D9.6
Website and dissemination plan

DOCUMENT	D9.6	**WORKPACKAGE**	WP9
DELIVERABLE STATE	FINAL	**PROGRAMME IDENTIFIER**	H2020-SU-DS-2020
REVISION	V0.3	**GRANT AGREEMENT ID**	101020560
DELIVERY DATE	31/12/2021	**PROJECT START DATE**	01/10/2021
DISSEMINATION LEVEL	PUBLIC	**DURATION**	3 YEARS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101020560

DISCLAIMER

ACKNOWLEDGEMENT

This document is a deliverable of CyberSEAS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020560.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

PROJECT ACRONYM	CyberSEAS
PROJECT TITLE	Cyber Securing Energy dAta Services
CALL ID	H2020-SU-DS-2020
CALL NAME	Digital Security (H2020-SU-DS-2018-2019-2020)
TOPIC	SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
TYPE OF ACTION	Research and Innovation Action
COORDINATOR	ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG)
PRINCIPAL CONTRACTORS	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), AIRBUS CYBERSECURITY GMBH (ACS), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER), GUARDTIME OU (GT), IKERLAN S. COOP (IKE), INFORMATIKA INFORMACIJSKE STORITVE IN INZENIRING DD (INF), INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA (ICS), RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN (RWTH), SOFTWARE IMAGINATION & VISION SRL (SIMAVI), SOFTWARE QUALITY SYSTEMS SA (SQS), STAM SRL (STAM), SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA (SYN), WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE (WIN), ZIV APLICACIONES Y TECNOLOGIA SL (ZIV), COMUNE DI BERCHIDDA (BER), COMUNE DI BENETUTTI (BEN), ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA (ELES), PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA (PET), AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (ARN), HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA DOO (HOPS), ENERIM OY (ENERIM), ELEKTRILEVI OU (ELV), COMPANIA NATIONALA DE TRANSPORT AL ENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERGIEI (CRE), TIMELEX (TLX).
WORKPACKAGE	WP9
DELIVERABLE TYPE	[REPORT]
DISSEMINATION LEVEL	[PUBLIC]
DELIVERABLE STATE	[FINAL]
CONTRACTUAL DATE OF DELIVERY	31/12/2021
ACTUAL DATE OF DELIVERY	05/04/2022
DOCUMENT TITLE	Website and dissemination plan
AUTHOR(S)	Mihai Macarie, Markus Mirz, Gianluca Lipari, Marco Angelini
REVIEWER(S)	Kaido Vaade
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY

KEYWORDS Dissemination, Website, Communication

Document History

Version	Date	Contributor(s)	Description
V0.1	10/12/2021	FRAUNHOFER	First draft
V0.2	17/12/2021	FRAUNHOFER	Second draft
V0.3	01/04/2022	CRE	Third draft

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

ECSO	European Cyber Security Organization
EPES	Electrical Power and Energy System
CI	Critical Infrastructure
CERT	Computer Emergency Response Team
SCIRT	Computer Security Incident Response Team
DOI	Digital Object Identifier
DSO	Distribution System Operator
ICT	Information and communication technology
IDSA	International Data Spaces Association
INATBA	International Association for Trusted Blockchain Association
KPI	Key Performance Indicator
NECC	North European Cybersecurity Cluster
TG	Target Group
TSO	Transmission System Operator
WG	Working Group
WP	Work Package

Executive summary

Cybersecurity is one of the most important challenges of our times. All grid elements, from production to the final user, are increasingly interconnected and the effects of any unwanted event cascades rapidly and irreversibly. The reliance on ICT infrastructure becomes more and more important in our lives, within the society. Communications, data management, the flow of information and the linkage between grid elements is done by ICT. Moreover, the EPES is one of the most complex cyber-physical systems, with high impact on all other critical infrastructures. EPES already experiences complex cyberattacks.

The overall communication and dissemination strategy sets out the methods and their application, to align the CyberSEAS security measures to the market and to foster their adoption. The strategy defines the delivery of messages to stakeholders for reaching the project's strategic goals. Consequently, the CyberSEAS project has designed a strategy based on five target groups and three project phases to increase the impact of communication activities. Through collaboration in the consortium, as well as through individual initiatives, the defined strategy aims to build and maintain relationships with stakeholders and to develop the best possible technological solutions that truly respond to EPES requirements and to advance research and innovation in cybersecurity.

The communication and dissemination activities are achieved by creating and distributing high-quality materials, relevant and up to date information throughout the project's lifetime. These materials and information are delivered using precise and easily recognizable visuals and identity (fonts and colors).

Moreover, CyberSEAS ensures open access to all scientific peers and relevant stakeholders, free of charge. The wide range of physical and virtual events, scientific and professional publications are essential for communicating the project's findings, networking with relevant communities and collecting feedback for project's research and for future projects.

The CyberSEAS consortium is comprised of 26 varied and complementary skilled partners and from 6 European countries, with a well-established network of contacts from the target audience.

1 Introduction

CyberSEAS: Cyber Securing Energy Data Services, falls under the topic SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armor against cyber and privacy attacks and data breaches. The project aims to improve the resilience of energy supply chains, protecting them from disruptions that exploit the enhanced interactions and extended involvement models of stakeholders and consumers in complex attack scenarios, characterised by the presence of legacy systems and the increasing connectivity of data feeds. It proposes to 1) counter the cyber risks related to highest impact attacks against EPES, 2) protect consumers against personal data breaches and attacks and 3) increase the security of the Energy Common Data Space.

