European Commission

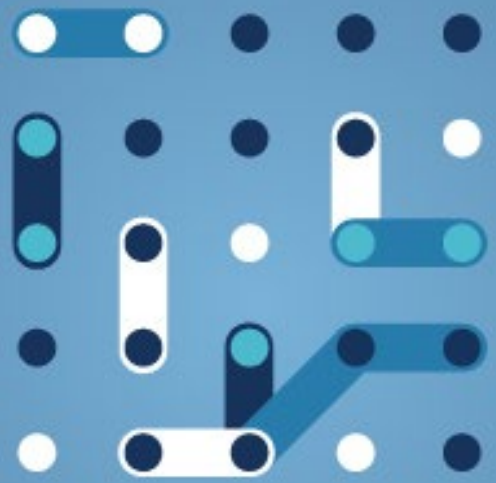
bridge

ENLIT - Session 4

12:30 – 13:30

1st December 2021

Moderated by Olivier Genest – BRIDGE Data Management WG Chair



Network code on cyber-security in energy

www.h2020-bridge.eu

Agenda

Time	Topic	Speaker
12.30 - 12.35	Introduction – scope of the session	Olivier Genest – Moderator
12.35 – 12.45	PHOENIX project Presentation	Paul Lacatus - Senior researcher in D&I Department ICT Manager, Romanian Energy Center – CRE
12.45 – 12.55	Panel Topic 1	All Panelists
12.55 – 13.00	Panel Topic 2	All Panelists
13.00 – 13.10	Panel Topic 3	All Panelists
13.10 – 13.15	Panels Wrap up	Olivier Genest – Moderator
13.15 – 13.30	Closing Words	CASTRO BARRIGON Felipe European Commission

European Commission

- *SCOPE OF THE SESSION*

  - **Which are the new digital data flows that appear with the new technologies.**
  - **In terms of cybersecurity risks, what do you consider specific to energy in your projects?**
  - **Do the new configurations introduce new cyber-risks, and if so, which ones?**
  - **Do you see policy gaps when addressing cybersecurity needs, and if so, in which domains?**
  - **How do the cybersecurity requirements in your projects contribute to the broader concept of resilience in the energy domain?**
  - **Assessing the need for a network code on flexibility markets (also as implementing provisions of the Electricity Regulation)**
  - **What are the R&I priorities based on projects experience?**

Project represented and speaker

PHOENIX

Paul Lacatus

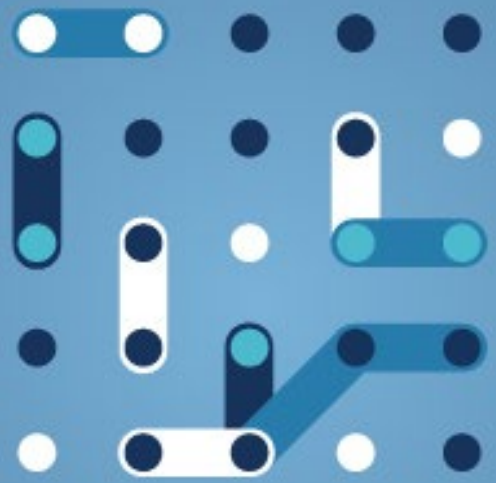
. Senior researcher in D&I Department ICT Manager, Romanian Energy Center – CRE

European Commission

European Commission

PHOENIX

Paul Lacatus



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

Cybersecurity in PHOENIX Project

Eng. Paul Lacatus
EU project senior researcher
Centrul Roman al Energiei – Romanian Energy Center

ENLIT Milano, 1.12.2021

Cybersecurity

Cybersecurity is one of the most important challenges of our time.

- The Information technology and communications ITC became more and more important in our life, society
- Our data is managed mostly by ITC systems
- Our communications , all types is done mainly by the ITC Systems

To keep all this secure, reliable and ethic is a complicated task.

