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

D7.9 –COMMUNICATION REPORT V2

	Document info
Contractual delivery	30/06/2021
Actual delivery	30/06/2021
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:	D7.9
Version date:	24/06/2021
Total number of pages:	35
Abstract:	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 course of the project, regular external communications will be made via ongoing media activities, newsletters or presence at industry seminars.
Keywords	Communication plan, strategy, goals, audience, channels, content

AUTHORS

Name	Organisation	Role
Simon Hacks	KTH	Overall Editor
Otilia Bularca	SIMAVI	Section Editor
Anna Georgiadou	NTUA	Section Editor

REVIEWERS

Name	Organisation	Role
Gianluca Serale	IREN	Overall Reviewer
Ana-Maria Dumitrescu	SIMAVI	QA Reviewer

VERSION HISTORY

0.1	16/04/2021	Initial Creation
0.2	22/04/2021	Editing section on collaboration
0.3	27/04/2021	Adding KT's planned activity
0.4	09/05/2021	Updating latest activities
0.5	21/05/2021	Updating SIM activities and removing events from first reporting period
0.6	21/05/2021	Including remarks of IREN
0.7	24/06/2021	Including PSI activities
1.0	30/06/2021	Version released to EC

EXECUTIVE SUMMARY

This report summarizes the activities performed by EnergyShield consortium partners to communicate project activities and results during the second 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 from the project once it is completed. 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 are shared with stakeholders via 18 publicly available reports along the project lifetime.

Considering pure R&D dissemination of knowledge, we are aiming to bring together relevant European expertise to build a sustainable community to foster future security research in the energy domain via conventional approaches like publications, conferences, industry forums, workshops, and standardization bodies.

In the second reporting period, consortium partners successfully continued to communicate along their established channels and promoted the project along 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.

Also, important steps were taken to continue and intensify collaboration with H2020 projects, such as BRIDGE and cyberwatching.eu radar and research hub (joined energy and Critical Insfrastructure clusters). EnergyShield project has joined ESCI and Cyber EPES clusters as foundation members.

Due to Covid-19, the project partners have shifted their communication efforts to digital venues last year and continue to communicate using online means and tools.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

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
RP2	Second Reporting Period (July 2020 – June 2021)
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

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 second year of the project.

1.2. STRUCTURE OF THE REPORT

The report is structured in 3 main parts covering strategy updates, 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 from two perspectives: per channels of distribution – involving multiple partners - and initiated by single consortium partners.

Thirdly, EU collaboration strategy (part of T7.4), accession to working groups and hubs together with forthcoming actions are presented. As T7.4 EU Collaboration leaded by NTUA started in M7 and has a single formal delivery in the last month of the project we are including the progress on this task in the communication report.

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

1.3. TASK DEPENDENCIES

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.

During the second reporting period, D7.2 **[ESC20]** took over and updated the communication strategy proposed in D7.1 Communication Plan [**ESC19**] and are continued in D7.9. The outcomes of T7.1 Communication Plan are used to present the performance per KPIs in D7.5 Dissemination report [**ESD20**].

T7.4 EU collaboration contributes to this report with the progress on the 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 last report and will most probable not change at least until the end of the year. Therefore, consortium partners further aligned the communication strategy considering the results obrained during the last reporting period. However, a short recap is presented in the next paragraphs.

As introduced in D7.1 Communication Plan [**ESC19**] the communication plan for EnergyShield project focuses on goal setting, targeted audience, message definition, and channels selection and the actions are distributed and focusing on to creating and building awareness in the first two years of project implementations, while in the last one focusing on raising awareness on 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.

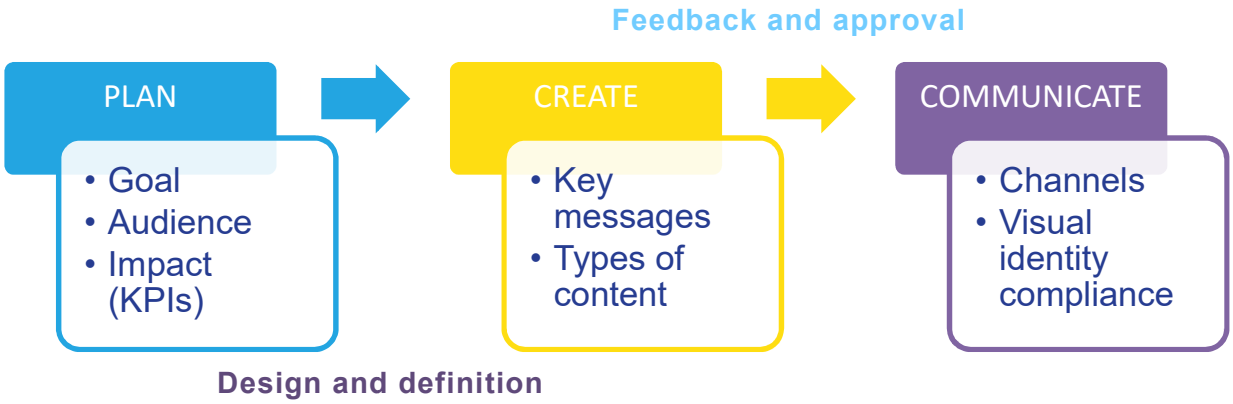


Figure 1. EnergyShield project approach to communication [ESC19]

The direct **beneficiaries** of the improvements proposed via the EnergyShield project are the European electrical energy generator, Transmission (TSO) and Distribution (DSO) System Operators, as well as prosumers and consumers. EnergyShield consortium covers the entire EPES value chain. This means that the stakeholder backbone is in place since the beginning of the project.

The selected **types of content** to promote the EnergyShield project are press release, scientific papers, brochures, white papers and video projects.

