SPEAR

Secure and PrivaTE smArt gRid

(Grant Agreement No 787011)

D8.4 – Interim Impact Creation Report

2020-05-31

Version 1.0

Published by the SPEAR Consortium
Dissemination Level: Public

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No 787011

Document Control Page

Document Details

Document Version	1.0
Document Owner	INC
Contributors	INC, 0INF, PPC, ED, TEC, UOWM, 8BELLS, LUH, PIMEE, TUS, VETS, CERTH, SCHN, ENI
Work Package	WP 8 - Dissemination and Exploitation
Deliverable Type	[R]
Task	Task 8.1 - Dissemination and Communication
Document Status	Final
Dissemination Level	Public

Document History

Version	Author(s)	Date	Summary of changes
0.1	Theodoros Rokkas, Vangelis Logothetis, (INC)	2020-02-17	Initial ToC
0.1c	Vasilis Argyriou, George Eftathopoulos (0INF)	2020-04-09	Update papers, events and future publications.
0.2	Aglaia Karagianni, Papadopoulos Anastasios, Papadimitriou Nikolaos, Papadopoulos Anastasios, Angelopoulos Michail, (PPC)	2020-04-15	Initial contribution to Section 3
0.3	Alkiviadis Giannakoulias (ED) Theodoros Rokkas, Vangelis Logothetis (INC)	2020-04-20	Contribution to sections 6, 7
0.4	Panagiotis Sarigiannidis, Panagiotis Radoglou Grammatikis,Dimitris Pliatsios, Stamatia Bibi, Pantelis Angelidis (UOWM)	2020-04-21	Contribution to section 4.1, 4.3, and 6
0.5	Vasilis Machamint (8BELLS)	2020-04-23	Contribution to section 6
0.6	Iheanyi Nwankwo (LUH)	2020-04-27	Contribution to sections 3, 6
0.7	Theodoros Rokkas, Vangelis Logothetts, (INC), Igor Kotciuba PIMEE, Valeri Mladenov (TUS), Anton Hristov (VETS)	2020-04-28	Contribution to sections 4, 5, 6
0.8	Dimos Ioannidis (CERTH)	2020-04-29	Contribution to sections 4,6

0.9	Theodoros Rokkas, Vangelis Logothetis (INC)	2020-05-06	Addressing comments from reviewers
1.0	Theodoros Rokkas, Vangelis Logothetis (INC)	2020-05-29	Final Version for submission

Internal Review History

Reviewed By	Date	Summary of Comments
Alfonso Rodriguez (SCHN)	2020-04-30	
Iheanyi Nwankwo (LUH)	2020-05-06	This deliverable clearly indicates various activities that have been carried out to disseminate the project within the second year. Minor proofreading/editing may be needed to finalise the draft.

Legal Notice

The information in this document is subject to change without notice.

The Members of the SPEAR Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

The Members of the SPEAR Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Possible inaccuracies of information are under the responsibility of the project. This report reflects only the author's view and that the Agency and the Commission are not responsible for any use that may be made of the information it contains.

Table of Contents

Table of Figures

Table of tables

Acronyms

Acronym	Explanation
AICC	Anonymous Incident Communication Channel
AMI	Advanced Metering Infrastructure
CIs	Critical Infrastructures
COVID-19	COronaVIrus Disease 2019
CPN	Coloured Petri Net
DIH	Digital Innovation Hub
DoS	Denial of Service
EC	European Commission
EE-ISAC	European Energy – Information Sharing & Analysis Centre
ESG	Electric Smart Grid
EUW19	European Utility Week 2019
GA	Google Analytics
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDS	Industrial Control Systems
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicators
PLC	Programmable Logic Controller
R&D	Research and Development
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SecSoft	Software-defined and Virtualized Infrastructures
SEO	Search Engine Optimisation
SG	Smart Grid
SME	Small and Medium-sized Enterprises
SPEAR	Secure and PrivatE smArt gRid
TV	Trust Value
URL	Uniform Resource Locator
V-IDS	SPEAR Visual-aided Intrusion Detection System

1. Executive Summary

This document presents the dissemination and communication activities that took place during the second year of the SPEAR project. These activities rely on the dissemination and communication strategy that was presented in D8.2.

In this second-year, fourteen publications have come out from SPEAR (twelve in conference and workshops and two in Journals). Two new versions of the newsletter have been published in the project's website along with three blog posts aimed at the general public. SPEAR was present in seven events and two workshops during the second year.

Most of the KPIs during the first year are on track with the original plan and plans were made to achieve those that are not in track.

2. Introduction

All SPEAR partners are engaged in the dissemination and communications activities according to the ignition plan that was included in D8.2. According to that, partners will interact with other projects to organize special events, workshops. Academic and industrial partners will be mainly responsible for publishing papers in journals and conferences.

This deliverable presents all the activities performed during the second year of the project along with the plan for the third year. It also records the KPIs achieved in order to evaluate the strategy and propose changes where is needed.

The document is structured as followed: chapter 3 presents the communication tools that were used along with their impact. Chapter 4 continues with the dissemination and communication activities during the first year, while chapter 5 presents the KPIs. Finally, the plan for dissemination and communication activities for the last year of the project is presented.

3. Communication tools

SPEAR employs numerous communication channels that assist the consortium in disseminating the project's outputs and maintaining interactive communication with the industry, academia, and stakeholders. Those channels are namely, the SPEAR's official website, a LinkedIn page, a YouTube channel, and leaflets that are posted on the website and the LinkedIn page.

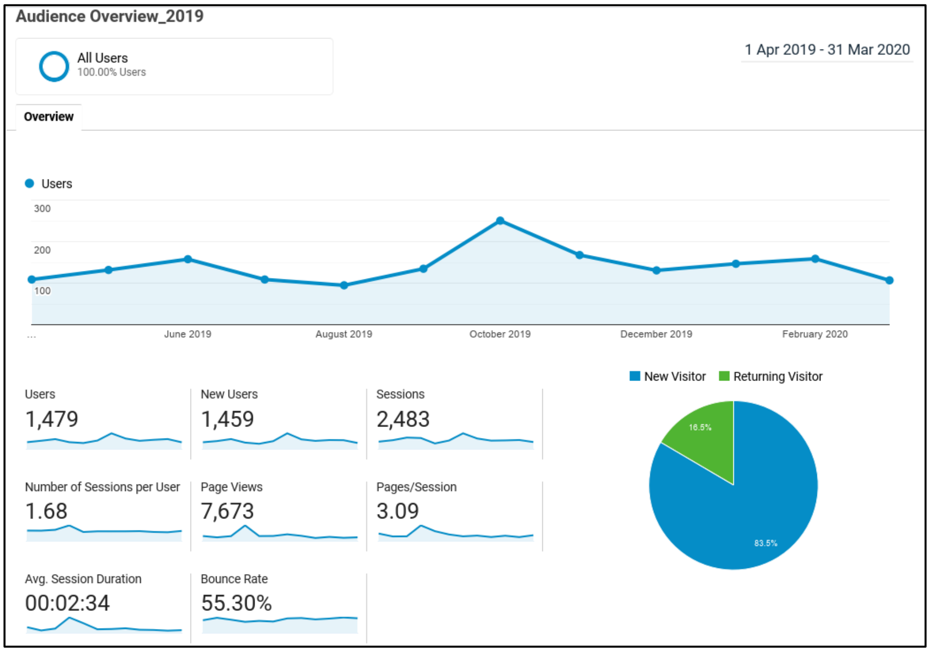
This section is devoted to analysing the status and utilisation of the SPEAR communication tools as well as their impact during the second year of the project, from 31 March 2019 to 31 March 2020.

3.1 SPEAR website impact

The website is the central dissemination tool of the SPEAR consortium and is developed to inform stakeholders and the general audience about the project's objectives, outcomes, and progress.

Following the comments of the first project's review, the SPEAR website has been redesigned and enriched with new content. In particular, the home page has been enriched with a carousel and more information about the SPEAR project and the pilots. Moreover, a new page named "Use Cases" has been introduced that showcases the SPEAR pilots and includes an interactive map that plots their locations in Europe. A similar map has also been added in the "Consortium" section. A gallery page has also been added that includes all images and photos of dissemination activities. Finally, a subscription option to the newsletter has also been added in the "Contact and Mailing List" page.

Regarding the impact of the SPEAR website during the second year, the Google Analytics (GA) service has been utilised to gain statistics and insights about the visitors. In more detail, Figure 1, a screenshot from the "Audience Overview" section of GA, provides an overview of visitor's activity on the website. During 2019, approximately 1,459 new unique visitors have visited our website, an 214% increase compared to the first year of the project. By examining the audience overview graph, we notice peaks in periods close to important dissemination events, for example, European Utility Week 2019 (EUW19) and the S^2 Hack4Energy hackathon. Lows are observed, as expected, during summer holidays and especially in August.



Audience Overview_2019

All Users
100.00% Users

1 Apr 2019 - 31 Mar 2020

Overview

Users
1,479

New Users
1,459

Sessions
2,483

Number of Sessions per User
1.68

Page Views
7,673

Pages/Session
3.09

Avg. Session Duration
00:02:34

Bounce Rate
55.30%

Figure 1: Website - Audience Overview

Figure 2 is a screenshot of the “Location” menu of GA and illustrates the visitor’s geolocation distribution. Compared to the first year, visitors originating from more countries around the world have visited the SPEAR website. Regarding countries that attract new visitors, Greece holds the first place with 458 new visitors (31%), while United Kingdom (6.4%), Spain (5.6%), United States (5.5%) and Germany (5%) follow.

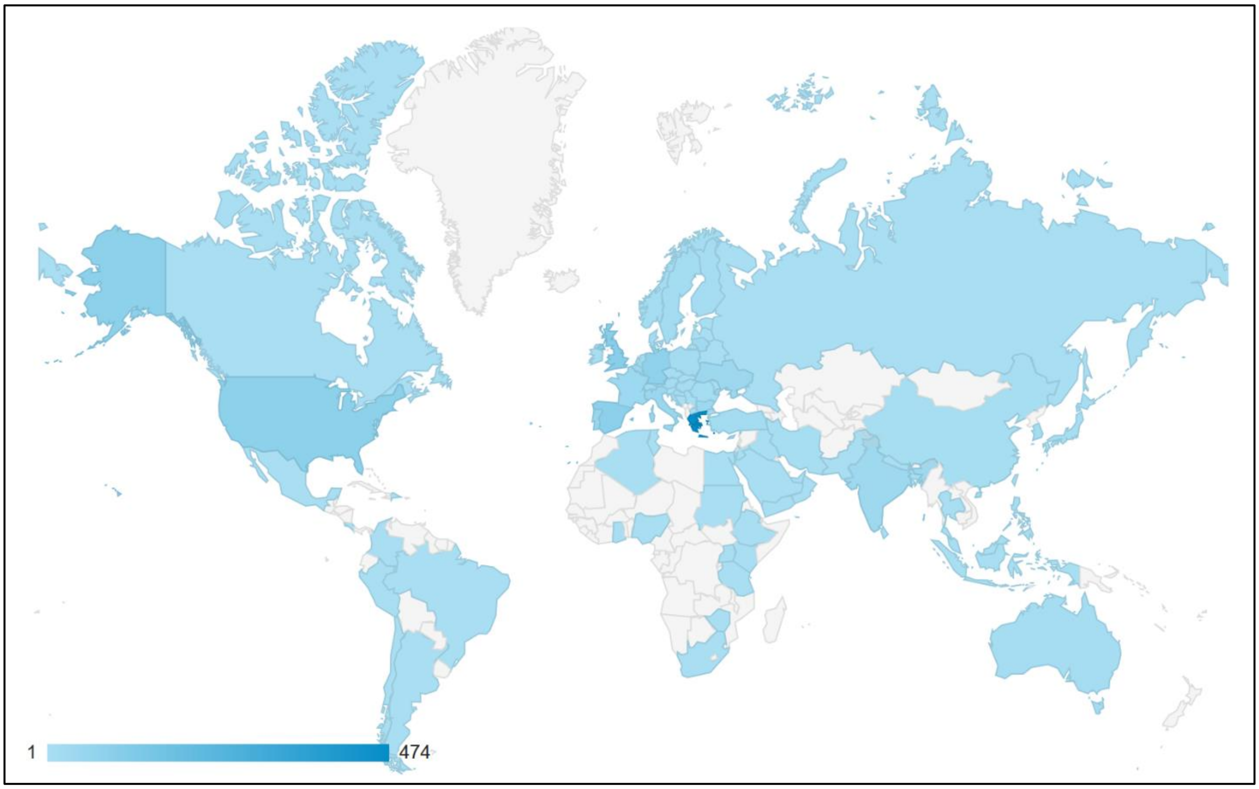
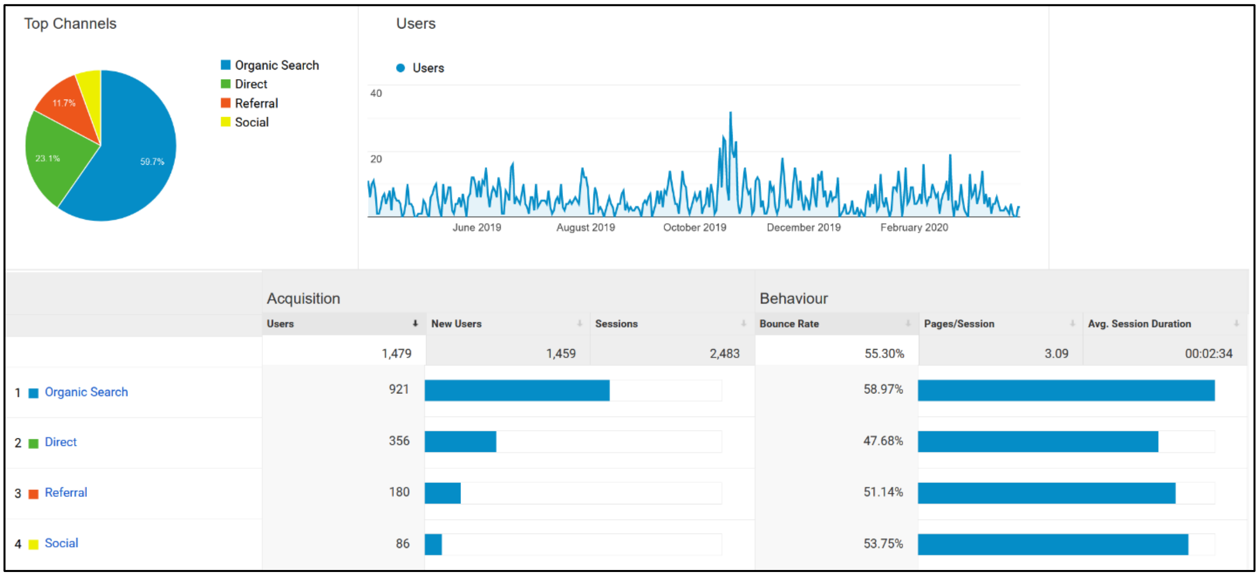


