system (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity. With the growing use of digital devices and advanced communications and interconnected systems, the EPES is increasingly exposed to external cyber-threats, and therefore it requires a thorough evaluation of the cybersecurity risk that allows the users to take proper countermeasures.

On the other hand, although smart grids (SG) support dynamic two-way information exchange between utility companies and their customers, contributing towards smart and sustainable energy management in Europe and the establishment of a wiser energy consumption mentality, the power grid is also exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities, related to the specific characteristics of the Smart Grids infrastructure, are emerging.

Attacks on EPES and SG may lead to cascading failures, ranging from destruction of other interconnected critical infrastructures to loss of human lives.

The European Commission adopted in April 2019 sector-specific guidance that identifies the main actions required to preserve cybersecurity and be prepared for possible cyberattacks in the energy sector, taking into account the characteristics of the sector such as the real-time requirements, the risk of cascading effects and the combination of legacy systems with new technologies.

This joint webinar entitled “EPES and Smart Grids: practical tools and methods to fight against cyber and privacy attacks”⁷ was organised by Cyberwatching.eu in accordance to its goal to cluster active projects with similar goals for their mutual benefit, by identifying possible opportunities for lightweight synergies and supporting them with targeted support activities. It took place on 12 November 2020 at 11 AM CET in collaboration with four research and innovation projects: DEFEND⁸, EnergyShield⁹, SDN-microSENSE¹⁰ and SealedGRID. The R&I projects presented their solutions to protect EPES and Smart Grids against cyber-threats, and preserve consumers' privacy.

⁷ <https://cyberwatching.eu/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks>

⁸ <https://www.cyberwatching.eu/projects/1039/defend>

⁹ <https://www.cyberwatching.eu/projects/2013/energyshield>

¹⁰ <https://www.cyberwatching.eu/projects/2325/sdn-microsense>

3 Insights and recommendations from R&I projects

3.1 DEFEND: Data Governance for Supporting GDPR

The DEFEND platform aims to raise the awareness of data controllers about the real status of an organisation, through enhanced visualization elements, and information that can be exploited for each department, third party and/or process. An important point for the board of an organisation is a synthetic dashboard with the status of the organisation compliance to Data Protection. The DEFEND platform includes a dashboard service to provide this kind of information to the board and stakeholders.

The DEFEND architecture is composed of the five (5) DEFEND services, the DSM service, the data process management (DPM) service, the data breach management (DBM) service, the general data protection regulation (GDPR) planning service, the GDPR reporting service and all the components included in the DEFEND service. The Defend Platform aims to support the Data Controller to define an improvement program to increase the maturity of the organization in data protection based on the law and related best practices.

Recommendations

- To have under control the status of the organisation compliance to Data Protection, a compliance status for each of the GDPR principles for the whole organization, for each department and each third party and compliance status information for the data subject.
- To define the list of processing activities, the connections with Departments and Third Parties involved in the activities' linked assets, systems and threats.
- To perform threats analysis, data minimisation analysis, privacy by design/by default based on the result of the analysis and design modelling techniques, and continuous risk assessment.

3.2 EnergyShield: Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures

EnergyShield's presentation entitled "Assessing, Enhancing and Cultivating a Cyber-Security Culture in the EPES Sector" started with an overview of the brief goals and objectives of the project. This introduction was followed with a description of one of the five (5) cyber-security tools contained within the EnergyShield toolkit, namely, the Security Behaviour Analysis (SBA) tool, implemented by the Management & Decision Support Systems Laboratory (DSS Lab) of the National Technical University of Athens. In a 15-minute session, participants were presented with the tool specifics including the cybersecurity needs which addressed its main features and challenges. This presentation was concluded with a short demo exhibiting a common use case scenario from the EPES sector reality showcasing the currently available version of the tool.

Recommendations

- Invest in promoting the personnel of an organisation from a profile of potential cyber-threat to a profile of valuable cyber-security asset.

- Get to know the vulnerabilities of the organization in order to be in a position to defend it.
- Auditing and monitoring are key mitigation policies for a robust cyber-reality.
- Being able to detect anomalies and ongoing attacks is the first step towards protecting assets.
- Information is valuable. Treat it as such. Encrypt it!