The data used by this deliverable is supplied by the project's most relevant work packages, as described in section 1.2, in line with the CyberSEAS protocols of confidentiality and restrictiveness, according to the work carried-out within the 100+ scenarios deployed inside the 6 piloting infrastructures in 6 European countries.

Communicating and disseminating the project's findings is accomplished mainly by building understanding and awareness of the data resulted from and validated by the 3 strategic objectives and 9 delivery objectives, described in the section 1.1.2 of the grant agreement. Moreover, the aim is to collect feedback from relevant stakeholders, which will be used during the project and will strategically guide the goals of the project.

1.1 Purpose and Scope

This document provides reference guidelines for the processes of dissemination and communication of the CyberSEAS project, by outligning the work and findings during the lifetime of the project. Furthermore, according to the project's Grant Agreement, article 28 Exploitation of Results, the CyberSEAS results will be used for a period of up to four years for activities such as (1) research, (2) developing, creating and marketing products and/or processes, (3) creating and providing services and (4) national and european sandardization.

During the project's implemenation and afterwards, each beneficiary must communicate the knowledge resulted during the project with the relevant stakeholders, through various means such as academic articles, specialised events (conferences, round tables) and media. Considering the security, data protection and personal data obligations, each beneficiary must inform the other consortia's beneficiaries prior to any publication and communication as well as the information which will be disseminated. The full process of disseminating and using the data will be according to the articles 28, 29, 30 and 31 from the Grant Agreement.

The dissemination activities will target strategic and effective activities, together with respecive audience.

The goals of this deliverable are as follows:

- Present the communication and dissemination tools, established in order to maximise the impact of CyberSEAS results and to create an efficient communication beween project's partners and relevant stakeholders;

- Identify the main communication tools, such as publications and events, intended to raise awareness of the project's findings and results;
- Collect feedback from the most relevant stakeholders;
- Identify future research ideas in the field of cybersecurity or other energy related fields;

1.2 Relations to other activities

This deliverable is related to:

- ✓ D1.1, which describes the internal and external communication processes;
- ✓ D2.1, which comprehensively describes the key mechanisms and model of interdependencies in the electricity supply chain;
- ✓ D3.1, which provides a detailed description of the piloting scenarios as well as the CyberSEAS technical specifications and toolset architecture;
- ✓ D6.2, which describes the guidelines for the cooperation model among EPES operators and other energy stakeholders;
- ✓ D6.6, which provides lessons learned from cases of data breaches as well as defines breach management plans and specific actions for all supply chain operators;
- ✓ D7.1 through D7.6, which demonstrate and validate on EPES relevant and operational environments, as long as the information to be disseminated doesn't breach the level of confidentiality and restrictiveness;
- ✓ D8.8, which delivers recommendations for certification and standardization, as well as the European wide strategy for secure and traceable deployment of new solutions;
- ✓ All other work perfomed within WP9, which supports the alignment of CyberSEAS security measures to the market and fosters their adoption, as long as the information to be disseminated doesn't breach the level of confidentiality.

The activities described by this deliverable will be implemented according to: dissemination obligations (art. 29), confidentiality obligations (art. 36) and security obligations (art. 37) from the Grant Agreement.

1.3 Document overview

This deliverable is intended to review the communication and dissemination activities within the CyberSEAS project, in order to foster the strategic and delivery objectives. The Sections 2 and 3 describe the key messages of the project as well as when and to what target groups these are communicated. The CyberSEAS dissemination goals are described in Section 4. Furthermore, the streams of communications in the frame of the project and the planned

activities are presented in Sections 5, 6 and 7. Lastly, the project website is introduced in Section 8.

2 Key messages of the project

The key messages that will be disseminated through our external communication channels are:

- Increase cyber-security awareness at consumers and prosumers, by creating understanding of the types of personal data breaches and attacks;
- Increase collaboration between energy operators and connected infrastructures, by mapping the highest impact attacks, creating a common understanding of the cyber-risks and delivering means and tool to counteract these risks;
- Facilitate connections between national authorities and bodies and European agencies, CERTs, and CSIRTs networks, by making available new and improved means to increase the security and governance of the Energy Common Data Space;
- Improve the decision-making process of investors, by providing continuous cyber risk assessment support and intra and cross domain impact analysis;
- Improve the efficiency and precision of preventing measures, through the use of machine learning techniques, cyber threat intelligence and augmented detection;
- Improve the real-time protection level, by providing timely cyber security monitoring support and state of the art protection mechanisms;

3 Target Audience

This deliverable identifies several relevant stakeholders to validate the CyberSEAS findings and to exploit the project's results.

The target audience is comprised of all relevant EPES (electrical power and energy systems) stakeholders (operators, aggregators, consumers, public authorities), as well as other stakeholders from adjacent sectors (i.e., cyber-security, ICT, standardization, etc.).

The target audience's relevance depends on the phase of the project:

Phase 1 – Awareness: focuses on generating initial awareness of critical cyber security issues for EPES across a wide range of stakeholders.

