SDN-µSense

SDN - microgrid reSilient Electrical eNergy SystEm

Introduction to SDN-microSENSE

CERTH

Dr. Dimosthenis Ioannidis

djoannid@iti.gr

June 2019, Thessaloniki, Greece

Project Summary

SDN-µSense

SDN-microSENSE: SDN - microgrid reSilient Electrical eNergy SystEm

- **Call**: H2020-SU-DS-2018
- **Topic**: SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
- **Project Grant Agreement**: NUMBER 833955
- **Budget**: EUR 7992462.50
- **Project Start Date**: 01/05/2019 (M01)
- **Project End Date**: 30/04/2022 (M36)

Project Consortium (1/4)

SDN-µSense

No	Name	Acronym	Country	Organization Type
1	Ayesa Advanced Technologies – AYESA	AYE	Spain	Industry
2	University of Western Macedonia	UOWM	Greece	University
3	Centre for Research and Technology Hellas	CERTH	Greece	Research
4	REALAIZ DOO	REAL	Serbia	SME
5	Atos Spain S.A.	ATOS	Spain	Large Industry
6	Schneider Electric France SAS	SEF	France	Large Industry
7	Public Power Corporation / Testing Research & Standards Center	TRSC/PPC S.A	Greece	Large Industry
8	Fundación Tecnalia Research & Innovation	TECN	Spain	Research
9	Municipality of Avdera	MOA	Greece	Municipality
10	Innovative Energy and Information Technologies LTD	IEIT	Bulgaria	SME
11	Bulgarian Electricity System Operator EAD	ESO	Bulgaria	TSO
12	CEZ Distribution Bulgaria AD	CEZ BG	Bulgaria	DSO
13	UBITECH LIMITED	UBITECH	Cyprus	SME
14	CyberLens Ltd	CLS	UK	SME

Project Consortium (2/4)

SDN-µSense

No	Name	Acronym	Country	Organization Type
15	Sidroco Holdings Limited	SID	Cyprus	SME
16	0 INFINITY Limited	0INF	UK	SME
17	Eight Bells Ltd	8BELLS	Cyprus	SME
18	INCITES Consulting SARL	INC	Luxemburg	SME
19	ENERGYNAUTICS	ENERGYNAUTICS	Germany	SME
20	Norges Teknisk-Naturvitenskapelige Universitet	NTNU	Norway	University
21	SIAXAMPANIS E.E.	ALKYONIS	Greece	SME
22	Gottfried Wilhelm Leibniz Universität Hannover	LUH	Germany	University
23	Ravna Hydro Ltd. – Ravna Hydro, Bulgaria	VETS	Bulgaria	SME
24	Fundació Institut de Recerca en Energía de Catalunya	IREC	Spain	Research
25	Estabanell Energia	EPESA	Spain	DSO
26	Checkwatt AB	CW	Sweden	SME
27	INDEPENDENT POWER TRANSMISSION OPERATOR	IPTO	Greece	TSO
28	SINTEF Energi AS	SINTEF	Norway	Research

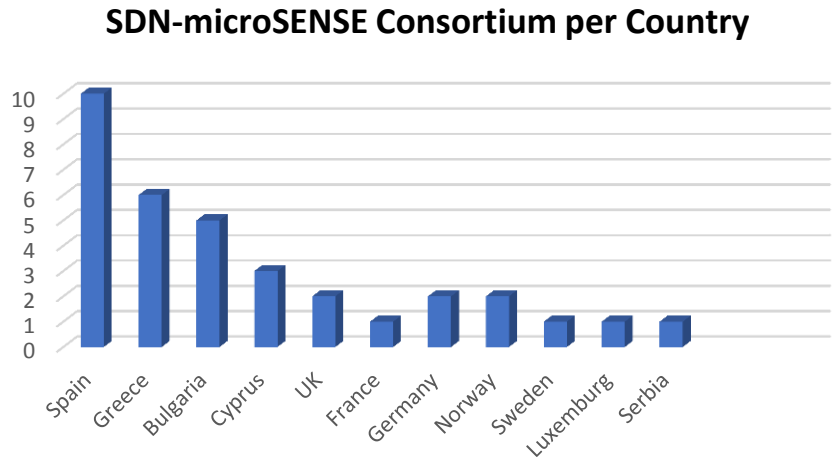
Project Consortium (3/4)

