PHOENIX

Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks

Deliverable D8.6
Dissemination and Standardisation Activities

Authors	Wafa Ben Jaballah (TSG), Hendrik Flamme (RWTH), Pasi Lassila (AALTO), Ganesh Sauba (DNV), Artemis Voulkidis (SYN), Elena Sartini (CEL), Tomaz Dostal (ISKRA), Tomaz Damjan (BTC), Tommaso Bragatto (ASM), Jose Ramon Martinez (ATOS IT)
Nature	Report
Dissemination	Public
Version	1.0
Status	Deliverable
Delivery Date (DoA)	28-02-2021
Actual Delivery Date	27-02-2021

Keywords	Dissemination, Standardization, Publications, Events, PHOENIX Cybersecurity certification centre
Abstract	This deliverable reports on the status of scientific, standardization, and dissemination activities performed in the first project period. The current status of work is still preliminary and will be completed by the second version of this deliverable. Specifically, PHOENIX has started a significant number of standardization activities. For this purpose the PHOENIX Cybersecurity Certification Centre was created that will also contribute to cyber security and privacy issues related to electrical Power and energy system. Moreover, consortium partners have been active in disseminating PHOENIX activities in terms of publications, scientific talks and presentations.

DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.
This document may contain material, which is the copyright of certain PHOENIX consortium parties, and may not be reproduced or copied without permission. All PHOENIX consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.
Neither the PHOENIX consortium as a whole, nor a certain party of the PHOENIX consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

	Participant organisation name	Short	Country
01	Capgemini Technology Services	CTS	France
02	THALES SIX GTS FRANCE SAS	TSG	France
03	THALES Research & Technology S.A.	TRT	France
04	SingularLogic S.A.	SiLO	Greece
05	DNV-GL	DNV	Norway & Netherlands
06	INTRASOFT International S.A.	INTRA	Luxemburg
07	Iskraemeco	ISKRA	Slovenia
08	ATOS IT SOLUTIONS AND SERVICES IBERIA SL	ATOS IT	Spain
09	ASM Terni	ASM	Italy
10	Studio Tecnico BFP srl	BFP	Italy
11	Emotion s.r.l.	EMOT	Italy
12	Elektro-Ljubljana	ELLJ	Slovenia
13	BTC	BTC	Slovenia
14	Public Power Corporation S.A.	PPC	Greece
15	E.ON Solutions Gmbh	EON	Germany
16	Delgaz Grid SA	DEGR	Romania
17	Transelectrica S.A.	TRANS	Romania
18	Teletrans S.A.	TELE	Romania
19	Centro Romania Energy	CRE	Romania
20	CyberEthics Lab	CEL	Italy
21	Synelixis Solutions S.A.	SYN	Greece
22	ComSensus	CS	Slovenia
23	AALTO-KORKEAKOULUSAATIO	AALTO	Finland
24	Rheinisch-Westfälische Technische Hochschule Aachen	RWTH	Germany

ACKNOWLEDGEMENT

This document is a deliverable of PHOENIX project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 832989.
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.

Document History

Version	Date	Contributor(s)	Description
V0.0	04/01/2021	TSG	Initial ToC
V0.1	25/01/2021	AALTO, RWTH, CEL, ISKRA, BTC, ASM, ATOS IT	First round of inputs
V0.2	13/01/2021	DNV, TSG	Second round of inputs
V0.3	22/02/2021	TSG	Pre-review version
V1.0	25/02/2021	TSG, RWTH, AALTO	Version ready to be submitted

Document Reviewers

Date	Reviewer's name	Affiliation
23/02/2021	Pasi Lassila	AALTO
22/02/2021	Hendrik Flamme	RWTH

Table of Contents

List of Tables

Definitions, Acronyms and Abbreviations

ACM	Association for Computing Machinery
AMS	Advanced Manufacturing Systems
CEN	European Committee for Standardization (FR : Comité européen de normalisation)
CENELEC	European Committee for Electrotechnical Standardization (FR : Comité européen de normalisation en électronique et en électrotechnique)
CCC	Cybersecurity Certification Centre
CPU	Central Processing Unit
DCS	Distributed control systems
DoA	Description of Action
ECSCI	European Cluster for Securing Critical Infrastructures
EE-ISAC	An industry-driven, information sharing network of trust
EPES	Electrical Power and Energy System
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HEMRM	Harmonized electricity market roles model
HMI	Human-Machine Interface
IA	Industry Association
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IED	Improvised Explosive Device
IoT	Internet of Things
ISG	INDUSTRY SPECIFICATION GROUP
PCB	Printed Circuit Board
PDL	Permissioned Distributed Ledger
PHOENIX	The PHOENIX project

PLC	Programmable Logic Controller
PRESS	Privacy, Ethics, Security and Societal
NFV	Network Function Virtualized
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDO	Standardization Development Organization
SDN	Software Defined Network
WoT	Web of Things

Executive Summary

The PHOENIX project regards standardization and dissemination activities as essential contributions and key results of the project. In particular, the project has identified several dissemination opportunities and standardization bodies in both the energy and cyber security sector. Moreover, a dissemination plan that covers publications, participation to events, talks and scientific venues was created. In particular, PHOENIX maintains a number of key venues for disseminating the technical project results in various panels and scientific talks. Furthermore, the PHOENIX project creates a Cybersecurity Certification Centre (CCC) to address security and privacy for the Electrical Power and Energy System (EPES).

Due to the Covid pandemic, many suitable dissemination and standardization events were cancelled, postponed or transformed to online or hybrid formats. Despite this and the fact that many PHOENIX activities are classified, partners have still managed to successfully initiate dissemination and standardization activities.

