3rd Newsletter

November 2023

WELCOME

In July 2023, we started our second year of the project. This third newsletter presents the project's main achievements over the last five months. From the technical point of view, we have been focused on the integration of the first release of the enablers for the AI-assisted Situational Awareness, Prediction & Response and for the Coordinated Response & Preparedness. Efforts from all partners have been devoted to the development of the MVP version of the PHOENI2X platform.

Review the past editions of the PHOENI2X newsletter to discover the technical advancements, as well as the events and news of the project during its first year of life. Stay tuned to our website, https://phoeni2x.eu/, and Twitter, @Phoeni2xProject, where key project results will be published periodically.

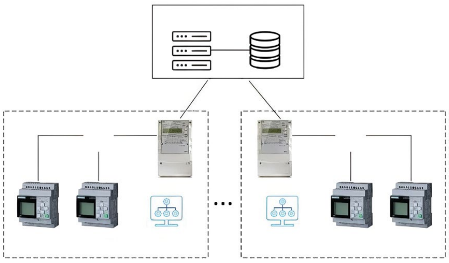
PHOENI2X TECHNICAL ACTIVITIES

PHOENI2X proposes a Cyber Resilience framework with AI-assisted orchestration, automation & response capabilities for business continuity, recovery, incident response, and information exchange, tailored to the needs of Operators of Essential Services and their National Authorities.

Over this period, the key achievements have been the development of the PHOENI2X enablers, their initial integration in the PHOENI2X framework and the establishment of the baseline for the demonstrators for the three use cases covering the essential services sectors: energy, transport and healthcare.

Use Case 1 demonstrates the PHOENI2X platform on an attack and response scenario that takes place on an energy infrastructure. The incident scenarios considered are:

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



CONCEPT 1
Data acquisition from PHY-devices
CONCEPT 2
Data processing from HW and SW products
CONCEPT 3
Data analytics exploiting AI tools

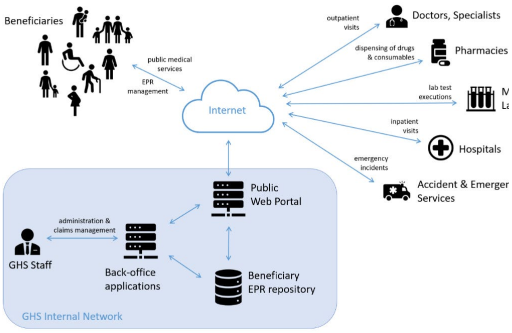
Use Case 2 demonstrates the PHOENI2X framework on a transport infrastructure for safety monitoring of a railway section. The incident scenarios considered are:

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.

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

Use Case 3 demonstrates the PHOENI2X framework in a healthcare environment. The incident scenarios considered are related to supply-chain attacks on the GHS public web portal, such as:

1. Unauthorized commit.
2. Malicious deletion of a source code branch.
3. Use of a compromised library.



PHOENI2X NEWS AND EVENTS

4th PHOENI2X Plenary Meeting

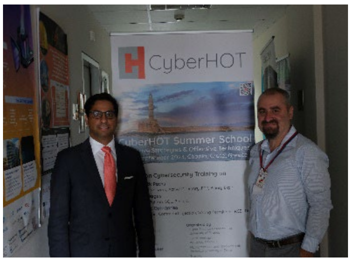
The PHOENI2X 4th Plenary meeting was celebrated on the 7th and 8th of September, 2023, in Athens, Greece. The meeting was hosted by Public Power Corporation (PPC), and its main objective was to discuss the three pilots of the project, focussing on the integration of the PHOENI2X tools, and to conclude the definition of the testbeds of the project for M18.