To better reach out to the **stakeholders**, the Consortium partners have started introducing 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**, 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 **impact** of the planned communication activities is evaluated via KPIs (Key Performance Indicators) which are evaluated every month and consolidated every

six months. The progress per KPIs is included D7.10 Dissemination Report v2 **[ESD21]**.

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

Due to Covid-19, the project partners have shifted their communication efforts to digital venues that substitute in-person meetings originally planned. Additionally, the dissemination materials are included on the project website and shared via 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 general public and relevant stakeholders are summarized. Also, the progress on collaborating with other H2020 projects is presented.

3. CONDUCTED COMMUNICATION ACTIVITIES

In this section, the conducted communication activities are briefly introduced together with provisioned activities. The activities performed are presented from two perspectives: joint activities, like a commonly organized workshop, and activities conducted by single Consortium partners.

This report focuses on a qualitative reporting, while the dissemination report, D7.10 **[ESD21]** focuses on a quantitative analysis.

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

Table 1. Summary of conducted communication activities in RP2

Channel	Involved Partners	Scope	Audience	Outcome RP2
Website	All	Central repository and information source for the project	All	~100 unique visitors per month
Twitter	All	Communicate recent activities	Industry, Research, Other	>260 followers
LinkedIn	All	Communicate with industrial stakeholders	Industry	>60 members
Newsletter	All	Summarize latest outcomes of the project	Industry, Consumer	3 newsletter and 74 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,	Communicate recent	Industry,	>90

	KTH, PSI	activities	Research	participants
Webinar	CITY	Present latest research on cyber security in the energy sector	Industry, Research	3 sessions on different topics
Workshop	SIM, KTH, NTUA, PSI, FOR	Communicate recent project results to stakeholders	Industry, Research, general audience	>130 participants
Scientific Articles	CITY, KTH, NTUA	Publish scientific outcomes	Research	17 articles
BioBioEnergia	SIM	Communicate the project to the energy sector	Industry	More than 600,000 participants at the co gress
Cybersecurity for CI webinar	SIM	Communicate the approach of EnergyShield project in addressing cybersecurity vulnerabilities in the Energy sector	Industry, research	>50 participants
EDDIE webinar	SIM	Preset the project to stakeholders running projects in Innovation and Digitalization of the Energy sector	Industry, research	>50 participants
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	Industry	>600

		to PSI's control system customers		participants
Academic presentation	PSI	Present the project to master students	Research	>60 participants
Conference	ESO	Presnet the project to 9th International Energy Conference - Energy and Cyber Security – Risks and Protections	industry	>50 participants

As presented in the table above all EnergyShield partners have contributed to increasing the visibility of the project via using project communication channels and/or organisation channels. These actions have contributed to increase the visibility of the project and to introduce the commitments of EnergyShield project to relevant stakeholders.

3.1. ACTIVITIES PER CHANNELS OF DISTRIBUTION

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

3.1.1. WEBSITE

EnergyShield **website** (https://energy-shield.eu) serves as the central repository for project key communication artefacts and as the primary information source for EnergyShield's target audience. To incentivise more visits to the website, partners started to provide additional information on the contribution of each partner, a more detailed description of the tools, and an overview of partner projects. The first two activities are still ongoing.

3.1.2. TWITTER

The EnergyShield **Twitter** channel (@EnergyShield_) has been created when the project started to ensure a continuous flow of information towards stakeholders. Since now all dissemination and communication activates have been notified via Twitter.

It has been proved a powerful tool to communicate and identify relevant events. EnergyShield has more than 260 followers on Twitter including consortium partners, organisation, H2020 projects, and experts in energy and cybersecurity.

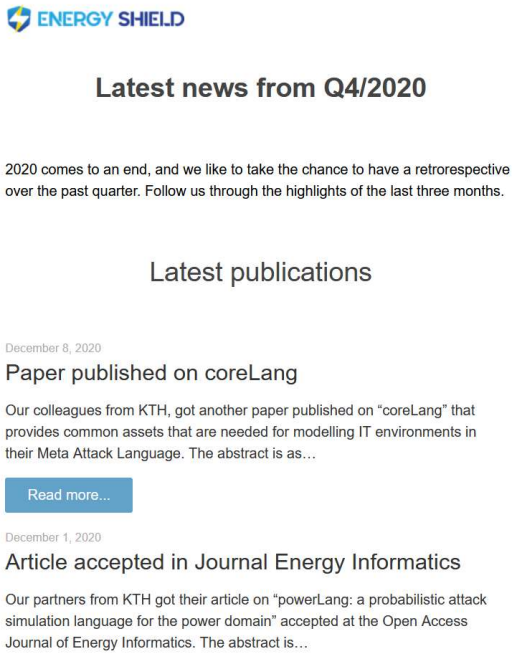
Figure 2. EnergyShield Twitter page

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 60 members and is used to exchange recent news on security related issues and events related to the project.

3.1.4. NEWSLETTER

On a regular basis, we send out a newsletter that informs about the latest activities of our project. Additionally, we summarise the latest submitted deliverables and sketch upcoming actions. A newsletter example is illustrated in Figure 3.


ENERGY SHIELD

Latest news from Q4/2020

2020 comes to an end, and we like to take the chance to have a retrorespective over the past quarter. Follow us through the highlights of the last three months.

Latest publications

December 8, 2020

Paper published on coreLang

Our colleagues from KTH, got another paper published on "coreLang" that provides common assets that are needed for modelling IT environments in their Meta Attack Language. The abstract is as…

Read more...

December 1, 2020

Article accepted in Journal Energy Informatics

Our partners from KTH got their article on "powerLang: a probabilistic attack simulation language for the power domain" accepted at the Open Access Journal of Energy Informatics. The abstract is…

Figure 3. Excerpt of one of our newsletters

During the first review meeting, it was recognized that the number of subscriptions to our newsletter lets room for improvement. Therefore, we intensified our efforts to reach out to more subscribers, which resulted in an increasement of subscriptions from 19 to 74 in one year.