Figure 2: Geolocation overview

Figure 3 is a screenshot from the “Acquisition overview” menu and provides a summary of the channel sources of our visitors. As was the case during the first year, most visitors reached the website through organic search, meaning that they found our website using search engines. The second source of generated traffic comes directly from visitors that type the website URL or click their bookmark (Direct), while the third source of incoming visitors is clicks of the website link from third-party websites and social media (Referral and Social).

The fact that the percentage of acquisition through organic search has increased compared to the first year, indicates the efficiency of the website’s Search Engine Optimisation (SEO) technology that has been deployed.



	Acquisition			Behaviour		
	Users	New Users	Sessions	Bounce Rate	Pages/Session	Avg. Session Duration
	1,479	1,459	2,483	55.30%	3.09	00:02:34
1 🟦 Organic Search	921			58.97%		
2 🟩 Direct	356			47.68%		
3 🟥 Referral	180			51.14%		
4 🟨 Social	86			53.75%		

Figure 3: SPEAR website - Acquisition overview

3.2 Social media impact

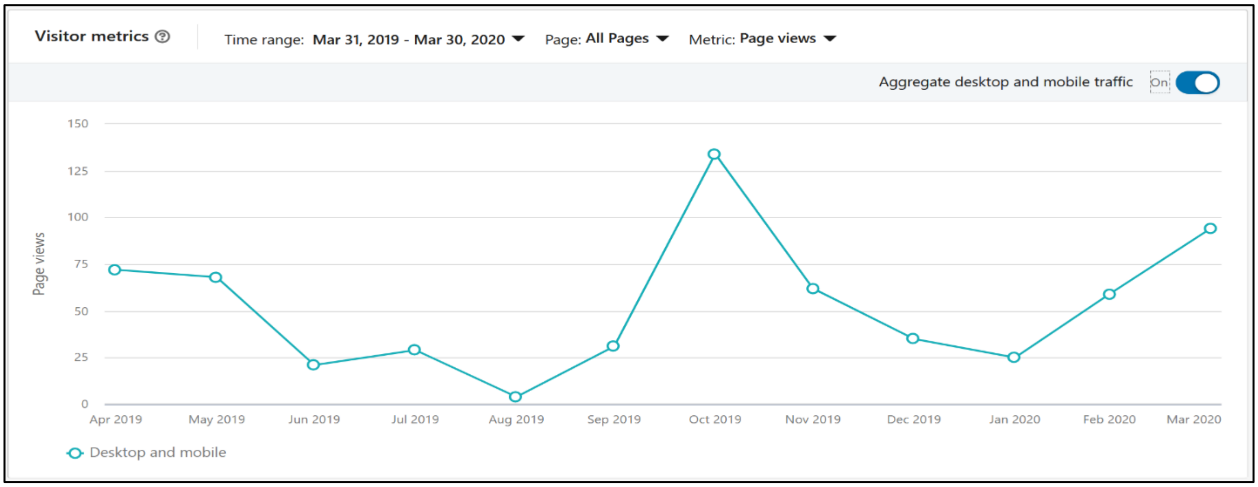
The SPEAR LinkedIn page has 117 followers in total as of 27/04/2020, marking the accomplishment of the relevant KPI of 100 followers. The following figures provide insights on the impact of the LinkedIn page during the last year, focusing on visitors per month, impressions, and new followers.

In more detail, Figure 4 displays the number of visitors per month. On average, more visitors per month are observed, compared to the previous year, and peaks are observed during significant dissemination events, like the European Utility Week 2019, while lows are observed during holidays.

Figure 5 shows the number of interactions that were observed in the SPEAR LinkedIn page. Examples of such interactions are likes, shares, comments, and clicks on posts. The number of impressions has significantly increased, compared to the first year, with over 1000 impressions on average per month, a fact that indicates that the audience is more engaged than before and interacts with the content. On average, each post gains approximately 20 likes.

Finally, Figure 6 presents the number of new followers per month. A significant peak is observed in October 2019, possibly due to the S^2 Hack4Energy hackathon and the EUW19 event that followed in the next month. It is also important that the trend of new followers is maintained until now.

In conclusion, the LinkedIn analytics seems to provide a clearer and more detailed view of the project's impact and the performance of the dissemination activities. This is because the audience is more targeted, and followers are notified about new posts and can interact in more ways with the published content. Moreover, we notice that the increase of the page's impact is consistent with the timeline of two important dissemination events, the S^2 Hack4Energy and EUW19, validating the impact of these activities.

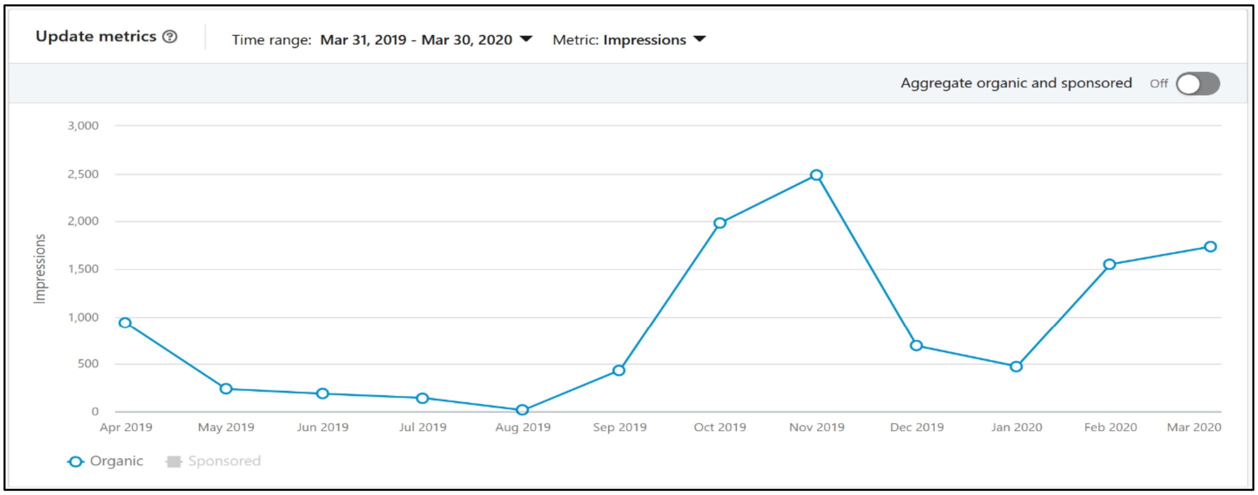


Visitor metrics ⓘ

Time range: Mar 31, 2019 - Mar 30, 2020 ▾ Page: All Pages ▾ Metric: Page views ▾

Aggregate desktop and mobile traffic On

Figure 4: LinkedIn - Visitors overview

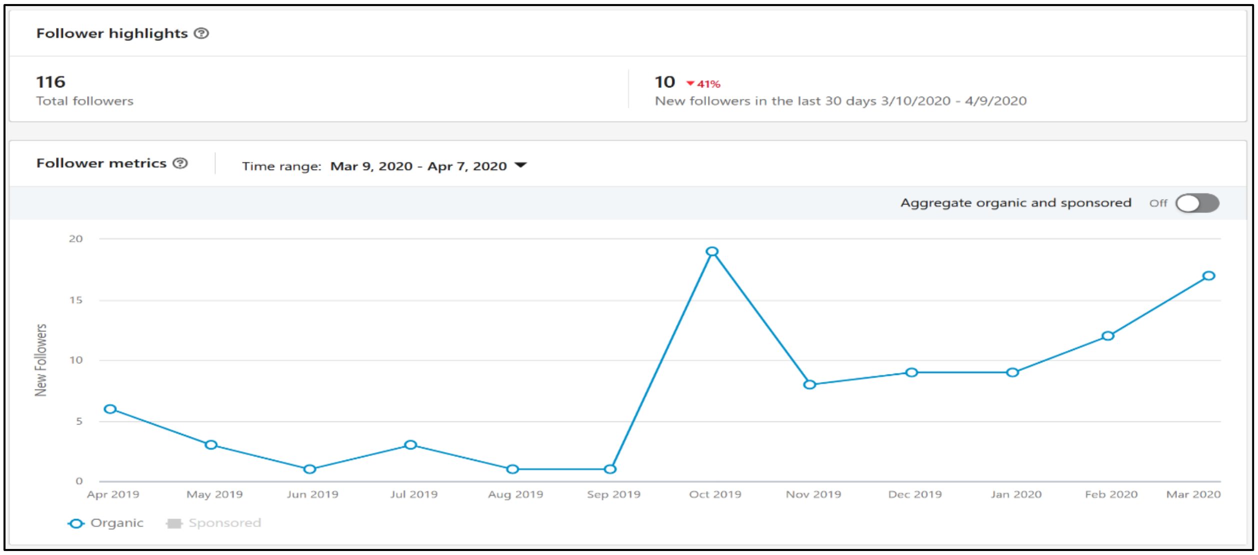


Update metrics ⓘ

Time range: Mar 31, 2019 - Mar 30, 2020 ▾ Metric: Impressions ▾

Aggregate organic and sponsored Off

Figure 5: LinkedIn - Updates overview



Follower highlights ⓘ

116
Total followers

10 ▾41%
New followers in the last 30 days 3/10/2020 - 4/9/2020

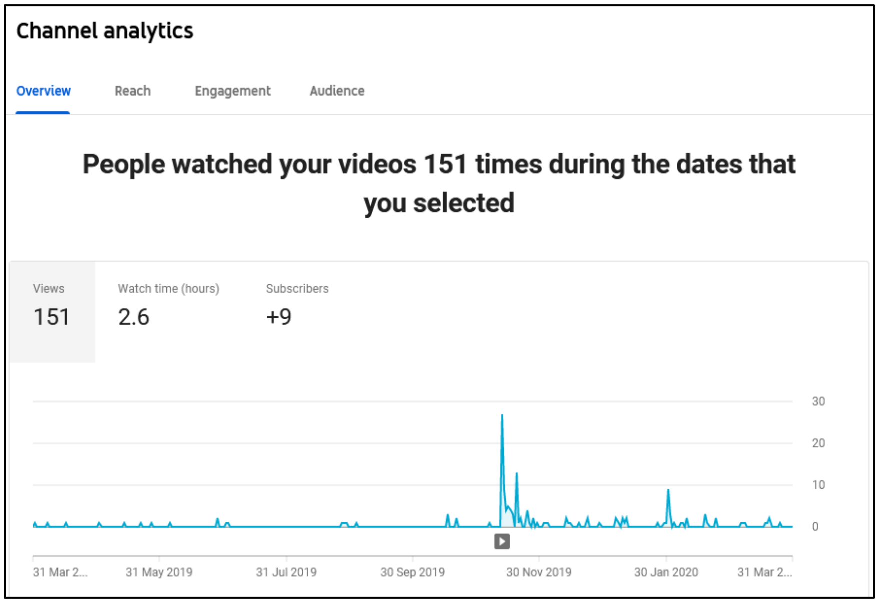
Follower metrics ⓘ

Time range: Mar 9, 2020 - Apr 7, 2020 ▾

Aggregate organic and sponsored Off

Figure 6: LinkedIn - New followers

Finally, the following figure focuses on the impact and the metrics that are obtained by YouTube Analytics for the SPEAR YouTube channel, which counts 16 subscribers so far. During the second year of the project, a new video has been uploaded that introduces the SPEAR concept and the SPEAR Visual-aided Intrusion Detection System (V-IDS). This video was utilised in the EUW19 event. It is anticipated that more effort will be put during the last year of the project, since the production of multimedia content will be mainly based on final and ready for demonstration outcomes.



