Project Info:

- GA number: 833955
- Call topic: H2020-SU-DS-2018
- Start date: 01/05/2019
- Duration: 36 months

Project Coordinator: Alfredo Gonzalez Naranjo (AYESA)

Dissemination Leader: Dr. Theodoros Rokkas (inCITES Consulting)

Use Cases:

Investigation of Versatile Cyberattack Scenarios and Methodologies Against EPES
Location: Trondheim, Norway

Massive False Data Injection Cyberattack Against State Operation and Automatic Generation Control
Location: Sofia, Bulgaria

Large-scale Islanding Scenario Using Real-life Infrastructure
Location: Lavrio, Attica, Greece

EPES Cyber-defence against Coordinated Attacks
Location: Spain

Distribution Grid Restoration in Real-world PV Microgrids
Location: Avdera, Xanthi, Greece

Realising Private and Efficient Energy Trading among PV Prosumers
Location: Sweden

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

Contact:

www.sdnmicrosense.eu

SDNmicroSENSE

info@sdnmicrosense.eu

Consortium:

SDN-µSense

SDN - microgrid reSilient Electrical eNergy SystEm

Our Vision

SDN-microSENSE aims at providing and demonstrating a secure, resilient to cyber-attacks, privacy-enabled, and protected against data breaches solution for decentralised Electrical Power and Energy Systems (EPES). All designed, developed, and tested technologies should consider the latest related research findings and maintain high compliance with current industrial standards (e.g., IEC standards)

OBJECTIVES

- To 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
- To design and develop a risk assessment and management framework
- To develop and implement applications which 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 cyberthreats and failures
- Deliver an energy trading platform for secure and flexible trading management
- To provide a robust, distributed and effective IT cyber-defence system for large-scale EPES ecosystem
- To design and deploy an anonymous channel of EPES which will allow secure and privacy-preserving information sharing among energy operators and actors
- To deliver a privacy-preserving framework for enhancing EPES against data breaches
- To 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.
- To design and demonstrate five large-scale pilots across Europe