The first day's discussions revolved around the definition of the Pilots' testbeds and tools integration. First, the progress on the Baseline Testbed deployment was reviewed, followed by the presentation of the three different use cases: Energy led by PPC and COSMOTE, Railway led by FGC and WS, and Health led by NPS. In the second session of the first day, partners discussed and selected the toolset for baseline prevention, detection and response. The first day ended with the review of the progress done in WP3 and WP4 for the PHOENI2X enablers, as well as for network and infrastructure management and orchestration and security assurance and certification.

The second day was organized into three sessions. First, innovation management and dissemination activities done in the last three months of the project were presented. This session's discussions were centred on standardisation activities and stakeholder engagement strategies. Second, integration, testing and use case validation activities were discussed. The meeting ended with a visit to the PPC's Innovation Hub, where meeting hosts presented their infrastructure, focussing on the main aspects of the project: cybersecurity, recovery and incident response, and business continuity. The meeting concluded with an open discussion and wrap-up of the 4th plenary meeting.

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

CyberHOT Summer school



PHOENI2X has co-sponsored the Cybersecurity Hands-On-Training (CyberHOT) Summer School organized in Chania, Crete, on Friday, 29th September 2023, under the auspices of NATO Maritime International Operational Training Center (NMIOTC).

The CyberHOT Summer school sessions addressed the research of vulnerabilities of known components, the exploitation of existing vulnerabilities and privilege elevation on compromised targets.

IEEE CSCN conference

IEEE CSCN
PHOENIIX
Risk Assessment Method for
5G-oriented DLMS/COSEM
Communications
Alexios Lekidis, Elpiniki I. Papageorgiou, Marinos Tsantekidis
06/11/2023
STANDARDS FOR COMMUNICATIONS AND NETWORKING
Thank You To Patrons
HUAWEI

PHOENI2X partners presented the paper *Risk assessment method for 5G-oriented DLMS/COSEM Communications* at the IEEE Conference on Standards for Communications and Networking (CSCN), co-located with the one6G Summit 2023, the 6th November 2023, in Munich, Germany.

The paper presented a risk assessment method, developed in the PHOENI2X energy use case, based on the NIST SP 800-30 standard, for identifying vulnerabilities, as well as to classify them according to a risk matrix based also on their impact on the AMI system.

ISBeRG Railways Biannual Meeting

ISBeRG is the International Suburban Rail Benchmarking Group
A consortium consisting of 15 suburban rail operators from 13 cities around the world.
113.64

During the week of the 6th of November, the ISBeRG Railways Biannual Meeting was held on FGC premises, in Barcelona.

ISBeRG is an International Suburban Rail Benchmarking Consortium, led by the Imperial College of London, and consisting of 15 suburban rail operators, coming from Copenhagen, Cape Town, Hong Kong, Barcelona, London, Melbourne, Munich, New York, Oslo, San Francisco and Sao Paulo. This program monitors and evaluates the efficiency of the operators using various Key Performance Indicators.

One of the sessions was dedicated to innovation, where Carles Miralpeix i Llorach, a member of FGC and enrolled in the PHOENI2X project, presented the current situation of the enterprise in terms of innovation, focusing on the main projects in which FGC is participating. In this presentation, he explained the importance of projects such as PHOENI2X to improve railway cybersecurity, one of the main pillars of the industry as a critical infrastructure and service.

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

“Cybersecurity, AI and quantum computing, will we ever be in a safe environment?” session of the “Equity and Artificial Intelligence Research Coffee”

PHOENI2X Project has been presented by Xavi Masip in the “Cybersecurity, AI and quantum computing, will we ever be in a safe environment?” session of the “Equity and Artificial Intelligence Research Coffee” held the 21st November 2023 in the Universitat Politècnica de Catalunya (UPC).

In the session, the role of AI in threats detection and prevention, as well as the PHOENI2X approach used for critical infrastructures, mainly energy, transport and health, were discussed.

Connect with PHOENI2X

phoeni2x.eu/

@Phoeni2xEUProject

@Phoeni2xProject

@Phoeni2x

PHOENI2X PARTNERS

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