Channel analytics

Overview Reach Engagement Audience

People watched your videos 151 times during the dates that you selected

Views	Watch time (hours)	Subscribers
151	2.6	+9

Figure 7: YouTube Analytics - Overview

3.3 Other tools

During the second year of SPEAR, two additional light digital leaflets/newsletters have been published that focus on the recent dissemination activities, accomplishments, and outcomes of the project. The new newsletters can be found on the following links:

- https://www.spear2020.eu/cmsMedia/Uploads/News/SPEAR_Newsletter_Sept19.pdf
- https://www.spear2020.eu/cmsMedia/Uploads/News/SPEAR_Newsletter_Dec19.pdf

Finally, three light blog posts have already been published on the website, with the most recent one introducing the SPEAR architecture. Two more blog posts have already been prepared and are scheduled for the upcoming weeks.

LUH published a blog post “Cybersecurity, Data Protection and Operational Efficiency in the Electricity Sector” in Beck-online ZD-Aktuell 2019, 06847 mentioning the work of the SPEAR project.

4. Dissemination and communication activities

4.1 Publications

During the second year of the project, nine articles were accepted for publication. The detailed list is the following:

- C. Dalamagkas, P. Sarigiannidis, D. Ioannidis, E. Iturbe, O. Nikolis, F. Ramos, E. Rios, A. Sarigiannidis and D. Tzovaras, "A Survey on Honeypots, Honeynets And Their Applications on Smart Grid", in 2019 IEEE Conference on Network Softwarization (NetSoft), 2019
- P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, “Attacking IEC-60870-5-104 SCADA Systems,” in 2019 IEEE World Congress on Services (SERVICES), 2019.
- G. Efstathopoulos, P. Radoglou-Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. Angelopoulos, and S. Athanasopoulos, "Operational Data Based Intrusion Detection System for Smart Grid", in 2019 IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks. Best Paper Award
- Igor Kotsiuba, Inna Skarga-Bandurova , Alkiviadis Giannakoulias , Oksana Bulda , “Basic Forensic Procedures for Cyber Crime Investigation in Smart Grid Networks”, 3rd International Workshop on Big Data Analytic for Cybercrime Investigation and Prevention, 2019.
- Igor Kotsiuba, Inna Skarga-Bandurova, Alkiviadis Giannakoulias, Mykhailo Chaikin, Aleksandar Jevremovic, “Technique for Finding and Investigating the Strongest Combinations of Cyberattacks on Smart Grid Infrastructure”, 3rd International Workshop on Big Data Analytic for Cybercrime Investigation and Prevention, 2019
- D. Pliatsios, P. Sarigiannidis, T. Liatifis, K. Rompolos, I. Siniosoglou, "A Novel and Interactive Industrial Control System Honeypot for Critical Smart Grid Infrastructure." 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2019.
- A. Triantafyllou et al., “Towards Anonymous Incident Communication Channel for Electric Smart Grids,” Azerbaijan Journal of High Performance Computing, vol. 2, no. 1, pp. 7–28, Jun. 2019
- N. Vakakis, O. Nikolis, D. Ioannidis, K. Votis, and D. Tzovaras, “Cybersecurity in SMEs: The Smart-Home/Office Use Case,” in 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019.
- D. Pliatsios, P. Sarigiannidis, T. Lagkas and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics,", IEEE Communications Surveys & Tutorials, 2020

Five more articles have been accepted for publication and are expected to be published in the following months:

- D. Pliatsios, P. Sarigiannidis, G. Efstathopoulos, A. Sarigiannidis, A. Tsiakalos, ‘Trust Management in Smart Grid: A Markov Trust Model’, Proceedings of 10th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2020
- I. Siniosoglou, G. Efstathopoulos, D. Pliatsios and P. Sarigianidis, “NeuralPot, An Industrial Honeypot Based on Convolutional Neural Networks”, 25th IEEE Symposium on Computers and Communications (ISCC), 2020
- P. Radoglou-Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios, A. Sarigiannidis, O. Nikolis, D. Ioannidis, V. Machamint, M. Tzifas, A. Giannakoulias, M. Angelopoulos, A. Papadopoulos, F. Ramos, “Secure and Private Smart Grid: The SPEAR Architecture”, 2nd International Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualised Infrastructures, 2020

- P. Radoglou-Grammatikis, I. Siniosoglou, T. Liatifis, A. Korouniadis, K. Rompolos and P. Sarigiannidis, “Implementation and Detection of Modbus Cyberattacks: A Case Study,” 10th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2020
- P. Radoglou-Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos, G. Efstathopoulos, ‘An Anomaly Detection Mechanism for IEC 60870-5-104’, Proceedings of 10th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2020, to appear.

The abstracts of both the published and submitted applications are presented in Table 1.

Table 1: Abstract of submitted publications

Title	Abstract
A Survey on Honeypots, Honeynets And Their Applications on Smart Grid	Power grid is a major part of modern CI. The rapid evolution of Information and Communication Technologies (ICT) enables traditional power grids to encompass advanced technologies that allow them to monitor their state, increase their reliability, save costs and provide ICT services to end customers, thus converting them into smart grids. However, smart grid is exposed to several security threats, as hackers might try to exploit vulnerabilities of the industrial infrastructure and cause disruption to national electricity system with severe consequences to citizens and commerce. This paper investigates and compares honey-x technologies that could be applied to smart grid in order to distract intruders, obtain attack strategies, protect the real infrastructure and form forensic evidence to be used in court.
Attacking IEC-60870-5-104 SCADA Systems	The rapid evolution of the Information and Communications Technology (ICT) services transforms the conventional electrical grid into a new paradigm called Smart Grid (SG). Even though SG brings significant improvements, such as increased reliability and better energy management, it also introduces multiple security challenges. One of the main reasons for this is that SG combines a wide range of heterogeneous technologies, including Internet of Things (IoT) devices as well as Supervisory Control and Data Acquisition (SCADA) systems. The latter are responsible for monitoring and controlling the automatic procedures of energy transmission and distribution. Nevertheless, the presence of these systems introduces multiple vulnerabilities because their protocols do not implement essential security mechanisms such as authentication and access control. In this paper, we focus our attention on the security issues of the IEC 60870-5-104 (IEC-104) protocol, which is widely utilized in the European energy sector. In particular, we provide a SCADA threat model based on a Coloured Petri Net (CPN) and emulate four different types of cyber-attacks against IEC-104. Last, we used AlienVault's risk assessment model to evaluate the risk level that each of these cyber-attacks introduces to our system to confirm our intuition about their severity.
Operational Data Based Intrusion Detection System for Smart Grid	With the rapid progression of Information and Communication Technology (ICT) and especially of Internet of Things (IoT), the conventional electrical grid is transformed into a new intelligent paradigm, known as Smart Grid (SG), providing significant benefits both for utility companies and energy consumers such as the two-way communication (both electricity and information), distributed generation, remote monitoring, self-healing and pervasive control. However, at the same time, this dependence introduces new security challenges, since SG inherits the vulnerabilities of multiple heterogeneous, co-existing legacy and smart technologies, such as IoT

	and Industrial Control Systems (ICS). An effective countermeasure against the various cyberthreats in SG is the Intrusion Detection System (IDS), informing the operator timely about the possible cyberattacks and anomalies. In this paper, we provide an anomaly-based IDS especially designed for SG utilising operational data from a real power plant. In particular, many machine learning and deep learning models were deployed, introducing novel parameters and feature representations in a comparative study. The evaluation analysis demonstrated the efficacy of the proposed IDS and the improvement due to the suggested complex data representation.
Basic Forensic Procedures for Cyber Crime Investigation in Smart Grid Networks	The paper outlines some aspects of developing a cyber-forensic framework for Smart Grid cyber-crime investigations. In this research, we examine a key forensic instrument in reconstructing events, the timeline, followed by correlation of data from different sources. Then, we deal with the tasks of collecting and storing the monitored data. The paper also covers some aspects of the legal ramifications from collecting this data and touches on the preconditions that must be met to enable network forensics. Then we present the logging architecture, based on the recommendations of the UK National Cyber Security Center. The final part presents the methodological framework that is the result of applying the OSCAR methodology and relevant open source tools in order to ensure that necessary forensic information can be collected, stored and used as legal evidence in court.
Technique for Finding and Investigating the Strongest Combinations of Cyberattacks on Smart Grid Infrastructure	Recently, smart grids have become a vector of energy policy of many countries. Because of structural and operation features, smart grids are a constant target of combined and simultaneous cyberattacks. To maximize security and to optimize existing network schemes to prevent cyber intrusion, in this paper, we propose an approach to decision support in finding and identifying the most potent attack combinations that can set the system to maximum damage. The main purpose is to identify the most severe combinations of attacks on smart grid components that potentially can be implemented from the perspective of the attacker. In this context, the problem of finding weaknesses points in the network configuration of a smart grid and assessing the impact of events on cyberinfrastructure is considered. The technique for detecting and investigating the strongest combinations of cyberattacks on the smart grid network is given with an example of the analysis of the spread of pandemic software in a system with arbitrary structure.
A Novel and Interactive Industrial Control System Honeypot for Critical Smart Grid Infrastructure	The Industrial Control Systems (ICS) are the underlying monitoring and control components of critical infrastructures, which consist of a number of distributed field devices, such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) and Human Machine Interfaces (HMIs). As modern ICS are connected to the Internet, in the context of their digitalization as a part of the Internet of Things (IoT) domain, a number of security threats are introduced, whose exploitation can lead to severe consequences. Honeypots and honeynets are promising countermeasures that attract attackers and mislead them from hacking the real infrastructure, while gaining valuable information about the attack patterns as well as the source of the attack. In this work, we implement an interactive, proof-of-concept ICS honeypot, which is based on Conpot, that is able to emulate a physical ICS device, by replicating realistic traffic from the real device. As the honeypot runs inside a Virtual Machine, it is possible to emulate the entire organization's ICS infrastructure, a fact that

	is very important for the security of the modern critical infrastructure. In order to assess the proposed honeypot, a real-life demonstration scenario was designed, which involves a hydro power plant. The honeypot architecture is provided, while the structural components are presented in detail.
Towards Anonymous Incident Communication Channel for Electric Smart Grids	The Electric Smart Grid (ESG) is referred to as the next generation electricity power network. It is an intelligent critical infrastructure aiming to create an automated and distributed advanced energy delivery network while preserving information privacy and offering protection against intrusions. This study proposes the implementation of an Anonymous Incident Communication Channel (AICC) amongst smart grids across Europe to improve situational awareness and enhance the security of the new electric intelligent infrastructures. All participating organizations will have the ability to broadcast sensitive information, stored anonymously in a repository, without exposing the reputation of the organization. However, the technical details of the attack will be available for everyone to take appropriate countermeasures. The advantages of the AICC are the exchange of real-time security data and analysis, the circulation of best countermeasures practices, the comparison of various security solutions both from a technical and operational viewpoint and the ability to establish an open dialogue amongst anonymous peers who represent smart grid organizations (e.g., power plants) across Europe. This work focuses on the requirements of establishment, the possible obstacles, and proposed data protection techniques to be applied in the AICC. Furthermore, were explained some details of the documentation of cyber-incidents Last but not least, were also provided the benefits and the potential risks of this AICC concept
Cybersecurity in SMEs: The Smart-Home/Office Use Case	Today, small and medium-sized enterprises (SME) can be considered as the new big target for cyber-attacks, while the cybercrime prevention is often neglected within their environment. This paper aims to investigate the characteristics of cybersecurity threats in the Digital Innovation Hub (DIH) ecosystem of a Smart-Home/Office environment being constituted by SMEs that contains various smart-devices and IoT equipment, smart-grid components, employees' workstations and medium sized networking equipment. As the Cyber-security in such an ecosystem is greatly demanding and challenging because of the various communication layers and the different supported IoT devices, we introduce a more robust, resilient and effective cybersecurity solution that can be effortlessly tailored to each individual enterprise's evolving needs and can also speedily adapt/respond to the changing cyber threat landscape. Thus, this Cyber-security framework will be evaluated through three major types of Smart-Home/Office datasets and will be supported from SME/ICT clusters under the framework of the Secure and Private Smart Grid (SPEAR) H2020 project. The first promising results of our work indicate the potential of implementing strong defence mechanisms for SMEs' environments within DIHs.
A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics	Supervisory Control and Data Acquisition (SCADA) systems are the underlying monitoring and control components of critical infrastructures, such as power, telecommunication, transportation, pipelines, chemicals and manufacturing plants. Legacy SCADA systems operated on isolated networks, that made them less exposed to Internet threats. However, the increasing connection of SCADA systems to the Internet, as well as corporate networks, introduces severe security issues. Security considerations for SCADA systems are gaining higher attention, as the