In the time span covered by this deliverable M1-M18, we can list the PHOENIX dissemination and standardization contributions as follows:

Publications: 2 International peer-reviewed journal papers and four international peer-reviewed conference papers published in conferences including IEEE International Energy Conference,

Presentations and Invited talks: Consortium partners have disseminated the project concepts and its results at more than 14 presentations including invited talks at EE-ISAC 15th Open Plenary, the European Utility Week, and the Slovenian cyber night event.

Standardization activities: In joint effort with the partners of the PHOENIX consortium, DNV will take the lead to establish a CCC that will contribute with cyber security and privacy issues relevant for EPES. Consequently, promoting new work items in Standardization Development Organizations (SDOs). PHOENIX partners have actively participated, monitored and contributed to several standardization efforts. In particular DNV, Thales SIX GTS France, and AALTO have actively contributed to the CEN/CENELEC-TC205- WG18, ETSI PDL, W3C WoT, 5G-IA Security Working Group, ETSI NFV-SEC, and ETSI ISI.

1. Introduction

This deliverable describes the dissemination and standardization activities performed by the consortium members. In particular, the deliverable details the actions taken by various consortium members and reports the publications related to the project.

Dissemination Activities:

The deliverable reports presentations, web sites, public reports, and publications as well as other dissemination actions. Scientifically relevant results have been produced in the format of conference and peer-reviewed journal publications. Moreover, a number of invited talks, panel discussion have been used to connect to the community and address all the potential stakeholders.

Standardization Activities:

PHOENIX has contributed to relevant standardization organisations by participating to regular hands-on meetings, calls, and work-in progress specifications. Furthermore, the PHOENIX cybersecurity certification centre will ensure cybersecurity and privacy of vendor products, services, and other assets in the smart grid through certification, testing, and verification. In this manner, it will ensure that platforms, systems, and devices adhere with industry consensus cybersecurity specification for the smart grid, including privacy protection, effective intrusion detection, and seamless interoperability.

2. Relevant Publications and Standardization Venues

PHOENIX identified a number of international dissemination venues for the project results. They cover both the industrial and academic areas. We target a list of potential high-value venues in order to increase the impact of the project results. We also identified a list of standardization bodies with the aim of proposing relevant PHOENIX results to be considered for the inclusion in future standards. Moreover, the PHOENIX cybersecurity certification centre will provide the main security and privacy issues to be addressed in the EPES.

2.1. Journals and Conferences

We built a list of potential publication venues balancing the scientific standing and the community outreach, as well as to have a global coverage and to extend PHOENIX dissemination beyond the academic community. In particular, in the DoA we have identified a collection of relevant journals, magazines and high quality peer-reviewed conferences and workshops. The list available in the DoA is still valid, but of course the list is not exhaustive and partners are free to submit papers to other publishers, as well.

For reference, below is the list from the DoA:

- Journals and magazines:
    - Cyber Security/Privacy: Elsevier "Computers & Security", Elsevier "The Journal of Information Security and Applications", Springer "European Journal for Security Research", IEEE "Cyber Security", IEEE "Forensics Journal", ACM "Transactions on Privacy and Security", Taylor & Francis "Journal of Cyber Security"
    - EPES: IEEE/ACM Transactions on Networking, Communications Magazine, Metering & Smart Energy International journal
    - Communications: ACM "Computer Communication Review", IEEE/ACM "Transactions on Networking", Elsevier "Computer Networks", Frontiers Media "Frontiers in Blockchains", IEEE Access
- Conferences:
    - Security/Privacy: Computers, Privacy and Data Protection (CPDP), ETSI Security Week Communications: IEEE Cybersecurity Development Conference, IEEE International Conference on Cyber Security and Cloud Computing, IEEE European Symposium on Security and Privacy, Blockchain Week
    - EPES: IEEE Smart Grid, IEEE GLOBECOM, IEEE SmartGridComm

2.2. Standardization Organizations

Here, we briefly, mention the list of SDOs that we target. More details will be described in section 4.2. In particular, we target SDOs including:

- CEN/CENELEC: CEN and CENELEC's standardization activities are divided into 14 different business sectors that cover a wide spectrum of areas, from chemicals to transport. Together with them, CEN and CENELEC have also identified priority horizontal topics which respond to specific societal needs and challenges such as smart grid, smart metering, smart house, eMobility, and artificial intelligence.
- ETSI PDL: INDUSTRY SPECIFICATION GROUP (ISG) PERMISSIONED DISTRIBUTED LEDGER (PDL). The aim of this ISG is to provide the foundations for the operation of permissioned distributed ledgers, with the purpose of creating an open ecosystem of industrial solutions to be deployed by different sectors, and therefore contributing to consolidate the trust on information technologies supported by global, open telecommunications networks.
- 5G IA Security WG: The purpose of the group is to foster development of the 5G Security Community made of 5G security experts and practitioners who pro-actively discuss and share information to collectively progress and align on the field. This while organizing specific communications/events (e.g. Whitepaper, Workshop …), interacting with other working groups whenever security input is needed and developing liaisons with other interested/interesting security communities. Thales SIX GTS France is co-chairing this working group and is active to disseminate the scientific results of the PHOENIX project.
- ETSI NFV-SEC: The original target of this SDO consisted in providing a pre-standardization study before considering later a broader standards proposal in a new or existing standardization group. It was important to first clearly define, agree, and share the goals of virtualising network functions with the whole industry.
- ENISA: The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieve a high common level of cybersecurity across Europe. The ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, and cooperates with member states and EU bodies. Through active participation of partners such as Thales SIX GTS France, this will help to disseminate the scientific results of the project in the scope of distributed intrusion detection, federated learning, and privacy preserving communications.
- W3C WoT: The Web of Things (WoT) seeks to counter the fragmentation of the IoT, making it much easier to create applications without the need to master the disparate variety of IoT technologies and standards. Digital twins for sensors, actuators and information services are exposed to consuming applications as local software objects with properties, actions and events, independently of the physical location of devices or the protocols used to access them.