Phase 2 – Evidence: aims at increasing the market potential of CyberSEAS through a results-oriented approach, which involves the presentation of the tangible mechanisms and results from the running pilots and security measures.

Phase 3 – Results: also extending beyond the end of the project, aims at stimulating the uptake of CyberSEAS results.

Four target groups have been identified starting from network operators (primary beneficiaries of CyberSEAS) to consumers and policy stakeholders, whose activities are key to the future of EPES:

- TgA) General public, citizens and prosumers: being connected to the network, they are potential sources of distributed and complex vulnerabilities as well as potential victims of privacy breaches.
- TgB) Academic, scientific and professional communities: ICT and energy research organizations, as well as other EU research consortia, acting as feedback providers or dissemination actors;
- TgC) Energy operators and connected infrastructures: TSOs, DSOs, manufacturers, aggregators, municipalities acting as operators of the EPES, for instance using the Berchidda and Benetutti model.
- TgD) National and European organizations (e.g. European institutions, National Energy agencies, Market regulators, Standardization bodies, IT Institutions): to fuel the effective involvement of policymakers, defining recommendations based on evidence emerging from the pilots and discussed within a group of experts of both cyber and energy domains. This includes targeting CERTs, CSIRTs networks, as well counterterrorism and Law Enforcement Authorities.

Table 1 – Dissemination activities planned for each phase of the project

Awareness M1-M12	Evidence M12-24	Results M24-M36	Target group
KEY MESSAGE 1): Increase cyber-security awareness of consumers and prosumers			
▪ Role of consumer/prosumer in energy cyber defense ▪ Impact of cyberattacks on consumers/prosumers ▪ Security skills	▪ Pilot results toward the role of a consumer in the cyber energy defense ▪ Project goals in relation to consumers/prosumers	Online information kit for consumers/prosumers	TG A) TG B)
KEY MESSAGE 2): Increase collaboration between energy operators and connected infrastructures			
▪ Opportunity/threats of cross infrastructure collaborations ▪ Value vs risks of cooperation between regional and national systems	▪ Project goals for CIs ▪ Cascading effects within CIs ▪ Continuity of services for operators and society	▪ Public Authorities role for both regulations and security procurement ▪ Increased business continuity	TG B) TG C)
KEY MESSAGE 3): Increase collaboration among energy operators			
▪ Opportunities of protected information sharing between operators ▪ Innovative flexible and adaptable framework to protect EPES ▪ Project goals	▪ Pilots first results ▪ Demonstrable increase in security ▪ Using increased security levels to increase consumer base ▪ Supporting compliance to regulations	▪ New services beyond distributed systems ▪ Recommendations based on project results and evidence from the pilots ▪ Increased competitiveness by introducing cyber-secure innovative services	TG C)
KEY MESSAGE 4): Connect to policy authorities and EU agencies, CERTs and CSIRTs networks			
▪ Detailed threat analysis of EPES on a base of penetration testing ▪ Secure energy system optimization with operators' collaboration ▪ Skills/awareness framework	▪ Need of comprehensive approach to the cyber defense of EPES ▪ Importance of public-private cooperation for the protection of CI	▪ Collaboration mechanisms for law enforcement in EPES	TG D)

4 Dissemination Goals and Communication Strategy

Considering the ambitious European energy and climate policies, digitalization is at the base level for all developments towards achieving the energy transition and overall decarbonization target. Moreover, according to the European Internal Energy Market project, regions and grid elements are increasingly interconnected and interdependent. Consequently, cybersecurity is becoming of paramount importance in order to protect the safety and operability of EPES system, and of the energy system as a whole.

We will direct our efforts towards the following goals:

- Identify, reach, and engage with stakeholders
- Promote the activities and the results of the project
- Make the produced knowledge more accessible
- Facilitate interaction and feedback on our work
- Identify new research avenues to further develop the scope of CyberSEAS

The goal of the CyberSEAS communication and dissemination strategy is to bring together the project's technical results with feedback and recommendations from the target groups on how these results can be effectively deployed in the market, in order to:

- Comprehensively map the challenges and constraints resulting from the increase use of decentralized renewable energy sources;
- Identify and address the highest impact attacks at the full energy supply chain level, from operators to consumers, the latter being both channels for attacks and targets of attacks;
- Fully identify and address attacks on the privacy and confidentially of citizen's data, as well as on the Energy data space in general;
- Improve the resilience of energy supply chains;
- Improve the stability and sustainability of the European EPES system;
- Effectively deploy the pilots on substantial infrastructures, to ensure the trustworthiness of results;
- Improve the information on which operators base their investment decisions;
- Improve the efficiency and precision of prevention measures;
- Improve the real time protection level;
- Reinforce the Human in the Loop dimension;

The dissemination goals will be reached by individual activities of the partners as described in the following section and joint efforts through the project's external communication streams as described in Section 6.