	number of security incidents against these critical infrastructures is increasing. In this survey, we provide an overview of the general SCADA architecture, along with a detailed description of the SCADA communication protocols. Additionally, we discuss certain high-impact security incidents, objectives, and threats. Furthermore, we carry out an extensive review of the security proposals and tactics that aim to secure SCADA systems. We also discuss the state of SCADA system security. Finally, we present the current research trends and future advancements of SCADA security.
Trust Management in Smart Grid: A Markov Trust Model	By leveraging the advancements in Information and Communication Technologies (ICT), Smart Grid (SG) aims to modernize the traditional electric power grid towards efficient distribution and reliable management of energy in the electrical domain. The SG Advanced Metering Infrastructure (AMI) contains numerous smart meters, which are deployed throughout the distribution grid. However, these smart meters are susceptible to cyberthreats that aim to disrupt the normal operation of the SG. Cyberattacks can have various consequences in the smart grid, such as incorrect customer billing or equipment destruction. Therefore, these devices should operate on a trusted basis in order to ensure the availability, confidentiality, and integrity of the metering data. In this paper, we propose a Markov chain trust model that determines the Trust Value (TV) for each AMI device based on its behavior. Finally, numerical computations were carried out in order to investigate the reaction of the proposed model to the behavior changes of a device.
An Industrial Honeypot Based on Convolutional Neural Network	Honeypots are powerful security tools, which are developed to shield commercial and industrial networks from malicious activity. Honeypots act as passive and interactive decoys in a network by attracting malicious activity away from critical network devices. Given that the security incidents against industrial and critical infrastructure are getting sophisticated and persistent, advanced security systems are needed. In this paper, a novel industrial honeypot implementation is presented, which is based on the Modbus protocol, entitled NeuralPot. The presented NeuralPot honeypot is able to emulate industrial Modbus entities in order to actively confuse the intruders. It achieves this by introducing two distinct deep neural networks, a Generative Adversarial Network and an Autoencoder Network, which learn Modbus device behavior and generate realistic-looking traffic behavior. Based on the evaluation results, the proposed industrial honeypot performs well in terms of accuracy, similarity, and elapsed time of data generation.
Secure and Private Smart Grid: The SPEAR Architecture	Information and Communication Technology (ICT) is an integral part of Critical Infrastructures (CIs), bringing both significant pros and cons. Focusing our attention on the energy sector, ICT converts the conventional electrical grid into a new paradigm called Smart Grid (SG), providing crucial benefits such as pervasive control, better utilisation of the existing resources, self-healing, etc. However, in parallel, ICT increases the attack surface of this domain, generating new potential cyberthreats. In this paper, we present the Secure and PrivatE smArt gRid (SPEAR) architecture which constitutes an overall solution aiming at protecting SG, by enhancing situational awareness, detecting timely cyberattacks, collecting appropriate forensic evidence and providing an anonymous cybersecurity information-sharing mechanism. Operational characteristics and technical specifications details are analysed for each component, while also the communication interfaces among them are described in detail.

Implementation and Detection of Modbus Cyberattacks	Supervisory Control and Data Acquisition (SCADA) systems play a significant role in Critical Infrastructures (CIs) since they monitor and control the automation processes of the industrial equipment. However, SCADA relies on vulnerable communication protocols without any cybersecurity mechanism, thereby making it possible to endanger the overall operation of the CI. In this paper, we focus on the Modbus/TCP protocol, which is commonly utilised in many CIs and especially in the electrical grid. In particular, our contribution is twofold. First, we study and enhance the cyberattacks provided by the Smod pen-testing tool. Second, we introduce an anomaly-based Intrusion Detection System (IDS) capable of detecting Denial of Service (DoS) cyberattacks related to Modbus/TCP. The efficacy of the proposed IDS is demonstrated by utilising real data stemming from a hydropower plant. The accuracy and the F1 score of the proposed IDS reach 81% and 77% respectively.
An Anomaly Detection Mechanism for IEC 60870-5-104	The transformation of the conventional electricity grid into a new paradigm called smart grid demands the appropriate cybersecurity solutions. In this paper, we focus on the security of the IEC 60870-5-104 (IEC-104) protocol which is commonly used by Supervisory Control and Data Acquisition (SCADA) systems in the energy domain. In particular, after investigating its security issues, we provide a multivariate Intrusion Detection System (IDS) which adopts both access control and outlier detection mechanisms in order to detect timely possible anomalies against IEC-104. The efficiency of the proposed IDS is reflected by the Accuracy and F1 metrics that reach 98% and 87%, respectively.

4.2 Presence at events

During the second year, SPEAR was represented at the following events:

Table 2: Events that SPEAR was represented

Title	Date	Location	Presenter
Malware Forum	June 5, 2019	Oslo, Norway	Igor Kotsiuba (PIMEE)
European Utility Week 2019	November 12 – 14, 2019	Paris, France	S. Athanasopoulos (PPC) and V. Argyriou (0INF)
12th EE-ISAC Open Plenary	November 27 - 28 2019	ENISA Headquarters (Athens, Greece)	Panagiotis Sarigiannidis (UOWM), Alkiviadis Giannakoulias (ED)
The 11th Electrical Engineering Faculty Conference (BulEF)	June 11 -14, 2019	Varna, Bulgaria	Valeri Mladenov (TUS) Anton Hristov (VETS)
The International Energy Forum 2019 organized by the Scientific and Technical Union of the Power Engineers	June 25-28, 2019	Varna, Bulgaria	Valeri Mladenov (TUS) Anton Hristov (VETS)
Open Day Go 4 Green	22 October 2019	Ministry of Energy, Athens, Greece	Konstantinos Stamatakis (PPC)

Education Festival 2019	31 May 2019	Athens, Greece	S. Athanasopoulos (PPC)

Malware Forum

The annual NTNU Malware Forum that is organized in close collaboration between NTNU/CCIS and NSM/NorCERT took place on June 5th, 2019 in Oslo. The Cyber Hygiene framework in smart grids and an overview of the SPEAR project was presented at the Malware Forum. Representatives of Critical Infrastructures from Norway and Sweden attended this event.

European Commission
Malware cyber hygiene in energy grids and critical infrastructure scenarios
Igor Kotsiuba, PhD
Researcher at PIMEE NAS of Ukraine
Head of Cybersecurity WG at American Chamber Ukraine
SPEAR
Scandic
NTNU
Malware Forum

Figure 8: Malware Forum

European Utility Week 2019

In 2019, European Utility Week and POWERGEN Europe offered an end-to-end European energy experience for the whole energy supply chain, under one roof. All of this is reflected throughout the event from the exhibition, with many global solution providers, to addressing the key business challenges. The event is a business, innovation, networking and information platform. This event is used as an annual meeting place to discuss and promote strategies and businesses aiming to help drive efficiencies in meeting the sustainable development goals.

A video overview of the SPEAR project and the developed tools for cyberattack detection and visual analytics was presented.

European Utility Week brings together 13,000 of Europe’s thought leaders and visionaries behind the world’s most successful utilities and solution providers. It is a unique opportunity to showcase your brand and services as one of the leading companies in the global smart energy market.

SPEAR
European Commission | EU Projects
See you in Milan
27-29 October 2020
Explore
SAP Cloud for Utilities
Project Goals
Build attack detection mechanisms and promote resilience operations in smart grids
Increase situational awareness in smart grids
Create and maintain an anonymous repository of incidents
To provide smart network forensics
To empower EU-wide consensus of cybersecurity in smart grids
Strengthen the role of European smart grid and cyber-security industry in the global market.
HORIZON 2020

Figure 9: Utility Week 2019

12th EE-ISAC Plenary Meeting

On 27-28 November 2019, the 12th EE-ISAC Plenary Meeting took place in Athens, where Dr. Panagiotis Sarigiannidis (UOWM) presented the SPEAR project. The 2-day meeting included presentations and discussions on the state of security of the European energy sector, as well as network forensics training by ENISA. The European Energy – Information Sharing & Analysis Centre (EE-ISAC) is an industry-driven, information-sharing network of trust. Both private utilities and solution providers and (semi-)public institutions such as academia, governmental and non-profit organizations share valuable information on cybersecurity & cyber resilience.

Figure 10: EE-ISAC plenary meeting

The 11th Electrical Engineering Faculty Conference (BulEF)

This conference is organized by the Faculty of Electrical Engineering, Technical University of Sofia, Bulgaria and the thematic areas covered are:

- The electrical power energy sector and the market
- Energy efficiency and renewable sources of electrical energy
- Lighting
- Studies and analyses on processes and phenomena

A presentation about the SPEAR objectives and the demo that will take place in VETS were presented. More than 75 researchers and experts in the thematic areas attended this event.

The International Energy Forum 2019

In the Forum, several scientists, specialists and representatives of enterprises, companies, and organizations, that are active in Bulgaria and intend to develop their business in the future participated. An open and engaged discussion has been initialized between all partners in the energy sector – state authorities, energy enterprises, scientists, energy producers, and consumers. A contribution to the positive results of the Forum has been made by the participation of foreign and Bulgarian experts as well as of representatives of leading companies from and outside of Europe. Companies and organizations have been provided with the opportunity to not only present their activities but also to establish business contacts with local and foreign partners. A presentation about the SPEAR objectives and the demo that will take place in VETS were presented. More than 90 researchers and experts from several countries participated in the event.

Open Day - Go 4 Green

The Greek Ministry of Environment and Energy organized in 22nd October 2019 the Open Day Go 4 Green event, inviting start-ups, programmers, researchers, students and stakeholders to contribute in an open discussion about open data and how they can be used to develop new innovative solutions around green energy and digital transformation. The SPEAR project participated in this event, presenting the innovative solutions that SPEAR introduces through its architecture, towards digital transformation and secured modern smart grids. SPEAR tried to inspire the audience by providing specific ideas for the hackathon that were based on the AI technologies utilised in the project. Last, the initiatives of the European Commission (EC) to foster R&D efforts were also presented, including the H2020 framework and the EC Open Research Data Pilot.