3.2. ACTIVITIES PER PARTNER

All EnergyShield Consortium partners have contributed to communication activities promoting the results of the project via own networks and via organisation social media accounts.

In the sub-sections below the most proeminent and engaging commnunication activities are presented per partner.

3.2.1. SIMAVI

SIMAVI was the main organiser of the workshop held in April 2021 with more than 130 participants The European workshop **Trends, opportunities and choices in designing a cyber resilient EPES infrastructure** on the 15th of April 2021, 10.00 CET was co-organized by KTH and NTUA and supported by PSI and FOR and gathered Critical infrastructure stakeholders, business, academia, and industry professionals from 8 European countries around cross-domain topics. The event visibility was increased by 5 european projects: BRIDGE, CYBERWATCHING.EU, PANTERA, INTEGRIDY and ECHO which endorsed the event. A detailed report [**ESR21**] and the recording [**ESV21**] of the event are available online.

AGENDA – ENERGYSHIELD WORKSHOP 15/04/2021, 10.00 CEST	
Opening sessions	
Welcome and brief introduction of EnergyShield project	Otilia Bularca, SIMAVI
Recent policy developments in cybersecurity for critical infrastructure protection	Christian Wilk, EC
ENISA's activities in the energy sector	Konstantinos Moulinos, ENISA
Bridging the gap between EPES and cybersecurity	Dr. Venizelos Efthymiou, UCY
Combining MAL with safety & functional modelling	Chris Few, Ofgem UK
EnergyShield toolkit demonstration	Iacob Crucianu, SIMAVI; Joar Jacobsson, foreseeti; Anna Georgiadou, NTUA
PANEL 1	**PANEL 2**
Work from home impact on the energy and IT infrastructures	Latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies
Moderator: Tommy Wahlman, Swedish Energy Agency **Panellists:** • Daniela Bichir, SIMAVI • Javier Valiño, ATOS • Prof. David Wallom, Oxford e-Research Centre • Dr. Mihai PĂUN , CRE • Loris Piana, IREN Italy	**Moderator**: Monica Florea, SIMAVI **Panellists:** • Sarah Fluchs, admeritia GmbH • Dr. Ing. Matthias Rohr, PSI • Dan Cîmpean, CERT-RO • Massimiliano Masi, Autostrade per l'Italia • Matteo Merialdo, RHEA Group

Figure 4. EnergyShield online workshop agenda

Additionally, SIMAVI presented the EnergyShield project at the BioBioEnergia conference (October 2020) to a Latin American audience, attened as a panellist to Cybersecurity for Critical Infrastructures - Resilience and trust in the Health and Energy sectors organized by cyberwatching.eu (June 2021), presented the project and Strengthening Education for Sustainable Energy Transition and Digitalization – EDDIE project – stakeholder consultation webinar (Novemebr 2020), participated in the BRIDGE assembly (February 2021), attended 11th and 12th ETIP SNET (April & June 2021) online regional workshops and was invited to present EnergyShield project in the next regional workshop.

Also, SIMAVI has attended several online events to increase project visibility and to catch up with the latest news and opportunities in cybersecurity and energy sector and events organized by other H2020 projects: ERIC forum, online events

organized by ENISA, EC, EASME, DG GROW (European R&I days, Masters of Digital, Advanced Technologies for Industry - Policy Seminar, workshops organized by www.cyberwatching.eu and webinars organized by European IP helpdesk.

3.2.2. PSI

PSI participated in two panel discussions. The first time in a webinar organized by FOR and the second time in the workshop organized by SIMAVI. Additionally, PSI presented EnergyShield and the VA-tool and an adaptation to the energy sector as industry workshop (online) to together approx. 600 PSI control system customers in December 2020. Moreover, they presented the project two times to master students at the TU Dortmund in the lecture “Smart Grids”.

3.2.3. FOR

FOR organized a webinar on July 9, 2020 to present their contribution to the project to an industrial and academic audience in addition to its daily communication on the EnergyShield project along FOR’s channels. Furthermore, FOR presented the VA tool in the workshop organized by SIMAVI and engaged with UK regulator Ofgem to present and pitch the EnergyShield cyber-risk analysis model.

3.2.4. CITY

CITY organized a webinar series on Information Security as a part of a joint workshop between Charusat, India, and CITY and gave a presentation on “Cyber-Security in the Smart Grid Environment”. Additionally, CITY published two articles **[ARC20a]**, **[ARC20b]**.

3.2.5. KTH

KTH participated in the workshop organized by FOR with two presentations. The first one discussed the future of cyber security in the energy sector, while the second presented KTH’s contribution to the vulnerability assessment tool. Moreover, KTH promoted the EnergyShield project in internal events (Horizon Europe week at KTH, lecture on threat modelling) and external events (CS3STHLM, SCADA-säkerhet) and supported SIMAVI in the organization of the workshop held in April 2021. To promote cyber awareness, KTH gave lectures in the #290CyberSecurity initiative. KTH contributed also with several scientific publications **[HHF21]**, **[HK21]**, **[HKLL20]**, **[KHJE20]**, **[LAHL21]**, **[LLE20]**, **[VHLF20]**, **[XHL21]**, **[HBL21]** during the last year.

3.2.6. NTUA

NTUA published several scientific articles **[GMA20]**, **[GMAB20]**, **[GMA21a]**, **[GMA21b]**, **[GMA21c]**, **[GMA21d]**, **[HBL21]**. Moreover, NTUA presented the SBA tool in several workshops such as organized from cyberwatching.eu and the one organized by SIMAVI. For the latter, NTUA supported SIMAVI in the organization of the online EnergyShield workshop in 15ht of April 2021.