The dissemination plan will aim towards achieving the project's estimated reach, according to the KPI's presented at the section 1.1.4 Impact and strategic monitoring approach within the Grant Agreement, namely:

- 15 energy grid operators external to the consortium:
- 50 energy stakeholders external to the consortium;
- 100+ security challenging use cases / misuse cases / attacks scenarios;
- 80% effectiveness of remediation actions for each category of threats;
- 100% coverage of attack scenarios classified as critical;
- Commitment of 2 energy stakeholders external to the consortium to long-term deployment of the skills improvement platform;
- Establish the operational interfaces with at least 5 CERT organization from at least 3 different countries;

Events (i.e. conferences, fairs), scientific publications and other articles will be available as open access and where possible the FAIR principles will be applied to resources produced in the frame of CyberSEAS. The CyberSEAS resources include lab and test site results, teaching materials and software tools.

5 Partner Dissemination Plans

The individual dissemination and communication plans describe each partners' activity to further extend the outreach of CyberSEAS through networks in which the partner is active, ranging from CERT networks to communities of operators and public authorities, as well as open source communities.

Table 2 – Dissemination plans for each partner

Partner	**Dissemination Plan**
ENG	ENG will disseminate the CyberSEAS messages to the BRIDGE initiative, to ECSO, to consortiums of on-going projects CyberSec4Europe, CitySCAPE and DEFENDER. It will also disseminate to the FIWARE and IDSA ecosystem. This dissemination will be achieved mainly through online communications and attendance to either the annual conference or specific workshops.
CINI	CINI will disseminate CyberSEAS results via: - Participation to Workshops or co-hosted H2020 events - Presentations in webinars, videos, social media, public reports. - Meeting with other people from academia - Participation to Conferences – planned: European Dependable Computing Conference (EDCC), 41st International Symposium on Reliable Distributed Systems (SRDS 2022). - Publications in Top-Tier Journals - planned: IEEE Transactions on Computers, IEEE Transactions on Industrial Informatics. - Release of open source software implemented in the context of the project
ACS	Airbus will contribute to dissemination and communication actions with a focus on communication to business. Airbus will introduce CyberSEAS outcomes at business events such as the European Utility week, ITSA, Cybersecurity & Cloud Expo or similar industry meetings. Internal dissemination activities will also take place, Airbus Cybersecurity All Hands presentations will take place throughout the duration of the project, and group-wide actions will be held in form of webinars, live sessions and Expert talks.
GT	GT will promote the project both internally and externally through its various online channels and interpersonal and diverse networks. Using its experience in cyber security (range, training and security solutions) we will disseminate the results through our business unit with a special focus on critical infrastructure. Guardtime's website has 80,000+ visitors per year, where the project will have a dedicated space on our project's subpage: guardtime.com/research. In addition,

	we use our social media platforms Facebook, LinkedIn and Twitter, to promote the project and its results in a timely manner to reach different audiences. In the upcoming year we plan to release at least one blog post on our website that will relate to CyberSEAS. We will contribute to the development of the dissemination strategy and participate in producing dissemination messages and materials related to the project, especially those relevant for the pilot(s), where GT intends to build tools for protecting the trust between energy market participants and contribute to the security challenges related to data leak, protection of private data and situational awareness of multi-party data sharing. Hence, the focus of Guardtime's dissemination will be placed towards distribution system operators (DSO) and transmission system operators (TSO), with the objective to inform them about available solutions, pilots and show the references for potential cooperation. Moreover, Guardtime is an active member of INATBA, ECSO, the North European Cybersecurity Cluster (NECC) and the Estonian Information Security Association (EISA), and a contributor to the work of European Blockchain Partnership, EU Blockchain Observatory and Forum, Energy BRIDGE as well as the CEN/CLC/JTC 19 Blockchain and Distributed Ledger Technologies standardisation committee, and the EIT Digital ecosystem. Guardtime will participate in these organisations' meetings and when applicable will promote and discuss the topics related to CyberSEAS. GT is actively looking for the possibility to present CyberSEAS in workshops like E.DSO webinar for cybersecurity, ENTSO-E security and energy webinars and cyberwatchin.eu initiatives.
INF	INF will disseminate CyberSEAS results through publications in Slovenian and international journals and magazines related to the energy sector. INF will promote CyberSEAS solutions at conferences targeting specific audience, strategic decision makers and local authorities with special focus to the Slovenian DSO Community. Knowledge and experiences will be presented and disseminated through different energy and business channels.
ICS	ICS leads the Slovenian Corporate Security Association where almost all Slovenian CI operators participate and is also a member of the SE Corporate Security Association where it will disseminate sharing of best practice and solutions from CyberSEAS. ICS will also exploit its strong cooperation with the national public authorities to disseminate CyberSEAS results towards the Ministry of Defense, Ministry of Interior, CERT, Slovenian Cyber security NSA, Slovenian Parliament and other important public institutions. Concrete dissemination action: - Presentation of Cyber SEAS project in Professional magazine "Corporate Security) – vol. 26, SEP 2020 (look at p. 53) https://www.ics-institut.si/en/magazine/26-%C5%A1tevilka – done

