IOTWeek | Dublin
June 20-23, 2022

“ELECTRON

rEsilient and seLf-healed EleCTRical pOwer Nanogrid

Panagiotis Sarigiannidis

ITHACA Lab

University of Western Macedonia

psarigiannidis@uowm.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936

ELECTRON

IOTWeek | Dublin
June 20-23, 2022

Project Identity & Consortium

Project Identity

- **Name:** ELECTRON - rEsilient and seLf-healed EleCTRical pOwer Nanogrid
- **Type of Action**: Innovation Action
- **Call Identifier**: H2020-SU-DS-2020
- **Topic**: SU-DS04-2018-2020 - Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
- **Duration**: 1 November 2021 to 30 September 2024 (36 months)
- **Overall Budget**: 10.207.562,50 €
- **EU Contribution**: 7.998.887,01 €
- **Grant Agreement ID**: 101021936
- **Project Coordinator**: Netcompany-Intrasoft
- **CORDIS Link**: https://cordis.europa.eu/project/id/101021936

Consortium Map

33 Partners

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

ELECTRON Consortium

ELECTRON

33 Partners

Energy Providers, TSO, DSO, Utilities, Manufacturers, Prosumers, Technology Providers

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936

https://electron-project.eu/

ELECTRON

IOTWeek | Dublin
June 20-23, 2022

Business Logic & Architecture

ELECTRON Business Logic

ELECTRON

Main Innovation Points

- Post Quantum Privacy Preserving in EPES
- Honeypot as a Service (HaaS)
- Federated AI Detection
- Proactive Islanding based on SDN/NFV
- Dynamic Certification & Authentication
- EPES Threat Intelligence

Four Main Pillars

Risk Assessment & Certification

Collaborative Risk Assessment, Honeypots As Service, Dynamic & Continuous EPES Asset Certification & Authentication

Intrusion Detection & Privacy

Federated Learning intrusion detection, post quantum privacy preserving, ELECTRON Threat Intelligence

Mitigation and Energy Optimization

Proactive Islanding, SDN/NFV-based Network Isolation and Recovery, electrical grid restoration, ELECTRON Energy Trading Framework

Personnel Training and Certification

AR/VR based EPES personnel training and certification

BORDER

CYPER

BRIDGE

PRINCE

ELECTRON

ELECTRON Platform

Integrated solution for enhancing the EPES resiliency, combining a plethora of technologies, such as Honeypots, Federated Learning, Visual Analytics, Post quantum cryptography, SDN/NFV, AR/VR, Crawling, MISP, SIEM, Blockchain, Mixed-integer linear programming, Deep Learning-based Islanding

ELECTRON Architecture

8-Layer Architecture

ELE-L: Electrical Layer

Physical and virtualized EPES assets/devices, e.g., RTUs, PLCs, smart meters, PMUs, PDCs, EPES Honeypots

SDN-L: SDN Layer

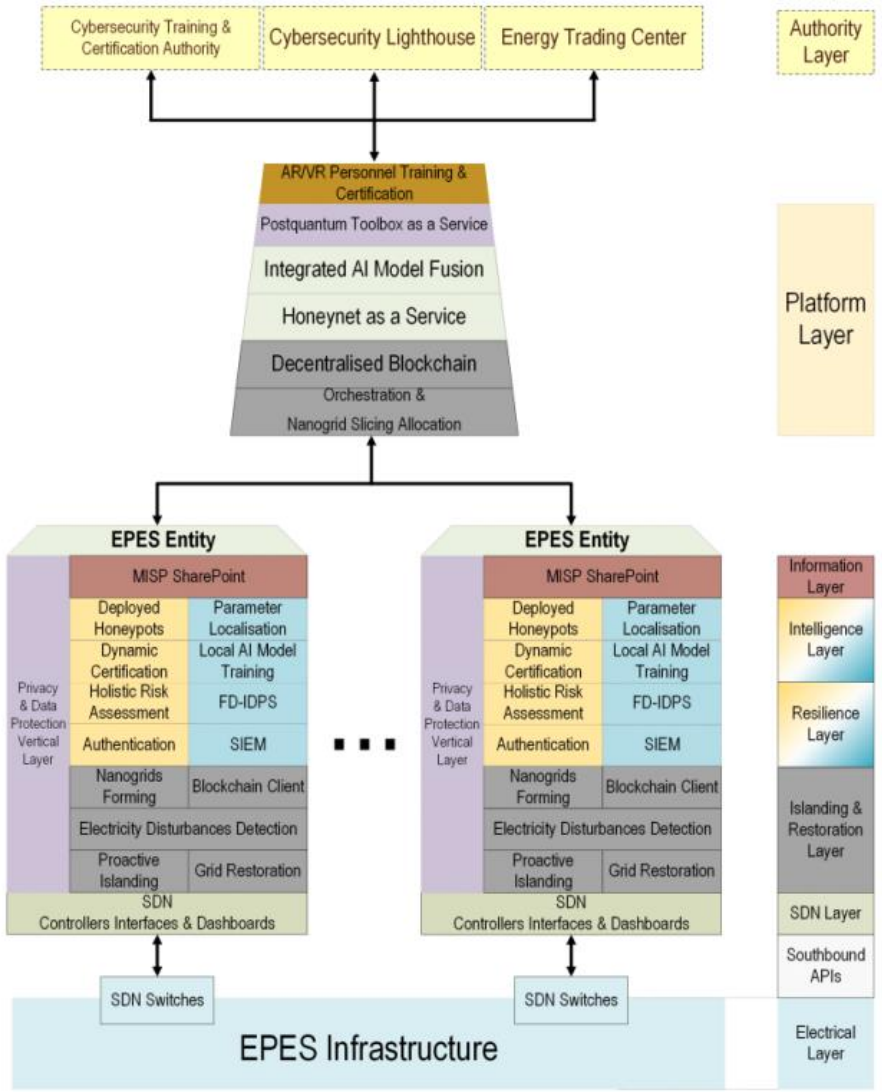
SDN Control, southbound interfaces, northbound interfaces