3.2.7. L7D

L7D initiated a working relationship with the USA Department of Energy to partner on the energy sector, this included several presentations demonstrating L7 Defense project for the Energy Shield and writing a plan for collaboration.

3.2.8. ESO

ESO has participated in the 9th International Energy Conference on Energy and Cyber Security – Risks and Protections that was held on 11.02.2021, where the project EnergyShield was presented (as part of the presentation "Implemented projects for cyber security in Central Dispatching Center of the national electrical grid")

Figure 5. Slides presented by ESO at 9th International Energy Conference

3.3. PROVISIONED ACTIVITIES

A series of communication activities have been provisioned for the next period of project implementation.

Table 2 includes a tentative list of communication and dissemination opportunities for the last reporting period per channels and involved partners as identified by consortium members.

Table 2. EnergyShield provisioned communication activities

Venue	Description	Date	Involved partners
BRIDGE	General Assembly	tbd	SIMAVI
SCADA säkerhet	Presentation of current developments in the project	September 2021	KTH

CAiSE'21	Presentation of a paper	June 2021	KTH
EMMSAD'21	Presentation of a paper	June 2021	KTH
EPESec	Joint publication of KTH and NTUA on the mapping between SBA and VA Supporting the event and member of the program committee	August 2021	KTH, NTUA, KT, SIMAVI
EPES SPR	KT handed in an article on enhancing the SIEM tool for EPES demands	July 2021	KT
CPS4CIP 202	Members of the programm committee and supporting the event as part of supported by the projects of the European Cluster for Securing Critical Infrastructures (ECSCI)	Tbd	KT, KTH, NTUA
ICISSP2022	A workshop inside the event is considered 8th international conference on Information System security and privacy	Viena, 9-11 february 2022	SIMAVI
ETIP SNET	13th Regional workshop	tbd	SIMAVI

The provisioned activities mainly aim at improving online visibility of project, sharing technical achievements, and engaging relevant stakeholders.

4. EU COLLABORATION ACTIVITIES

This chapter briefly presents the collaboration activities performed and initiated during the second reporting period. As the corresponding task, T7.4 EU Collaboration, leaded by NTUA, started in M7 and has a single formal delivery in the last month of the project, we are including the activities performed and planned in the communication report.

4.1. COLLABORATION PROCESS

As a starting point, a comprehensive and flexible collaboration process has been defined, presented in Figure 6, consisted of 3 distinctive steps:

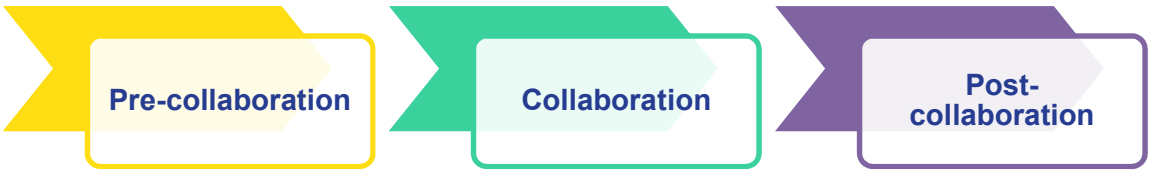


Figure 6. Collaboration process

Pre-collaboration: this step refers to the identification of a new collaboration opportunity and to its reporting via the completion of a collaboration opportunity template. All reports are indexed in a collaboration opportunities repository file, stored in the project file sharing service (Alfresco), and communicated to all consortium partners encouraging creative elaboration, participation and further identification of possible synergies.

Collaboration: this step refers to the actual collaboration activity which could be any of the following:

- co-organize or participate to a workshop / event / webinar / hackathon
- share / join forces on social media communication channels / networking boost
- collaboratively work on a publication
- work together towards a common standardization goal
- exchange know-how / expertise / technical documents
- exchange tools / module developed within each project
- collaboration on the development of a tool
- collaboration on evaluation of the tools
- collaboration on the exploitation / marketing of project's assets
- share a framework or toolkit so as to amplify its features
- share data collections and exchange results

Post-collaboration: this step refers to a reporting collaboration activity undertaken by the participating partners. This activity is possible either via completing a simple collaboration report or by filling the corresponding EU Survey. Reports are again indexed by updating the corresponding collaboration repository file.

4.2. COLLABORATION PERSPECTIVES

During the second semester of the project life-cycle, consortium partners were asked to fill in a brief EU survey reporting any collaboration opportunities identified in order to initiate a collaboration repository. A number of EU projects and initiatives were put forward constructing a rich collaboration pool. Table 3 briefly presents the information gathered.

Table 3. Collaboration Opportunities

Project/Initiative Suggested	Website	Description
SOCCRATES	https://www.soccrates.eu/	SOCCRATES, although it does not focus on the EPES sector, has a similar toolkit setup. The project is bearing a similar life cycle. There are many possibilities of joint activities.
SPHINX	https://sphinx-project.eu/	Exchange know-how and modules of SPHINX Distributed Cyber Situational Awareness Framework & Real Time Risk Assessment.
Infrastructure Resilience - ELVIRA	https://www.his.se/en/research/informatics/distributed-real-time-systems/elvira/	The Elvira project develops time-based infrastructure dependency analysis for the power-grid to model risk assessment and resilience index, which assist decision makers in anticipating failures and their cascading effects.
United Grid	https://united-grid.eu/	The UNITED-GRID project objective is to develop technical solutions to serve needs and opportunities for distribution system operators (DSOs) in their electricity grids.
inteGRIDy	http://integridy.eu/	inteGRIDy aims to integrate cutting-edge technologies, solutions and mechanisms in a Framework of replicable tools to connect existing energy networks with diverse stakeholders, facilitating optimal and dynamic operation of the Distribution Grid (DG), fostering the

