



ENERGY SHIELD

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

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

W7 COMMUNICATION, DISSEMINATION & ECOSYSTEM DEVELOPMENT

D7.3 –COMMUNICATION REPORT FINAL

Document info	
Contractual delivery	30/06/2022
Actual delivery	30/06/2022
Responsible Beneficiary	KTH
Contributing beneficiaries	all
Version	1.0



This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907



DOCUMENT INFO

Document ID:	D7.3
Version date:	30/06/2022
Total number of pages:	27
Abstract:	<p>This task will plan and execute external communication of the project results, through a variety of channels. At the beginning of this task, the project consortium will specify the project's communication strategy and a time plan, which will be re-assessed and refined periodically, including 1) development of a communication plan, 2) identification of communication activities, 3) organisation, and implementation per partner or jointly among partners 4) impact assessment analysis, and 5) participation of the consortium in various events related to the theme of the project. This task will also include the development of an external project website hosted at www.energyshield.eu, that will be used both for communication and dissemination purposes. The website will include a description of the project, the consortium, and the field trials. A partner-restricted information repository will be hosted at SIMAVI for project internal communication and collaboration. During the project, regular external communications will be made via ongoing media activities, newsletters, or presence at industry seminars.</p>
Keywords	Communication plan, strategy, goals, audience, channels, content

AUTHORS

Name	Organisation	Role
İsmail Bütün	KTH	Overall Editor
Robert Lagerström	KTH	Manager Editor
José Eduardo Urrea Cabus	KTH	Section Editor
Otilia Bularca	SIMAVI	Section Editor
Anna Georgiadou	NTUA	Section Editor

REVIEWERS

Name	Organisation	Role
Milena Sultina Kovacheva	DIL	Overall Reviewer
Roy D'Souza	FOR	QA Reviewer

VERSION HISTORY

0.1	05/03/2022	Table of content
0.2	05/05/2022	Editing section on collaboration
0.3	20/05/2022	Editing section on collaboration
0.4	10/06/2022	Editing section on collaboration
0.5	27/06/2022	Editing section on collaboration
1.0	30/06/2022	Final version released to the EC

EXECUTIVE SUMMARY

This report summarizes the activities performed by EnergyShield consortium partners to communicate the project during the third year of implementation.

EnergyShield's communication plan aims at communicating the project results and developing an ecosystem of partners along the value chain, in order to guarantee a sustainable impact of the project upon completion. All consortium partners of the EPES value chain validate the technology and disseminate the project results to their industry.

The direct beneficiaries of the improvements proposed via the EnergyShield project are the European energy generator, transmission (TSO), and distribution (DSO) operators, as well as the final consumers. The results of the research and innovation activities performed as part of the EnergyShield project were shared with stakeholders via 18 publicly available reports along the project lifetime

Relevant European expertise to build a sustainable community that foster future security research in the energy domain via conventional approaches like publications, conferences, industry forums, workshops, and standardization bodies were considered for pure R&D dissemination of knowledge

Consortium partners successfully communicated along their established channels and promoted the project along with their networks and at domain-specific events. The industrial partners presented the project to stakeholders while the academic partners continued to publish and present their outcomes at scientific venues.

Due to Covid-19, the project partners have shifted their communication efforts to digital venues and continue to communicate digitally with small a small number of face-to-face or hybrid events attendance.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
List of figures	6
List of tables	7
Acronyms	8
1. Introduction	9
1.1. Scope and objectives	9
1.2. Structure of the report	9
1.3. Task dependencies	9
2. Communication approach & strategy updates.....	10
3. Conducted Communication Activities	12
3.1. Activities per channel of distribution	13
3.1.1. Website	13
3.1.2. Twitter	14
3.1.3. LinkedIn.....	15
3.1.4. Newsletter	15
3.2. Activities per Partner	16
3.2.1. SIMAVI	16
3.2.2. PSI	17
3.2.3. KT	18
3.2.4. KTH.....	18
3.2.5. NTUA	19
3.3. Accomplished Activities	20
3.4. EnergyShield Closing Event.....	21
4. Conclusion	25
References.....	26

LIST OF FIGURES

Figure 1. EnergyShield project approach to communication [ESC19]	10
Figure 2. EnergyShield Website page	14
Figure 3. EnergyShield Twitter page	15
Figure 4. EnergyShield LinkedIn page	15
Figure 5. Excerpt of one of our newsletters.	16
Figure 6. Excerpt of the EnergyShield closing event ad, main website	23
Figure 7. Excerpt of the EnergyShield closing event ad, Twitter	23
Figure 8. Newsletter EnergyShield closing event ad	23
Figure 9. Form for EnergyShield closing event registration form.....	24
Figure 10. EnergyShield online final event overview	24

LIST OF TABLES

Table 1. Summary of conducted communication activities	12
Table 2. EnergyShield accomplished communication activities	20
Table 3. EnergyShield outline closing event	21