IS-RE-L: Islanding and Restoration Layer

ISODINE(Intentional iSOlation anD IslaNding modulE), ELISE (Electrical Grid Restoration Module), NIRO (Network Isolation and Recovery mOdule)

RES-L: Resilience Layer

ARMY (Collaborative Risks Assessment), DARCY (Cybersecurity Certification), STRONGBOX (post quantum privacy preserving), EDAE (Electric Data Analysis Engine), Network Isolation and Recovery mOdule (NIRO)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

ELECTRON Architecture

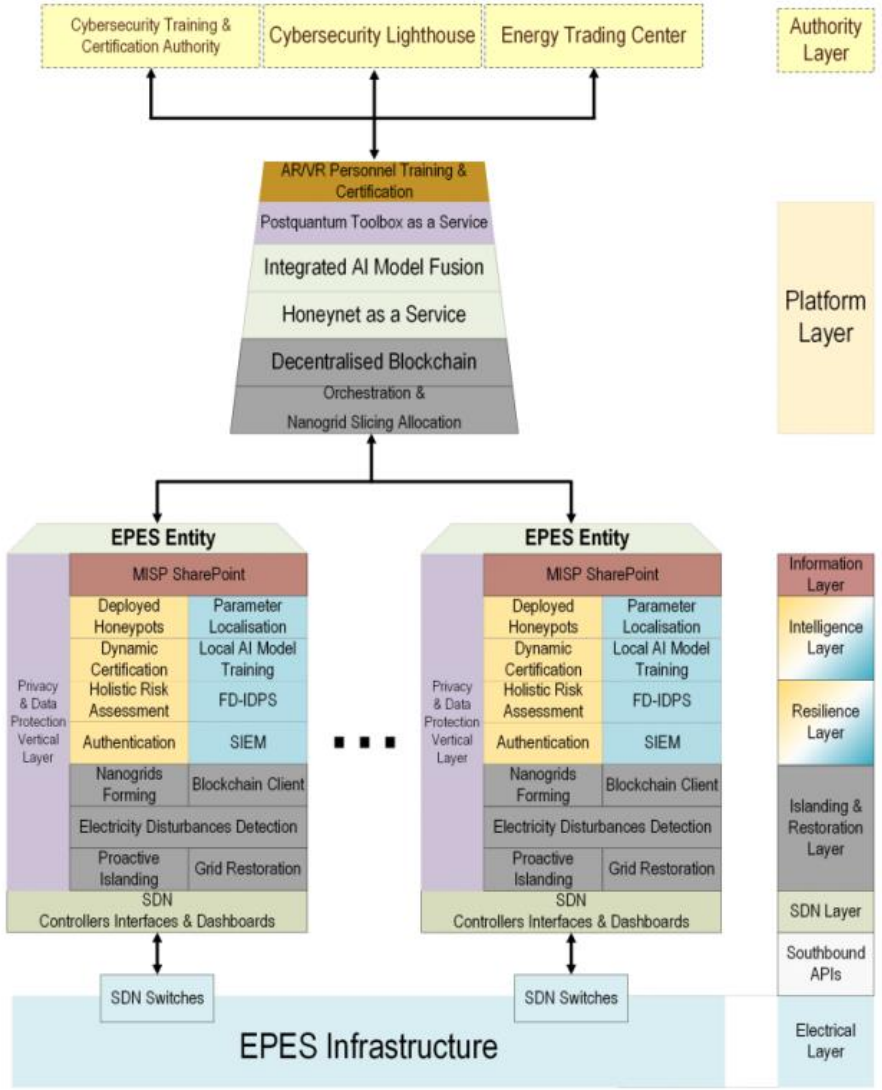
8-Layer Architecture

Intelligence Layer
Honeypot as a Service, Federated Learning-based IDPS, XL-SIEM +, ELECTRON APT Shield