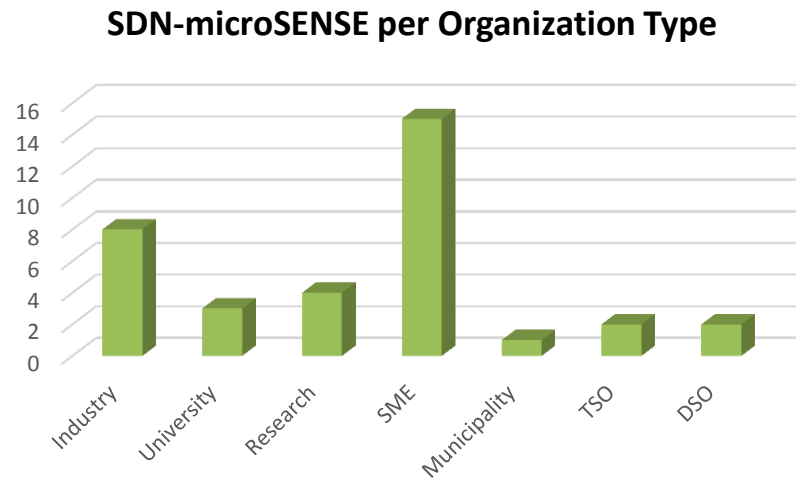
SDN-µSense

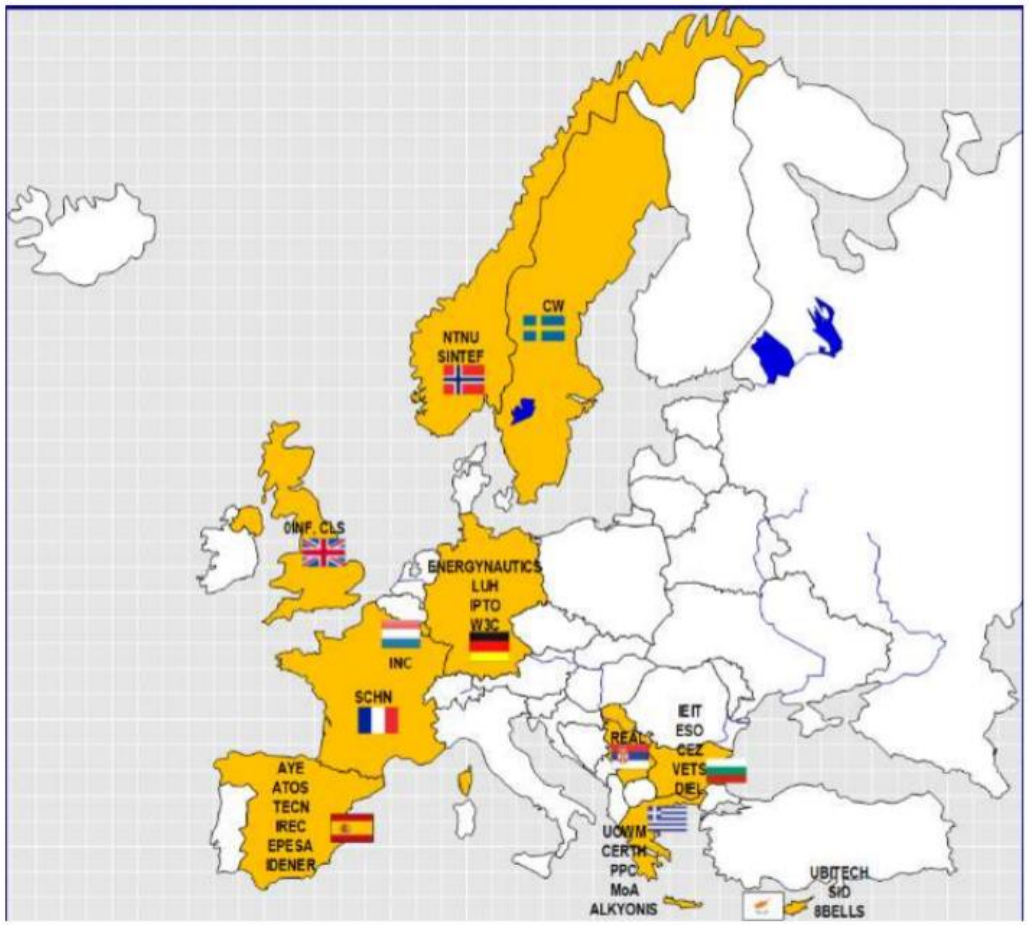
No	Name	Acronym	Country	Organization Type
29	D I L DIEL LTD	DIEL	Bulgaria	End User
30	IDENER	IDENER	Spain	SME
31	GEIE ERCIM	W3C	France	SME
		Third Parties		
32	Fundación Ayesa (third party of AYE)	FA	Spain	Industry
33	ACT Sistemas (third party of AYE)	ACT	Spain	Industry
34	Schneider Electric España SA (third party of SEF)	SCHN ES	Spain	Large Industry
35	Atos IT Solutions and Services S.L (third party of ATOS)	ATOS IT	Spain	Large Industry

Project Consortium (4/4)

SDN-µSense







Project Motivation

SDN-µSense

According to the European Network and Information Security Agency (ENISA):

"A cyber security incident to power grids could be defined as any adverse event that can impact the confidentiality, integrity or availability of the Information and Communication Technology systems supporting the different processes of the organisations involved in the well-functioning of the power system, including all its domains (e.g., markets, operation of the distribution or transmission grid, customers, etc.)".