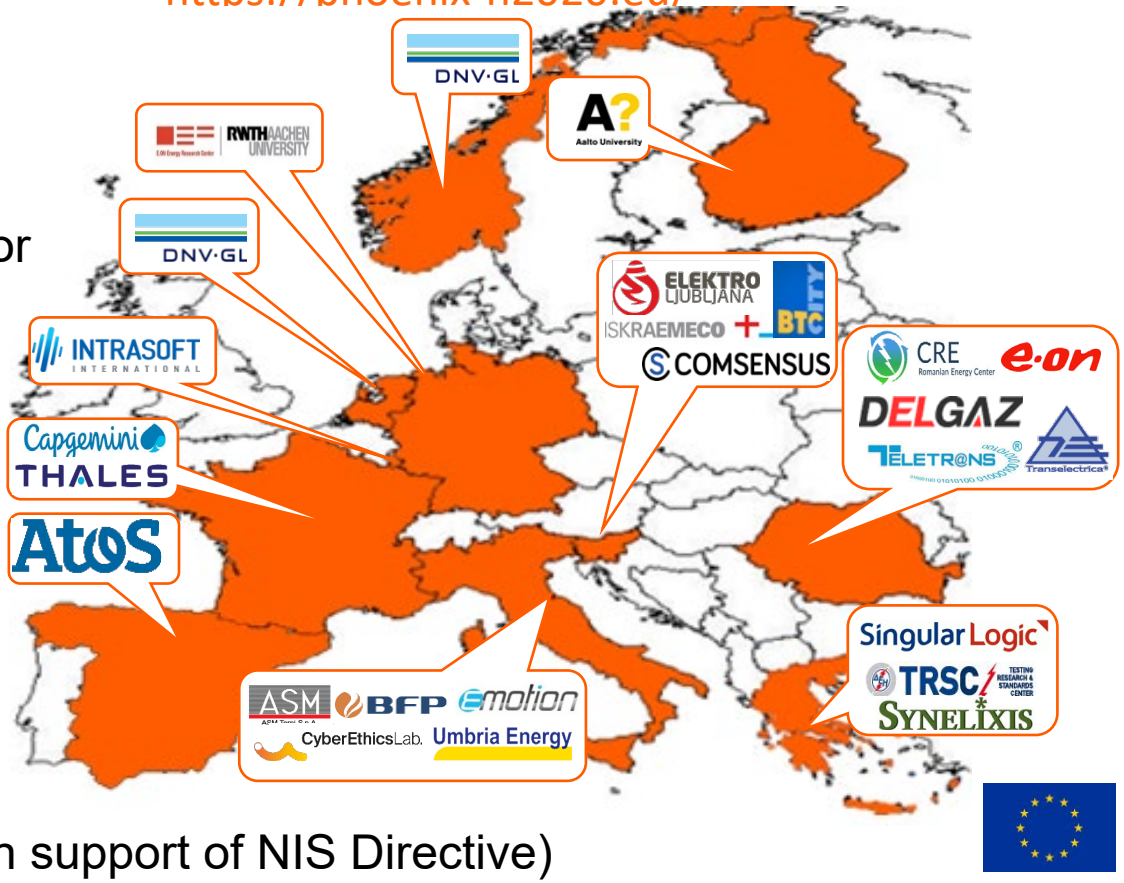
PHOENIX

https://phoenix-h2020.eu/

Project Overview

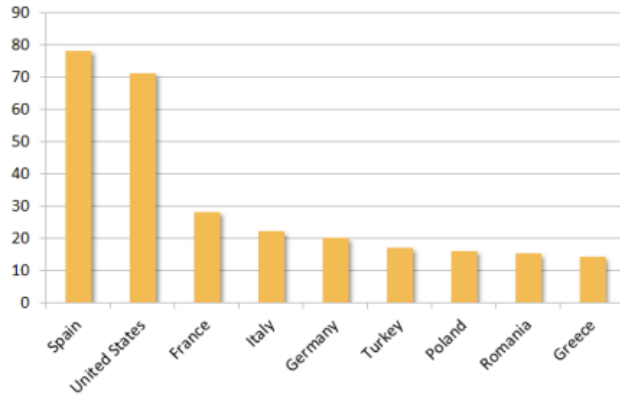
24 partners from 11 countries:

- ✓ 6 Technology Providers
- ✓ 1 TSO + 1 TSO Network Operator
- ✓ 4 DSOs + 2 Energy Retailers
- ✓ 4 Electricity generators
- ✓ 3 Equipment manufacturers
- ✓ 2 End users
- ✓ 1 EPES Association
- ✓ 3 Specialized Technology SMEs
- ✓ 2 Leading Research Institutions
- ✓ CERT-RO is indirectly involved (in support of NIS Directive)

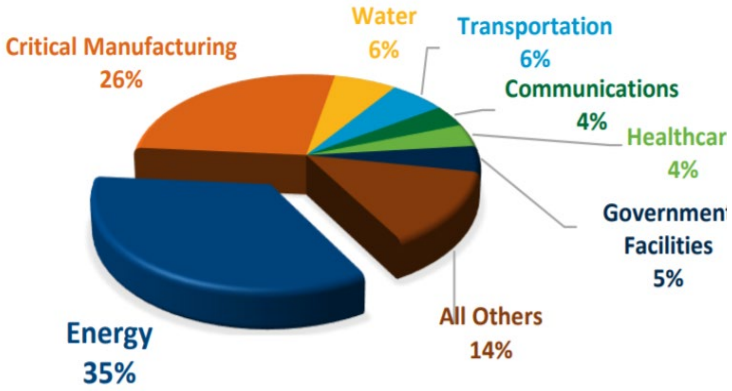


PHOENIX Challenge

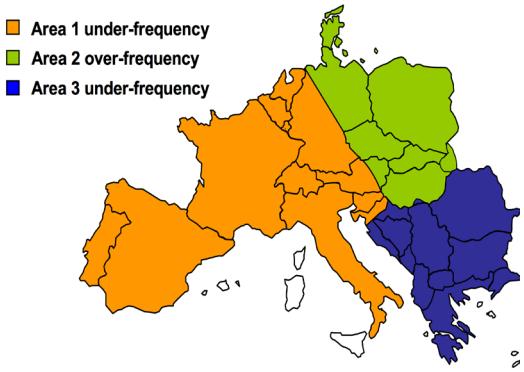
- EPES is considered among the **most complex Cyber-Physical system** with huge (cascading) effects to other critical infrastructures (i.e. water supply, communications, transportation, industry, finance)
- EPES has already experienced significant complex cyber-attacks.



Dragonfly EPES attacks since 2014



Incidents of Cyber Attacks in US
(source: US Department for Homeland Security)