3. Dissemination Activities

PHOENIX partners have been actively present in various talks and panels. Below, we provide the details of these presentations.

3.1. Talks and Presentations

Table 1: Presentation at EE-ISAC Open Plenary

Title	The H2020 PHOENIX project and its Incidents Information Sharing Platform for Energy Stakeholders and CERTs/CSIRTs
Speaker	Sofia Tsekeridou, ISOFT
Type	Closed group session / EE-ISAC 15th Open Plenary
Venue	Online
Website (if applicable)	https://www.ee-isac.eu/ee-isac-plenary
Date	25 November 2020
Abstract	PHOENIX and I2SP was presented to the EE-ISAC during a closed group session.

Table 2: Presentation at Working Group Discussion of H2020 Bridge

Title	PHOENIX Data management
Speaker	Multiple
Type	Working group discussion
Venue	Online
Website (if applicable)	https://www.h2020-bridge.eu/working-groups/data-management/
Date	6 November 2020
Abstract	PHOENIX also participated and contributed to the BRIDGE Data Management Working Group, providing feedback with respect to the DM WG preliminary draft reports and contributed to the EU data exchange reference architecture version 1, by providing business roles identified within the Phoenix project and mapping them to the Harmonized electricity market roles model (HEMRM)

Table 3: Presentation at the European Utility Week 2019

Title	European Utility Week 2019
Speaker	Smilja Dolgan Paternoster, ISKRA
Type	Exhibition
Venue	Paris Expo Porte de Versailles, Paris, France
Website (if applicable)	https://www.enlit-europe.com/euw
Date	12 – 14 November 2019
Abstract	ISKRA were presenting the PHOENIX project at the European Utility Week in the context of their security programme. We included the PHOENIX description in our presentation application. This application is used on all events Iskraemeco is participating at and it is also the part of our Customer Experience Center.

Table 4: Presentation at the Utilitalia-webinar

Title	Utilitalia – Webinar
Speaker	Tommaso Bragatto, ASM
Type	Webinar
Venue	Online meeting
Website (if applicable)	http://www.utilitalia.it:80/eventi/prossimi?d2040f01-2223-49d7-8109-c89cf6ad2d3b
Date	23 October 2020
Abstract	During the presentation of the project results, the main concept of PHOENIX project was disseminated.

Table 5: Presentation at the Future Grid Day-Webinair

Title	FUTURE GRID DAY
Speaker	Massimo Cresta, ASM
Type	Webinar
Venue	Online meeting

Website (if applicable)	https://www.utilitenergy.it/evento/11008/future-grid-day/agenda
Date	25 November 2020
Abstract	The presentation introduced the cybersecurity aspects related to the electrical distribution network.

Table 6: Presentation at the Slovenian 24/7/365 Conference

Title	24/7/365 Conference
Speaker	Teja Setničar, BTC
Type	Conference
Venue	Virtual Conference
Website (if applicable)	https://www.gzs.si/Dogodki/2-10-2020/konferenca-247365
Date	2 October 2020
Abstract	In October 2020, BTC Company, as a sponsor, financially and substantively supported the implementation of the Conference 24/7/365 (https://www.gzs.si/Dogodki/2-10-2020/konferenca-247365) and the CyberNight event (https://cybernight.org), organized by the Chamber of Commerce and Industry of Slovenia and Digital Innovation Hub of Slovenia. The event took place on 2nd of October in the premises of the Chamber of Commerce and Industry, participants were also able to watch the conference online. Conference addressed following main topics: • Levers to increase cyber security resistance, • Global challenges and cyber security management, • Important points and lessons in dealing with incidents, • Ethical hacker - the profession of the future. The conference was attended by many Slovenian companies, universities, and state institutions of Slovenia. As part of the conference, BTC Company presented its activities and projects in the field of cyber security, as well as the Phoenix project where BTC participates as one the pilot fields for new developed solutions on electrical power system cyber security. The 24/7/365 conference was simultaneously accompanied by the CyberNight event, during which a hackathon took place. The purpose of hackathon was to address the following areas (Hacking applications, Reverse Engineering, Osint). Hackathon has recorded the international participation of individuals and companies which work in the field of cyber security.

Table 7: Presentation at the Internal Strategic Conference BTC

Title	Internal Strategic Conference BTC
Speaker	Damjan Kralj, BTC
Type	Conference
Venue	Radisson Blu Plaza Hotel
Website (if applicable)	Internal BTC Intranet
Date	25 February 2020
Abstract	In February 2020, BTC Company held an internal strategic conference for employees at which strategies, goals, projects and action plan was presented. The CEO of BTC, Damjan Kralj, held a presentation in which he presented key strategic projects that are important for the development of BTC in the future. Among the key projects he presented the PHOENIX project, its goals and benefits.