	- International Conference "Challenges in protection Industry and Infrastructure" 27-28. OCT 2021 Zagreb, Croatia. Dr. Denis Čaleta, Institute for Corporative Security Studies (ICS): Key challenges regarding resilience of Critical Infrastructure" (Also key information about project CyberSEAS was presented); - done - International conference: Days of Corporate Security 2022 – 24-25 May 2022 in Ljubljana (presentation of CyberSEAS project) - Organize presentation of CyberSEAS in 2nd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop, 27-29. April 2022
RWTH	As academic partner, RWTH is planning to undertake traditional exploitation activities of universities: teaching activity as well as scientific publications in peer-reviewed magazines and journals such as IEEE Transactions on Smart Grid. Furthermore, dissemination will be performed by their researchers both in the regular teaching and in industry-oriented teaching activity. As part of dissemination activities for task 2.1, the developed tool for interdependencies model is planned to be made open source, and a short document about the tool will be submitted together.
SMV	SMV will disseminate the results of the project to the Romanian ICT industry through various channels: participation at the "International Fair of Inventions, Scientific Research and New Technologies Bucharest"," International Technical Fair Bucharest", etc. Present the project results to critical infrastructure operators in Central & Eastern Europe (in finance and other industries) – liaise with EnergyShield project (leaded by SIMAVI)
STAM	STAM will disseminate project key messages towards the industrial community, end users, customers and policy makers / influencers. STAM plans to publish a scientific paper describing methodologies and tools developed in the project, in cooperation with significant partners. STAM is a member of the SOSIA (System of System and Intelligent Automation) and EASS (Energy, Environment, Sustainable Development) Ligurian networks, which include players and stakeholders in the fields of risk management, cybersecurity and EPES. STAM will disseminate CyberSEAS among the members of these networks through the participation to organized periodic events (conferences, webinar, etc.). Furthermore, the cooperation with energy providers of the Italian pilot will facilitate the arrangement of a dedicated workshop in Sardinia region to disseminate results obtained in the two smart grids involved.
SYN	SYN will disseminate the CyberSEAS outcomes to the BRIDGE initiative, and to consortiums of ongoing projects, such as DEFENDER and PHOENIX. Dissemination activities will also include the attendance and presentation of the project's outcomes on annual conferences and/or dedicated workshops. Additionally, press releases will inform a wider base of stakeholders and enterprises that are interested in cybersecurity and smart energy grids.

WIN	WIN will disseminate CyberSEAS at the national, European and international levels. WIN will establish links with the Greek energy ecosystem (e.g., primarily operators, organizations from the policy / ministry domain, etc.) and will communicate CyberSEAS objectives in EU R&D energy projects (E.g. InterConnect). Moreover, WIN will disseminate through bodies like ECSO, in cybersecurity conferences / fairs, organized by the EC (E.g., Security Research Event) or other institution. At least one main magazine / journal publication will be conducted, in addition to, at least, one conference publication per year. In addition to the above, WINGS will seek dissemination to EuCNC (European Conference on Networks and Communications), supported by the European Commission and other conferences and fora and will continue building links with 6G industry association especially for promoting security in energy domain. National dissemination actions will be sought and we'll monitor events related to energy and security according to consortium interests as well.
ZIV	ZIV will provide necessary resources and effort to stablish a dissemination plan that could be extended, not only internally to the Company, but to consumers, energy operators and any interested partner in relation to cyber-security awareness. The goal of this dissemination plan will be making the knowledge more accessible to all parts (internally and externally to the Company) to interact with them and get feedback to be applied on daily work and business. Increase the culture of Cybersecurity is the main goal. To get this, several dissemination solutions will be used as internal training programs with different levels of detail, external trainings and meets through different online platforms already used for other purposes and through ZIV technical and commercial existing network all around the world, participation in industrial clusters and digital innovation hubs and seminars and international conferences organized by entities like CIRED or IEEE, in order to provide teaching material, laboratory results and improvements in our own products and services. The defined strategy aims to build and maintain relationships with stakeholders and to develop the best possible technological solution that truly responds to EPES requirements and to advance research in cybersecurity.
SQS	SQS will disseminate the results internationally through conferences and sectorial seminars. Special efforts will be made to disseminate CyberSEAS at the QA&Test international conferences. SQS will also provide workshops among industry via their participation in industrial clusters and digital innovation hubs (DIH). SQS will also disseminate the results via the SQS Newsflash magazine.
Fraunhofer	Fraunhofer will disseminate the results within the BRIDGE activities and, in particular, by creating a synergy with the project OneNet where it is acting as coordinator. Furthermore, Fraunhofer plans to participate to workshops and conferences both in Germany and at international level to promote the knowledge acquired and to advertise in particular the new educational activities that are planned within the project. Dissemination opportunities are, for example, Energy informatics, IEEE International Conference on Information Technology, IEEE International Energy Conference as well as the Grid Forum (GRIFOn) events organized by the OneNet project. Through the cooperation with RWTH within the Centre for Digital Energy, Fraunhofer plans also to reach out to university students and to increase awareness about cybersecurity in power systems.