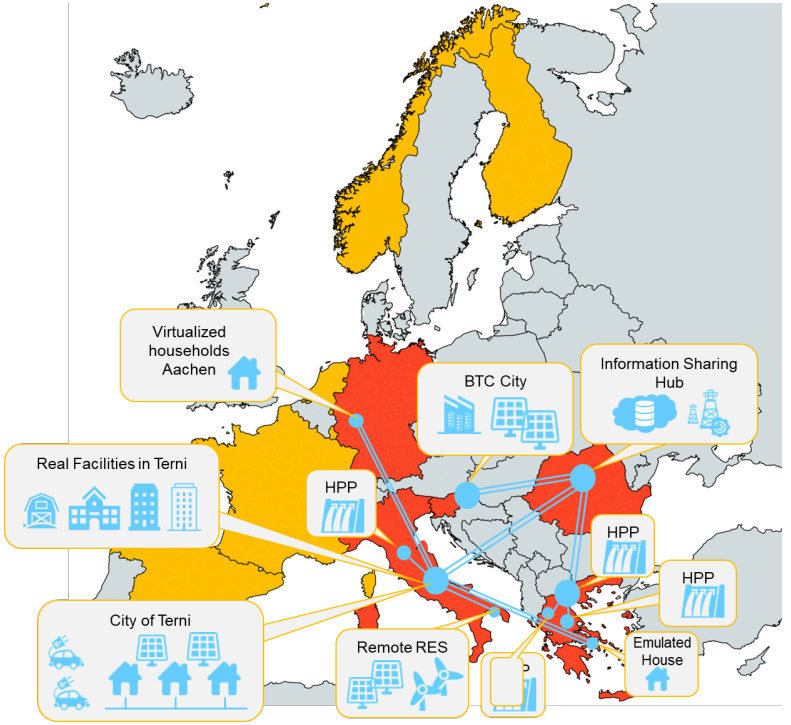


European blackout due to human error
(Nov. 2006)

Overview of PHOENIX Large Scale Pilots

5 diverse Large-Scale Pilots

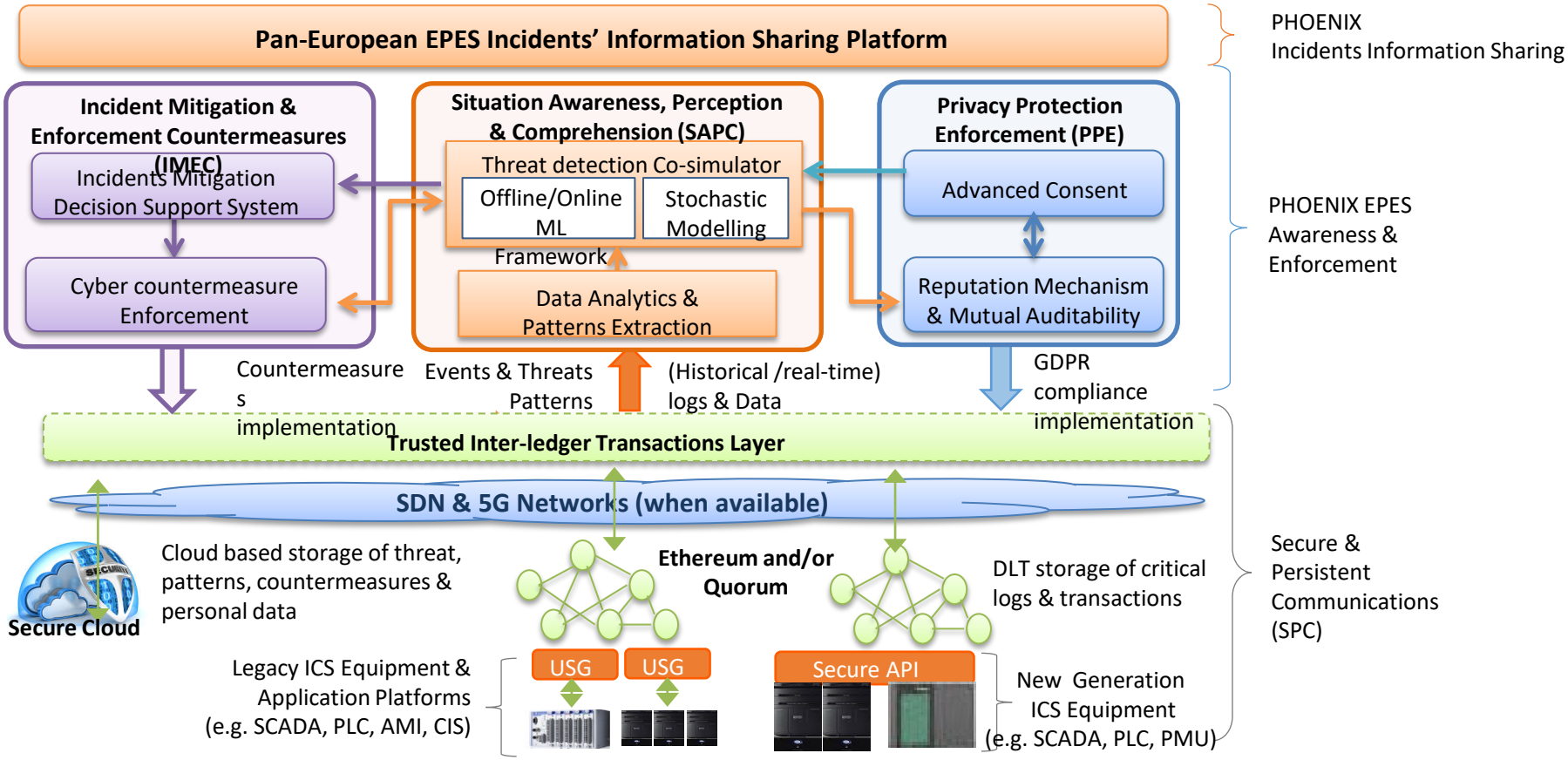
- Multi-utility/Multi-owner RES cyberthreats and data breach detection (Italy)
- National-wide cooperative remotely controlled HPP (Greece)
- Collaborative Microgrid-enabled cyber risks mitigation (Slovenia)
- Collaborative / DSO flexibility vs cybersecurity and privacy (Italy, Germany, Greece)
- National vs Pan-European cooperative cyber threat information sharing (Romania)



