The project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No 832989. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

For more details contact:

Ghasan Bhatti
Project Coordinator
Capgemini Technology Services, France
ghasan.bhatti@capgemini.com

EU H2020 Electrical Power System’s Shield against complex incidents and extensive cyber and privacy attacks
PHOENIX Objectives

- Strengthen EPES cybersecurity preparedness by employing a) “security by design” via novel protective concepts for resilience, self-healing and accountability, and b) security by innovation via adapting, upgrading, integrating and validating a number of TRL5 developments to TRL7-8.
- Coordinate EPES cyber incident discovery, response and recovery, contributing to the implementation of the NIS Directive by developing and validating at national and pan-European level, a novel fully decentralized near real-time synchronized information awareness exchange platform, among authorized utilities, CSIRTs, ISACs, CERTs, NRAs and the strategic NIS cooperation group.
- Accelerate research and innovation in EPES cybersecurity by a novel prevent, detect and mitigate DevSecOps mechanism, secure and privacy preserving federated Machine Learning (ML) algorithms and definition of certification methodologies and procedures.

Concept and Methodology

PHOENIX Architecture

- Secure and Persistent Communication Layer (SPC) for federated and traceable EPES information exchange
- EPES Awareness and Enforcement enabling Situation Awareness, Perception and Comprehension (SAPC), Incidents Mitigation & Enforcement Countermeasures (IMEC) and Privacy Protection Enforcement (PPE)
- Pan-European EPES Incidents Information Sharing Platform (I2SP) as a fully distributed information sharing system, operating as a crowdsourced cyberthreat analysis platform.

Laboratory Testing and Evaluation

The PHOENIX platform will be extensively tested at laboratory environment using semi-automatic procedures for stability and efficiency. This will ensure that the PHOENIX components achieve the expected Technology Readiness Level (TRL) upon the platform integration by establishing suitable evaluation procedures, such as STEP (Systematic Test and Evaluation Process) and benchmark criteria.

Real-life Validation through Pilots

PHOENIX will involve real-world scenarios to validate the effectiveness of PHOENIX across five European Large-Scale Pilots (LSPs) in Germany, Italy, Slovenia, Greece and Romania involving the complete end-to-end generation, transmission, distribution and prosumption value chain. Beyond the individual LSPs, cascading effects even to other critical infrastructures will be simulated and cross-border security and privacy sites will be tested and validated.