Information Layer
MISP-based ELECTRON Sharepoint, ELECTRON Threat Explorer

Platform Layer
Honeypot as a Service, Federated Learning-based IDPS, Network & Application Orchestrator

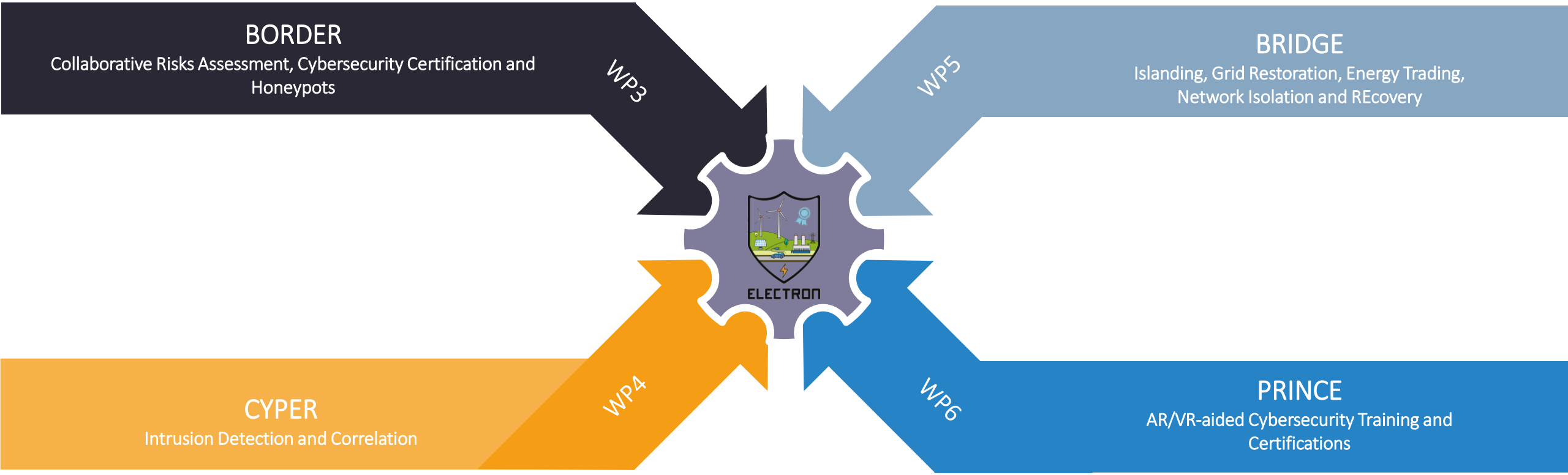
Authority Layer
ELECTRON Cybersecurity Lighthouse, Energy Trading Centre, AR/VR Cybersecurity Training, Certification Authority



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

ELECTRON Architectural Frameworks

Architectural Frameworks and Relation with other technical WPs



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

ELECTRON

IOTWeek | Dublin
June 20-23, 2022

ELECTRON Use Cases

Use Case #1: Shielding the EU borders: Addressing and Mitigating Cyberattacks and Data Leaking in Ukraine

ELECTRON

5 Scenarios

Involved Actors

CSDFC (Technology Provider), JSC (Ukrainian DSO), PIMEE (Ukrainian End User & Technology Provider), ENERGOATOM (Nuclear Plant Generator/Operator), and DTEK (Ukrainian Operator, generator, and DER)

