Secure and resilient electrical power and energy systems: the SDN-microSENSE project

Panagiotis Radoglou-Grammatikis and Panagiotis Sarigiannidis
Department of Electrical and Computer Engineering,
University of Western Macedonia
Thomas Lagkas
Department of Computer Science, International Hellenic University

Abstract

In the era of digital economies, the smart electrical grid has provided numerous benefits, such as two-way communication, pervasive control and self-healing. However, this evolution raises severe cybersecurity and privacy risks that can lead to disastrous effects. False data injection attacks, large-scale denial of service and unauthorised access represent common cyber threats against critical infrastructures. Based on the sensitive nature of the smart electrical grid, SDN-microSENSE provides an overall cybersecurity solution that increases the resilience and reliability of the Electrical and Power Energy Systems (EPES), combining multiple technologies capable of detecting and mitigating various kinds of cyberattacks and cascading effects.

Motivation and challenges

The road ahead for European energy-related systems is a tough one, filled with significant and far-reaching challenges. Electricity plays a vital role in transportation, communications and resource management (water and air), and the impact of the electrical power and energy systems (EPES) on other areas, such as finance, agriculture and automation, is growing. It is evident that the need for electrical energy is increasing. This provides an excellent opportunity to integrate a higher share of renewables and promote a more efficient and decentralised energy system involving advanced digital technologies and systems (e.g. advanced metering infrastructure (AMI) and software-defined networking (SDN)-enabled industrial systems). Nonetheless, this transformation comes with a significant cost: the need for cyber-defence mechanisms and strategies integrated into a resilient, reliable and self-healing architecture.

Due to the digitisation of the energy infrastructure, the risk of cyberattacks has increased dramatically. Despite the economic benefits, this evolution brought several cases where malicious software took control over energy equipment. For instance, in December 2015, a Ukrainian power grid was attacked, and electricity was knocked out for 225,000 people. Other characteristic examples are Black Energy 3, Crashoverride, Stuxnet and Trisis.

Legacy systems, such as supervisory control and data acquisition system/industrial control systems (SCADA/ICS), constitute a weak point of failure since they were designed when cybersecurity was not part of the technical specifications for the system design. In fact, cyberattacks have become increasingly sophisticated, stealthy, targeted and multi-faceted. Consequently, incidents like power outages, brownouts and blackouts are likely to happen, and they may affect the energy domain and other critical infrastructures (CIs). For example, a cyber-attack on an energy production unit may cause damage and failures to a nearby water management system controlling water facilities for a wide area or a town. Strong cyber-defence measures are required along with sophisticated strategies in the EPES domain, where emerging solutions should guarantee cybersecurity and resilience (Radoglou-Grammatikis *et al.*, 2018).

In addition, the energy sector should further be enhanced for supporting self-healing mechanisms in case of emergency. Backup power islanding and restoration concepts constitute promising solutions for modern power grids. For instance, isolating a problematic region from the neighbouring grids by making it an island could strengthen the EPES resiliency and reliability by making it robust against cyberattacks and hardware failures. To this end, the idea of energy management and trading among various energy actors seems quite attractive, especially when it happens online. Thus, new security measures are needed, not only from the information technology (IT) point of view but by combining the arsenals from both domains: IT and electrical engineering. EPES will surely be promoted to a more energy-efficient system by exploiting innovative solutions and technologies from both fields.

SDN-microSENSE objectives

SDN-microSENSE (microgrid reSilient Electrical eNergy SystEm) is an Innovation Action (IA) project co-funded by the Horizon 2020 framework programme of the European Union, with the goal to introduce an integrated architecture capable of: *(a)* implementing collaborative risk assessment comprising all energy stakeholders; *(b)* optimising EPES systems with self-healing mechanisms, utilising islanding and fast restoration procedures; *(c)* allowing efficient energy data exchange between energy organisations; *(d)* constructing a security information and event management (SIEM) (Radoglou-Grammatikis *et al.*, 2021) system for detecting intrusions and anomalies against energy systems; *(e)* realising a privacy-preserving framework with respect to AMI; and *(f)* contributing to standardisation and certification actions for promoting sustainable and compatible EPES cybersecurity approaches. Therefore, SDN-microSENSE focuses on the following primary objectives.