IKE	IKE disseminates towards the scientific and industrial communities, including dissemination to the scientific community through publications in journals, conferences and workshops, dissemination of the outcomes of CyberSEAS in new research projects (European or funded by local government) and in transfer projects with private companies and providing demonstrators to show technology developments to industrial players, especially equipment manufacturers.
BEN	Municipalities will disseminate the CyberSEAS project and its results first at local level, by informing the citizens about the impact that CyberSEAS will have on their life, in terms of increased security in their daily use of the electrical grid and its components. This will be achieved thanks to the production of informative material (leaflet, poster, etc.), as well as by adding a specific section on the municipality website. This will also turn into an increased security awareness of the Municipality employees and end users, both as consumers and prosumers.
BER	The project will be disseminated to public authorities and administrations, also with the support of Sardegna Ricerche (the Regional body promoting R&D activities), by organizing workshops and press releases to inform a wider base of stakeholders. These will be jointly organized with the Berchidda and Benetutti Municipalities.
ELES	ELES will disseminate CyberSEAS results through publications in Slovenian journals and magazines related to the energy sector. ELES will promote CyberSEAS solutions at conferences targeting specific audience, strategic decision makers and local authorities (ministers, secretaries, etc.). Knowledge and experiences will be presented and disseminated to the European network of transmission system operators for electricity (ENTSO-E) as well as to other EU project partners (Migrate, FutureFlow, etc.) and to the BRIDGE community.
Petrol	PETROL is one of the top income company in Slovenia, and as such has a great influence and responsibility to our surroundings. We strive to include our name and experiences into the interests that are good for our growth and development. It is our key responsibility that we have a long lasting and rewarding relationship with our partners and society. We already have in place a share and care program where our know how is shared among employees. They are our best ambassadors for all our programs for learning and teaching among our business partners and other interested parties. New skills and key finding will be delivered through our already established learning channels (universities, meetings, conferences and other events).
ARN	As important part of cyber security network, ARN (SI-CERT) will disseminate results and project best practices with the national and international cyber security community, including the EU CERT network. SI-CERT will also promote CyberSEAS solutions at conferences targeting specific audience, strategic decision makers and local authorities.
HOPS	HOPS will disseminate CyberSEAS results through publications in Croatian and international journals and magazines related to the energy sector. HOPS will promote CyberSEAS solutions at conferences targeting specific audience, strategic decision makers and local authorities (ministers, secretaries, etc.). Knowledge and experiences will be presented and disseminated to the European network of transmission system operators for electricity (ENTSO-E) as well as to other EU project partners community.

EMP	EMP will disseminate CyberSEAS results through publications in scientific journals or conferences and industrial events in Finland and in Europe. In the dissemination of the results, EMP will collaborate with the Finnish TSO Fingrid who is the responsible for the Datahub implementation and disseminate the results nationally.
ELV	Elektrilevi is one of the main contributors to power grid management in Estonia and well connected with neighboring countries. With sharing the same challenges Elektrilevi intends to use its network to share the knowledge and expertise created in CyberSEAS and contribute to the dissemination activities in different levels from consumer, prosumer and operator side to the regulators and legislation area.
TEL	TEL will disseminate the knowledge acquired from the project and project results and tools to all its business contacts. As TSO, TEL is in direct contact with DSOs, Renewable Power producers, Energy services operators, Energy market players that could be interested of cybersecurity problems and threats. Crossing borders, TEL is in direct contact with neighbor area TSOs.
CRE	CRE is one of the most important energy professional association in Romania, and the only one with representation in Brussels. It has continuous contacts with important Energy domain players, its own members, other energy related companies and critical infrastructure companies from Romania and from the European Union. CRE hosts conferences, workshops, direct or online in Romania and in Brussels where CRE has an office. CRE maintains an active relationship with all major players of the Energy domain in Europe and abroad. Dissemination Initiatives CRE, being the leading partner regarding dissemination and communication activities, will regularly and proactively present and promote the project results and goals as follows: - Online Conferences and Workshops, organized by CRE and by other partners and stakeholders from the target groups - In Person Conferences and Workshops - Regular Press Releases (CRE Press Releases) - Blogs contribution - Newsletter Contribution - Social Media (LinkedIn, Twitter and Facebook) - EU Projects Cluster events - Standardization Events - The CyberSEAS project results will be disseminated to all members of CRE and related companies, the contacts from other EU funded projects where CRE is an active participant. The contacts of CRE on all level of decision makers up to strategic decision makers in the Energy domain, European Distribution

	system operators, European Transmission System Operators, ENTSO-E, E-DSO, will also be used as dissemination targets.
TLEX	TLEX will disseminate the outputs from this project via the various academic and professional workshops, trainings, and events to which it frequently contributes as a speaker, as well as through targeted articles in specialized legal publications, and broader publications for the general public.

6 Streams of communication and tools

This deliverable is considering two streams of communication in CyberSEAS:

1. Internal communication, among the partners of the consortium. The internal stream is organized as described in Deliverable D1.1. The main communication channels are direct mails, mailing lists and MS Teams©.

2. External communications are the responsibility of WP9. Input and updates from the other work packages are key to the success of the external communications activities. Therefore, an Excel file has been shared on MS Teams to collect input from all project partners, which is considered part of the internal communication, and keep track of all the dissemination activities carried out by the consortium or the partners.

The following channels will be used to communicate our key messages to our external target groups:

- Website: https://cyberseas.eu/
- Social media
    - Twitter (https://twitter.com/cyberseas_eu)
    - LinkedIn (https://www.linkedin.com/company/cyberseas-project/)
    - Facebook (https://www.facebook.com/Cyberseas-Project-102249289126271)
- Partners' newsletters
- Blogs
- GitHub and Zenodo
- Public relations (i.e. press releases and conferences, radio and tv interviews)
- Partners websites
- Virtual and in-person events (i.e. conferences, panel discussions, round tables, fairs)
- Articles (i.e. academic and scientific journals, newspapers, specialized magazines)
- Printed materials (i.e. brochures, flyers)

Integrations between these tools will be used as well. For example, a software project made available and developed on GitHub can be tagged and provided with a DOI through Zenodo. Then, these results can be communicated via social media accounts, the website etc.