ACRONYMS

ACRONYM	DESCRIPTION
CEZ	CEZ Distribution Bulgaria
CITY	City University London
CoTTP	Cogen Zagore Ltd
D	Deliverable
DIL	D I L DIEL Ltd aka Goldline
DSO	Distribution System Operator
EPES	Electrical Power & Energy Systems
ESO	Bulgarian Electricity System Operator EAD
EUW	European Utility Week
FOR	foreseeti AB
IREN	IREN S.p.A.
KPI	Key Performance Indicator
KT	Konnekt-able Technologies
KTH	KTH Royal Institute of Technology
L7D	L7Defense
M	Month
MIG	MIG 23 Ltd
NTUA	National Technical University of Athens
PSI	PSI Software AG
R&D	Research and Development
SC	Software Company Limited
SIGA	Si-Ga Data Security Ltd
SIV	Software Imagination & Vision Romania
T	Task
TEC	Tech Inspire Limited
TSO	Transmission System Operator
VETS	VETS Lenishta OOD
WP	Work package

1. INTRODUCTION

1.1. SCOPE AND OBJECTIVES

WP7 Communication, Dissemination & Ecosystem Development focuses on the dissemination of project results and the development of an ecosystem of partners along the value chain and includes reports referring to both strategy and progress per communication, dissemination, and collaboration activities. The objective of this deliverable is to illustrate the outcomes of the communication plan and execution of both internal and external communication of the project results through a variety of channels during the third year of the project.

1.2. STRUCTURE OF THE REPORT

The report is structured into 3 main parts covering strategy update, activities performed per channels of distribution together with planned activities, and planned communication and collaboration activities.

Firstly, the communication strategy is recalled and the COVID-19 adjustments from last year are shortly illustrated.

Secondly, the conducted communication activities are briefly introduced together with provisioned activities. The activities performed are presented as follows: per channels of distribution (involving multiple partners) and initiated by single consortium partners.

Lastly, the report concludes with the communication outcomes at the end of the third reporting period.

1.3. TASK DEPENDENCIES

D7.3 took over and updated the communication strategy proposed in D7.1 [ESC19] and D7.2 Communication Plan [ESC20] and is continued in D7.9 [ESC21]. The outcomes of T7.1 Communication Plan are used to present the performance per KPIs in D7.5 [ESD20], D7.10 [ESD21], and D7.6 [ESD22] Dissemination report.

The T7.4 EU collaboration report contributions have been referred to as the D7.8 collaboration report [ESC22], which provides updates on proposed activities to collaborate with other H2020 projects, create synergies, and ensure cross-fertilization.

WP8 Exploitation & Scale Up builds upon both the dissemination and communication activities and aims at scaling them up beyond the project horizon.

2. COMMUNICATION APPROACH & STRATEGY UPDATES

In general, the situation regarding COVID has not changed since the submission of the last report, and the EnergyShield Consortium continued to communicate the results via digital means. Therefore, no significant adjustments were made to the communication strategy as the results obtained during the previous reporting period were meaningful and ensured progress towards the anticipated performance indicator. A brief overview of the strategy is presented in the following as an introduction to the performed activities.

As introduced in D7.1 Communication Plan [ESC19], the communication plan for the EnergyShield project focuses on goal setting, targeted audience, message definition, and channel selection. The actions are distributed and focused on creating and building awareness in the first two years of project implementation, while in the last one, they focus on raising awareness of the outcomes of the project.

The overall communication strategy is governed by a tri-folded concept alongside a two-step implementation proposal as detailed in Figure 1, below.

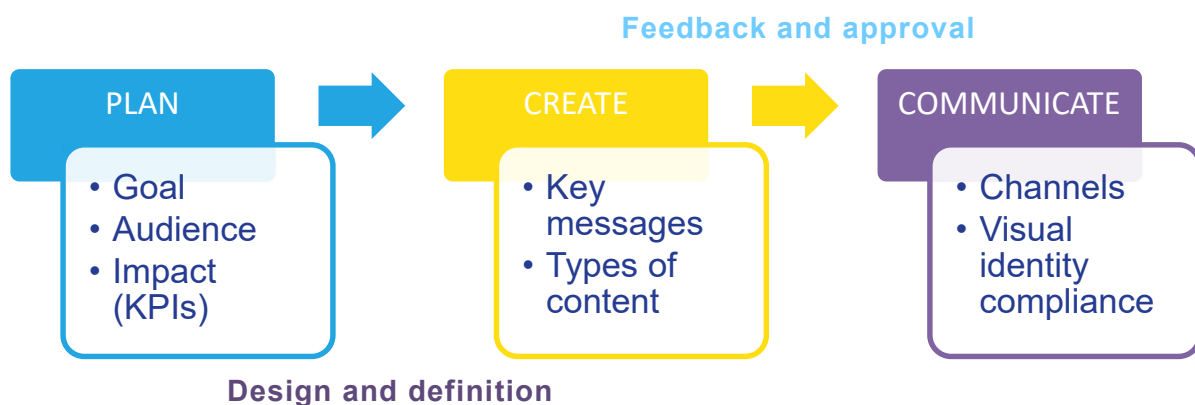


Figure 1. EnergyShield project approach to communication [ESC19]

The direct beneficiaries of the improvements proposed via the EnergyShield project are the European electrical energy generators, transmission (TSO), and distribution system operators (DSO), as well as prosumers and consumers. The EnergyShield consortium covers the entire EPES value chain. This means that the stakeholder backbone has been in place since the beginning of the project.

The selected types of content to promote the EnergyShield project are press releases, scientific papers, whitepapers, and video projects.

To better reach out to the stakeholders, the consortium partners have started introducing the EnergyShield project to multi-project online workshops and conferences; adhered to hubs and working groups focusing on energy and cybersecurity; published scientific articles; and created a project video.