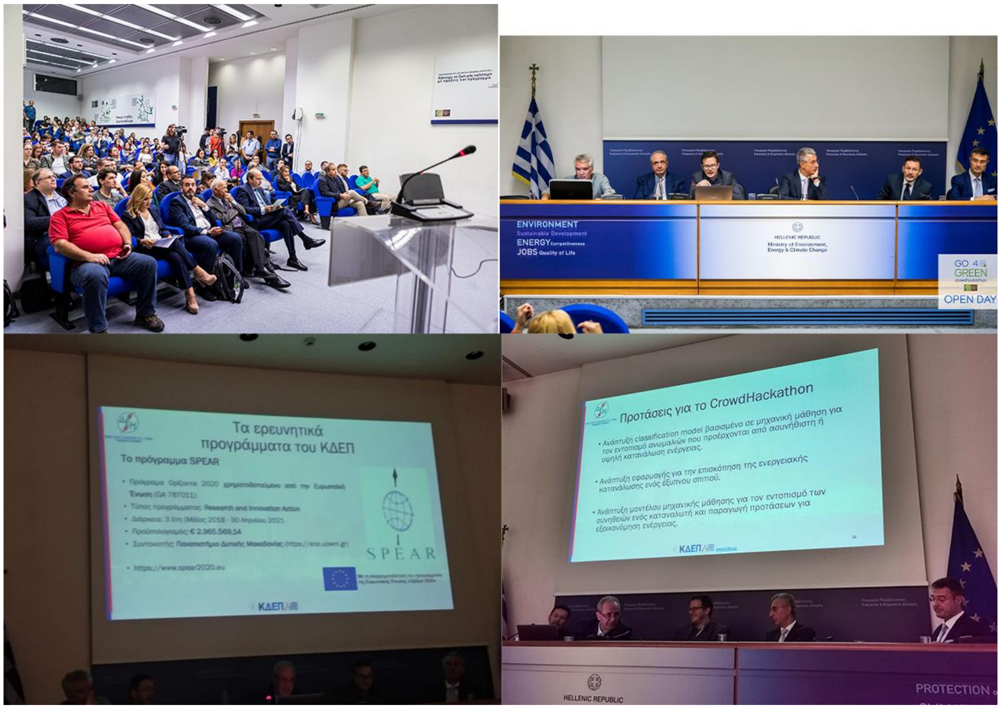

ENVIRONMENT Sustainable Development
ENERGY Competitiveness
JOBS Quality of Life
HELLENIC REPUBLIC
Ministry of Environment, Energy & Climate Change
GO 4 GREEN
OPEN DAY
Τα ερευνητικά προγράμματα του ΚΔΕΠ
Το πρόγραμμα SPEAR
Πρόγραμμα Ορίζοντα 2020 χρηματοδοτούμενο από την Ευρωπαϊκή Ένωση (GA 787011)
Τύπος προγράμματος: Research and Innovation Action
Διάρκεια: 3 έτη (Μάιος 2018 - 30 Απριλίου 2021)
Προϋπολογισμός: € 2.965.569,14
Συντονιστής: Πανεπιστήμιο Δυτικής Μακεδονίας (https://ece.uowm.gr)
https://www.spear2020.eu
SPEAR
ΚΔΕΠ
Προτάσεις για το CrowdHackathon
Ανάπτυξη classification model βασισμένο σε μηχανική μάθηση για τον εντοπισμό ανωμαλιών που προέρχονται από ασυνήθιστη ή υψηλή κατανάλωση ενέργειας.
Ανάπτυξη εφαρμογής για την επισκόπηση της ενεργειακής κατανάλωσης ενός έξυπνου σπιτιού.
Ανάπτυξη μοντέλου μηχανικής μάθησης για τον εντοπισμό των συνηθειών ενός καταναλωτή και παραγωγή προτάσεων για εξοικονόμηση ενέργειας.
HELLENIC REPUBLIC
PROTECTION

Figure 11: Open Day - Go 4 Green

Education Festival 2019

Education Festival is an annual event, organized by IIEK ALFA and the Mediterranean College, that offers more than 140 training seminars on various topics, including Information Technology (IT), financing, management, and engineering amongst others. The seminars are open for students, stakeholders, and individuals, upon registration, to the public. In this context, a seminar was organised in cooperation with IIEK ALFA, in which the concept of smart grids was presented as well as their benefits and the cybersecurity challenges that modern societies face during the transition to smart grids. In addition, an overview of the SPEAR project was presented, focusing on the motivation and the innovation that the project introduces.

SMART GRIDS AND CHALLENGES
THE SPEAR PROJECT
Απεικόνιση του έξυπνου δικτύου
Καινοτομίες και Αντίκτυπος του SPEAR
ΠΛΗΡΟΦΟΡΙΚΗΣ

Figure 12: Education Festival 2019

4.3 Workshops and clustering

Table 3: Workshops

Title	Activity Type	Date	Location	Presenter(s)
Hack4Energy	Hackathon	23-24 October 2019	Thessaloniki, Greece	Panagiotis Sarigiannidis (UOWM), Panagiotis Radoglou-Grammatikis (UOWM), Dimitrios Pliatsios (UOWM) Odysseas Nikolis (CERTH), Nikolaos Vakakis (CERTH), Dimosthenis Ioannidis (CERTH)
1st Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SecSoft)	Workshop	24 June 2019	Paris, France	Panagiotis Sarigiannidis (UOWM)

Hack4Energy

On 23-24 October 2019, CERTH and UOWM organized the Hack4Energy joint hackathon event that took place at CERTH premises. The hackathon challenges included the development of appropriate visualization mechanisms, that will assist the smart grid security administrator in identifying potential anomalies, and the development of classification models leveraging Machine Learning techniques, that will detect and identify various cyberattacks against the smart grid. Furthermore, during the event, the SPEAR project was presented by Dr. Panagiotis Sarigiannidis (UOWM). Finally, more than 50 people participated in the event.

1st Secsoft (2019)

The 1st Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SecSoft) is a joint initiative from the H2020 EU Projects ASTRID, SPEAR, CYBER-TRUST, REACT, SHIELD, and 5GENESIS to initiate a dialogue on emerging cyber-security paradigms for virtualized environments and critical infrastructures. The workshop aims to bring closer novel approaches for providing organizations the appropriate situational awareness in relation to cybersecurity threats allowing them to quickly detect and effectively respond to sophisticated cyber-attacks.

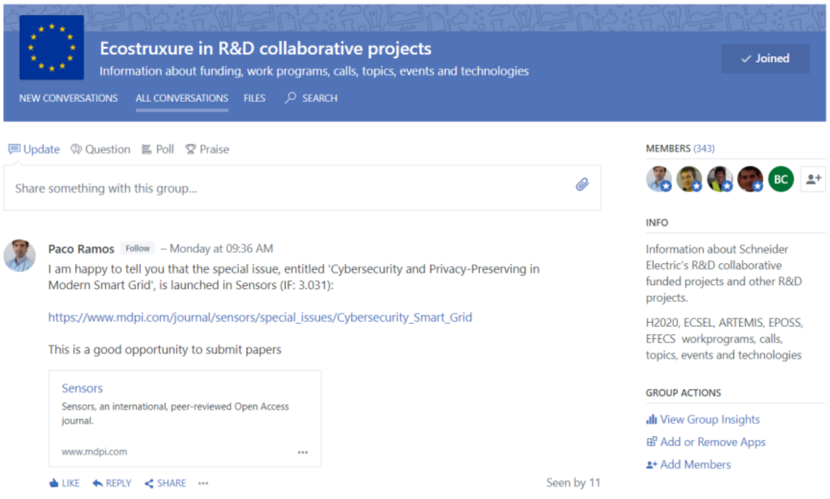
4.4 Dissemination within organizations

Schneider and Enel disseminate their involvement in SPEAR in their internal platforms and services.

Schneider Electric has two platforms for publishing news about R&D projects. These are shown in the following sections 4.4.1 and 4.4.2.

4.4.1 Yammer

It is an internal social networking service, where Schneider employees publish company achievements or events. The SPEAR related group is called "Ecostruxure in R&D collaborative projects" and is active with 343 followers. Below is depicted the main page:



Paco Ramos – Monday at 09:36 AM

I am happy to tell you that the special issue, entitled 'Cybersecurity and Privacy-Preserving in Modern Smart Grid', is launched in Sensors (IF: 3.031):

https://www.mdpi.com/journal/sensors/special_issues/Cybersecurity_Smart_Grid

This is a good opportunity to submit papers

Sensors

Sensors, an international, peer-reviewed Open Access journal.

www.mdpi.com

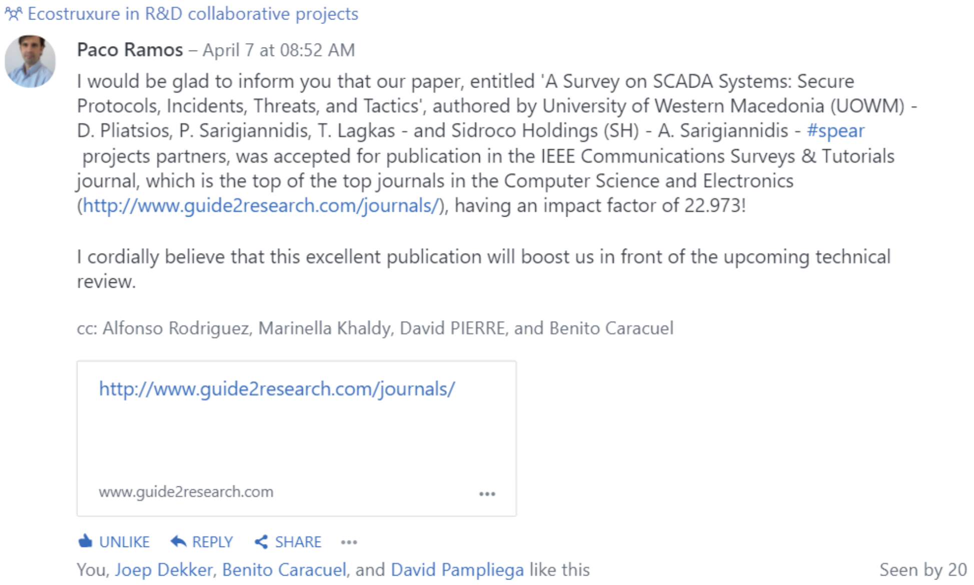
Seen by 11

Information about Schneider Electric's R&D collaborative funded projects and other R&D projects.

H2020, ECSEL, ARTEMIS, EPOSS, EFECS workprograms, calls, topics, events and technologies

Figure 13: Yammer group page

All posts related to the SPEAR project are attached below showing the date, and the views received. In total, 295 views have been obtained. These are as follows:



Ecostruxure in R&D collaborative projects

Paco Ramos – April 7 at 08:52 AM

I would be glad to inform you that our paper, entitled 'A Survey on SCADA Systems: Secure Protocols, Incidents, Threats, and Tactics', authored by University of Western Macedonia (UOWM) - D. Pliatsios, P. Sarigiannidis, T. Lagkas - and Sidroco Holdings (SH) - A. Sarigiannidis - #spear projects partners, was accepted for publication in the IEEE Communications Surveys & Tutorials journal, which is the top of the top journals in the Computer Science and Electronics (http://www.guide2research.com/journals/), having an impact factor of 22.973!

I cordially believe that this excellent publication will boost us in front of the upcoming technical review.

cc: Alfonso Rodriguez, Marinella Khaldy, David PIERRE, and Benito Caracuel

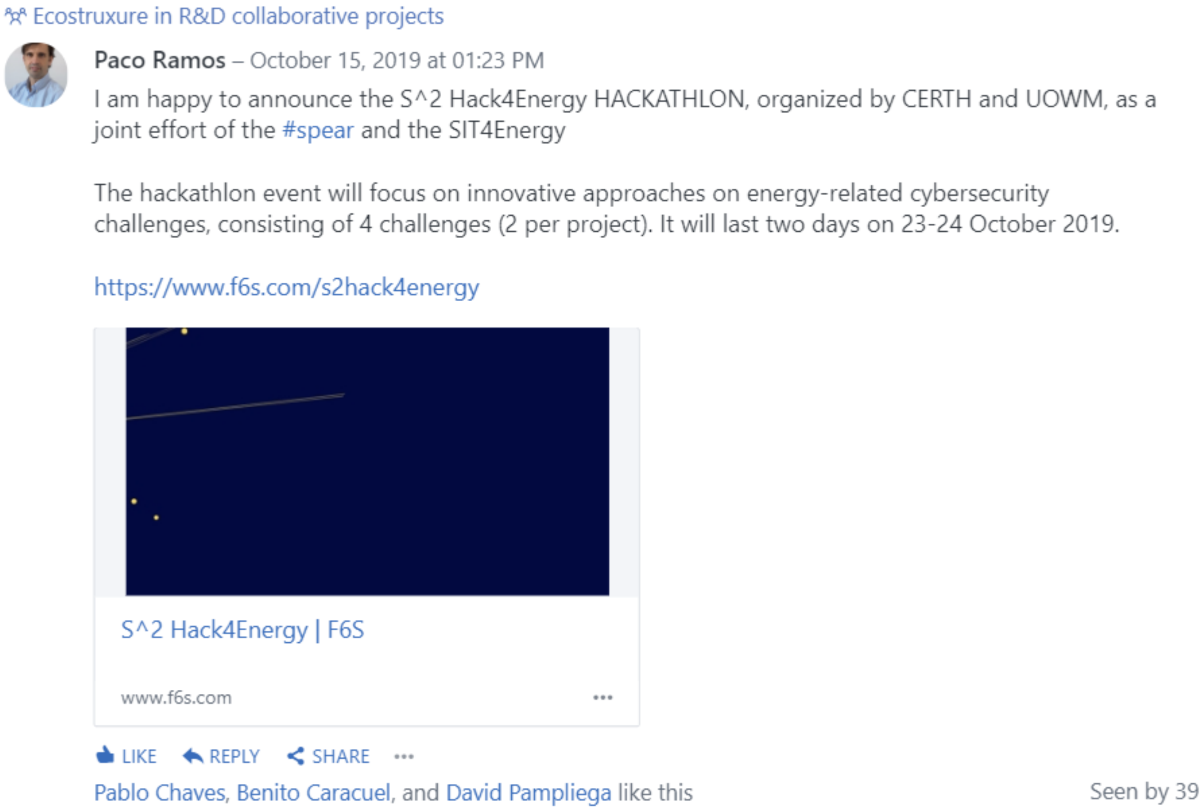
http://www.guide2research.com/journals/

www.guide2research.com

You, Joep Dekker, Benito Caracuel, and David Pampliega like this

Seen by 20

Figure 14: Yammer post accepted paper



Ecostruxure in R&D collaborative projects

Paco Ramos – October 15, 2019 at 01:23 PM

I am happy to announce the S^2 Hack4Energy HACKATHLON, organized by CERTH and UOWM, as a joint effort of the #spear and the SIT4Energy