Scenario #1 – Spear Phishing

Preventing Spear Phishing via AR/VR Training

ELECTRON Components: PRINCE

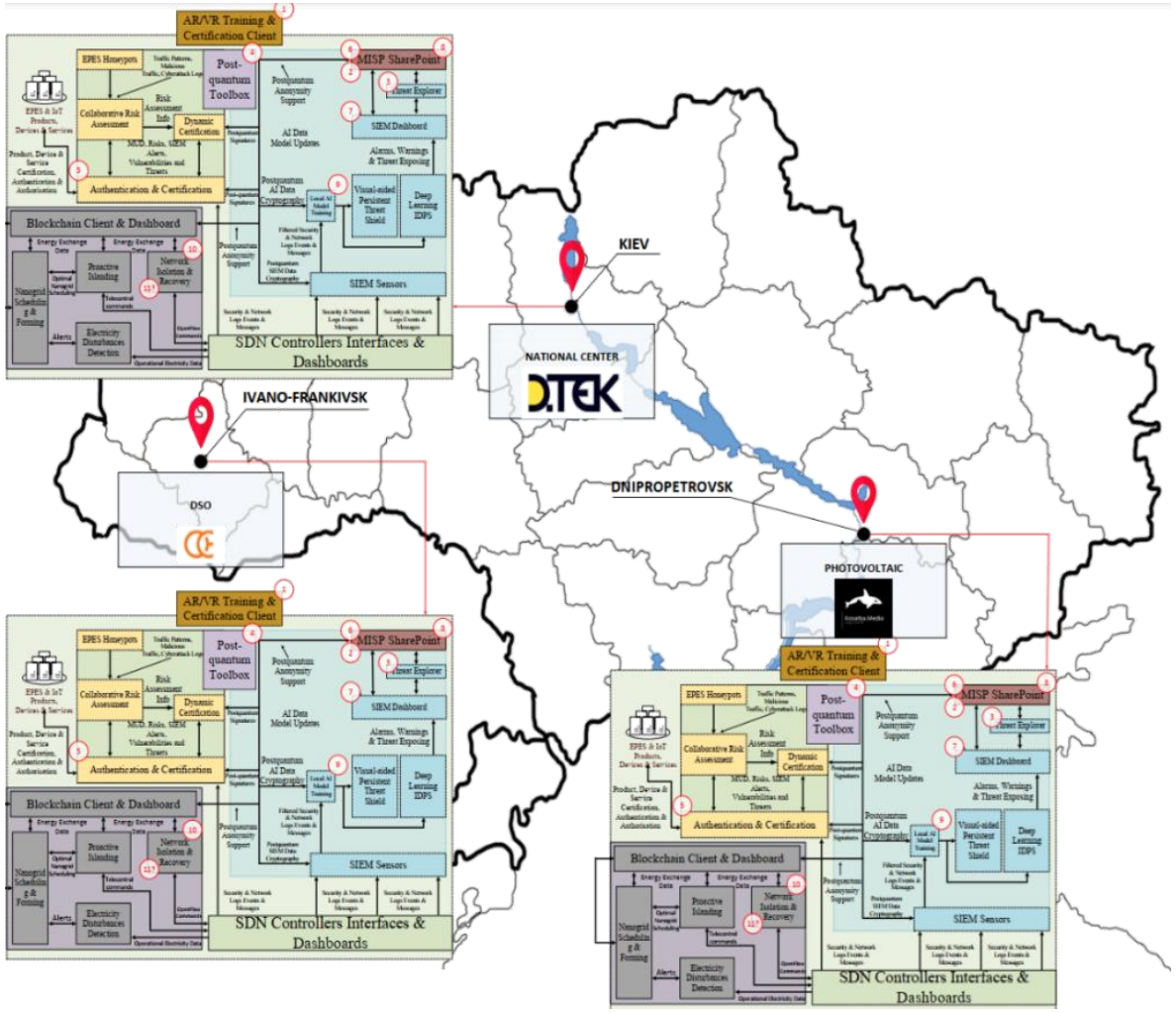
KPIs: Participation percentage of the total energy personnel > 90%, . Percentage of certified energy personnel after running PRINCE > 95%.

Scenario #2 – Malware

Detecting and Mitigating Malware

ELECTRON Components: ELECTRON SIEM, ELECTRON Sharepoint, ELECTRON Threat Explorer (Patch identification)

KPIs: Malware threat detection and prevention: 99.9%, Time needed to detect and prevent the malware threat: < 10 ms



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Use Case #1: Shielding the EU borders: Addressing and Mitigating Cyberattacks and Data Leaking in Ukraine

ELECTRON

5 Scenarios

Scenario #3 – SCADA Control Units Hijacking

Detecting and mitigating Man In the Middle attacks

ELECTRON Components: STRONGBOX

KPIs: MitM attacks detection and prevention: 99.9%, Time needed to detect and prevent the malware threat: < 10 ms

Scenario #4 – Unauthorised Access Attacks

Using VPN access to get authorised and authorisation for taking control of the inner ICS systems