Table 8: Presentation at the IEEE International Energy Conference- Flexible Framework

Title	A flexible framework to investigate cascading in interdependent networks of power systems
Speaker	Nikolaus Wirtz, RWTH
Type	Conference
Venue	IEEE International Energy Conference 2020
Website (if applicable)	https://web.cvent.com/event/5569bdf7-1e9a-43c8-9f19-d068c2ef2267/summary
Date	28 September— 1 October 2020
Abstract	see Section 3.2

Table 9: Presentation at the IEEE International Energy Conference – A stochastic assessment of attacks

Title	A Stochastic Assessment of Attacks based on Continuous-Time Markov Chains
Speaker	Nikolaus Wirtz, RWTH

Type	Conference
Venue	IEEE International Energy Conference 2020
Website (if applicable)	https://web.cvent.com/event/5569bdf7-1e9a-43c8-9f19-d068c2ef2267/summary
Date	28 September2020— 1 October 2020
Abstract	see Section 3.2

Table 10: Presentation at the RWTH Annual Report 2020

Title	Annual Report 2020
Type	Report
Website (if applicable)	https://www.iaew.rwth-aachen.de/global/show_document.asp?id=aaaaaaaaaqmvdkc
Date	31 December 2020
Abstract	Presentation and dissemination of the PHOENIX project and the current state of progress.

Table 11 Presentation at the EnergyShield-PHOENIX-SDN-microSENSE Workshop

Title	EnergyShield - PHOENIX - SDN-microSENSE: Workshop
Speaker	Elena Sartini, CEL
Type	Inter – projects workshop
Venue	Online meeting
Website (if applicable)	N/A
Date	23 July2020
Abstract	The workshop was organized to foster the collaboration among three energy projects, i.e. Energy Shield, PHOENIX and SDN - microSense. During the workshop, CEL had the opportunity to present the PRESS framework explaining the pillars on which it is based, showing in particular the importance of creating a collaborative environment between ethics, legal and data protection experts and technical experts. In the end, CEL also had

	the chance to present the main privacy and data protection aspects that the project at that time had faced and addressed.

Table 12: Presentation at the Synergies with H2020 research projects in digitalization of the energy sector

Title	Synergies with H2020 research projects in digitalization of the energy sector – EDGEFLEX and PHOENIX
Speaker	Mihai PAUN – CRE Emiliano MARQUESINI – CRE Theodore ZAHARIADIS – SYN
Type	Stakeholders Consultation Event
Venue	Online
Website (if applicable)	http://www.eddie-erasmus.eu/events-eddie/eddie-webinar-evsw-2020/
Date	17 November 2020
Abstract	The EDDIE Webinar aims to respond to key questions raised by the 4th Revolution, addressing the main forces of change in ENERGY transition: Low carbon objectives & digitalization. Using EDUCATION lenses we will look at the ENERGY sector to find solutions for the LEARNING transition, as well.

Table 13: Presentation at the Stakeholders consultation event and synergies within the European H2020 Projects

Title	Stakeholders Consultation Event and synergies within the European H2020 Projects SOGNO, WISEGRID, PHOENIX, CROSSBOW and DEFENDER
Speaker	Mihai PAUN – CRE Farhan SAHITO – CTS
Type	Stakeholders Consultation Event
Venue	Online
Website (if applicable)	https://phoenix-h2020.eu/wp-content/uploads/2020/04/CRE_draft_program_April_30_2020.pdf
Date	30 April, 2020
Abstract	The event was organized by CRE (Romanian Energy Center) as an online video conference to stimulate discussions and

	demonstrations of the tools and solutions developed within the EU projects.

3.2. Publications

3.2.1. Peer-reviewed International Journals

Table 14: Publication at the IEEE Open Journal of the Communications Society – Incidents Information Sharing Platform for Distributed Attack Detection

Title	**Incidents Information Sharing Platform for Distributed Attack Detection**
Author list with their affiliations	**Konstantina Fotiadou (Synelixis Solutions)** **Terpsichori Helen Velivassaki (Singular Logic)** **Artemis Voulkidis (Synelixis Solutions)** **Konstantinos Railis (Synelixis Solutions)** **Panagiotis Trakadas (University of Athens)** **Theodore Zahariadis (Synelixis Solutions)**
Conference/Journal	IEEE Open Journal of the Communications Society
DOI or link	https://doi.org/10.1109/OJCOMS.2020.2989925.
Status	**Published**
Publication/Submission date	**27 April 2020**
Abstract	**Intrusion detection plays a critical role in cyber-security domain since malicious attacks cause irreparable damages to cyber-systems. In this work, we propose the I2SP prototype, which is a novel Information Sharing Platform, able to gather, pre-process, model, and distribute network-traffic information. Within the I2SP prototype we build several challenging deep feature learning models for network-traffic intrusion detection. The learnt representations will be utilized for classifying each new network measurement into its corresponding threat level. We evaluate our prototype's performance by conducting case studies using cyber-security data extracted from the Malware Information Sharing Platform (MISP)-API. To the best of our knowledge, we are the first that combine the MISP-API in order to construct an information sharing mechanism that supports multiple novel deep feature learning architectures for intrusion detection. Experimental results justify that the proposed deep feature learning techniques are able to predict accurately MISP threat-levels.**

Table 15: Publication at the MDPI Energies Journal-Proactive Critical Energy Infrastructure Protection via Deep Feature Learning

Title	Proactive Critical Energy Infrastructure Protection via Deep Feature Learning. Energies, 13 (10), 2622.
Author list with their affiliations	Konstantina Fotiadou (Synelixis Solutions) Terpsichori Helen Velivassaki (Singular Logic) Artemis Voulkidis (Synelixis Solutions) Dimitrios Skias (Intrasoft International) Corrado De Santis (BFP Group) Theodore Zahariadis (Synelixis Solutions)
Conference/Journal	Energies (ISSN 1996-1073; CODEN: ENERGA)
DOI or link	https://www.mdpi.com/1996-1073/13/10/2622/htm
Status	Published
Publication/Submission date	21 May 2020
Abstract	Autonomous fault detection plays a major role in the Critical Energy Infrastructure (CEI) domain, since sensor faults cause irreparable damage and lead to incorrect results on the condition monitoring of Cyber-Physical (CP) systems. This paper focuses on the challenging application of wind turbine (WT) monitoring. Specifically, we propose the two challenging architectures based on learning deep features, namely—Long Short Term Memory-Stacked Autoencoders (LSTM-SAE), and Convolutional Neural Network (CNN-SAE), for semi-supervised fault detection in wind CPs. The internal learnt features will facilitate the classification task by assigning each upcoming measurement into its corresponding faulty/normal operation status. To illustrate the quality of our schemes, their performance is evaluated against real-world's wind turbine data. From the experimental section we are able to validate that both LSTM-SAE and CNN-SAE schemes provide high classification scores, indicating the high detection rate of the fault level of the wind turbines. Additionally, slight modification on our architectures are able to be applied on different fault/anomaly detection categories on variant Cyber-Physical systems.

