For more details contact:

Farhan Sahito
Project Coordinator
Capgemini Technology Services, France
farhan.sahito@capgemini.com

PHOENIX Admin Team
phoenix-info.fr@capgemini.com

Join Us

@H2020Phoenix

/phoenix-h2020/

https://phoenix-h2020.eu/

PHOENIX

PHOENIX

EU H2020

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

The project has received funding from the European Union's Horizon2020 research and Innovation programme under grant agreement N°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.

About PHOENIX

The PHOENIX project is a European Union funded collaborative project aiming at offering a cyber-shield armour to the European Electrical Power Energy Systems (EPES).

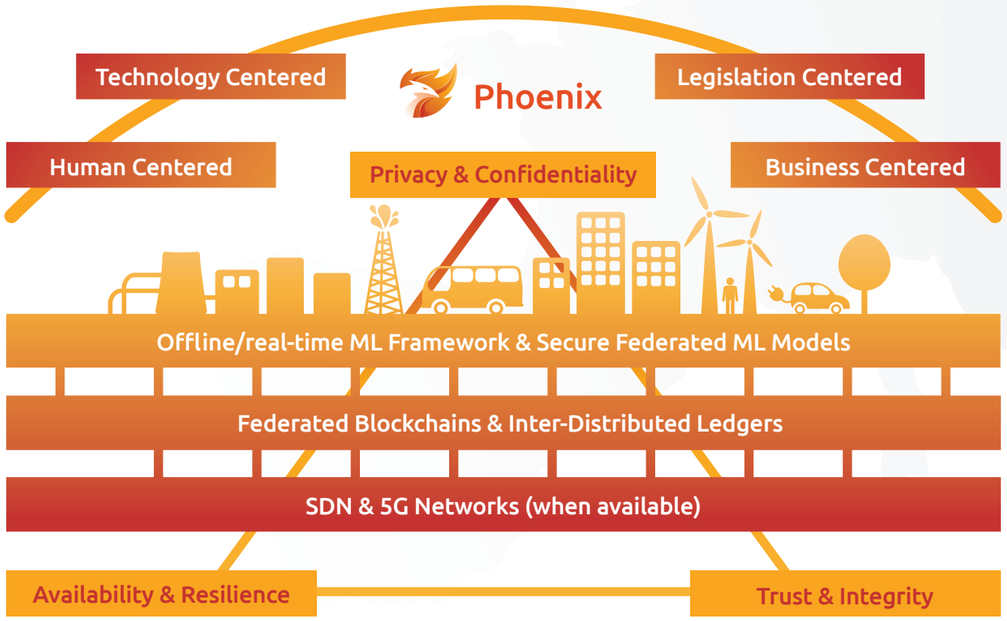
It focuses on the protection of the European end-to-end EPES (from energy production to prosumption) via prevention, early detection and fast mitigation of cyber-attacks.

PHOENIX will involve real-world scenarios to validate the effectiveness of results across 5 European Large-Scale Pilots (LSP) in Italy, Sweden, Slovenia, Greece and Romania involving the complete end-to-end generation, transmission, distribution and prosumption value chain.

H2020 PHOENIX: Project At A Glance

Title:	Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks		
Type of Action:	Innovation Action		
Topic:	H2020-SU-DS04-2018-2020 (Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches)		
Grant Number:	832989		
Total Cost:	11 M Euros	**End Date:**	August 2022
EC Contribution:	8 M Euros	**Duration:**	36 Months
Start Date:	September 2019	**Project Coordinator:**	Capgemini

Key Challenges, Pillars and Technologies



Large Scale Pilots (LSPs)

LSP1 (by ASM, EMOT and BFP) in Italy will validate PHOENIX at operator and prosumer level on a regional and cross-site information exchange at national level. It will validate geographical horizontal regional-scale cyber-threats scenarios and privacy/data breaches governance management.

LSP2 (by PPC) will be provided at distributed renewable energy resources generation level and will feature 3 Hydroelectric Power Plants (HPPs) located in **Greece**. It will validate cybersecurity attacks on hydropower plant assets and measure subsystems, **cybersecurity attacks on ultra-low delay (5G) communications, and energy cascading effects**.

LSP 3 (by ELLJ and BTC) will be implemented in the commercial and industrial area of BTC (shopping, entertainment, business, commercial, and logistics centre) in **Ljubljana, Slovenia**. LSP3 will **demonstrate cyber threats mitigation and data privacy management in a decentralized environment.**

LSP4 (by EON and RWTH) in **Sweden** will use a **demand side response platform** with more than 20 households connected to validate micro grid flexibility versus cybersecurity and privacy attacks. PHOENIX will analyze logs and events from home assets and the DSR system, along with aggregated energy data at neighborhood section to validate several cybersecurity scenarios.

LSP5 (by TELE, TRANS and DEGR) in **Romania** will validate national and cross-border information and incidents exchange and governance hierarchies sharing models as foreseen by NIS Directive. Various **governance models and the complete platform will be validated and response in data sharing from 5 countries, national and regional CERTs and CSIRTs will be evaluated**.