ELECTRON Components: ARMY and DARCY

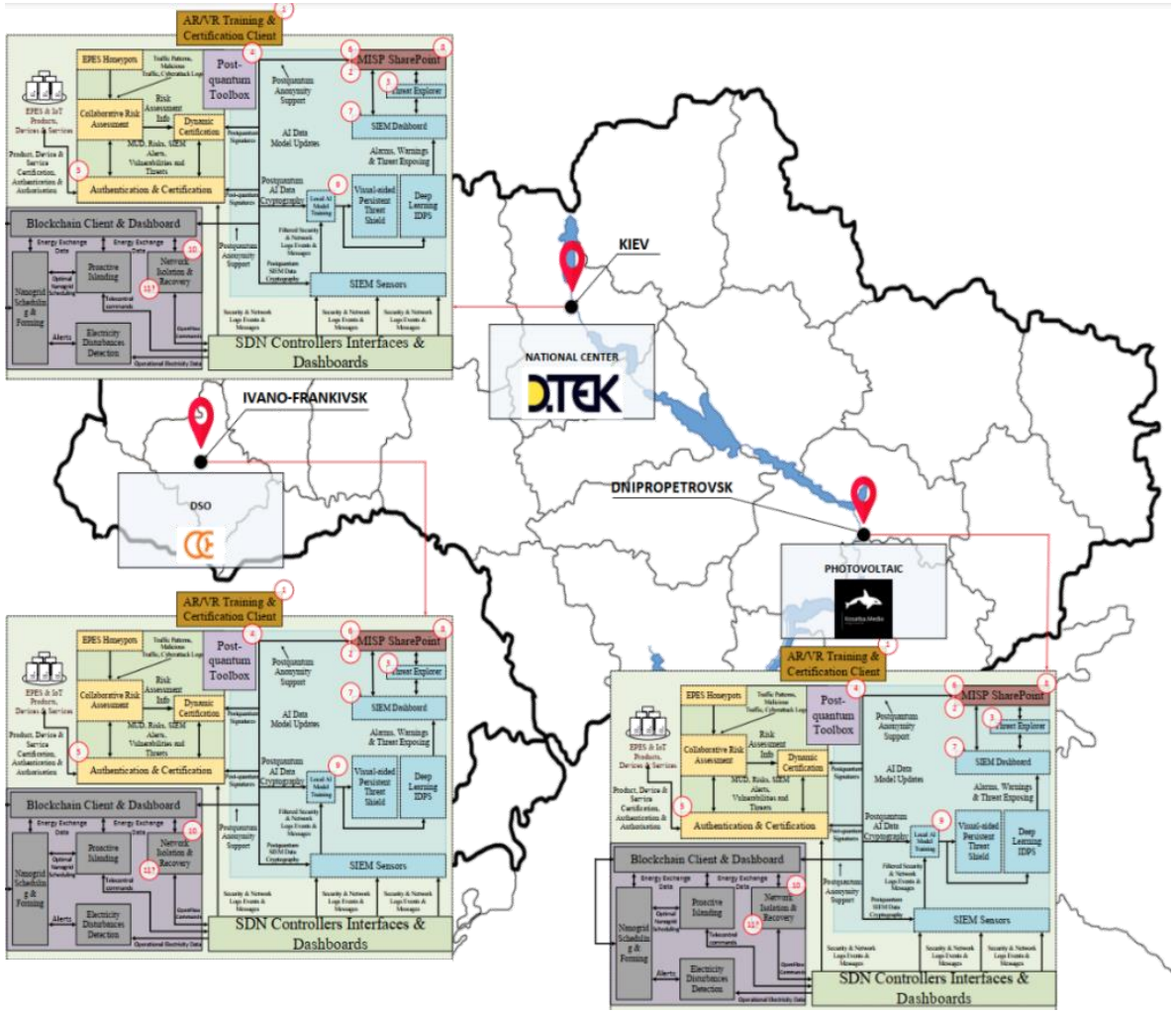
KPIs: Authentication & authorisation denial of the custom VPN: 99.9%, Time to detect & prevent the malware/threat: < 10 ms

Scenario #5 – DoS and DDoS attacks

Detecting and Mitigating DoS and DDoS Attacks

ELECTRON Components: ELECTRON SIEM, FL-IDPS, ELECTRON Sharepoint, NIRO, SDN Controller

KPIs: DoS and DDoS attack detected and mitigated: 99.9%, Time needed to restore the nanogrid under the attack: < 100 ms



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Use Case #2: Providing a Resilient Electric Vehicle Ecosystem

