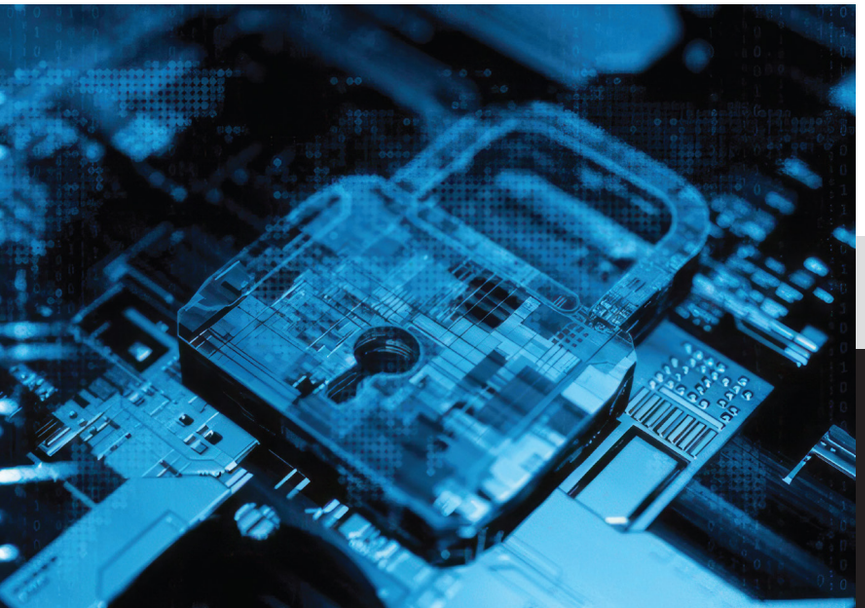
PHOENIIX

Use Cases

will demonstrate and validate the project's functionalities:

- Enhanced Situational Awareness with AI-assisted Prediction, Prevention, Detection & Response capabilities, and business risk impact assessment - based prioritization.
- Proactive and reactive Resilience Automation, Orchestration, and Response (ROAR) mechanisms, providing Business Continuity, Recovery and Cyber & Physical Incident Response.
- Increased Preparedness through relevant Serious Games and realistic Resilience Cyber Range (RCR) Assessment & Training.
- Timely and actionable Information Exchange between OES, National Authorities and EU actors, leveraging interoperable and standardised alerting and reporting mechanisms and processes.



Πανεπιστήμιο Πατρών University of Patras · Sphynx Analytics · ΔΕΗ Public Power Corporation · National Cyber Security Authority Hellenic Republic · COSMOTE · FGC Ferrocarrils de la Generalitat de Catalunya · World Sensing · National CSIRT-CY · Nodalpoint · Atos · Social Engineering Academy · AEGIS IT Research · APIROPLUS SOLUTIONS · Eunomia Ltd. Consulting Services · Universitat Politècnica de Catalunya BarcelonaTech · UiO : University of Oslo

PHOENIIX

A European Cyber Resilience Framework with Artificial Intelligence (AI) – assisted orchestration & automation for business continuity, incident response & information exchange

phoeni2x.eu/ · @Phoeni2xProject · @Phoeni2xEUProject · @Phoeni2x

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No101070586.

PROJECT

Use Cases

PHOENIIX

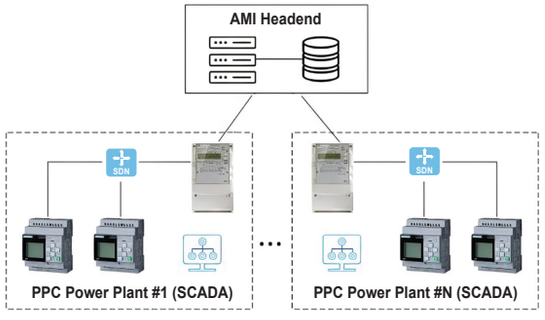
ENERGY

Title: Cascading effects of cyber-attacks against Advanced Metering Infrastructure

Partners: Public Power Corporation (PPC), COSMOTE, National Cyber Security Authority (NCSA) - GREECE

Pilot Description:
Smart meters hold a significant role in the proper operation of the energy market. The collected measurements are used for transparent billing, market clearance, as well as for determining additional actions that ensure load and supply balance. Illegal access and disturbances in the operation of smart meters can result in inaccurate detection and response to emergencies and energy demand, possibly leading to blackouts, and inability to balance the market.