Vision and Scope

- **Strengthen EPES cybersecurity preparedness**
  - Cybersecurity Preparedness/Privacy by Design & Cybersecurity by Innovation
- **Coordinate EPES cyber incident discovery, response and recovery**
  - Facilitate cyber threat intelligence (CTI) sharing among authorized utilities, CERTs, CSIRTs, ISACs, NRAs and the NIS cooperation group
  - Accelerate Directive on Security of Network and Information Systems
- **Accelerate research and innovation in EPES cybersecurity**
  - DevSecOps mechanism to ensure code security during its lifetime
  - Applied privacy preserving (federated) Machine Learning
  - Definition of certification methodologies and procedures

PHOENIX Simplified Architecture



PHOENIX achievements
Analysis & Design

1. Risk Identification & Classification

- **Risk identification**
- Effective ***cyber incident & attack*** detection, categorization, prioritization and mitigation
- ***Focus on high availability*** *(resilience, survivability)*, ***fast recovery*** and ***data privacy***.

✓ Analysis of all aspects of Interdependent cyber-human EPES Protection

✓ Designed a risk assessment framework to classify the EPES into secure tiers

✓ Security / Privacy / Survivability by design principles identified and adopted

✓ Privacy, data Protection, Ethics, Security and Societal (PRESS) framework

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

PHOENIX

Thank you

Eng. Paul Lacatus
Romanian Energy Center
Centrul Roman al Energiei
Paul.Lacatus@crenerg.org

Panel Discussion

Panellists

Elena Boskov-Kovacs
ETIP SNET WG4 Co-chair
Managing Partner at
Blueprint Energy Solutions
GmbH

Paul Lacatus
PHOENIX Repr.
Senior researcher in
D&I Department ICT
Manager, Romanian
Energy Center – CRE

European Commission

PANEL Discussion – Starting point for cybersecurity topic

- *EC recommendation on cybersecurity in the energy sector (2019) , that describes in particular energy-sector specificities such as cascading effect, real-time requirements and combination of legacy and state-of-the-art technologies:*

European Commission

1st Questions for the Panelists

Based on EC recommendation on cybersecurity in the energy sector (2019)

1. *Do you see additional specificities?*
2. *How do you tackle them in your project?*

European Commission

2nd Questions for the Panelists

Based on EC recommendation on cybersecurity in the energy sector (2019)

1. *What are you missing from cybersecurity perspective?*
2. *What are the priority issues for future R&I?*

European Commission

3rd Questions for the Panelists

Based on EC recommendation on cybersecurity in the energy sector (2019)

1. *How do you see secure data sharing between energy stakeholders?*
2. *What are your expectations regarding network codes for cybersecurity?*

European Commission

Closing Words (video recorded)

CASTRO BARRIGON Felipe

European Commission

bridge

European Commission