In terms of channels, the EnergyShield consortium focused on the project website, Twitter, and LinkedIn groups but also considered partners' communication channels and Youtube for disseminating the video project.

The **effectiveness** of planned communication activities is measured using KPIs (Key Performance Indicators), which are reviewed monthly and consolidated every six months. The D7.6 Dissemination Report Final [ESD22] includes the progress per KPIs.

The results of the research and innovation activities performed as part of the EnergyShield project are shared with stakeholders via 18 publicly available reports during the project's lifetime. The public reports are published on the project website following the approval of the European Commission.

Because of COVID-19, the project partners' communication efforts have shifted to digital venues, which have taken the place of previously planned in-person meetings. Furthermore, the dissemination materials are posted on the project website and distributed through social media channels.

In the following sections, both the performed and provisioned activities are assessed from a qualitative perspective, i.e., the messages shared with the general public and relevant stakeholders are summarized. In addition, the status of collaboration with other H2020 projects is presented.

It is necessary to note that certain tasks in this project are inside the EU's restricted category. As a result, those tasks and deliverables that are subject to EU constraints are transmitted to PO over secure channels.

3. CONDUCTED COMMUNICATION ACTIVITIES

This section provides a brief overview of the communication activities carried out during the reporting period, together with provisioned activities. The activities performed are presented as follows: joint activities, like a commonly organized workshop, and activities conducted by single consortium partners.

This report focuses on qualitative reporting, while the dissemination report Final, D7.6 [ESD22] focuses on quantitative analysis.

Table 1, summarizes the communication activities performed during the third year of the project.

Table 1. Summary of conducted communication activities

Channel	Involved Partners	Scope	Audience	Outcome
Website	All	Central repository and information source for the project	All	~250 unique visitors per month
Twitter	All	Communicate recent activities	Industry, Research, Other	>600 followers
LinkedIn	All	Communicate with industrial stakeholders	Industry	>90 members
Newsletter	All	Summarize the latest outcomes of the project	Industry, Consumer	9 newsletter and 127 subscribers
Bridge Initiative	All	Identify possible synergies with other projects	Research	Ongoing
Cyberwatching EU	All	Make the project visible to the cyber security domain	Industry, Research	Ongoing, Project of the Week January 2021
Enlit Europe	All	Make the project visible to the energy domain	Industry, Research	Ongoing
Webinar	FOR, PSI	Communicate recent activities	Industry, Research	>90 participants
Seminar/ Webinar	KTH	Communicate recent activities at SCADA-säkerhet	Industry, Research	>200 participants
Webinar	CITY	Present the latest research on cyber security in the energy sector	Industry, Research	3 sessions on different topics

Webinar	SIM, NTUA, PSI, FOR	Communicate recent activities	Industry, Research	>130 participants
Scientific Articles	CITY, KTH, NTUA	Publish scientific outcomes	Research	31 articles
BioBioEnergia	SIM	Communicate the project to the energy sector	Industry	More than 600 participants at the conference
Internal communication	KTH	Present KTH's role in the project	Research	A workshop on Horizon projects
#290CyberSecurity	KTH	Raise cyber security awareness of pupils	Other	Teaching several classes
Industry workshop	PSI	Present the project to PSI's control system customers	Industry	>600 participants
Academic presentation	PSI	Present the project to master students	Research	>60 participants

All EnergyShield partners have contributed to increasing the visibility of the project by using project communication channels and/or organisation channels as presented in the table above. These actions have contributed to increasing the visibility of the project and introducing the commitments of the EnergyShield project to relevant stakeholders.

3.1. ACTIVITIES PER CHANNEL OF DISTRIBUTION

The activities conducted by multiple EnergyShield partners per channel of distribution are presented in this sub-section.

3.1.1. WEBSITE

The EnergyShield **website** (<https://energy-shield.eu>) serves as the central repository for project key communication artifacts and as the primary information source for EnergyShield's target audience, see Figure 2. In order to encourage more visits to the website, partners began to provide additional information on each partner's contributions, such as a more detailed description of the tools and an overview of partner projects. As a result, it attracted the attention of stakeholders.

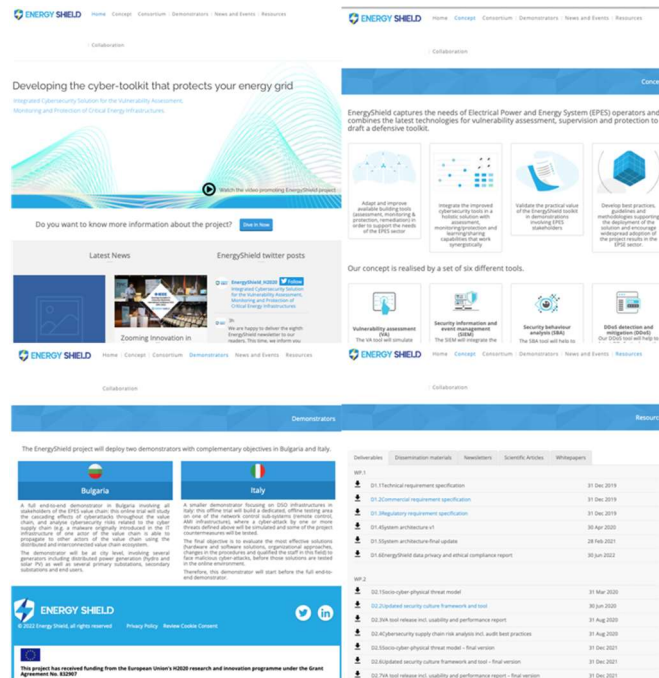


Figure 2. EnergyShield Website page

3.1.2. TWITTER

To ensure a continuous flow of information to stakeholders, the EnergyShield **Twitter** channel (@EnergyShield_) was created when the project started, see Figure 3. Since then, Twitter has been used to notify followers of all dissemination and communication activities and to promote the events organised by the consortium.