		stability and coordination of distributed energy resources and enabling collaborative storage schemes within an increasing share of renewables.
BRIDGE	https://www.h2020-bridge.eu/	BRIDGE is a European Commission initiative which unites Horizon 2020 Smart Grid and Energy Storage Projects to create a structured view of cross-cutting issues which are encountered in the demonstration projects and may constitute an obstacle to innovation. EnergyShield could be part of the proposed working groups and could contribute to the results of the BRIDGE initiative.
FARCROSS	https://farcross.eu/	Present the EnergyShield project targets during the 2020 plenary meeting of FARCROSS which is under the BRIDGE initiative in order to ignite their interest in the project and its results and investigate any possible synergies.
FLEXITRANSTORE	http://www.flexitranstore.eu/	Present the EnergyShield project targets during the 2020 plenary meeting of FLEXITRANSTORE which is under the BRIDGE initiative in order to ignite their interest in the project and its results and investigate any possible synergies.
PHOENIX	https://phoenix-h2020.eu/	Project funded under the SU-DS04-2018-2020 programme and sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).
SDN-microSENSE	https://www.sdnmicrosense.eu/	Project funded under the SU-DS04-2018-2020 programme and sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).
E.DSO-ENCS-ENTSO-E Workshop	https://mailchi.mp/774dd826cbab/edsoencsentso-e-invitation-cybersecurity-	The Association of European Distribution System Operators (E.DSO), the European Network for

	workshop-brussels-22-october-2019-still-possible-to-register-12439756?e=c3907bfe90	Cyber Security (ENCS) and the European Network of Transmission System Operators for Electricity (ENTSO-E) co-organise a Conference on Cybersecurity. The event is scheduled in Brussels on 7 October 2020 and EnergyShield project shall be represented.
ReachOut	https://www.reachout-project.eu/	ReachOut is a Coordination and Support Action (CSA) helping H2020 projects in the area of software technologies to implement beta-testing campaigns. ReachOut act as an operational intermediary between research projects and the open market. ReachOut helps research projects implement beta testing best practices and recruit beta-testers by running promotion initiatives. ReachOut is planning to collaborate with Energyshield for beta-testing tools from the Energyshield toolkit.

Based on the collaboration repository constructed during the first project year and having reached a project and toolkit readiness level suitable for collaborations, partners have initiated a number of collaboration activities with different objectives to communicate EnergyShield project goals and progresses and investigate possible synergies.

4.3. ACTIVITIES PERFORMED

A number of important synergies have been established empowering various collaboration activities. The most important ones are presented in the following paragraphs whereas a detailed list of the materialised collaboration attempts is hosted in the last section.

4.3.1. BRIDGE INITIATIVE

The EnergyShield project attended BRIDGE General Assembly in Brussels on the 11th and 12th of February 2020. As part of this event, the partners introduced the main objectives of the project together with identifying the task forces that could be supported by the project team.

The meeting was a great opportunity for engaging with new and old energy sector projects and for networking with projects aiming to achieve similar results. As a new

BRIDGE project, EnergyShield got the opportunity to present its challenges in a poster session.

EnergyShield Consortium has allocated members in all working groups and is contributing to Action 1 of Data Management - Use case repository.

4.3.2. CYBERWATCHING EU

EnergyShield project was accepted in cyberwatching.eu project hub. In the pre-accession phase, the market and technology readiness were evaluated, and the project was included on the Cybersecurity and Privacy Project Radar.

The Cybersecurity and Privacy Project Radar (https://radar.cyberwatching.eu/radar) provides an overview of the complete collection of EU funded projects in the cybersecurity space. Projects have volunteered in a technology and market readiness assessment by Cyberwatching.eu to different degrees.

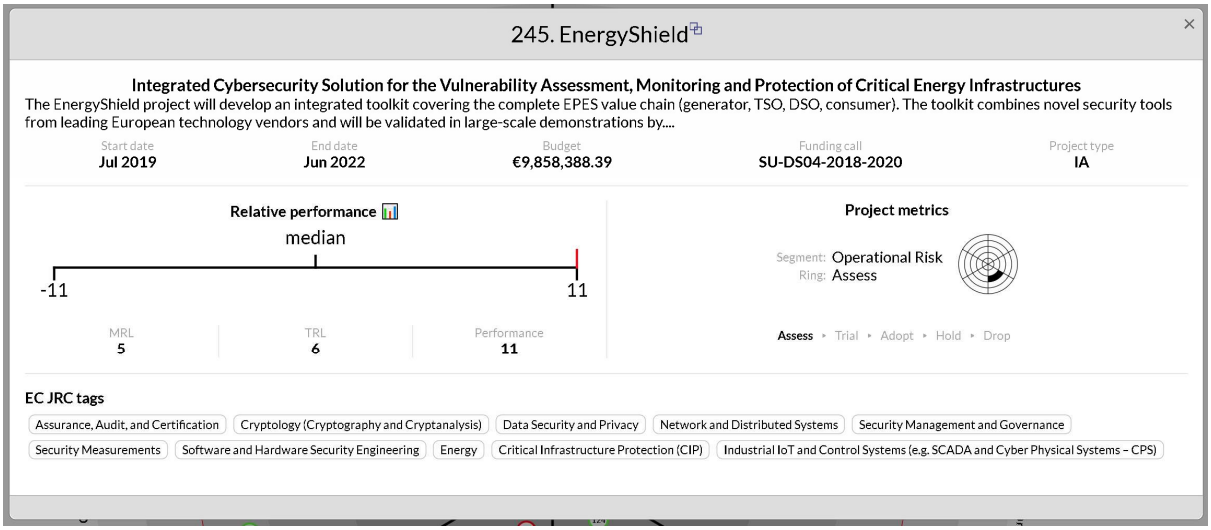


Figure 7. EnergyShield screenshot from cyberwatching.eu radar

As part of the cyberwatchig.eu hub, EnergyShield was promoted as Project of the Week on 18-22 January 2021.