Visual identity is key to ensure that project's activities and communications are recognisable as part of CyberSEAS. It will equally be used internally and externally, and all marketing materials, printouts and digital formats will use the project's especially design visuals.

The logo has been developed by ENG and the monogram represents abstract waves/fluids that converge towards the center in a soft, graceful way. The shape has a circular motion that metaphorically represents the co-existence of different forms of energy on the planet,

while the soft shapes provide a link to the acronym "SEAS". The brand visual identity guidelines is completely showed in Annex 1.

7 Planning

Communication activities will be synchronized with the project's timeline:

- Milestones and deliverables
- Publications (i.e. conference proceedings, academic journals, articles in press, blogs, social media)
- Events (i.e. conferences, round tables, fairs)
- News from the project network

The planning includes a list of objectives (during the lifetime of the project):

- A minimum of 6 social media posts, news each quarter starting from M6 (by-monthly)
- Promotional material sent to 500 contacts starting from M6
- A minimum of 20 press releases through all partners
- participation at 15 events and conferences
- 4 publications in highly ranked international journals
- Involvement in working groups s (e.g. ECSO WGs, BRIDGE WGs), establishing links with initiatives (e.g. EE-ISAC, TNCEIP) and 15 references to work produced in CyberSEAS across at least 5 initiatives
- website ready by M3 and generating 100 monthly visits from M6 onwards

Statistics on the impact of the website and social media as well as input from the partners regarding their communication activities will be collected to support the project coordinator and partners in revising and improving the communication strategy.

7.1 List of relevant event

The table below shows the events with a specific relevance for the project.

Table 3 – Events

No.	Event Name	Venue	Date	Link
1	Critical Infrastructure Protection & Resilience Europe 2022	Hybrid (Bucharest and online)	14th-16th of June 2022	https://www.cipre-expo.com/
2	Energy Tech Summit	Hybrid (Warsaw and online)	26th-28th of April 2022	https://energytechsummit.com/#about

3	2nd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop	Hybrid	27th-29th of April 2022	https://www.finsec-project.eu/ecsci
4	Days of Corporate Security 2022	Hybrid	31st of May – 01st of June 2022	https://www.ics-institut.si/en/events/13th-international-conference-days-of-corporate-security
5	InnoGRID Project Sessions	Hybrid	14th of June 2022	https://www.innogrid.eu/
6	Spark 2022 – Energy Reimagined	London	21st – 22nd of June 2022	https://www.terrapinn.com/exhibition/spark/index.stm
7	E-World Energy and Water	Essen, Germany	21st-23rd of June 2022	https://www.e-world-essen.com/de/
8	InnoGRID Policy Conference	Hybrid	29th of June 2022	https://www.innogrid.eu/
9	International Workshop on Next Generation Security Operations Centers	Hybrid	23rd – 26th of August 2022	https://www.ares-conference.eu/workshops-eu-symposium/ng-soc-2022/
10	SEST 2022 - 5th International Conference on Smart Energy Systems and Technologies	Eindhoven, The Netherlands	5th-7th of September 2022	https://www.sest2022.org/
11	European Sustainable Energy Week	Hybrid (Brussels and online)	26th-30th of September 2022	https://eusew.eu/
12	ISGT Europe 2022 – Together towards digitized, decarbonised and distributed smart grids	University of Novi Sad, Serbia	10th-12th of October, 2022	https://ieee-isgt-europe.org/
13	AEE – Engineering the Future of Energy in Europe	Dublin, Ireland	26th-27th of October	https://aeeeuropeenergy.com/
14	Enlite Europe	Frankfurt, Germany	29th November – 1st December 2022	https://www.enlit-europe.com/euw
15	11th Romanian Energy Day	Brussels	(TBD) Second half of 2022	The flagship event organised by the Romanian Energy Center

16	CyberSEAS Stakeholders Meeting	Bucharest, Romania	(TBD)	The main CyberSeas yearly conference

Table 2 - Events

8 Website and social media

The project website, which is the main tool for communicating and disseminating the CyberSEAS information, is available since December 2021. It provides an overview of the project goals, recent activities and the status in terms of project deliverables and results. The website also makes available the relevant information on all partners involved in CyberSEAS.

The URL is www.cyberseas.eu

The website is based on the open source WordPress solution and supports desktop computers as well as mobile devices with smaller screens. The website's sections are shown below:

Apart from the mandatory web page about the privacy policy, the website is structured in six content pages:

- **Home**: it is the website homepage. It shows a summary of everything is available on the website: overview of the project, pilots, news, results;
- **About**: it includes a description of the project and provides the project numbers, objectives and solutions. It shows the management team, the list of project partners and the linked projects together with CyberSEAS into the CyberEPES cluster;
- **Pilots**: it provides the list of the project pilots as well as the testing labs where the solution will be demonstrated. It also contains an interactive European map where the pilots and testing labs are located;
- **News and Events**: this page contains the list of news, events and newspapers published by the project;
- **Results**: here will be made available the publications, deliverables and videos released;
- **Contacts**: is a form for the website user who wants to get in touch with us.