It has been demonstrated to be an effective method of communication and event identification. More than 600 Twitter users are EnergyShield followers. This group includes consortium partners, organizations, H2020 projects, and experts in energy and cybersecurity.



Figure 3. EnergyShield Twitter page

3.1.3. LINKEDIN

An important channel to communicate with industrial stakeholders is the **LinkedIn Group**. A group called “Energy Shield” has been created on LinkedIn. So far, this group has more than 110 members and is used to exchange recent news on security-related issues and events related to the project.

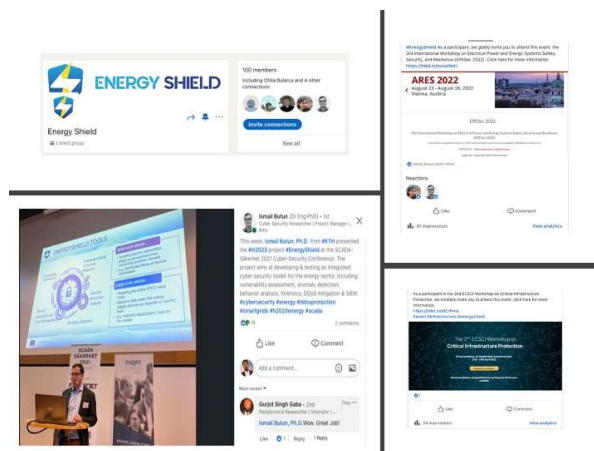


Figure 4. EnergyShield LinkedIn page

3.1.4. NEWSLETTER

We publish a newsletter regularly, in which we tell readers about the most recent actions of our initiative. In addition, we summarize the most recent deliverables that have been submitted and sketch-out forthcoming activities. Figure 5 shows an example of a newsletter.

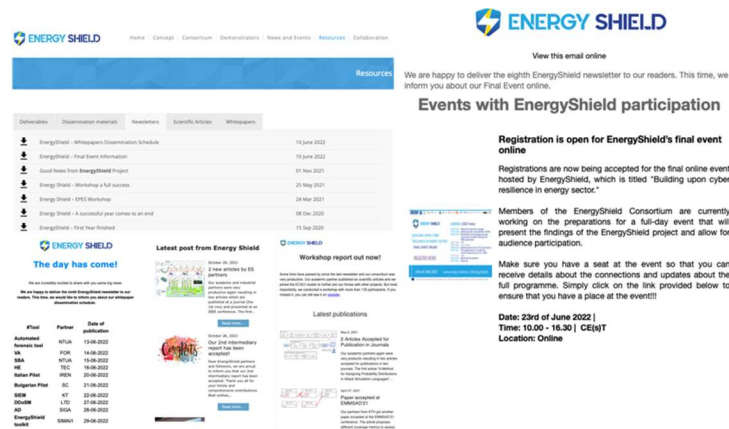


Figure 5. Excerpt of one of our newsletters.

During the first review meeting, it was noted that there is an opportunity for improvement in the number of people who subscribe to our newsletter. Because of this, we stepped up our efforts to reach out to new subscribers, which increased up to 127 subscriptions in a certain year.

3.2. ACTIVITIES PER PARTNER

3.2.1. SIMAVI

SIMAVI attended several standardization events in the last year of the project:

- 1) PANTERA & SUPEERA joint workshop: “Boosting the R & I activity on Smart Grid Technologies” on-demand, held in Split and Bol (island of Brac), Croatia, on September 8–11, 2021. The objectives to be achieved during the workshops were to declare policies for achieving a low-carbon economy. However, the following areas are still a concern in achieving carbon neutrality, and they were addressed in this workshop that brought together stakeholders in the fields of smart grids, storage, and local energy systems.
- 2) “Biobío Energía 2021”, the energy sector forum in Latin America, was held from Chile by streaming on October 19, 2021. Among other things, the program looked at energy efficiency, the energy transition, ways to work together and encourage foreign investment, industry 4.0, smart cities, innovation, and the newest digital technologies.
- 3) “The Role of Standardization for Fostering the Digitalization of the Electricity Grid” in Brussels, Belgium on November 3, 2021. The main aim of the online event was to identify industrial challenges and standards needs within the CROSSBOW framework and synergies with the PHOENIX Project regarding the standardization topic. Further, identify synergies with the PHOENIX H2020 Research and Innovation Project in terms of standardization and allow a better understanding of the

landmarks for the mandatory development of new standards, based on the results of the two projects.

- 4) “Cybersecurity Standardisation Conference 2022” held in Brussels, Belgium on March 15, 2022. The conference aimed to foster dialogue among policymakers, industry, research, and standardisation organisations, given the effective implementation of the EU cybersecurity legislation. The event attracted 3000 registered experts in 2022.