3.3 SDN-microSENSE: SDN – microgrid reSilient Electrical eNergy System

The Smart Grid (SG) is considered as the next-generation electrical grid, transforming the conventional energy model into a new era with a variety of benefits, such as two-way communications, increased reliability, pervasive control and self-healing. However, this evolution raises severe cybersecurity concerns due to both the insecure nature of the legacy systems (e.g., supervisory control and data acquisition (SCADA)) and the new vulnerabilities originating from smart technologies. Moreover, it is noteworthy that the vast amount of SG sensitive data attracts even more cyber attackers. The characteristic advanced persistent threats (APTs) against energy-related infrastructures are, for example, Stuxnet, Dragonfly, Dragonfly 2.0, BlackEnergy3, TRITON and Crashoverride.

The SDN-microSENSE project aims to address the cybersecurity risks in electrical power and energy system (EPES), by introducing an integrated platform of four pillars, namely (a) risk assessment, (b) intrusion detection and prevention, (c) self-healing and energy management and (d) privacy-preservation.

The **first pillar** introduces a collaborative risk assessment methodology and tool, which cooperates with the other components of the SDN-microSENSE architecture to assess the risk level of the various security alerts dynamically.

A large-scale security information and event management (SIEM) system orchestrate the **second pillar**, including several artificial intelligence (AI) detectors related to industrial protocols, such as Modbus, IEC 60870-5-104, IEC 61850, MQTT and DNP3. Furthermore, it adopts advanced visual analytics to identify possible threats and electricity-related disturbances.

Next, the **third pillar** takes full advantage of software-defined networking (SDN) technology to mitigate possible cyberattacks in real-time. In addition, it comprises islanding and grid restoration mechanisms that can be adopted in emergencies. Furthermore, it is worth noting that through the blockchain technology, it also provides energy management and transaction platform among various energy-related stakeholders.

Finally, the **fourth pillar** focuses on privacy, introducing an overlay privacy framework, which is responsible for ensuring the confidentiality, integrity and authenticity of the various energy-related data, by using homomorphic encryption and anonymisation techniques.

A honeypot is an asset with no production value that imitates the behaviour of real assets, aiming to protect them and collect valuable information about the cyberattackers. It can play a significant role in the risk assessment procedure since it is an effective detection countermeasure by hiding the real assets and, in parallel, it can act as a threat intelligence mechanism. In the context of the SDN-microSENSE project, three main EPES honeypots were developed, namely (a) Modbus Honeypot, (b) IEC 60870-5-104 Honeypot and (c) IEC 61850 Honeypot. These honeypots are

deployed dynamically by a Honeypot Manager, which also can communicate with the SDN controller to re-direct malicious network traffic to an EPES honeypot, thus (a) protecting the real assets and (b) receiving insights about the cyberattacker activities. The security events originating from the EPES honeypots can raise the application of an islanding mechanism, thus mitigating the devastating consequences of a critical cyber-attack. Through a clustering approach, the project introduces an Isolating and Islanding Mechanism (IIM), which solves the problem of the intentional islanding, thereby guiding the system operator to apply the most optimum islanding scheme, taking into account the various constraints and the available Distributed Energy Resources (DERs).

Recommendations

Based on the current progress of the SDN-microSENSE project, the following recommendations for the Critical Infrastructures (CIs) are identified.

- **Adoption of the IEC 62351 security controls.** IEC 62351 establishes a set of security and privacy controls, specially designed for industrial environments. In particular, it consists of 14 parts that cover multiple cybersecurity and privacy aspects, such as authentication, access control, privacy, security profiles, key management and security architecture.
- **Timely intrusion detection.** The critical infrastructures include ingredients and communications that were designed without having cybersecurity in mind. However, they are necessary for their core operation. Therefore, appropriate intrusion detection mechanisms should be adopted, considering the unique properties of each individual infrastructure.
- **Timely mitigation.** Smart mitigation mechanisms should act as fast as possible, thus mitigating or even preventing the potential cyberattacks. Smart authentication and access control systems compose characteristic examples. Moreover, intentional islanding and grid restoration compose efficient mitigation measures for energy-related CIs. Finally, the proper usage of SDN technology can contribute significantly to the mitigation of the possible intrusions coming from malicious insiders.
- **Privacy-preservation.** The critical infrastructures comprise a plethora of sensitive data. This data should be protected from many privacy risks. Blockchain, holomorphic encryption and differential privacy are sufficient mechanisms that can ensure the confidentiality and authenticity of the various data transactions.
- **Threat-Intelligence.** Cyberattacks are evolving rapidly. Therefore, it is crucial to adopt and design adequate systems and methods that can mine information and knowledge about these cyberattacks and malware. Honeypots and anonymous repositories of incidents are characteristic examples that can contribute to this aspect. However, the presence of proactive relevant countermeasures is necessary.