Figure 8. Banner promoting EnergyShield "project of the week"

Also, cyberwatching.eu promoted the events and news related to the progress aof EnergyShield project, while EnergyShield partners attented and contributed to different online events organized or supported by the hub:

- EPES and smart grids: practical tools and methods to fight against cyber and privacy attacks 11th of November 2020
- Cyberwatching.eu workshop on ePrivacy – 10th of May 2021
- How to reactively defend against advanced cyber threats – 20th f May 2021
- Financial Sector Cybersecurity Collaboration and Engagement of Stakeholders – 21st of May 2021
- Swforum.eu Webinar: Market & Technology Readiness Levels – 26th of May 2021

4.3.3. SU-DS04-2018-2020 FUNDED PROJECTS

EnergyShield initiated an attempt bridging the three H2020 EU projects, EnergyShield, PHOENIX and SDN-microSENSE, funded under the SU-DS04-2018-2020 programme and, consequently, sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).

Sisterhood has been created among these projects, and many events and joint attempts have been fruitfully promoting their goals and common objectives.

4.3.4. ECSCI

EnergyShield reached out to the European Cluster for Securing Critical Infrastructures (https://www.finsec-project.eu/ecsci) and joint their effort aiming to participate in the common activities of the ECSCI cluster, such as stakeholders and scientific workshops, joint scientific publications, European common platform for cascading effects on the different critical infrastructures, a platform for combined

safety and security for European critical infrastructures, standards and regulations on the protection of critical infrastructures, etc.

4.3.5. CYBER-EPES

The five projects funded under the call "Cybersecurity in the Electrical Power and Energy System" agreed to join forces in a Cybersecurity Innovation Cluster for EPES (named CYBER-EPES), being an EC initiative. The cluster kick-off virtual event took place on Friday 4 June 2021 with representatives from the Research Executive Agency and European Commission. The cluster participant projects are:

- PHOENIX
- SDN-µSense
- Energy Shield
- CyberSEAs
- ELECTRON

4.3.6. ETIP_SNET

EnergyShield partners have attented the 11th ETIP SNET Regional Workshop on 21st April 2021 submitted and application to present the project at the the **12th ETIP SNET Regional Workshop** that will take place **on 22 June 2021**.

4.3.7. EUROPEAN UTILITY WEEK

The European Utility Week has been rebranded to the unifying forum Enlit: The inclusive guide for the energy transition.The annual trade fair, which will take place in Milan this year (November 30th - December 2nd, 2021) will also have a virtual part - the 365-digital platform.

EU funded projects to disseminate can be disseminated within the EU Projects Zone to raise awareness and gain visibility for the project's research and findings in various ways. EnergyShield project has alos joined the EU Projects zone of Enlit.

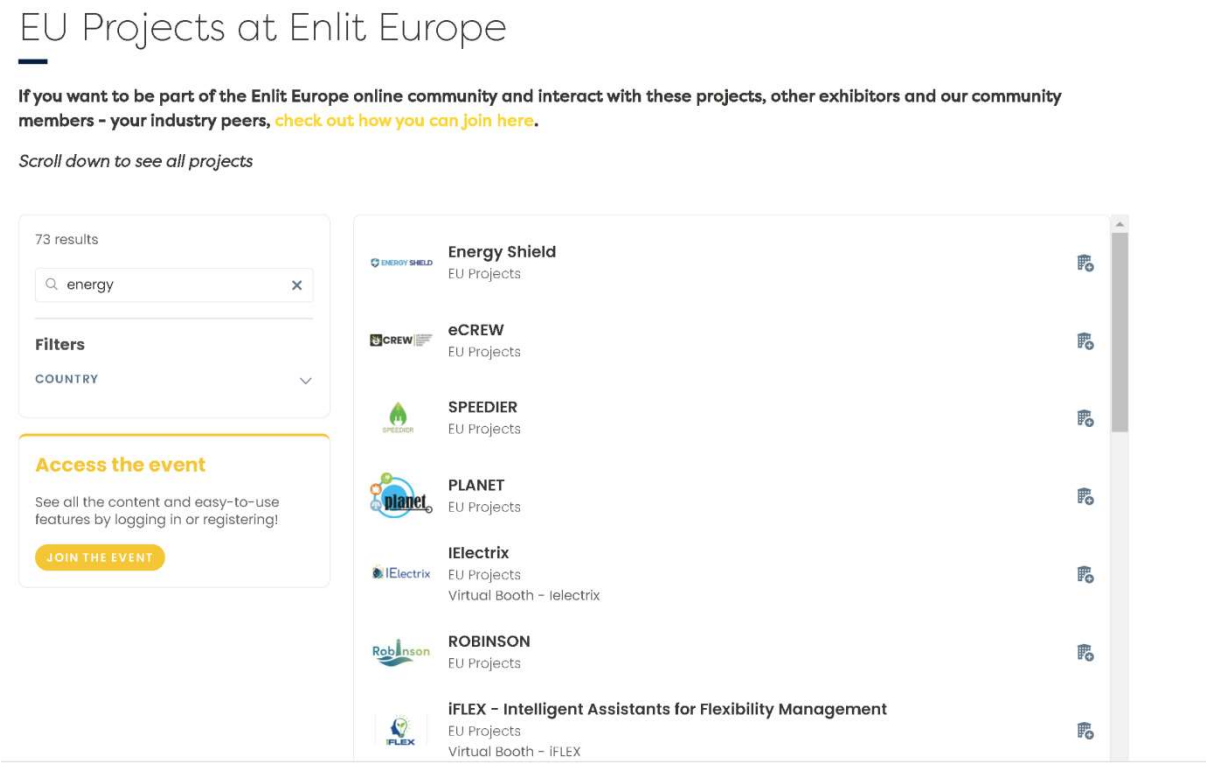


Figure 9. Participating project at Enlit

4.3.8. FULFILLED ACTIVITIES

Table 4 briefly presents the fulfilled collaboration activities of the first two years of the project.