3.2.2. Peer-reviewed International Conferences

Table 16: Publication at the IEEE International Energy Conference- A flexible framework to investigate cascading in interdependent network of power systems

Title	A Flexible Framework to Investigate Cascading in Interdependent Networks of Power Systems
Author list with their affiliations	Nikolaus Wirtz (RWTH Aachen University) Antonello Monti (RWTH Aachen University)
Conference/Journal	2020 6th IEEE International Energy Conference (ENERGYCon)
DOI or link	10.1109/ENERGYCon48941.2020.9236542
Status	Published
Publication/Submission date	29 October 2020
Abstract	This paper introduces a flexible framework to analyze cascading effects in the interdependent power and information and communications technology (ICT) networks that that comprise a power system. This framework supports integration of interdependencies between the power grid and various ICT networks, but also of domain-specific intra-dependencies of these different subsystems. The framework is applied to model a simple example system, where three failure scenarios are defined and simulated to showcase the applicability of the framework for the investigation of cascading effects.

Table 17: Publication at the IEEE International Energy Conference – A stochastic assessment of attacks based on continuous time Markov chains

Title	A Stochastic Assessment of Attacks based on Continuous-Time Markov Chains
Author list with their affiliations	Abhinav Sadu (RWTH Aachen University) Marija Stevic (RWTH Aachen University) Nikolaus Wirtz (RWTH Aachen University) Antonello Monti (RWTH Aachen University)
Conference/Journal	2020 6th IEEE International Energy Conference (ENERGYCon)
DOI or link	10.1109/ENERGYCon48941.2020.9236600

Status	Published
Publication/Submission date	29 October 2020
Abstract	This paper introduces a flexible framework to analyze cascading effects in the interdependent power and information and communications technology (ICT) networks that that comprise a power system. This framework supports integration of interdependencies between the power grid and various ICT networks, but also of domain-specific intra-dependencies of these different subsystems. The framework is applied to model a simple example system, where three failure scenarios are defined and simulated to showcase the applicability of the framework for the investigation of cascading effects.

3.2.3. Professional Conferences

Table 18: Publication at the 22nd Days of Energy Conference

Title	The 22nd Days of Energy Conference
Author list with their affiliations	Media company Finance
Conference/Journal	Conference
DOI or link	https://dnevi-energetikov.si/
Status	Published
Publication/Submission date	23 November 2020
Abstract	The 22nd Days of Energy Conference took place on 23rd and 24th November 2020 as an online conference and was organized by Slovenian media company Finance (https://dnevi-energetikov.si/). Days of Energy is a central event for energy managers and experts from Slovenian companies, research institutions and all those who operate on the principle of efficient energy use. The conference was attended by many Slovenian companies, universities, and state institutions of Slovenia. As part of the conference, BTC Company presented PHOENIX brochure with its activities. At the end of conference there was a ceremonial awarding of energy prizes and recognitions for energy efficiency.

Table 19: Publication at the annual report 2019 (Internal)

Title	Internal publications
Author list with their affiliations	BTC d.d.
Conference/Journal	Internal publications
DOI or link	www.btc.si
Status	Published
Publication/Submission date	March 2020, January 2020, February 2020
Abstract	Annual Report 2019, Business Plan 2020, Energy Management Report 2019

Table 20: Publications at the Energetika.net

Title	External publications
Author list with their affiliations	BTC d.d.
Conference/Journal	External publications
DOI or link	www.btc.si https://www.energetika.net/novice/ove-in-ure/lani-v-btc-prihranili-96-milijona-kwh-energije-in-proizvedl
Status	Published
Publication/Submission date	December 2020, November 2020
Abstract	Moj BTC 2020, Article on Energetika.net

3.3. Organizations of Workshops and Events

Due to the Covid pandemic, many suitable dissemination events were cancelled, postponed or transformed to online or hybrid formats. PHOENIX partners have still managed to successfully initiate dissemination activities and are planning to intensify these as described below.

3.3.1. Innovation events

The (co-)organization of innovation events is focused on the second half of the project duration, according to the progress of the project and the availability of significant (intermediate) results to be disseminated. Taking into account the ongoing pandemic and related uncertainties, we are planning online workshops, presentations and discussions instead of physical meetings. These activities will include co-organization of dissemination events as part of the European Cluster for Securing Critical Infrastructures (ECSCI, see below).

Two large-scale dissemination events will be organized after the first half of the project and at the end of the project, respectively. The first large scale dissemination events will be organized as a participation in a relevant exhibition (such as Enlit Europe 2021, https://www.enlit-europe.com/) to reach a maximum number of interested people.

3.3.2. Linking with other projects

PHOENIX has joined ECSCI in November 2020. The cluster brings together projects focusing on critical infrastructure protection in various domains to bring about synergetic, emerging disruptive solutions to security issues via cross-projects collaboration and innovation. A first ECSCI workshop in 2020 and an open access book on critical infrastructure protection were two of the results of the cluster activities to date and while PHOENIX was not yet part of the cluster during these achievements, we are planning to participate in future activities, such as co-organizing the 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection in October 2021 in Darmstadt, Germany. Moreover, we have initiated collaboration in various standardization and certification task forces.