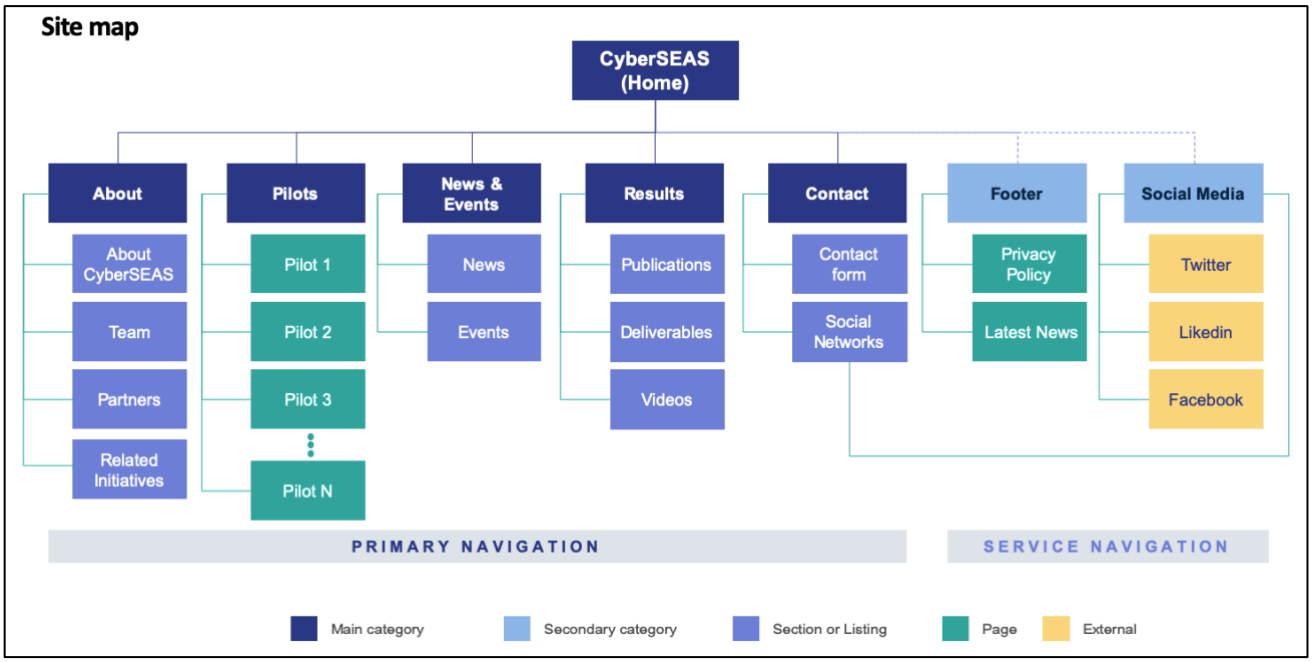

Figure 1: Project website

Social Media, together with the website, is a key pillar in the project's communication and dissemination activities. A LinkedIn page was created under the name https://www.linkedin.com/company/cyberseas-project/, as well as a Twitter account https://twitter.com/cyberseas_eu, intended for the professional community. Moreover, a dedicated Facebook page using the name CyberSEAS Project was designed for the wider energy community and general public.

Annex 1 Brand Visual Identity Guidelines

CyberSEAS

Brand Visual Identity Guidelines

keywords.

Ecosystem - Technology - Connection - Energy - Fluidity

concept.

The monogram represents abstract waves/fluids that converge towards the center in a soft, graceful way. The shape has a circular motion that metaphorically represents the co-existence of different forms of energy on the planet, while the soft shapes provide a link to the acronym **SEAS.**

ACCOSTAMENTO 1

ACCOSTAMENTO 2

VERSIONE ISTITUZIONALE

x= ingombro marchio - logotipo orizzontale

y= altezza marchio

GRIGLIA COSTRUTTIVA

GRIGLIA COSTRUTTIVA

LOGOTIPO POSITIVO/NEGATIVO

70mm | A2

45mm | A3

30mm | A4/A5

Minimum Size

20mm | 60px

App Icon

32 x 32px

70mm | A2

45mm | A3

30mm | A4/A5

Minimum Size

20mm | 60px

App Icon

32 x 32px

Aa Bb Cc Dd Ee Ff
Gg Hh Ii Jj Kk Ll Mm
Nn Oo Pp Qq Rr Ss Tt
Uu Vv Ww Xx Yy Zz

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna.

Logotype

Montserrat Bold

Bodycopy / Current Text

Montserrat Regular

PRIMARI

PANTONE
P 105-16 C

CMYK
100, 80, 30, 10

RGB
0, 55, 115

HEX
#003973

PANTONE
7840 UP

CMYK
55, 0, 55, 0

RGB
125, 195, 145

HEX
#7CC18F

SECONDARI / FACOLTATIVI

PANTONE
7541 UP

CMYK
10, 0, 0, 0

RGB
240, 245, 250

HEX
#F1F7F9

PALETTE CROMATICA

PALETTE CROMATICA