The hackathlon event will focus on innovative approaches on energy-related cybersecurity challenges, consisting of 4 challenges (2 per project). It will last two days on 23-24 October 2019.

https://www.f6s.com/s2hack4energy

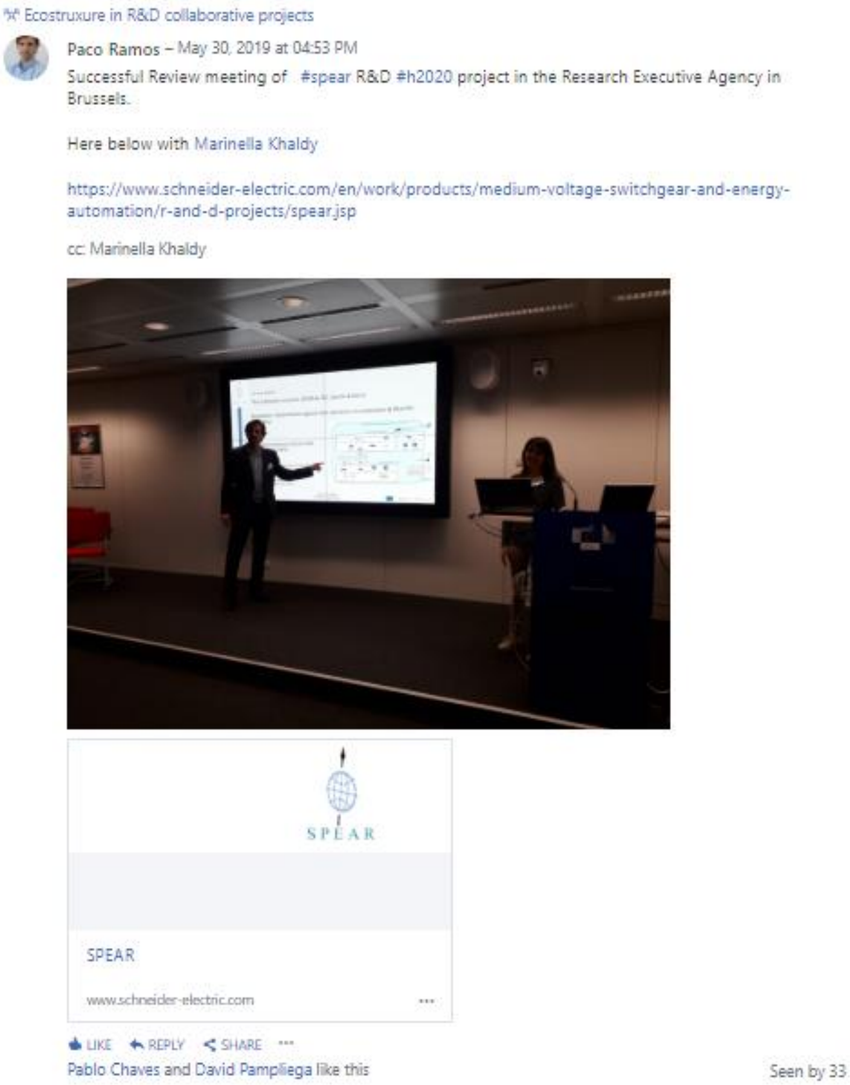
S^2 Hack4Energy | F6S

www.f6s.com

Pablo Chaves, Benito Caracuel, and David Pampliega like this

Seen by 39

Figure 15: Yammer post S^2 Hack4Energy



Ecostruxure in R&D collaborative projects

Paco Ramos – May 30, 2019 at 04:53 PM

Successful Review meeting of #spear R&D #h2020 project in the Research Executive Agency in Brussels.

Here below with Marinella Khaldy

https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/spear.jsp

cc: Marinella Khaldy

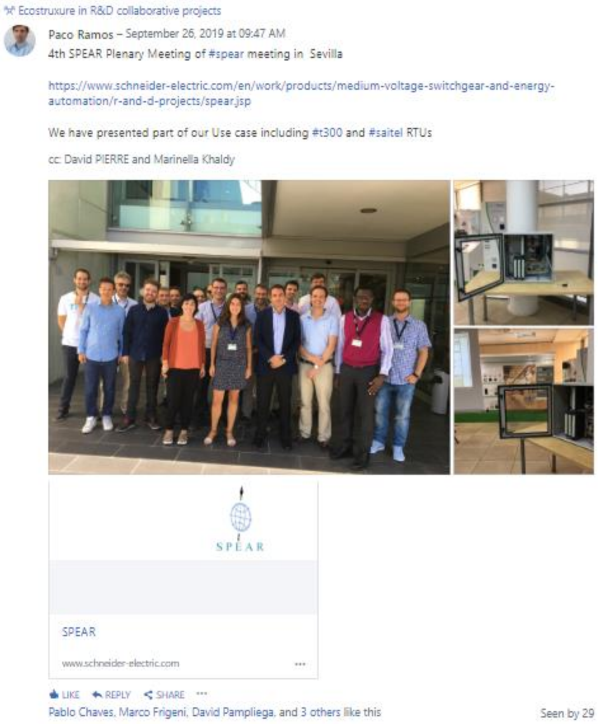
SPEAR

www.schneider-electric.com

Pablo Chaves and David Pampliega like this

Seen by 33

Figure 16: Yammer post SPEAR first review



Ecostruxure in R&D collaborative projects

Paco Ramos – September 26, 2019 at 09:47 AM

4th SPEAR Plenary Meeting of #spear meeting in Sevilla

https://www.schneider-electric.com/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/spear.jsp

We have presented part of our Use case including #t300 and #saitel RTUs

cc: David PIERRE and Marinella Khaldy

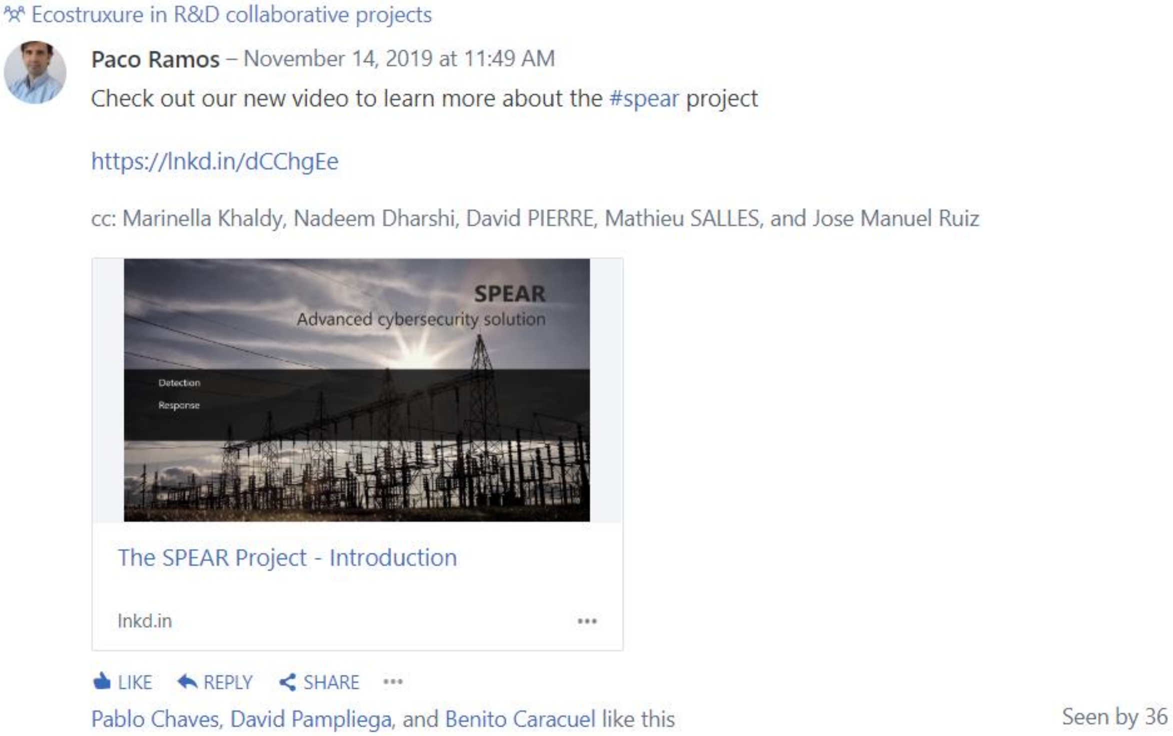
SPEAR

www.schneider-electric.com

Pablo Chaves, Marco Frigeni, David Pampliega, and 3 others like this

Seen by 29

Figure 17: Yammer post SPEAR 4th meeting



Ecostruxure in R&D collaborative projects

Paco Ramos – November 14, 2019 at 11:49 AM

Check out our new video to learn more about the #spear project

https://lnkd.in/dCChgEe

cc: Marinella Khaldy, Nadeem Dharshi, David PIERRE, Mathieu SALLES, and Jose Manuel Ruiz

The SPEAR Project - Introduction

lnkd.in

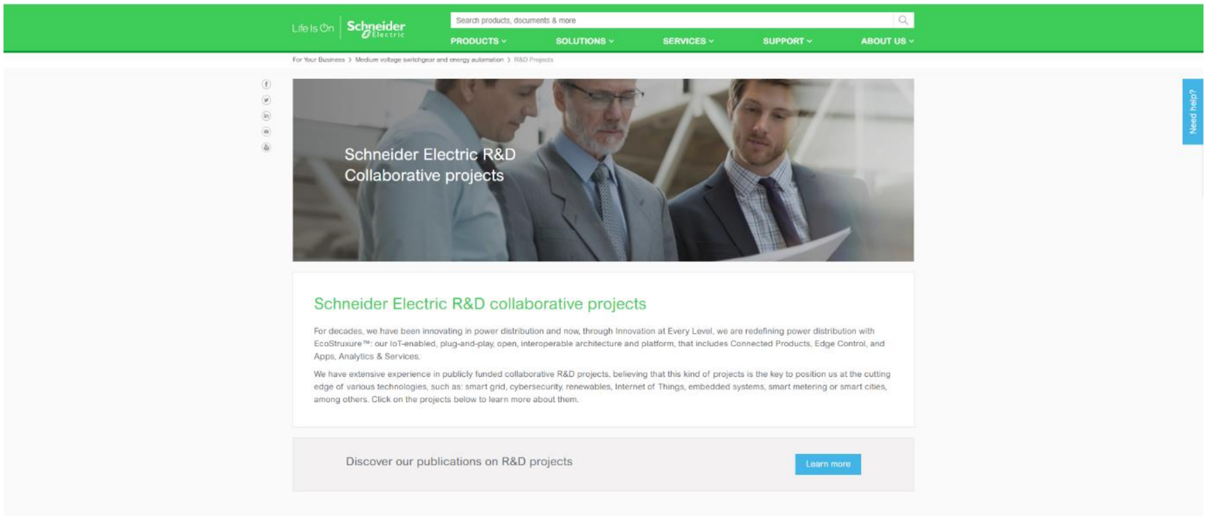
Pablo Chaves, David Pampliega, and Benito Caracuel like this

Seen by 36

Figure 18: Yammer post SPEAR Video

4.4.2 Schneider Electric R&D collaborative projects

Schneider Electric also has a public platform, a website, where all our collaborative projects are shown. To access you must use the following link: http://www.se.com/rdenergy



Schneider Electric R&D collaborative projects

For decades, we have been innovating in power distribution and now, through Innovation at Every Level, we are redefining power distribution with EcoStruxure™: our IoT-enabled, plug-and-play, open, interoperable architecture and platform, that includes Connected Products, Edge Control, and Apps, Analytics & Services.