Apart from ECSCI, initial collaboration activities, e.g. presentations and exchange on technical approaches and challenges, have been conducted with the projects SDN-microSENSE and ENERGYSHIELD. In the future, we intend to increase collaboration activities.

3.3.3. Exhibition stands and special sessions in conferences

As described above we are planning the participation in an exhibition after the first half of the project. This activity will include an exhibition stand and will be one of the large-scale dissemination events of PHOENIX. We are aiming for the second half of 2021, with Enlit Europe (taking place from November 30th – December 2nd) being a potential candidate for this activity.

As part of ECSCI, we will engage in co-organizing future events and workshops, including participation in conferences and co-organization of special sessions.

3.4. Website

3.4.1. Website summary

The PHOENIX website was launched on time in 2019 and is available at:

- https://phoenix-h2020.eu/

The number of visitors of the PHOENIX website exceeds the initial expectations significantly. Blog posts, newsletters, relevant events and publications are added on a weekly basis. Each of these are also shared on the two social media channels used by PHOENIX, LinkedIn and Twitter. There are also occasional adjustments, such as a recent addition of the project’s first video as well as the second brochure.

3.4.2. KPIs

Below are short comments regarding the KPIs on web site and social media.

- The project is behind on the number of required blog posts (36/80).
- The project is meeting the required number of newsletters published (5/5).
- PHOENIX is meeting search engine visibility requirements and has well exceeded the required number of website visitors (4000 visitors/year, required: 500 visitors).
- The projects has met the required number of LinkedIn followers (149, required: 50) but it is behind on the number of required Twitter followers (129, required: 300), as well as the number of required tweets (53, required: 100).

4. Standardization Activities

This chapter will describe the PHOENIX Cybersecurity Certification Centre (CCC) along with its objectives and relevant assets of focus. Five key objectives will be enumerated and briefly explained. In this context, the PHOENIX monitoring and contribution activities will also be put forward.

4.1. PHOENIX Cybersecurity Certification Centre

Description

In joint effort with the partners of the PHOENIX consortium, DNV will take the lead to establish a CCC that will contribute with cyber security and privacy issues relevant for EPES. By means of comprehensive threat modelling and countermeasures in the PHOENIX project, the focus will be to devise electric grid communications and operations that is secure, seamless, and interoperable. In accordance with identified and applicable international standards, CCC will provide the necessary knowledge and routes for cybersecurity certification. Hence, enabling quality assurance and accreditation of the platforms, systems, and critical components therein that comprise the smart grid, thereby assisting the suppliers to demonstrate the security characteristics and specifications required by the industry going forward [1].

Objectives

The proposed objectives are provided below, and participants of PHOENIX are encouraged to devise new and relevant objectives that support the creation of CCC. The realization of these objectives will provide PHOENIX with the information to create a fully-fledged CCC that ensures cybersecurity and privacy of vendor products, services, and other assets of the smart grid cyber-physical system through certification, testing and verification. In this fashion, ensuring that platforms, systems, components, and manufacturing devices adhere with industry consensus cybersecurity specifications for the smart grid, including privacy protection, effective intrusion detection, seamless interoperability, among others.

A comprehensive focus will be towards the achievement of the following objectives, including but not limited to:

- How will certification, testing and verification be performed?
- How to objectively assess effectiveness of cyber security detection systems, e.g. IDSs?
- How to ensure a seamless interoperability between platforms, systems, and components?
- How to prevent privacy breaches?
- Collaboration with relevant SDOs

4.1.1. How will certification, testing and verification be performed?

There is no silver bullet to achieve this objective, as conformance to a wide range of standards are most likely to be required also in the future. It is therefore necessary to facilitate certification against all applicable specifications, as well as unifying and combining the certification processes as much as possible, and thereby integrating the many test cases that each platform, system, and component will undergo [2]. Many relevant and different certification authorities do already exist and can grant certificates for a particular type of product. Organisations can easily become a certification authority; the main difference comes down to whether the certification authority is a public agency or a private organisation. In some cases, private actors are acknowledged as certification authorities which must abide to governmental laws. Each of these three scenarios are applicable for the cyber security domain of critical infrastructures and are further described in [3].

In December 2014, ENISA published a comprehensive document about smart grid security certification in Europe [4]. The document provides a list of certification standards and schemes, how schemes are currently applied in Europe, and recommendations on certification approaches, as well as a list of statements from stakeholders that underline the need of pan European smart grid certification. By emphasizing security and mitigation risk, accreditation and certification schemes would increase end consumers' confidence in smart grid services and systems and accelerate their acceptance. However, certification is not only a means to give the users of smart grid the confidence and assurance that security and privacy is in place, but also to create trust across the entire smart grid supply chain [4].

PHOENIX invests a lot of time and research in Federated Blockchain & Inter-Distributed Ledgers, which has been proposed as the backbone technology of the PHOENIX project [5]. Blockchain should be introduced as one of the most essential and state-of-the-art technologies behind trust assurance. A blockchain is fairly simple yet powerful in functionality and is described as being a growing list of records, also known as blocks, which are linked together with cryptography. Each block normally contains three items: a cryptographic hash of the previous block, a timestamp, and transaction data [6]. The three items are enough to ensure that completed transactions cannot be altered, tampered, or modified in any way without being noticed. In short, blockchain is a distributed ledger and if used correctly it will show an immense power in distributing authority to certify every transaction through a decentralized platform [7].