3.4 SealedGRID: A Secure Interconnection of Technologies for Smart GRID Applications

Security for smart industrial systems is prominent due to the proliferation of cyber threats threatening national critical infrastructures. The smart grid comes with intelligent applications that

can utilize the bidirectional communication network among its entities. Microgrids are small-scale smart grids that enable machine-to-machine (M2M) communications as they can operate with some degree of independence from the main grid. In addition to protecting critical microgrid applications, an underlying key management scheme is needed to enable secure M2M message transmission and authentication. Existing key management schemes are not adequate due to microgrid special features and requirements. SealedGRID proposes the Micro sElf-orgaNiSed mAnagement (MENSA), which is the first hybrid key management and authentication scheme that combines public key infrastructure (PKI) and web-of-trust concepts in micro-grids. Our experimental results demonstrate the efficiency of MENSA in terms of scalability and swiftness.

The major challenges, which specifically concern key management in microgrid networks, are the following:

- **C1.** a microgrid is a network with high churn meaning that nodes frequently join and leave, affecting the efficiency of centralized solutions due to the overhead created by multiple and constant node connection requests to a single entity;
- **C2.** when the Certification Authority (CA) is compromised, the traditional approach is to revoke all certificates issued and this is an administratively intensive task that would temporarily obstruct smooth operations and impair information exchange;
- **C3.** a microgrid can operate either in parallel with an existing power grid or in an “islanded” mode using the M2M communication paradigm; if smart meters lose connectivity to the CA, e.g., due to network outages, it is not currently feasible to validate their certificates affecting the security level of the entire microgrid and the seamless execution of the processes performed inside the network; and
- **C4.** the storage of certificates on a central server creates a single point of failure which may result in the discontinuation of all network operations.

4 Conclusion

The Cyberwatching.eu webinar on “EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks”¹¹ provided very useful insights and tangible solutions in protecting the electrical power, energy systems and smart grids against cyber-attacks and how to preserve the privacy of the data.

During the webinar, the key solutions demos coming from the four (4) research and innovations (R&I) projects were presented, providing different offerings:

- EnergyShield is developing the **integrated cybersecurity solution/tool** for vulnerability assessment, monitoring and protection of critical energy infrastructures.
- The **DEFEND platform** should help GridPocket to follow GDPR rules at different processing levels to respect the privacy and security rights of its customers and data controller.
- Inside the SDN-microSENSE project, **novel international islanding solutions** are proposed, exploiting powerful fitting and generalization capabilities offered by deep learning architectures, offering a real-time solution with increased time efficiency.
- The SealedGRID project proposed **Micro sElf-orgaNised mAnagement (MENSA)**, the first distributed key management and authentication system for microgrids, paving the way toward developing microgrids further and it will help to realise their full potential in terms of scalability and performance efficiency.

The above projects have very promising results and offer a great opportunity for those who are interested to explore the presented products and services for the energy sectors.

¹¹ <https://cyberwatching.eu/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks>

5 Contributing Projects

The projects contributing to this document are the following:



Website: www.defendproject.eu

Grant agreement number: 787068

Duration: 1 July 2018 – 31 March 2021

Contributors:

- ◆ Jean-Baptiste-Bernard¹², Product Manager at GRIDPOCKET
- ◆ Annarita Iodice¹³, Business Analyst at MATICMIND
- ◆ Andrea Praitano¹⁴, Privacy and cybersecurity Team Advisory Lead at MATICMIND



Website: www.energy-shield.eu

Grant agreement number: 832907

Duration: 1 July 2019 – 30 June 2022

Contributor: Anna Georgiadou¹⁵, Research Associate at the National Technical University of Athens