Objective #1:

Design and provide a new resilient, multi-layered and SDN-enabled microgrid architecture, which will leverage the global system visibility for preventing and addressing disruptions to the underlying SCADA and ICS infrastructure.

Unlike the traditional communication paradigm, SDN decouples the network control from the forwarding functions in network devices, offloading the decision functions to logically centralised SDN controller(s). In this way, an additional SDN control layer is added in the new EPES architecture, which provides high-level abstraction and application programming interfaces (APIs) for interacting with, thereby managing, monitoring and programming the communication network consisting of SCADA/ICS systems, sensors, actuators and networking devices. Furthermore, the new SDN layer allows the development of innovative EPES security and safety services to dynamically configure and adjust the EPES network, including smart and legacy devices.

Objective #2:

Design and develop a risk assessment and management framework, where a holistic methodology will be followed involving asset risk management considering all the existing SCADA/ICS components and devices using an additional layer of threat management.

A crucial need is to identify the attack surface of the energy value chain by performing a risk and vulnerability assessment, identifying vulnerabilities attributed to ICT and industrial assets, processes and people. The proposed risk assessment includes: (a) asset identification and prioritisation; (b) threat and vulnerability identification; (c) determining the likelihood that a vulnerability might be exploited; (d) impact analysis; and (e) risk prioritisation followed by recommended controls that will mitigate (minimise or eliminate) risk. Special care will be given to all critical EPES assets such as control and measurement units, generators, smart meters, IoT devices and gateways.

Objective #3:

Develop and implement applications that exploit direct networking controllability and programmability offered by SDN to investigate multiple security applications, including self-healing attack-resilient PMU and RTU, for going toward achieving resilient and secure operations in the face of various cyber threats and failures.

One of the main characteristics of the smart grid paradigm is the self-healing capability against various abnormal situations, such as a disturbance or a cyber-attack. The term self-healing is closely related to the ability of the smart grid to be split into multiple islands that can operate independently and collaborate with each other. According to IEEE standard 1547.4, the division of the main utility grid into multiple islands can optimise the functionality of the whole ecosystem. Therefore, SDN -microSENSE will provide a self-healing framework, which takes full advantage of SDN mitigation capabilities, islanding mechanisms, fast restoration processes and blockchain-based energy trading systems.

Objective #4:

Deliver an energy trading platform for secure and flexible trading management.

Peer-to-peer (P2P) energy trading platforms are currently being implemented to facilitate transactional activities between disparate electricity sector actors with a special focus on small producers, prosumers, and microgrids. Although several efforts consider the energy demand and response, the current solutions do not consider state awareness and cybersecurity threats. Thus, SDN-microSENSE implements a blockchain-based trading environment that can respond to real-time outages caused by network conditions or cyberthreats. It will be able to adapt trading agreements supporting network flexibility, stability, and energy balancing valorisation.

Objective #5:

Provide a robust, distributed and effective IT cyber defence system for a large-scale EPES ecosystem.

SDN-microSENSE will provide a cyber defence framework consisting of four layers to detect and mitigate potential intrusions and anomalies in near real-time. First, both signature-based and specification-based intrusion detection and prevention systems (IDPS) are adopted to detect known cyberattacks. They take full advantage of SDN to mitigate the presence of an intrusion. Next, machine learning (ML) and deep learning (DL) detection mechanisms are activated, thus recognising cyber threats against industrial communication protocols, such as Modbus, IEC 61850, IEC 60870-5-104 and IEEE C37.118. Moreover, visual analytics are utilised to detect unknown anomalies. The aforementioned detectors are organised through a large-scale SIEM system, which aggregates, normalises and correlates the various security events.