The ISA/IEC 62443 family of standards for cybersecurity of industrial automation and control systems is evolving and gaining acceptance. Certification of product development organizations, as well as IACS components and systems are to be set out by an operational group within ISA, called the ISA Security Compliance Institute [8] . Other applicable standards and frameworks that would be of interest within this task: ISO/IEC 15408 (Computer Security Certification), IEC 62351 (Securing Power Systems), IEC 61508 (Functional Safety), UL Cybersecurity Assurance Program, ISO/IEC 27001 (Information Security Management Systems), Network and Information Security (NIS) Directive, all of which are more described in [2]. Certification standards of cryptographic modules, software security, and personnel could also be addressed.

4.1.2. How to objectively assess effectiveness of cyber security detection systems, e.g. IDSs?

Malicious attacks cause irreparable damages to cyber-physical systems and implementation of proper and effective intrusion detection systems becomes a critical part in the smart grid cybersecurity domain. Incidents Information Sharing Platform (I2SP) for distributed attack detection, as described in WP5 (Pan-European EPES Incident's Information Sharing), was brought first by the DEFENDER H2020 Project, and now adopted by the PHOENIX Project. I2SP is a novel Information sharing platform able to gather, pre-process, model, and distribute network traffic information with respect to privacy and detection mechanisms [9].

In recent deliverables, the large-scale pilots (LSPs) within PHOENIX have created the necessary attack-trees for the respective critical energy infrastructures, such as solar PV parks, wind farms and hydropower facilities, and have been comprehensively discussed in the use and implementation of intrusion detection systems, as further explained in Deliverable D1.2 (Threat Modelling and Analysis of unknown threats). One of the challenges is to understand and recognize where to position detection system components, software, and sensors that provide the most beneficiary and effective solution. Besides, applicable standards must be identified and followed for this purpose.

4.1.3. How to ensure a seamless interoperability between platforms, systems, and components?

Interoperability is defined as the ability to exchange information in a timely and actionable manner. Different areas in the smart grid domain utilize diverse data semantic models, which have caused interoperability issues among power systems and components. Hence, interoperability issues have become a major barrier towards smart grids and can also arise in smart grid communications [10]. In that context, APIs will play a critical role to ensure adequate seamless interoperability. Several advancements in API development have been proposed, including client-server data communication, quality of service testing and policies.

In July 2020, the National Institute of Standards and Technology (NIST) U.S Department of Commerce published a *Framework and Roadmap for Smart Grid Interoperability Standards* found in [11]. The framework is intended to assist smart grid stakeholders in future decision making and provide a foundation to guide the smart grid interoperability process moving forward.

PHOENIX WP2 (Secure and Persistent Communications), in particular Deliverable D2.3 (Data sovereignty and semantic interoperability), have already addressed the issue of smart grid interoperability. This objective will be followed up in D8.6 with comprehensive focus on the standardization and certification aspect.

4.1.4. How to prevent privacy breaches?

Addressing how to prevent privacy breaches, a certification against the relatively new established General Data Protection Regulation (GDPR) would be a natural entry point for this objective. GDPR is an EU regulation that obliges all organisations processing personal data in any form, within the EU or relating to EU citizens to comply with sensitive and personal data protection rules. Different solutions within PHOENIX can potentially process consumers' private data after or in the course of the project. For example, client workstations within SCADA systems could store personal information or the smart meters' database that handles, stores and process consumption data. Conformance to GDPR can prevent organisational and personal disclosure of sensitive information within PHOENIX and the smart grid in general [2].

State-of-the-art technologies in the smart grid having both wired and wireless mediums may create a big attack surface with respect to privacy breaches. In that sense, more standards and privacy regulations are needed as GDPR alone would not be sufficient. The well-known ISO/IEC 27001 standard which greatly overlaps with GDPR will be one example of addition that enables some common specifications, such as the assurance of data integrity, confidentiality by data encryption, as well as data availability and security testing [12].

PHOENIX is working on a so-called Privacy, Ethics, Security and Societal (PRESS) framework, which describes a process with three main pillars:

- privacy and data protection,
- ethics and social concerns,
- and security elements.

The approach is applicable in all sectors, including energy and renewables, as is further described in the public Deliverable D4.1 – PRESS Analysis Framework [13]. The ultimate privacy objective in PHOENIX is to establish a Privacy Protection Enforcement (PPE), an advanced legal framework for managing data, ensuring adequate levels of GDPR compliance, well beyond legacy Data Management Platforms [14].

4.1.5. Assets to focus

The identified assets are mainly the security products, such as firewalls, detection systems, TPM devices, SIEM products, etc. that will protect the smart grid and encompass one or more of the following levels:

- Manufacturing (CPUs, PCBs, etc.)
- Components (PLCs, IEDs, RTUs, HMIs, AMS, etc.)
- Distributed systems and platforms (SCADA, DCS, SDN, 5G telecom, blockchain, cloud, etc.)

It is necessary to identify relevant standard requirements for the desired cybersecurity properties that covers hardware and software on the component, system, and manufacturing level. Vendor components and systems need suitable requirements to ensure safe, secure, and reliable operations, whilst the manufacturing level would for instance need requirements on secure design and development [2]. Hence, state-of-the-art cybersecurity products and technologies created to protect the smart grid must be addressed.

4.2. Monitoring and Contribution Activities

Table 21: Consortium Activities in the CEN/CENELEC

SDO Body	CEN/CENELEC -TC205- WG18
Partner	DNV
Status	DNV is a contributor
PHOENIX Interest	PHOENIX project will provide guidelines to the working committee of TC205 WG18 on various aspects of cybersecurity that can affect the interface between the home and the electricity grid. This is done through an interface called the CEM in the standards document in preparation prEN50491-12-2.