- Increase the **EPES resilience** in addressing cyber threats and attacks
- **Protect SCADA, ICS** and all the interconnected systems from power outages, brownouts and blackouts
- Apply **collaborative risk assessment** and management in a large-scale level
- Enhance the effectiveness of the EPES domain **against versatile and sophisticated cyberattacks**
- **Advance the current SCADA and ICS infrastructure** in guaranteeing the level of cybersecurity and resilience in modern smart grid and energy networks and systems
- Develop innovative solutions for enhancing the EPES resilience in the power level such as **self-healing and islanding**
- Setting up **common security principles and requirements** in the physical level of the energy domain
- **Demonstrate the provided solutions in large-scale environments** by involving all energy-related stakeholders
- **Foresee standardisation activities** in all layers of the EPES ecosystem based on best practices and lessons learnt

EPES: Electrical Power and Energy System

SCADA: Supervisory Control and Data Acquisition System

ICS: Industrial Control Systems

Project Concept and Objectives (1/2)

SDN-µSense

- OBJ #1: 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.
- OBJ #2: To 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**.
- OBJ #3: 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.
- OBJ #4: Deliver an **energy trading platform** for secure and flexible trading management.
- OBJ #5: To provide a **robust, distributed and effective IT cyber-defence system** for large-scale EPES ecosystem.

PMU: Phasor Measurement Unit

RTU: Remote Terminal Unit

Project Concept and Objectives (2/2)

SDN-µSense

- OBJ #6: To design and deploy an **anonymous channel of EPES** which will allow secure and privacy-preserving information sharing among energy operators and actors.
- OBJ #7: To deliver a **privacy-preserving framework** for enhancing EPES against **data breaches**.
- OBJ #8: To design and develop a **policy recommendation framework** based on the SDN-microSENSE results, **lessons learnt and best practices** for formulating recommendations for standardisation and certification.
- OBJ #9: To design and **demonstrate six large-scale pilots** across Europe, including well-developed and developing countries in the energy efficient systems, where TSO, DSO, electricity generators, energy utilities, energy equipment manufacturers, aggregators, energy retailers and technology providers will be involved.
- OBJ #10: To design an innovative a **business model** and conduct a **cost-benefit techno-economic analysis** to strengthen the role of European energy and cyber-security industry in the global market.

SDN-Technology

SDN-µSense

- SDN is a **modern approach** to networking that **eliminates the complex** and static nature of legacy distributed network architectures through the use of a standards-based s**oftware abstraction between the network control plane** and underlying data forwarding plane, including both physical and virtual devices.
- The **OpenFlow protocol** is the only standards-based SDN protocol in the world that enables a central controller to **remotely provision the underlying data plane** device forwarding tables in a common, scalable way, and eliminates the vendor-specific, proprietary nature of legacy networking equipment.
- **Network virtualization** is an SDN technology application that creates unmatched network agility and dramatically **reduces costs of network** operations by automating network provisioning for both increasingly dynamic virtual workloads as well bare metal workloads.
- Network virtualization **leverages the OpenFlow protocol** to dynamically and automatically provision virtual network segments and virtual routing services on both physical and virtual networking devices.

SDN-microSENSE Use Cases

SDN-µSense

- Use Case 1: Investigation of Versatile Cyberattack Scenarios and Methodologies Against EPES, Trondheim, Norway
- Use Case 2: Massive False Data Injection Cyberattack Against State Operation and Automatic Generation Control, Sofia, Bulgaria
- Use Case 3: Large-scale Islanding Scenario Using Real-life Infrastructure, Lavrio, Attica, Greece
- Use Case 4: EPES Cyber-defence against Coordinated Attacks, Spain
- Use Case 5: Distribution Grid Restoration in Real-world PM Microgrids, municipality of Avdera, Xanthi, Greece
- Use Case 6: Realising Private and Efficient Energy Trading among PV Prosumers, Sweden

Use Case 1: Trondheim, Norway

Use Case 2: Sofia, Bulgaria

Use Case 3: Lavrio, Greece

Use Case 4: Spain

Use Case 5: Avdera, Greece

Use Case 6: Sweden

Thank You!

Questions?