Website: www.sdmicrosense.eu

Grant agreement number: 833955

Duration: 1 May 2019 – 30 April 2022

Contributor: Panagiotis Sarigiannidis¹⁶, Head of the Distributed Computing Systems Lab at FORTH-ICS



Website: www.sgrid.eu

Grant agreement number: 777996

Duration: 1 January 2018 – 31 December 2021

Contributor: Prof. Christos Xenakis¹⁷, Professor at the University of Piraeus and Project Manager at SealedGRID

¹² <https://cyberwatching.eu/jean-baptiste-bernard>

¹³ <https://cyberwatching.eu/annarita-iodice>

¹⁴ <https://cyberwatching.eu/andrea-praitano>

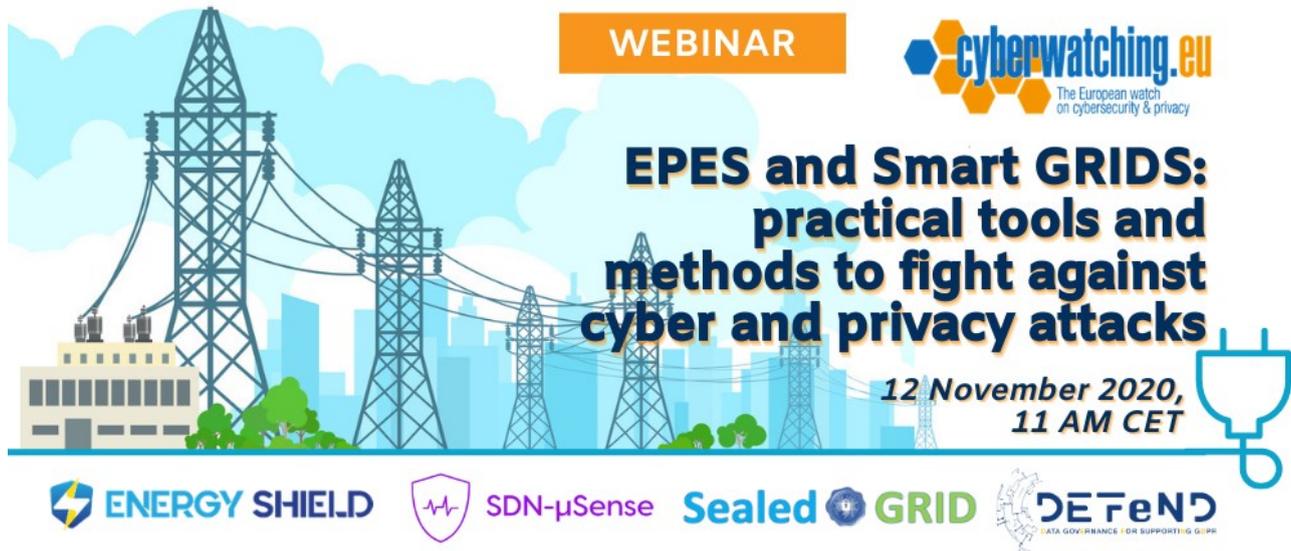
¹⁵ <https://cyberwatching.eu/anna-georgiadou>

¹⁶ <https://cyberwatching.eu/panagiotis-sarigiannidis>

¹⁷ <https://cyberwatching.eu/christos-xenakis>

Watch the recorded workshop video now!

You may also download the speakers' presentations on the [webinar page](#).



WEBINAR

cyberwatching.eu
The European watch
on cybersecurity & privacy

**EPES and Smart GRIDS:
practical tools and
methods to fight against
cyber and privacy attacks**

12 November 2020,
11 AM CET

ENERGY SHIELD **SDN-μSense** **Sealed GRID** **DEFEND**
DATA GOVERNANCE FOR SUPPORTING GRID

How to reach us



 www.cyberwatching.eu

 [@cyberwatchingeu](https://twitter.com/cyberwatchingeu)

 [in/company/cyberwatchingeu](https://www.linkedin.com/company/cyberwatchingeu)

cyberwatching.eu consortium



234567890D48E1563QW

HORIZON 2020



cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.