We have extensive experience in publicly funded collaborative R&D projects, believing that this kind of projects is the key to position us at the cutting edge of various technologies, such as: smart grid, cybersecurity, renewables, Internet of Things, embedded systems, smart metering or smart cities, among others. Click on the projects below to learn more about them.

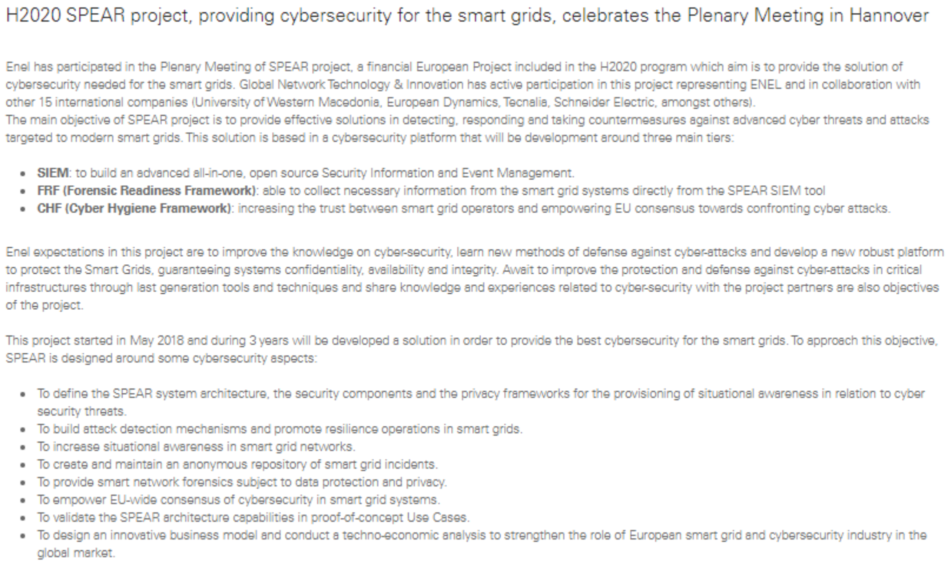
Discover our publications on R&D projects

Figure 19: SPEAR at Schneider Electric website

Once the SPEAR project has been selected, the objectives are detailed and the link to the official page of the project has been included.

https://www.se.com/ww/en/work/products/medium-voltage-switchgear-and-energy-automation/r-and-d-projects/spear.jsp

ENEL is also publishing information about SPEAR in their internal portal that is available to its employees. Some screenshots of these posts are presented in the following figure:



H2020 SPEAR project, providing cybersecurity for the smart grids, celebrates the Plenary Meeting in Hannover

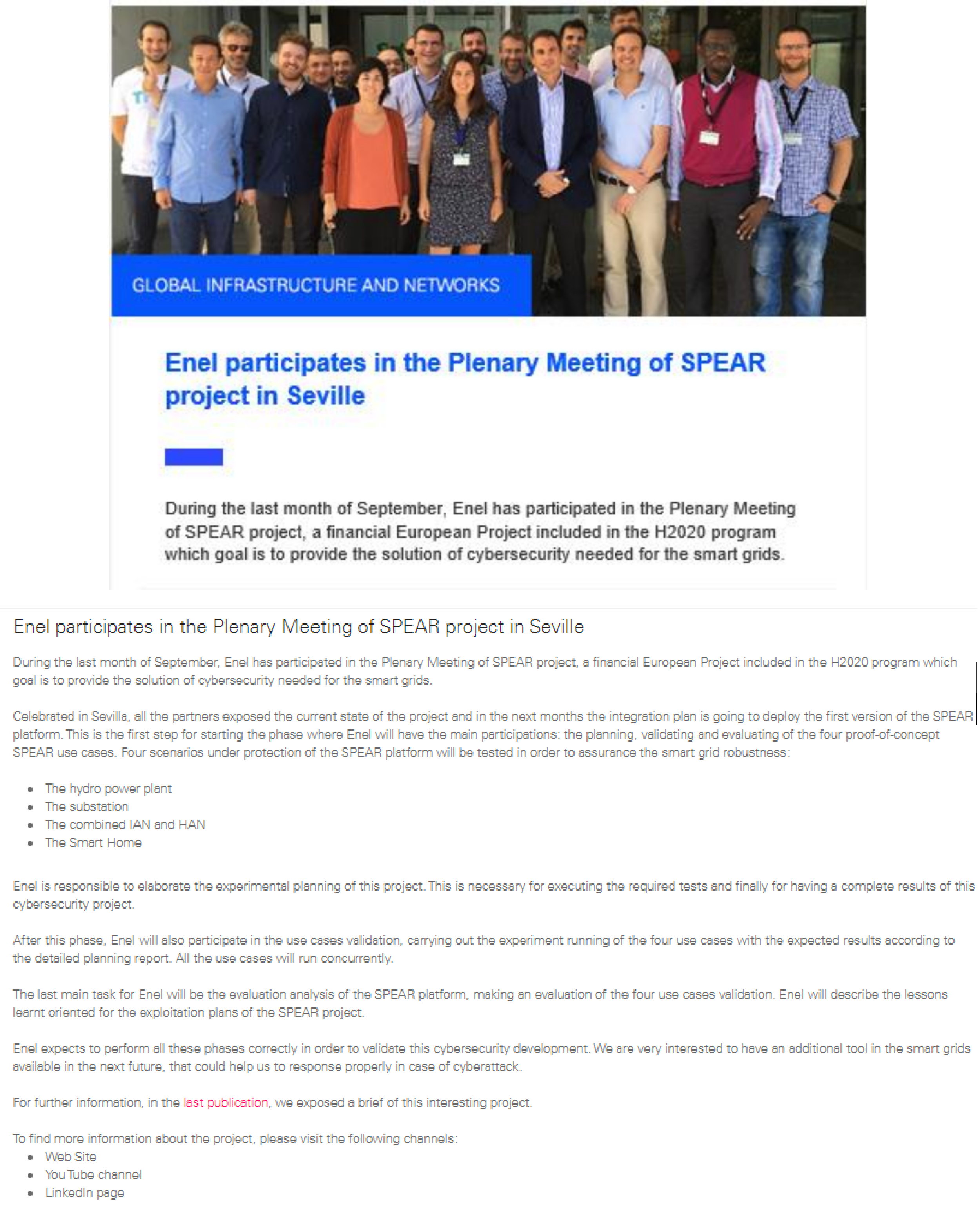
Enel has participated in the Plenary Meeting of SPEAR project, a financial European Project included in the H2020 program which aim is to provide the solution of cybersecurity needed for the smart grids. Global Network Technology & Innovation has active participation in this project representing ENEL and in collaboration with other 15 international companies (University of Western Macedonia, European Dynamics, Tecnalia, Schneider Electric, amongst others).
The main objective of SPEAR project is to provide effective solutions in detecting, responding and taking countermeasures against advanced cyber threats and attacks targeted to modern smart grids. This solution is based in a cybersecurity platform that will be development around three main tiers:

- **SIEM**: to build an advanced all-in-one, open source Security Information and Event Management.
- **FRF (Forensic Readiness Framework)**: able to collect necessary information from the smart grid systems directly from the SPEAR SIEM tool
- **CHF (Cyber Hygiene Framework)**: increasing the trust between smart grid operators and empowering EU consensus towards confronting cyber attacks.

Enel expectations in this project are to improve the knowledge on cyber-security, learn new methods of defense against cyber-attacks and develop a new robust platform to protect the Smart Grids, guaranteeing systems confidentiality, availability and integrity. Await to improve the protection and defense against cyber-attacks in critical infrastructures through last generation tools and techniques and share knowledge and experiences related to cyber-security with the project partners are also objectives of the project.

This project started in May 2018 and during 3 years will be developed a solution in order to provide the best cybersecurity for the smart grids. To approach this objective, SPEAR is designed around some cybersecurity aspects:

- To define the SPEAR system architecture, the security components and the privacy frameworks for the provisioning of situational awareness in relation to cyber security threats.
- To build attack detection mechanisms and promote resilience operations in smart grids.
- To increase situational awareness in smart grid networks.
- To create and maintain an anonymous repository of smart grid incidents.
- To provide smart network forensics subject to data protection and privacy.
- To empower EU-wide consensus of cybersecurity in smart grid systems.
- To validate the SPEAR architecture capabilities in proof-of-concept Use Cases.
- To design an innovative business model and conduct a techno-economic analysis to strengthen the role of European smart grid and cybersecurity industry in the global market.



GLOBAL INFRASTRUCTURE AND NETWORKS

Enel participates in the Plenary Meeting of SPEAR project in Seville

During the last month of September, Enel has participated in the Plenary Meeting of SPEAR project, a financial European Project included in the H2020 program which goal is to provide the solution of cybersecurity needed for the smart grids.

Enel participates in the Plenary Meeting of SPEAR project in Seville

During the last month of September, Enel has participated in the Plenary Meeting of SPEAR project, a financial European Project included in the H2020 program which goal is to provide the solution of cybersecurity needed for the smart grids.

Celebrated in Sevilla, all the partners exposed the current state of the project and in the next months the integration plan is going to deploy the first version of the SPEAR platform. This is the first step for starting the phase where Enel will have the main participations: the planning, validating and evaluating of the four proof-of-concept SPEAR use cases. Four scenarios under protection of the SPEAR platform will be tested in order to assurance the smart grid robustness:

- The hydro power plant
- The substation
- The combined IAN and HAN
- The Smart Home

Enel is responsible to elaborate the experimental planning of this project. This is necessary for executing the required tests and finally for having a complete results of this cybersecurity project.

After this phase, Enel will also participate in the use cases validation, carrying out the experiment running of the four use cases with the expected results according to the detailed planning report. All the use cases will run concurrently.

The last main task for Enel will be the evaluation analysis of the SPEAR platform, making an evaluation of the four use cases validation. Enel will describe the lessons learnt oriented for the exploitation plans of the SPEAR project.

Enel expects to perform all these phases correctly in order to validate this cybersecurity development. We are very interested to have an additional tool in the smart grids available in the next future, that could help us to response properly in case of cyberattack.

For further information, in the last publication, we exposed a brief of this interesting project.

To find more information about the project, please visit the following channels:
- Web Site
- You Tube channel
- LinkedIn page

Figure 20: SPEAR news at the internal portal of ENEL

5. Dissemination KPIs

The monitoring of dissemination and communication activities is an essential process to evaluate the success and efficiency of the plan. SPEAR defined a set of Key Performance Indicators (KPIs) that monitor the progress and impact of the dissemination and communication activities and act as guidance to take proper actions. Table 4 presents the KPIs that were introduced in D8.2 and updates on the current achieved status (cumulative for the first two years of the project).

Table 4: SPEAR Dissemination and Communication KPIs

No	KPI	Audience	Objective (min value)	Value at the end of second year
1	Organization and/or Attendance to exhibitions	Strategic stakeholders, Industry	200 visitors	SPEAR was present at seven events with an estimated number of 500 people
2	Workshops co-located with major conferences	Research community, Strategic stakeholders, Industry, Other Projects	1-2 workshops per year	SPEAR was present in 2 workshops
3	On-site demonstrations	Research community, Strategic stakeholders, Industry	3 demonstrations	This activity is planned to take place during the third year of the project
4	Publications in workshops, conferences and journals	Research community	Workshop papers (1-3 per year) Conference papers (1-2 per year) Journal papers (1-2 per year)	16 conferences and workshops (12 the second year) 3 journals (2 the second year)
5	Online publications (magazines, newspapers, blogs)	Research community, Strategic stakeholders, Industry, Public	10 publications per year 500 views	15 posts (12 news, 3 blog posts)
6	Posts to social networks	Research community, Strategic stakeholders, Industry, Public	10 posts 100 contacts 50 likes/share 5 comments	32 posts 117 followers 582 likes, 54 shares 2 comments
7	Participation in CeBIT	Research community, Strategic stakeholders, Industry, Public	5 brochure copies delivered	This activity will take place the third year of the project

8	Project website	Research community, Strategic stakeholders, Industry, Other Projects, Public	Top 5 SEPR	• spear • spear project • spear security • www spear • h2020 cybersecurity project
9	Inclusion of light content for non-specialized audience in the project website, blog, social media, as well as publishing "lighter" versions of project newsletters, leaflets, flyers, etc.	Public	5 material 100 reads	3 newsletters have been published in the SPEAR website (2 the second year)
10	Summer schools / open events with free access, where visitors will realize in a lively way the SPEAR benefits.	Research community, Strategic stakeholders, Industry, Other Projects, Public	1 summer school 50 attendees 1 open event	This activity is planned for the last year
11	Participation in media (TV, newspapers, radio) events	Public	10 media appearances	2 appearances in media

The following section provides information about each of the KPIs along with the plan to meet them.