Objective #6:

Design and deploy an anonymous channel of EPES that will allow secure and privacy-preserving information sharing among energy operators and actors.

SDN-microSENSE implements a cloud-based anonymous repository of incidents across multiple energy stakeholders, including critical information related to cybercrimes, cyber-attack incidents and important software updates and patches critical for addressing ongoing exploits. This repository is implemented in line with similar initiatives, such as the European Energy - Information Sharing & Analysis Centre (EE-ISAC), while it will further develop the idea of using a network of trust. In particular, it combines malware information sharing platform (MISP) with anonymisation techniques, such as k-anonymity, t-closeness and i-diversity. Hence, energy operators across Europe will be able to broadcast sensitive cybersecurity incident information anonymously without risking their organisation's reputation.

Objective #7:

Deliver a privacy-preserving framework for enhancing EPES against data breaches.

Data gathered by smart meters may include sensitive information, such as energy consumption information, user patterns and type of appliances. Thus, the privacy of AMI is a challenging aspect requiring an effective and well-suited solution. SDN-microSENSE introduces a privacy protection framework where both k-anonymity and homomorphic encryption are combined to preserve data breaches. In particular, the privacy protection framework is applied at the consumer's or prosumer's side in line with IEC 62351-7. The transmitted electricity consumption data remain private and cannot be 0overheard. As a result, the AMI ecosystem becomes private, especially at the consumer and prosumer premises, where privacy attacks are likely to happen.

Objective #8:

Design and develop and a policy recommendation framework based on the SDN-microSENSE results, lessons learnt and best practices for formulating recommendations for standardisation and certification.

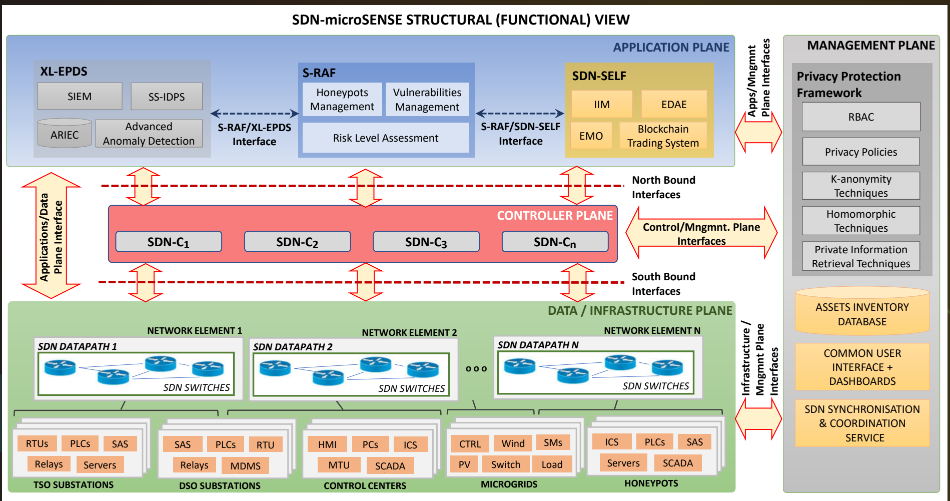

Figure 1: SDN-microSENSE architecture.

SDN-microSENSE will formulate recommendations for certification by meeting all requirements stipulated in the General Data Protection Regulation (GDPR). The recommendations will rely on the project results and lessons learnt. In addition, an in-depth analysis over existing global/European certification schemes around energy chains, e.g. ISA99/IEC 62443, CSSA and GICSP and specifically the European Network and Information Security (NIS) driving licence, will be conducted since they could be used as a solid ground for the proposed SDN-microSENSE recommendations. In addition, SDN-microSENSE will try to fill in several technical gaps by adopting new SCADA/ICS standardisation activities. These standards will aim at covering several areas like incident response and business continuity.