Contribution	Contribution from PHOENIX is through regular committee meetings (currently online) on the writing of the standards and analysis of comments obtained from experts of the 27 EU member states.
Links or documents	prEN50491-12-2

Table 22: Consortium Activities in the ETSI/NFV-SEC

SDO Body	ETSI /NFV-SEC
Partner	TSG
Status	TSG is contributor to different specs in the NFV-SEC.
PHOENIX Interest	PHOENIX provides secure persistent communications. It leverages the 5G as a security enabler with low latencies and high throughput.
Contribution	Contributions are ongoing for different specs in particular for orchestration and trust management.
Links or documents	The document is a working copy, not published yet.

Table 23: Consortium Activities in the 5G IA Security WG

SDO Body	5G IA Security WG
Partner	TSG
Status	TSG is co-chairing the 5G IA Security WG
PHOENIX Interest	Our 5G activities in PHOENIX will be further disseminated in this working group, in terms of white papers, or participation to workshops.
Contribution	TSG is active in this working group, and participates in all the meetings, providing more opportunities to disseminate PHOENIX activities in terms of contributions to whitepapers or workshops.
Links or documents	Status of documents: ongoing

Table 24: Consortium Activities in the ETSI ISI

SDO Body	ETSI ISI
Partner	TSG
Status	TSG is a member and contributor
PHOENIX Interest	Machine learning based threat detection
Contribution	TSG participates to the meetings. There may be contribution in some specs writing in the context of PHOENIX.
Links or documents	https://portal.etsi.org/TB-SiteMap/ISI/ISI-List-members

Table 25: Consortium Activities in the ETSI PDL

SDO Body	ETSI PDL
Partner	AALTO
Status	Contributor
PHOENIX Interest	DLT and interledger technology
Contribution	AALTO team participated in several contribution drafts that were also accepted during 2020. Contributions so far (during 2020) in context of another EU project (SOFIE). But there may be some contribution also in PHOENIX context later on.
Links or documents	https://www.etsi.org/committee/1467-pdl

Table 26: Consortium Activities in the W3C WoT

SDO Body	W3C WoT
Partner	AALTO
Status	Following
PHOENIX Interest	IoT technology, e.g. related to smart meters
Contribution	AALTO team is following the developments of this interest group.
Links or documents	https://www.w3.org/WoT/IG/

5. Conclusions

In this deliverable, we reported several dissemination and standardization activities performed by the consortium in the period M1-M18 of PHOENIX project.

PHOENIX successfully targeted several international journals and conferences/workshops meeting the KPI set for the dissemination activities for the given period. More activities are being planned for the second period of the project.

We presented the diverse standardization bodies and dissemination opportunities identified by PHOENIX to develop the key innovations while contributing to the international standardization effort and disseminating the progresses.

PHOENIX has actively participated, monitored and contributed to several standardization and homogenization efforts. Partners have been active in joining the standardization activities such as CEN/CENELEC, ETSI PDL, W3C WoT, ETSI NFV-SEC, and 5G-IA Security Working Group. Furthermore, the PHOENIX cybersecurity certification centre will address the main cybersecurity and privacy threats for the EPES including the intrusion detection, machine learning based detection, privacy attacks and privacy-preserving mechanisms, distributed ledger based communications, and cloud native based communications.

6. References

[1] PHOENIX, “Admin GA - Amendment Reference No AMD-832989-4,” 2019.

[2] SUCCESS, “Deliverable D6.8 v1.0: Report on Certification Preparations,” 2018.

[3] CRISP, “Deliverable D2.1: Report on security standards and certification in Europe - A historical/evolutionary perspective,” 2017.

[4] ENISA, “Smart grid security certification in Europe – challenges and recommendations,” 2014.

[5] PHOENIX, “Blockchain for Electrical Power Energy Systems. [Online]. Available: https://phoenix-h2020.eu/blockchain-for-electrical-power-energy-systems-phoenix-h2020/. [Accessed 13 February 2021].,” 2021.

[6] PHOENIX, “Will blockchain be a game changer in energy?,” [Online]. Available: https://phoenix-h2020.eu/will-blockchain-be-a-game-changer-in-energy/. [Accessed 10 February], 2020.

[7] IEEE, “Blockchain applications in Smart Grid-Review and Frameworks. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8730307. [Accessed 9 February 2021].,” 2019.

[8] PHOENIX, “A more secure supply chain through certification in EPES. [Online]. Available: https://phoenix-h2020.eu/a-more-secure-supply-chain-through-certification-in-epes/. [Accessed 8 February 2021].,” 2020.

[9] IEEE, “Incidents Information Sharing Platform for Distributed Attack Detection . [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9079479. [Accessed 8 February 2021].,” 2019.

[10] IEEE, “Toward Interoperability of Smart Grids. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7984755. [Accessed 9 February 2021].,” 2017.

[11] NIST, “Framework and Roadmap for Smat Grid Interoperability Standards, 2020. [Online]. Available: https://www.nist.gov/system/files/documents/2020/07/24/Smart%20Grid%20Draft%20,” 2020.

[12] NQA, “Does ISO 27001 Cover the Requirements of GDPR? [Online]. Available: https://www.nqa.com/en-gb/resources/blog/august-2017/iso-27001-gdpr-requirements. [Accessed 11 February 2021].,” 2017.

[13] PHOENIX, “PRESS Framework, [Online]. Available: Privacy and Data Protection, Ethics, Social and Security Framework Analysis within the Energy Sector - PHOENIX - H2020 (phoenix-h2020.eu). [Accessed 10 February].,” 2020.

[14] PHOENIX, “Privacy Protection Enforcement. [Online]. Available: https://phoenix-h2020.eu/. [Accessed 8 February 2021].,” 2021.