4 Scenarios

Involved Actors

PPC, IPTO

Scenario #1 – Uncertified SCADA Assets

Blocking access to uncertified SCADA assets

ELECTRON Components: DARCY, ARMY, XL-SIEM, ELECTRON Sharepoint, SDN Controller

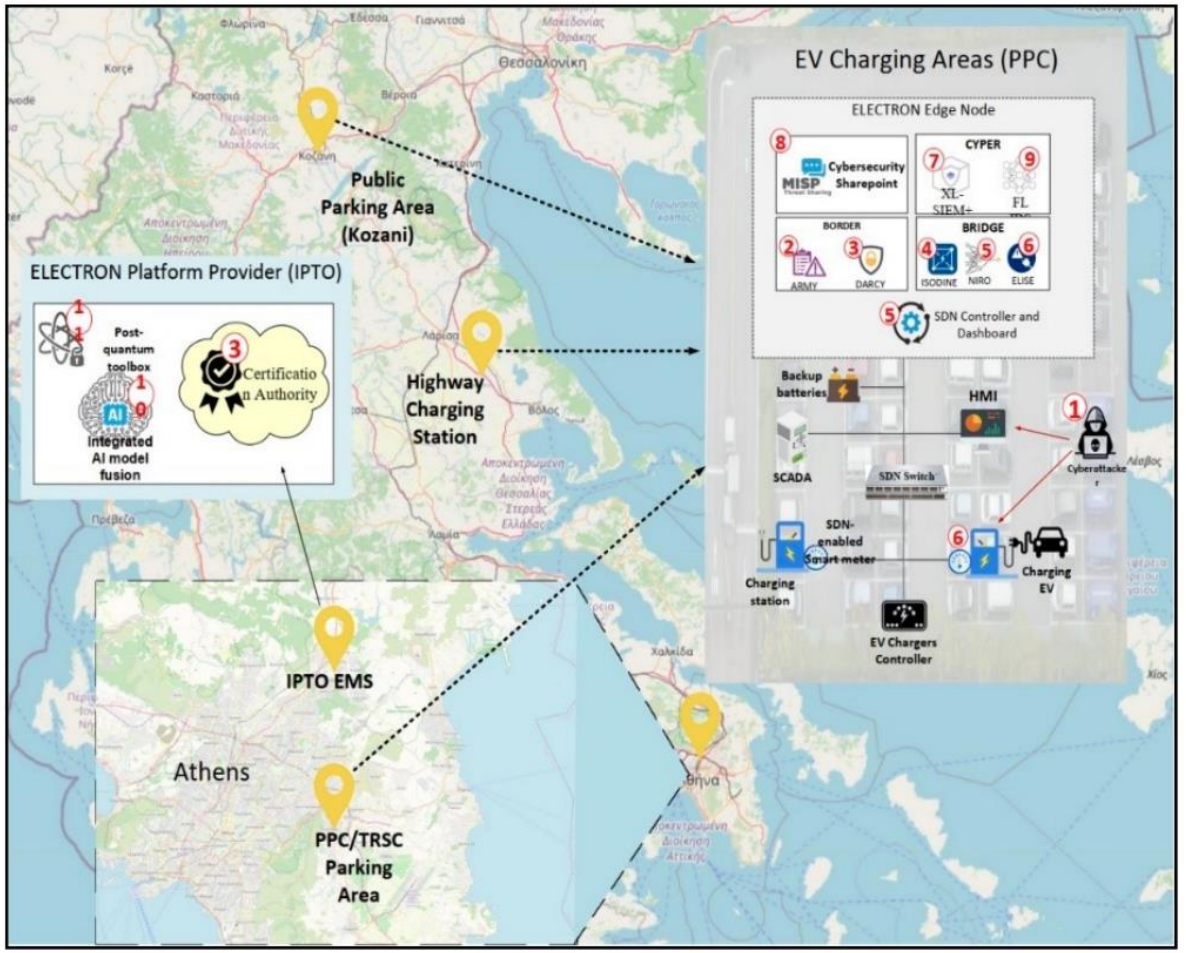
KPIs: Accuracy of ELECTRON to identify the vulnerabilities of the HMI: > 99%, Time needed to determine the certification status of the HMI: < 10 ms

Scenario #2 – FDI Attacks against PPC Electrical Vehicles (Evs)

Detecting and Mitigating False Data Injection Attacks

ELECTRON Components: ELECTRON SIEM and its detectors, ISODINE, NIRO, SDN Controller, ELISE

KPIs: Detection accuracy of the upcoming fault: > 95%, Restoration time of the nanogrid: < 100 ms



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Use Case #2: Providing a Resilient Electric Vehicle Ecosystem

Involved Actors

PPC

Scenario #3 – DoS Attacks against PPC EV Charging Stations

Detecting and Preventing DoS attacks

ELECTRON Components: ELECTRON SIEM, FL-IDPS, Threat Explorer, ELECTRON Sharepoint

KPIs: Malware threat detection and prevention: 99.9%, Time needed to detect and prevent the malware threat: < 10 ms