The telecom operator's role is to provide a reliable and highly available communication channel between the smart meters and the central Advanced Metering Infrastructure (AMI) headend.



PHOENI2X will enhance the cybersecurity level (detection, alerting, mitigation, recovery, reporting) of the operators' critical infrastructure, adding AI-assisted capabilities and advanced information exchange.

Incident Scenarios:
1. Massive cyber-attack against smart meters at residential houses, industrial customers, distribution (sub)stations.
2. DDoS attacks against the AMI Headend.

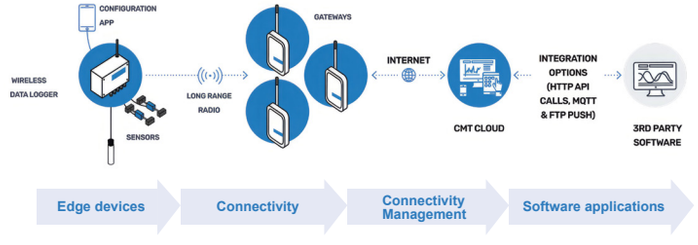
TRANSPORT

Title: Cyber & physical attacks and risk management service to railway management system

Partners: Ferrocarrils de la Generalitat de Catalunya (FGC), Worldsensing - SPAIN

Pilot Description:
Rail infrastructure operators face challenges when operating their infrastructure, as they need to ensure safe operations using resources efficiently. One possible approach is to monitor such critical infrastructures continuously to ensure safety and improve maintenance activities. But the deployment of sensors across the infrastructure may introduce new attack vectors into existing OT/IT infrastructure, which can impact other systems. Such attack vectors may affect data and availability of sensors, and also the robustness of the software platform in charge of managing the deployed sensors.

Therefore, there is a need to assess the security robustness of newly deployed solutions to monitor the infrastructure, and their supporting IT solutions.



PHOENI2X will enhance the preparedness and incident handling capabilities of a next generation digital railway infrastructure, improving the proactive strategy to predict cyber-attacks.

Incident Scenarios:
1. Data security and integrity for the whole end-to-end IoT solution
2. Cyber-robustness of the OT software suite supporting device and network management, alert generation and data integration.

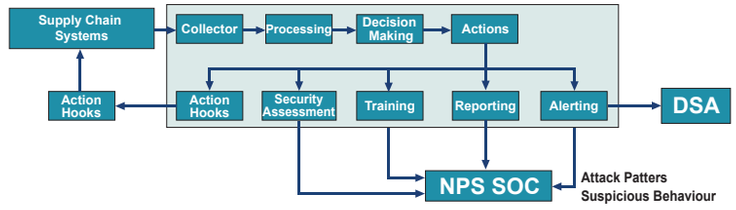
HEALTHCARE

Title: Cyber-attacks aiming to cripple the Public Healthcare System

Partners: Nodalpoint, Digital Security Authority (DSA) - CYPRUS

Pilot Description:
Of particular concern in the field of cybersecurity are supply-chain attacks. The healthcare industry relies on an ever-expanding network of supply-chain vendors, third-party service providers and cloud-based systems. Malicious actors may exploit vulnerabilities within this supply-chain to gain unauthorized access, introduce malicious code, and, ultimately, steal sensitive data or disrupt operations.

The impact of supply-chain attacks in healthcare may vary from delays in treatments, identity theft and regulatory fines to life-threatening situations for patients and loss of business.



PHOENI2X will bolster resilience against supply chain attacks, employing state-of-the-art Situational Awareness, while also enabling advanced business continuity and automated recovery capabilities.

Incident Scenarios:
Supply-Chain attacks to the GHS public web portal, such as:
1. Unauthorized commit,
2. Malicious deletion of a source code branch,
3. Use of a compromised library.