Moreover, SIMAVI attended the 2nd International Workshop on Cyber-Physical Security for Critical Infrastructure Protection (CPS4CIP 2021) held in Darmstadt, Germany on October 04–08, 2021. CPS4CIP 2021 is the second workshop on cyber-physical security, which aims to protect the critical infrastructures that support finance, energy, health, air travel, communication, gas, and water.

The purpose of SIMAVI’s participation in the 2nd ESCI-workshop CyberKit4SME Synergy was to create a collaborative environment across similar EU initiatives, such as Energy Shield, Geiger, Curex, Protego, PLANTIR, TRAPEZE, and AI4HealthSEC, in order to find methods to incorporate the outcomes of other projects into Cyber-Kit4SME while also providing great potential to expand the project's impact under the understanding of cyber security in SMEs and MEs’ design.

Furthermore, EnergyShield’s primary achievements were presented at the “Trends in Managing Current Security and Predictive Maintenance Challenges in Smart Energy Grids in Romania” workshop on April 29, 2022. The workshop was arranged by the Bucharest Electrical Engineering Faculty (www.electro.upb.ro) and various companies. to the final event.

Results of EnergyShield project were shared by SIMAVI between the 14th and 16th of June, the event Critical Infrastructure Protection & Resilience Europe 2022 at the Parliament Palace in Bucharest.

Also, SIMAVI leaded the organization of the final event “Building upon cyber resilience in energy sector” on the 23rd of June 2002. Industry and academia representatives were invited and almost 100 persons attended the event.

3.2.2. PSI

PSI participated in BMBF Innovation Forum “Civil Security” on May 3rd and 4th, 2022, in Berlin, Germany organized by the Federal Ministry of Education and Research. The two-day conference has the motto “Prepared for Tomorrow: Shaping the Future of Civil Security”. The federal government’s framework program “Research for Civil Security” has been dealing with the global challenges of civil security since 2007. Actors in civil security research are working on application-oriented solutions in order to implement strategic goals such as improving social resilience, dealing with natural disasters, increasing the resilience of critical infrastructures, and improving protection against terrorism and crime. Session 6: Security research as a tool to protect critical infrastructures in Europe, was showing what contribution, in particular, European se-

curity research can make to the resilience of critical infrastructures (KRITIS). Protection against natural hazards as well as man-made threats must be addressed. The aim was to discuss with experts what contribution civil security research can make to the European CER Directive, how the interactions between physical and cyber threats can be researched, and what the special features are for the successful transfer of results in the field of KRITIS.

Matthias Rohr participated in the panel “security research for the protection of critical infrastructures” to present EnergyShield. Many participants from research and standardization were expected and the event was fully booked. Further, a university seminar/lecture will be held on 2022-06-07 at the Technical University of Dortmund as part of Dr.-Ing. Ulf Häger’s lecture “Smart Grids”. Matthias Rohr gave a presentation/discussion on smart grids, including some points about EnergyShield. The majority of participants were master’s level electrical engineering students. The theme of this seminar/lecture was “Cybersecurity is an essential part of future smart grids”. We also had similar events in 2020 and 2021 – presentations as part of the university course on smart grids at TU Dortmund.

3.2.3. KT

A presentation on Konnekt-able Technologies’ SIEM Solution for critical infrastructures was made during the virtual 2nd ECSCI workshop (European Cluster for Securing Critical Infrastructures), which took place on April 27-29, 2022. Several approaches to integrating cyber and physical security in different industrial sectors were presented during the workshop. These included energy and transport, water supply and wastewater treatment and disposal, health care, digital infrastructure, banking, and financial markets, space exploration, and public administration. The presentation of novel techniques in the areas of integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, distributed ledger technologies for security information sharing, and increased automation in the areas of detection, prevention, and mitigation measures, on the other hand, was particularly noteworthy.

Moreover, KT participated in the International Conference on Cyber Security and Resilience, which took place in Rhodes, Greece between July 26–28, 2021. The IEEE conference focused on theoretical and practical aspects of security, privacy, trust, and resilience of networks, systems (including complex cyber-physical systems – CPS), applications, and services, as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber-attacks. During the conference, KT presented a paper about EnergyShield’s SIEM Tool, part of the EnergyShield solution toolkit.

3.2.4. KTH

KTH took part in the seminar “Security Assessment of Connected Devices”, where a framework denominated “PatrIoT” was developed. The “PatrIoT” framework consists of four steps: planning, threat modelling, exploiting, and reporting. To validate the

proposed framework, the project involved hacking a connected house, which was carried out by undergraduate and graduate students under the supervision of Ph.D. students, postdocs, and professors.

In addition, KTH participated in the SCADA-säkerhet event held on September 13–14, 2021, where the most pertinent information regarding the Energy Shield project, “Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring, and Protection of Critical Energy Infrastructures”, was presented by Ismail Bütün, with the assistance of Simon Hacks, Robert Lagerström, and Otilia Bularca. Later, Dr. Ismail Butun, under the management of Assoc. Prof. Robert Lagerström, from KTH, has presented the EnergyShield project at a Horizon Europe event organised by KTH Research Office to give hints on dissemination and communication activities (on November 25th, 2021). KTH contributed also to several scientific publications [\[BIAS21\]](#) and [\[EVRL22\]](#) during the last year.