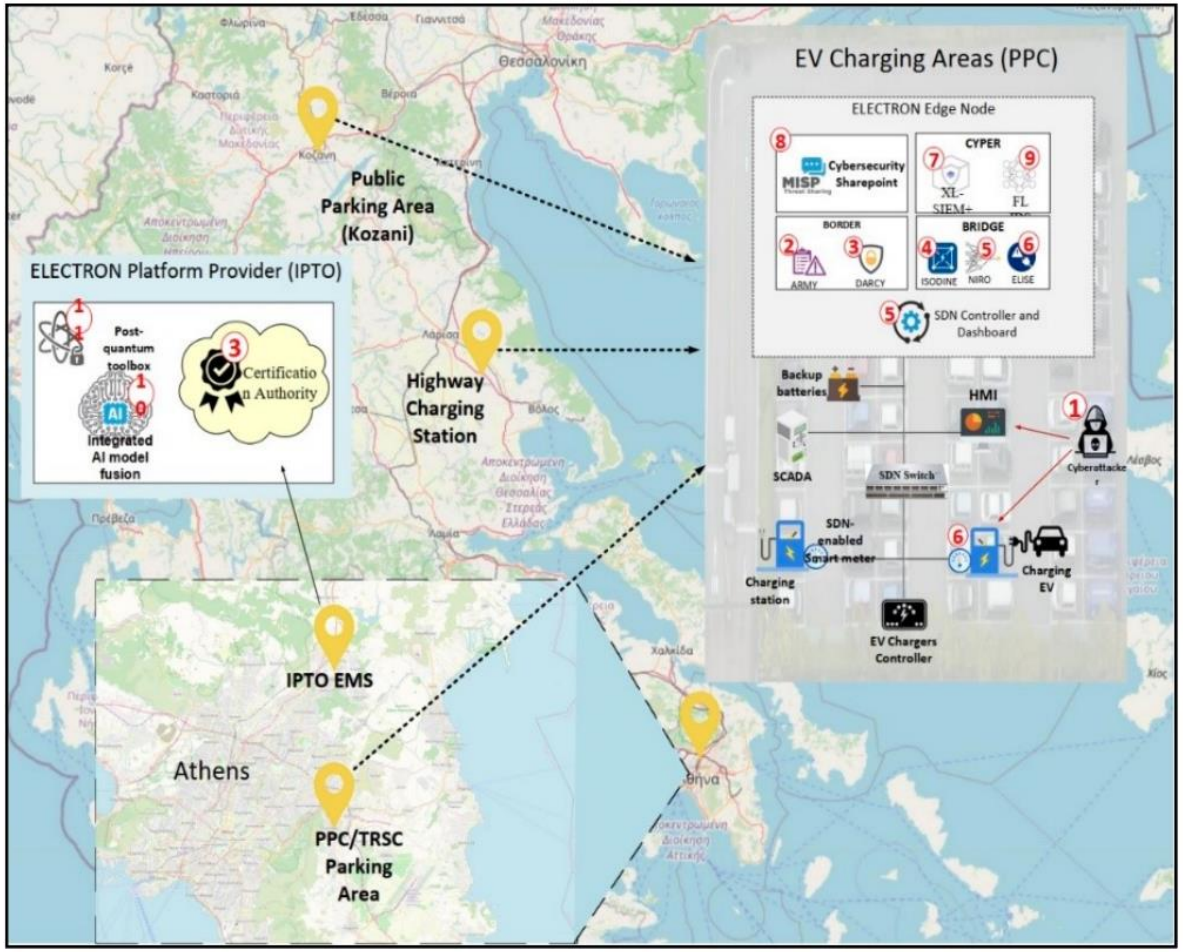
Scenario #2 – MITM Attacks against PPC Electrical Vehicles

Detecting and Preventing MITM attacks

ELECTRON Components: ELECTRON SIEM and its detectores, ELECTRON Sharepoint, NIRO, SDN Controller, STRONGBOX

KPIs: MITM attacks detection and prevention: 99.9%, Time needed to detect and prevent the malware threat: < 10 ms.

4 Scenarios



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Use Case #3: Protecting the Renewables Energy Chain from Cyberattacks and Data Leaking

Involved Actors

Enerfin (Operator/Generator), SCHF & SCHE (Manufacturer), Isotrol (Technology provider/Scada Manufacturer), Tecnalia (Research Centre), TUVSPAIN (Certification/Industry).

Detecting a number of cyberattacks against Enerfin Wind Farm

ELECTRON Components: FL-IDPS, ELECTRON SIEM, ELECTRON SP (MISP), ELECTRON APT Shield, ARMY

AR/VR-based Cybersecurity Training

ELECTRON Components: PRINCE

Relevant KPIs

KPI#1: Number of critical cybersecurity vulnerabilities detected in assessments and penetration tests; KPI#2 Number of actions proposed for acting in monitoring and control infrastructures in current and in legacy systems; KPI#3 Number of pattern-based detection rules based on IT and OT with alert to control centers; KPI#4 Number of employees trained and certified on the IEC 62443 standard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Use Case #4: Proactive Islanding Meets Efficient Threat Detection: Addressing & Mitigating Cyberattacks in the Romanian Energy Chain

Involved Actors

Transelectrica (Romanian TSO), Electrica SA (Romanian DSO), UPB (Technology Provider)

Scenario #1 – FDI Attacks against Transelectrica and Electrica SA

Detecting and Preventing False Data Injection Attacks

ELECTRON Components: FL-IDPS, ELECTRON SIEM, ELECTRON SP (MISP), ARMY, NIRO, DARCY, SDN-C, STRONGBOX

KPIs: Detection accuracy > 90%, 2 Detection False Positive Rate < 20%, Intrusion Mitigation Time < 1 min, Certification accuracy > 90%