Table 4. Completed collaboration activities

Project / Initiative Involved	Date	Type	Participants	Objective
Cyberwatching.eu	16/07/2020	Workshop	CS-AWARE, SCOTT, STOP-IT, POSEIDON, THREAT-ARREST, CyberSec4Europe, ECHO, SecureIoT, SECREDAS, InfraStress, CARAMEL	Identify possible opportunities for lightweight synergies between EU projects similar MRL score.
SU-DS04-2018-2020	23/07/2020	Workshop	PHOENIX, SDN-microSENSE	Bridge three H2020 EU projects, funded under the SU-DS04-2018-2020 programme and sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).
E.DSO-ENCS-ENTSO-E	07/10/2020	Workshop	E.DSO, ENCS and ENTSO-E	Bring together experts in the field of Cybersecurity to share the latest industry knowledge and present

				learnings from past threats with a so-lutions-based approach.
Cyberwatching.eu	12/11/2020	Webinar	SDN-Microsense, SealedGRID, DEFeND	Present projects' solutions to protect EPES and Smart Grids against cyber-threats, and preserve consumers' privacy.
Cyberwatching.eu		Booklet	SDN-Microsense, SealedGRID, DEFeND	Present a joint webinar summary and recommendations brief that can be send to the EC.
SOCCRATES & HONOR	25/11/2020	Joint publicatio n	SOCCRATES, HONOR	Title: powerLang: a probabilistic attack simulation language for the power domain
Cyberwatching.eu		Project Clustering	SDN-microSENSE, SealedGRID, DEFeND	Energy cluster is focused on cybersecurity applied to the electrical power and energy systems (EPES).
EnergyShield	15/04/2021	Workshop	ENISA, UCY, UK Ofgem, RHEA Group	Present the trends, opportunities and choices in designing a cyber resilient EPES infrastructure.
ECSCI	05/05/2021	Clustering	ANASTACIA, CyberSANE, Defender, FINSEC, RESIST and many others	Joining European Cluster for Securing Critical Infrastructures to initiate a number of EU collaboration activities.
CYBER-EPES	04/06/2021	Clustering	PHOENIX, SDN-µSense, Energy Shield, CyberSEAs, ELECTRON	The five projects funded under the call "Cybersecurity in the Electrical Power and Energy System" agreed to join forces in a Cybersecurity Innovation Cluster for EPES (named CYBER-EPES), being an EC initiative.

4.4. ONGOING AND PLANNED ACTIVITIES

Additionally to the completed collaboration activities and the accomplished synergies, there is a number of ongoing and planned collaboration efforts, which are presented in short in Figure 10.

EPESec 2021	• **Date**: 17/08/2021 - 20/08/2021 • **Type**: Conference • **Participants**: SDN-microSENSE, CYBER-TRUST, FORESIGHT, PHOENIX, SPEAR • **Objective**: co-organize the second edition of the "International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2021)" in the ARES conference
CyberWatching	• **Date**: - • **Type**: Project Clustering • **Participants**: CYBERSANE, CYBERWISER, INFRASTRESS, STOP-IT, RESISTO, CRITICAL-CHAINS, FINSEC, PANACEA, SDN-MICROSENSE, • **Objective**: projects related to cybersecurity applied to Critical Infrastructure are encouraged to join this cluster.
SPHINX	• **Date**: - • **Type**: Tool Eploitation • **Participants**: SPHINX • **Objective**: SBA tool exploitation to perform a number of cyber-security culture evaluation campaigns.
FLEXGRID	• **Date**: - • **Type**: Tool Eploitation • **Participants**: FLEXGRID • **Objective**: SBA tool exploitation to perform a number of cyber-security culture evaluation campaigns.
CyberWatching	• **Date**: TBD • **Type**: Workshop • **Participants**: TBD • **Objective**: presentations from projects and results followed by roundtable on how cluster is addressing key challenges.
CPS4CIP 2021	• **Date**: 04/10/2021 - 08/10/2021 • **Type**: Workshop • **Participants**: FINSEC, ANASTACIA, CyberSANE, DEFENDER, ENSURESEC, FeatureCloud, ... • **Objective**: co-organize the second edition of the "International Workshop on Cyber-Physical Security for Critical Infrastructures Protection".
ETIP SNET	• **Date**: TBD • **Type**: 13th Regional Workshop • **Participants**: TBD • **Objective**: introducing H2020 projects to relevant stakeholders in guiding Research and Innovation activities to support Europe's energy transition.

Figure 10. Ongoing and planned collaboration activities

5. CONCLUSION

In the first year of implementation, EnergyShield partners set the basis for a successful communication of project progress, while the second year (RP2) continued their efforts, elaborated on activities that were identified to contain improvement potential, and intensified the communication along the working channels. Moreover, EnergyShield contributed to Horizon 2020 initiatives like BRIDGE or Cyberwatching.eu, clustering inside cyberwatching.eu, being a foundation member in ESCI and Cyber EPES clusters.

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

The academic partners submitted scientific articles on the artefacts created in the project and presented the contents in different scientific venues.

All proposed communication channels have been used to improve project visibility and they communicated along their channels different material of the project.

The communication flow remained to the digital channels as pandemics restrictions and recommendations were still in place.Partners are still focusing on improving the online presence of EnergyShield project.