KPI 1: Organization and/or attendance to exhibitions

SPEAR has participated in seven events (see section 4.2), with an estimated audience of 500 attendees. This KPI is on track.

KPI 2: Workshops co-located with major conferences

SPEAR results were presented in one workshop that was organized by the GHOST project. The 1st International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures was co-organized by SPEAR.

KPI 3: On-site demonstrations

This activity is planned to take place during the final year of the project.

KPI 4: Publications in workshops, conferences and journals

There were sixteen conference and workshop publications and three Journal publications during the first two years, while there are two more submitted and under review (see section 4.1). This KPI for the first two years has been met.

KPI 5: Online publications (magazines, newspapers, blogs)

This KPI is slightly lower for the first two years but is in line with the plan that was introduced in 8.3. Increased effort is expected in the last year where most of the results will be available.

KPI 6: Posts to social networks

The KPI is on track for the first two years. More specifically, the LinkedIn account of SPEAR has 117 followers in total, 32 posts exceeding the target KPI, and 2 out of 5 needed comments. The target for likes and shares has been met since 582 likes and 54 shares have been gathered.

KPI 7: Participation in CeBIT

Since CeBIT 2019 was cancelled the consortium plans to identify an alternative exhibition to participate, something that will happen in the last year of the project. The status of COVID-19 outbreak may affect the fulfilment of this KPI as most of the exhibitions in the following months have been cancelled or will take place through virtual meeting tools.

KPI 8: Project website (SEPR)

The Google Search Console platform has been employed in order to measure the SEPR KPI. The platform shows the following top-5 SEPR keywords that visitors search in search engines in order to find our website:

- spear
- spear project
- spear security
- www spear
- h2020 cybersecurity project

KPI 9: Light content for general public

Three newsletters have been published until now (see section 3.3). Two more are planned to be produced in the following weeks. More are to come in the last year in order to achieve this KPI.

KPI 10: Summer schools/open events

This activity is planned to take place during the final year of the project.

KPI 11: Media appearances

Two appearances took place in the first two years, their number is expected to increase during the third year as more results are produced.

The following diagram illustrates the current percentage for each of the KPIs along with the planned value at end of the second year and the planned final value (100%). As we see there are KPIs that have already reached the value expected at the end of project, while most of them are in track based on the initial planning.

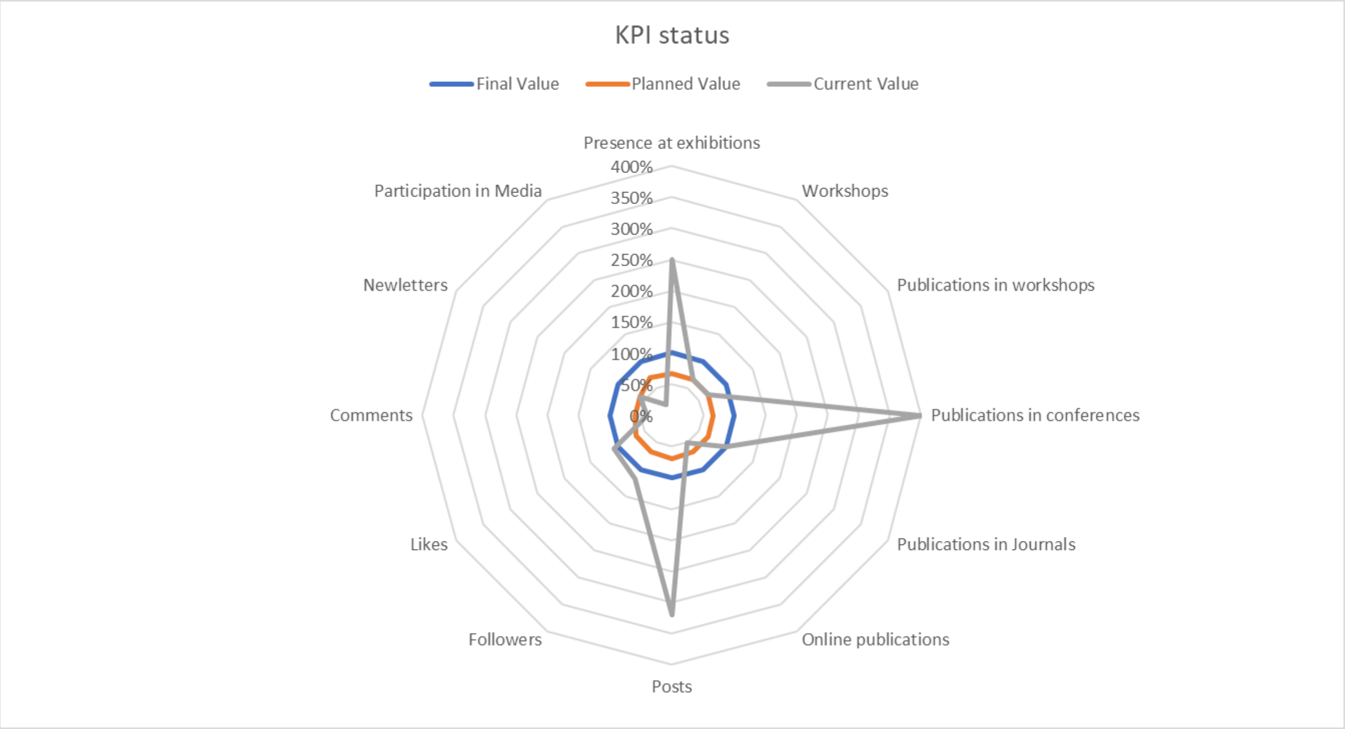


Figure 21: Status of KPIs

6. Plans for third year

To share the project progress with the scientific community, the consortium will draft articles and other contributions for the technical literature and dedicated journals. Such contributions will be written by academic and technology partners, through peer-reviewed journals and magazines and also through papers presented at conferences and other events.

SPEAR is organizing the First International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2020 https://www.ares-conference.eu/workshops-eu-symposium/epesec-2020/). The workshop is in conjunction with the ARES workshops EU Projects Symposium 2020 at 15th International Conference on Availability, Reliability and Security (ARES 2020 – http://www.ares-conference.eu). The workshop is co-organized from the following H2020 R&D projects: SDN-microSENSE, SPEAR, FORESIGHT, CYBER-TRUST.

A list of Journals that are covering the research areas of SPEAR has been compiled and presented in Table 5, while a list of conferences that will take place the next year are presented in Table 6.

Table 5: Journals for last year

Journal	Link
Computers & Security	https://www.journals.elsevier.com/computers-and-security
Cybersecurity and Privacy-Preserving in Modern Smart Grid, Sensors	https://www.mdpi.com/journal/sensors/special_issues/Cybersecurity_Smart_Grid
Applied Energy	http://www.sciencedirect.com/science/journal/0306261
Computers & Electrical Engineering	http://www.sciencedirect.com/science/journal/0045790/open-access
Computers, Environment & Urban Systems	http://www.sciencedirect.com/science/journal/01989715/open-access
Computers in Human Behavior	http://www.sciencedirect.com/science/journal/07475632
The Electricity Journal	http://www.sciencedirect.com/science/journal/10406190
Electric Power Systems Research	http://www.sciencedirect.com/science/journal/03787796
Energy - an international journal	http://www.sciencedirect.com/science/journal/03605442
Energy Policy	http://www.sciencedirect.com/science/journal/03014215
Energy Reports	http://www.sciencedirect.com/science/journal/23524847
Energy Research & Social Science	http://www.sciencedirect.com/science/journal/22146296
Energy Strategy Reviews	http://www.sciencedirect.com/science/journal/22146296

Journal	Link
Energy Conversion & management	http://www.journals.elsevier.com/energy-conversion-and-management
Journal of Electrical Systems and Information Technology	http://www.journals.elsevier.com/journal-of-electrical-systems-and-information-technology
Journal of Environmental Management	http://www.journals.elsevier.com/journal-of-environmental-management
Sustainable cities and societies	http://www.journals.elsevier.com/sustainable-cities-and-society
Sustainable Energy Technologies and Assessments	http://www.journals.elsevier.com/sustainable-energy-technologies-and-assessments
Utilities Policy	http://www.journals.elsevier.com/utilities-policy
IEEE Transactions on Industry Applications – Special Issue, Security, Reliability, Privacy, and Quality in Industrial Automation and Control	https://ias.ieee.org/publications/ieee-transactions-on-industry-applications.html http://jolfaei.info/IEEE-Trans-IAS.html
IEEE Transactions on Power Systems	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=59
IEEE Transactions on Industrial Informatics	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9424
Pattern Recognition Elsevier	https://www.journals.elsevier.com/pattern-recognition
IEEE Transactions on Industrial Informatics for Special Section on Industrial Internet of Things (IIoT): Where we are and What's next?	http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics
Special Issue on Artificial Intelligence: The Security & Privacy Opportunities and Challenges for	https://www.journals.elsevier.com/future-generation-computer-systems/call-for-papers/the-security-privacy-opportunities

Journal	Link
Emerging Applications	

Table 6: Conferences that will take place the last year

Conference	Date	Place
25th IEEE Symposium on Computers and Communications (ISCC)	July 8-10 2020	Rennes, France
IEEE DCOSS 2020	May 25 - 27, 2020	ONLINE
International Conference on Availability, Reliability, and Security (ARES) 2020	August 25 – 28, 2020	Dublin, Ireland, Online
First International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2020)	August 25, 2020	Dublin, Ireland, Online
MEDPOWER 2020 - Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion	November 9 – 12, 2020	Paphos, Cyprus
4th International Workshop on Big Data Analytic for Cybercrime Investigation and Prevention, co-located with IEEE Big Data 2020 (bdaccip)	December 10-13, 2020.	Atlanta, Georgia, USA

SPEAR plans to participate in the European Utility Week 2020 that will take place in Milan, and in Hannover Messe 2021.

The roadmap of presence in industrial events and workshops/conferences is illustrated in the next figure.

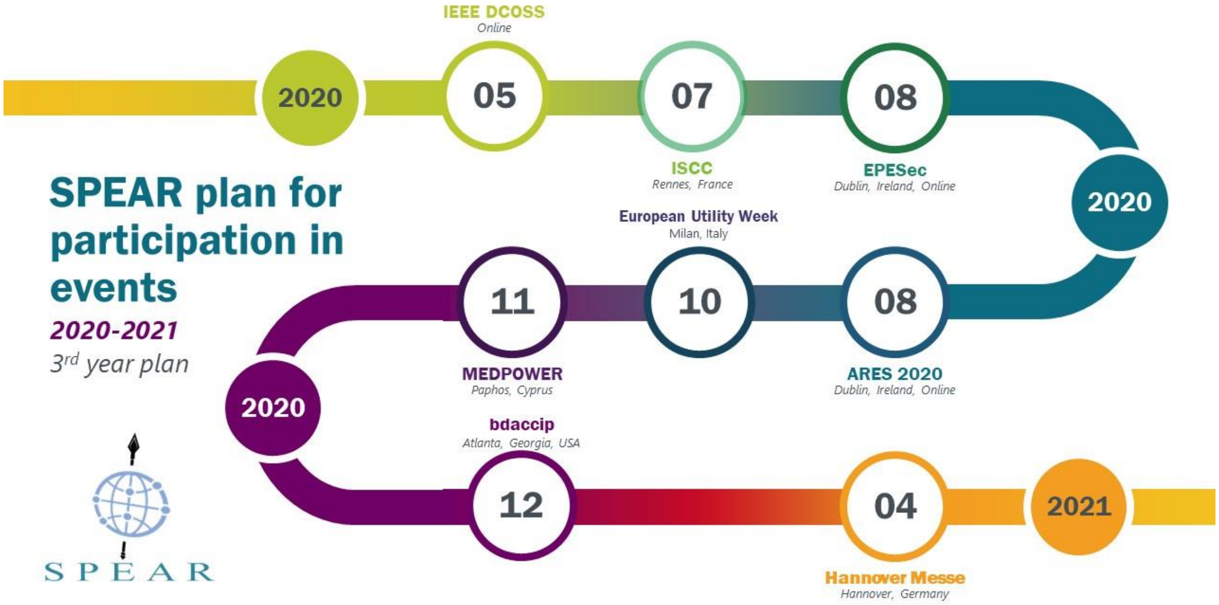


Figure 22: SPEAR plan for participation in events

The participation in events and conferences depends on the travel restrictions that are imposed all over Europe due to COVID-19. Some events have been postponed, and others have transformed into virtual ones using teleconference applications and platforms. We will monitor the status and update the plan accordingly when new information becomes available.