KTH published several scientific conference papers. Moreover, three more manuscripts were submitted and two of them are already presented:

- Security Considerations for Remote Terminal Units, IEEE Zooming Innovation in Consumer Electronics International Conference 2022 (ZINC 2022), May 2022, (Presented).
- Towards Smart Sensing Systems: A New Approach to Environmental Monitoring Systems by Using LoRaWAN, IEEE Zooming Innovation in Consumer Electronics International Conference 2022 (ZINC 2022), May 2022, (Presented).
- Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis, the 17th International Conference on Availability, Reliability and Security (ARES 2022), Aug 2022, (currently undergoing review).

3.2.5. NTUA

NTUA, as leader of Task 7.4 – EU Collaboration, initiated, facilitated, and participated in numerous collaboration activities and events, communicating the EnergyShield’s goals, innovations, and results, e.g. the International Workshop on Electrical Power and Energy Systems Safety, Security, and Resilience (EPESec 2021), the 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021), the 2021 IEEE International Conference on Big Data (Big Data), and many others as presented in detail in D7.8 – Collaboration Report.

NTUA has been invited to participate in research on insider threats conducted on behalf of the UK Government. The specific research examines the existing indicators and frameworks that have been developed to understand and predict insider threat activities.

The CyberSecurity Culture Framework and Security Behaviour Analysis Tool, developed in the context of the EnergyShield project, meeting the criteria of this endeavor, were discussed in detail in an hour-long interview. Our approach and focus on the

human-related cyber-security factors, as presented in our various scientific publications, were analysed and our findings from the numerous CSC framework applications were presented.

NTUA published several scientific articles in the last year of the project [TK21], [TK21], [HB21], and [GF22]. Moreover, three more manuscripts are submitted to journals and conferences (currently undergoing review):

- Cyber-Security Culture Assessment in Academia: A COVID-19 Study
- A Cyber-Security Culture Evaluation in the Energy Sector
- Evaluating The Cyber-Security Culture of the EPES Sector

3.3. ACCOMPLISHED ACTIVITIES

This chapter provides a summary of the activities that were developed in conjunction with the ongoing research being conducted by the EU and the EnergyShield project during the closing ceremony. The purpose of this effort is to present the most pertinent outcomes from the project's applications as well as use the contacts that consortium partners who are involved in other relevant EU research projects and industry groups can provide.

Table 2 summarized the accomplished activities per channel and involved partners during the last year of implementation..

Table 2. EnergyShield accomplished communication activities

Venue	Description	Date	Involved partners
EPES SPR	KT handed in an article on enhancing the SIEM tool for EPES demands	Jul-21	KT
EPESec 2021	Joint publication of KTH and NTUA on the mapping between SBA and VA	Aug-21	KTH, NTUA
SCADA säkerhet	Presentation of current developments in the project	Sep-21	KTH
CPS4CIP 2021	SIMAVI – presentation of current developments in the project NTUA – co-organizing the workshop	Oct-21	NTUA, SIMAVI
IEEE Big Data 2021	NTUA handed in an article on the forensic tool	Dec-21	NTUA

ECISSP2022	A workshop inside the event is considered the 8th international conference on Information System Security and Privacy	Feb-22	SIMAVI
2nd ECSCI Workshop 2022	Participated in the virtual 2nd in ECSCI workshop (European Cluster for Securing Critical Infrastructures)	Apr-22	NTUA, KT
BRIDGE	General Assembly (Online)	Mar-22	SIMAVI
CIPRE2022	Critical Infrastructure Protection & Resilience Europe	Jun-22	SIMAVI
Final Event	Building upon cyber resilience in energy sector	June-22	SIMAVI, all

3.4. ENERGYSHIELD CLOSING EVENT

On June 23, 2022, there was a virtual event “Building upon cyber resilience in energy sector” workshop that served as the concluding event for the review of the EnergyShield project. Participants, including representatives from 20 countries and the European Union (EU), UN organisations, and related domestic and overseas organisations, confirmed that the EnergyShield project captures the needs of Electrical Power and Energy System (EPES) operators and combines the most recent technologies for vulnerability assessment, supervision, and protection in order to draught a defensive toolkit. The outline of the closing event is presented in Table 3.

EnergyShield’s project efforts were based on important synergies and project clustering, which enabled the sharing and exchange of knowledge and experience among security professionals and experts, academics and researchers, policy-making representatives, and regulatory parties, ultimately increasing the project’s results and promoting their communication, dissemination, and exploitation.

Table 3. EnergyShield outline closing event

Time (CEST)	Session(s)	Speaker(s)
10.00 -11.30	Welcome <ul style="list-style-type: none"> Keynote speech from DG CNECT Project overview - Shielding the power grid from cyberattacks 	CNECT, SIMAVI
11.30-12.00	Addressing the vulnerabilities of EPES	FOR, NTUA