SDN-microSENSE architecture

As illustrated in Figure 1, SDN-microSENSE composes an integrated platform consisting of three main frameworks: *(a)* SDN-microSENSE risk assessment framework (S-RAF); *(b)* cross-layer energy prevention and detection system (XL-EPDS); and *(c)* SDN-enabled self-healing Framework, (SDN-SELF). S-RAF is devoted to the collaborative risk assessment processes mentioned earlier. Furthermore, it includes EPES honeypots and honeypot manager to mitigate possible risks. In particular, through the SDN-controller, the honeypot manager redirects the malicious network traffic detected by XL-EPDS to EPES honeypots. XL-EPDS includes the various detectors orchestrated by a SIEM system. Signature/specification-based IDPS communicates with the SDN controller to receive network-related operational data to detect potential anomalies. Finally, SDN-SELF is responsible for the mitigation and energy management mechanisms, including and automating islanding processes, energy restoration and energy-data trading. Finally, SDN-SELF includes the electric data analysis engine (EDAE), which receives multiple kinds of data, such as security events and operational measurements about the status of the electrical grid, and undertakes to appropriately guide the SDN controller to mitigate potential cyberattacks or anomalies.

References

Radoglou-Grammatikis, P., Sarigiannidis, P., Liatifis, T., Apostolakos, T. and Oikonomou, S. (2018) 'An overview of the firewall systems in the smart grid paradigm', *2018 Global Information Infrastructure and Networking Symposium (GIIS).* Thessaloniki, Greece, October 2018, pp. 1–4.

Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, I., Sesis, N., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulias, A., Angelopoulos, M. and Ramos, F. (2021) 'SPEAR SIEM: A Security Information and Event Management system for the Smart Grid', *Computer Networks*, p. 108008. doi: 10.1016/j.comnet.2021.108008.

PROJECT NAME

SDN-microSENSE

PROJECT SUMMARY

The smart energy ecosystem constitutes the next technological leap of the conventional electrical grid. However, although it brings beneficial changes, it also generates significant cybersecurity challenges due to the various heterogeneous technologies. Thus, the SDN-microSENSE project intends to provide a set of cyberattacks mechanisms, thus ensuring the normal operation of the Electrical Power and Energy Systems (EPES).

PROJECT LEAD

SDN-microSENSE offers an integrated security platform devoted to electrical power and energy systems (EPES). In particular, SDN-microSENSE focuses on: *(a)* collaborative risk assessment; *(b)* intrusion detection and prevention; *(c)* self-healing mechanisms; *(d)* smart energy management; and *(e)* energy trading. The various SDN-microSENSE components take full advantage of the software-defined networking (SDN) technology, thus mitigating the potential anomalies and cyberattacks.

PROJECT PARTNERS

AYESA ADVANCED TECHNOLOGIES SA; University of Western Macedonia; Centre for Research and Technology Hellas (CERTH); Preduzeće za telekomunikacijske usluge Realaiz d.o.o. Beograd; Atos IT Solutions And Services Iberia, SL; Schneider Electric Industries SAS; Public Power Corporation SA; Fundación TECNALIA Research and Innovation; Municipality of Avdera; Innovative Energy and Information Technologies LTD; Elektroenergien Sistemen Operator EAD; CEZ Distribution Bulgaria AD; UbiTech Ltd; CYBERLENS Ltd; SIDROCO Holdings Ltd; 0 infinity Limited; Eight Bells Ltd; inCITES CONSULTING SA; Energynautics GMBH; Norwegian University of Science and Technology (NTNU); SIAXAMPANIS E.E.; Gottfried Wilhelm Leibniz Universität Hannover; Ravna Hydro Ltd; Fundacio Institut de Recerca de l'Energia de Catalunya; Estabanell y Pahisa Energía SA; Checkwatt AB; Independent Power Transmission Operator SA; SINTEF Energi AS; Dil Diel; Optimización orientada a la sostenibilidad; GEIE ERCIM.

CONTACT DETAILS

Panagiotis Sarigiannidis

psarigiannidis@uowm.gr

www.sdnmicrosense.eu

www.linkedin.com/groups/12248810

FUNDING

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833955.