Moving communication exclusively online threats face-to-face interaction but also creates significant opportunities in terms of coverage and logistics limitation. Especially, with the two workshops conducted onlinereached a broad audience.

As the online rule communication applies to all (audience, facilitator, and promoters) the impact is expected to be mitigated in the forthcoming period. Large events have already started moving online (e.g European Sustainably Week) and project leaders have also initiated cross-project stakeholder engagement workshops.

The forthcoming period is of great importance for using the created visibility of EnergyShield project and to share the generated results. This is why we will intensify the work in joined working groups and organize thematic workshops with projects funded under similar topics.

REFERENCES

[ARC20a] Acarali, Rajarajan, Chema, Ginzburg (2020): Modelling DoS Attacks & Interoperability in the Smart Grid. In: ICCCN 10th Internal Workshop on Security, Privacy, Trust, and Machine Learning for Internet of Things. Online: https://openaccess.city.ac.uk/id/eprint/25091/1/

[ARC20b] Acarali, Rajarajan, Chema, Ginzburg (2020): A Characterisation of Smart Grid DoS Attacks. In: EAI International Conference on Security and Privacy in New Computing Environments.

[ESC19] EnergyShield Consortium (2019), D7.1 Communication Plan

[ESC20] EnergyShield Consortium (2020), D7.2 Communication Report

[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

[ESR21] EnergyShield Consortium (2021) Workshop Report https://energy-shield.eu/wp-content/uploads/2021/05/EnergyShield_Workshop-Report_v0.6.pdf

[ESV21] EnergyShield Consortium (2021), Workshop video https://www.youtube.com/watch?v=McifpS9BBy8&t=9209s

[GMA20] Georgiadou, Mouzakitis, Askounis (2020): Towards Assessing Critical Infrastructures' Cyber-Security Culture during COVID-19 crisis: A Tailor-made Survey. In: 4th International Conference on Networks and Security (NSEC2020). Online: https://aircconline.com/csit/papers/vol10/csit101806.pdf

[GMA21a] Georgiadou, Mouzakitis, Askounis (2021): Designing a Cyber-security Culture Assessment Survey Targeting Critical Infrastructures During Covid-19 Crisis. In: The International Journal of Network Security and Its Applications (IJNSA). Online: https://aircconline.com/abstract/ijnsa/v13n1/13121ijnsa03.html

[GMA21b] Georgiadou, Mouzakitis, Askounis (2021): Working from home during COVID-19 crisis: a cyber security culture assessment survey. In: Security Journal. Online: https://doi.org/10.1057/s41284-021-00286-2

[GMA21c] Georgiadou, Mouzakitis, Askounis (2021): Detecting Insider Threat via a Cyber-Security Culture Framework. In: Journal of Computer Information Systems. Online: https://www.linkedin.com/posts/anna-georgiadou-64297871_detecting-insider-threat-accepted-manuscript-activity-6795808343345643520-Cg79/

[GMA21d] Georgiadou, Mouzakitis, Askounis (2021): Assessing MITRE ATT& CK Risk Using a Cyber-Security Culture Framework. In: Sensors. Online: https://www.mdpi.com/1424-8220/21/9/3267/pdf

[GMAB20] Georgiadou, Mouzakitis, Askounis, Bounas (2020): A Cyber-Security Culture Framework for Assessing the Organization Readiness. In: Journal of Computer Information Systems. Online: https://www.linkedin.com/posts/anna-georgiadou-64297871_a-cyber-security-culture-framework-for-assessing-activity-6737352178077331456-BNU_

[HBL21] Hacks, Butun, Lagerström, Buhaiu, Georgiadou, Michalitsi – Psarrou

(2021): Integrating Security Behavior into Attack Simulations. In: International Conference on Availability, Reliability and Security (ARES 2021)

[HHF21] Hersén, Hacks, Fögen (2021): Towards Measuring Test Coverage of Attack Simulations. In: EMMSAD'21. To be published

[HKLL20] Hacks, Katsikeas, Ling, Lagerström, Ekstedt (2020): powerLang: a probabilistic attack simulation language for the power domain. In: Energy Informatics. Online: https://link.springer.com/article/10.1186/s42162-020-00134-4

[HK21] Hacks, Katsikeas (2021): Towards an Ecosystem of Domain Specific Languages for Threat Modeling. In: 33rd International Conference on Advanced Information Systems Engineering. To be published

[KHJE20] Katsikeas, Hacks, Johnson, Ekstedt, Lagerström, Jacobsson, Wällstedt, Eliasson (2020): A probabilistic attack simulation language for the IT domain. In: Graphical Models for Security. Online: https://www.gramsec.uni.lu/preproceedings/GraMSec_2020_paper_7.pdf

[LAHL21] Loxdal, Andersson, Hacks, Lagerström (2021): Why Phishing Works on Smartphones: A Preliminary Study. In: 54th Hawaii International Conference on System Sciences. Online: https://scholarspace.manoa.hawaii.edu/handle/10125/71484

[LLE20] Ling, Lagerström, Ekstedt (2020): A Systematic Literature Review of Information Sources for Threat Modeling in the Power Systems Domain. In: 15th International Conference on Critical Information Infrastructures Security (CRITIS 2020). Online: https://dx.doi.org/10.1007/978-3-030-58295-1_4

[VHLF20] Välja, Heiding, Lagerström, Franke (2020): Automating threat modeling using an ontology framework. In: Cybersecurity, Springer Open, journal. Online: https://link.springer.com/content/pdf/10.1186/s42400-020-00060-8.pdf

[XHL21] Xiong, Hacks, Lagerström (2021): A Method for Assigning Probability Distributions in Attack Simulation Languages. In: Complex Systems Informatics and Modeling Quarterly. Online: https://csimq-journals.rtu.lv/article/view/csimq.2021-26.04

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

www.energy-shield.eu