	<ul style="list-style-type: none"> VA + SBA tools presentation- focusing on the integration of those tools 	
12.00-12.45	Monitoring and managing security and privacy incidents through the EPES value chain <ul style="list-style-type: none"> AD + DDoSM + SIEM tools presentation and outcomes/results consolidation 	SIGA, L7D, KT
12.45-13.00	Q&A	
13.00– 14.00	Lunch break	
14.00-14.30	Deploying the tools in OT environment <ul style="list-style-type: none"> Bulgarian and Italian pilots presentation – focus on the lessons learned, challenges, 	SC, IREN
14.30-15.15	The opportunity of a toolkit for Critical Infrastructures (CI) / EPES <ul style="list-style-type: none"> Energy Shield toolkit, dashboards + SIEM Exploitation strategy & business cases 	SIMAVI, KT, PSI
15.15-15.30	Q&A	
15.30 -16.15	Reaching the audience <ul style="list-style-type: none"> Communication, dissemination, collaboration, standardization/policy Presentation of European Cluster for Securing Critical Infrastructures (ECSCI) - https://www.finsec-project.eu/ecsci Presentation of Cybersecurity Innovation Cluster for EPES (CyberEPES) https://cyber-seas.eu/cyberepes/ 	KTH, NTUA, PSI
16.15-16.30	Q&A / Wrap-up	

The final event was disseminated through the EnergyShield website (see Figure 6), as well as social media platforms such as Twitter (see Figure 7), in order to reach the stakeholders in a massive way. In addition, a newsletter was published and sent out to the people who had subscribed to receive it, see. Within the newsletter, the link to register for the online event was included, see Figure 8. In order to take part in the event, attendees were required to register for it using the form that is depicted in Figure 9 and Figure 10 presents an overview of the online final event.

08 Jun 2022 Registration open for EnergyShield's final event online

Written by Otilia B Category: Events, News

Registrations are now open for EnergyShield's final event online "Building upon cyber resilience in energy sector ". [Book your seat](#) to the event to receive connection details and updates about the full program.

A full day event to present the results of the EnergyShield project and to interact with the audience is prepared by EnergyShield Consortium members.

AGENDA (CEST time)

AGENDA (CEST time)	
10.00-11.30	Welcome & keynote message
11.30-12.00	Addressing the vulnerabilities of EPES
12.00-12.45	Monitoring and managing security and privacy incidents through the EPES value chain
12.45-13.00	Q&A 13.00-14.00 Lunch break
14.00-14.30	Deploying the tools in OT environment
14.30-15.15	The opportunity of a toolkit for Critical Infrastructures (CI) / EPES
15.15-15.30	Q&A
15.30-16.15	Reaching the audience
16.15-16.30	Wrap-up

Looking forward to seeing you at the event!

[PREVIOUS POST](#)

Figure 6. Excerpt of the EnergyShield closing event ad, main website

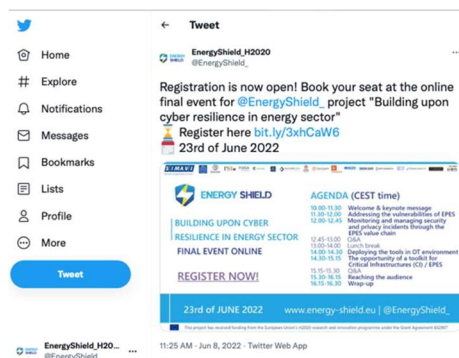
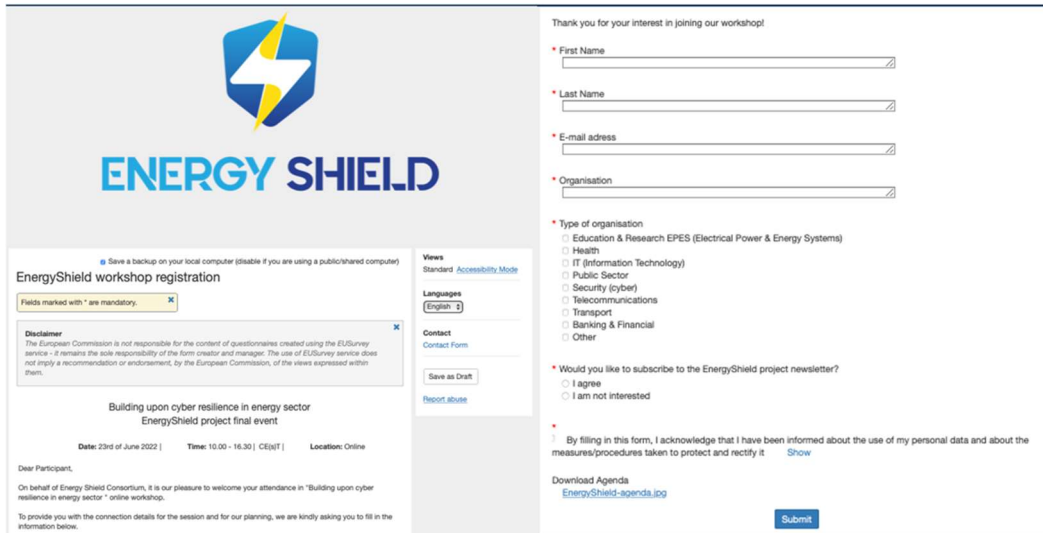


Figure 7. Excerpt of the EnergyShield closing event ad, Twitter



Figure 8. Newsletter EnergyShield closing event ad



ENERGY SHIELD

Save a backup on your local computer (stable if you are using a public/shared computer)

EnergyShield workshop registration

Fields marked with * are mandatory.

Disclaimer
The European Commission is not responsible for the content of questionnaires created using the ESurvey service - it remains the sole responsibility of the form creator and manager. The use of ESurvey service does not imply a recommendation or endorsement, by the European Commission, of the views expressed within them.

Building upon cyber resilience in energy sector
EnergyShield project final event

Date: 23rd of June 2022 | Time: 10:00 - 16:30 | CE[ET] | Location: Online

Dear Participant,

On behalf of Energy Shield Consortium, it is our pleasure to welcome your attendance in "Building upon cyber resilience in energy sector" online workshop.

To provide you with the connection details for the session and for our planning, we are kindly asking you to fill in the information below.

Views
Standard Accessibility Mode

Language
(English)

Contact
Contact Form

Save as Draft
Report abuse

Thank you for your interest in joining our workshop!

* First Name

* Last Name

* E-mail address

* Organisation

* Type of organisation

- ☐ Education & Research EPES (Electrical Power & Energy Systems)
- ☐ Health
- ☐ IT (Information Technology)
- ☐ Public Sector
- ☐ Security (cyber)
- ☐ Telecommunications
- ☐ Transport
- ☐ Banking & Financial
- ☐ Other

* Would you like to subscribe to the EnergyShield project newsletter?

☐ I agree
☐ I am not interested

* By filling in this form, I acknowledge that I have been informed about the use of my personal data and about the measures/procedures taken to protect and rectify it [Show](#)

Download Agenda
[EnergyShield-agenda.log](#)

Submit

Figure 9. Form for EnergyShield closing event registration form



Figure 10. EnergyShield online final event overview

4. CONCLUSION

EnergyShield partners set the basis for successful communication of project progress from the first year of implementation and during the second and third years, the partners continued their efforts, elaborated on activities that were identified to contain improvement potential, and intensified the communication along the working channels.

Consortium partners led communication activities to make the project visible to relevant stakeholders. Workshops, conferences, and webinars were attended by technology providers to share insights about the tools and the toolkit proposed in EnergyShield.

The academic partners submitted scientific articles on the artifacts created in the project and presented the contents in different scientific venues. All the proposed communication channels were used to increase project visibility, and they communicated various materials related to the project through their channels. The communication flow remained on the digital channels as pandemic restrictions and recommendations were still in place. Moving communication exclusively online threatens face-to-face interaction but also creates significant opportunities in terms of coverage and logistics limitations. In particular, the workshops conducted online reached a broad audience.

As the online rules of communication apply to all (audience, facilitator, and promoters), the impact was expected to be mitigated in the forthcoming period. Large events have already been presented online (e.g. European Sustainability Week) and project leaders have also led cross-project stakeholder engagement workshops.

Furthermore, it has intensified the work in joint working groups and organized thematic workshops with projects funded under similar topics. This period was of great importance for using the created visibility of the EnergyShield project and sharing the generated results.

REFERENCES

- [ARRCG] Acarali, Rao, Rajarajan, Chema and Ginzburg, Modelling smart grid IT-OT dependencies for DDoS impact propagation. *Computers & Security*, 112 (2022), p.102528.
- [ESC19] [EnergyShield Consortium \(2019\), D7.1 Communication Plan](#)
- [ESC20] [EnergyShield Consortium \(2020\), D7.2 Communication Report](#)
- [ESC21] [EnergyShield Consortium \(2021\), D7.9 Communication Report v2](#)
- [ESD19] [EnergyShield Consortium \(2019\), D7.4 Dissemination Plan](#)
- [ESD20] [EnergyShield Consortium \(2020\), D7.5 Dissemination Report](#)
- [ESD21] [EnergyShield Consortium \(2021\), D7.10 Dissemination Report v2](#)
- [ESD22] [EnergyShield Consortium \(2022\), D7.6 Dissemination Report Final](#)
- [ESC22] [EnergyShield Consortium \(2022\), D7.8 Collaboration report](#)
- [GA21] Georgiadou, Anna, et al. "Hospitals' Cybersecurity Culture during the COVID-19 Crisis." *Healthcare*. Vol. 9. No. 10. Multidisciplinary Digital Publishing Institute, 2021. <https://doi.org/10.3390/healthcare9101335>
- [TK21] Touloumis, Konstantinos, et al. "Vulnerabilities Manager, a platform for linking vulnerability data sources." 2021 IEEE International Conference on Big Data (Big Data). IEEE, 2021. [doi: 10.1109/BigData52589.2021.9672026](https://doi.org/10.1109/BigData52589.2021.9672026)
- [HB21] Hacks, S., Butun, I., Lagerström, R., Buhaiu, A., Georgiadou, A., & Michalitsi Psarrou, A. (2021, August). Integrating Security Behaviour into Attack Simulations. In *The 16th International Conference on Availability, Reliability and Security* (pp. 1-13). <https://doi.org/10.1145/3465481.3470475>
- [GF22] Gioulekas, Fotios, et al. "A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures." *Healthcare*. Vol. 10. No. 2. MDPI, 2022. <https://doi.org/10.3390/healthcare10020327>
- [BIAS21] Butun, Ismail, and Alparslan Sari. "Early Detection and Recovery Measures for Smart Grid Cyber-Resilience." *Decision Support Systems and Industrial IoT in Smart Grid, Factories, and Cities*. IGI Global, 2021. 91-110. <https://doi.org/10.4018/978-1-7998-7468-3.ch005>
- [EVRL22] Engströma, Viktor, and Robert Lagerströma. "Two Decades of Cyberattack Simulations: A Systematic Literature Review." *Computers & Security* (2022): 102681. <https://doi.org/10.1016/j.cose.2022.102681>

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID



www.energy-shield.eu