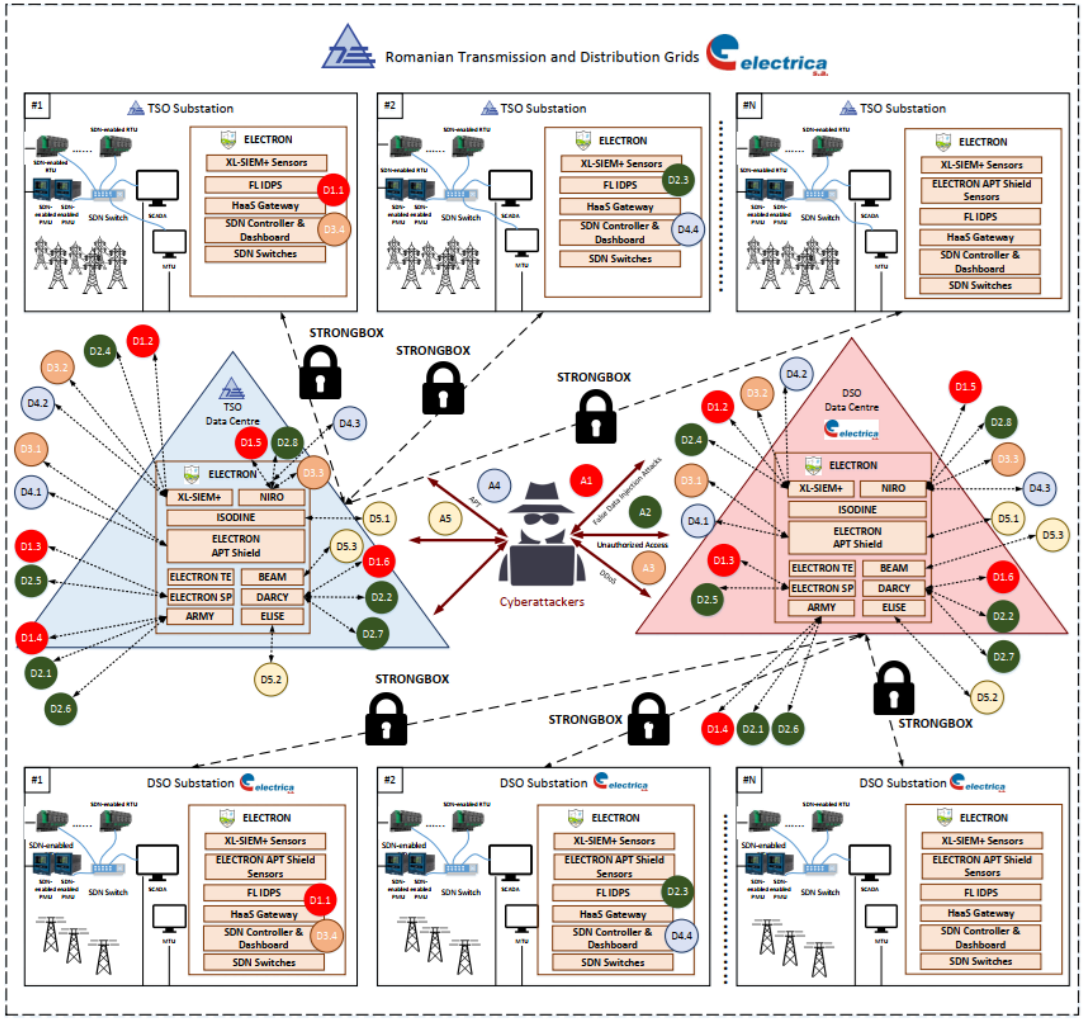
Scenario #2 – Unauthorised Attacks against Transelectrica and Electrica SA

Detecting and Preventing Unauthorised Access Attacks

ELECTRON Components: ARMY, DARCY, ELECTRON SP, ELECTRON Threat Explorer, FL IDPS, ELECTRON SIEM, NIRO, SDN-C, STRONGBOX

KPIs: Detection accuracy > 90%, 2 Detection False Positive Rate < 20%, Intrusion Mitigation Time < 1 min, Certification accuracy > 90%

5 Scenarios



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Use Case #4: Proactive Islanding Meets Efficient Threat Detection: Addressing & Mitigating Cyberattacks in the Romanian Energy Chain

Scenario #3 – DDoS Attacks against Transelectrica and Electrica SA

Detecting and Preventing DDoS Attacks

ELECTRON Components: APT Shield, HaaS (EPES Honeypots), ELECTRON SIEM, NIRO, SDN-C, STRONGBOX

KPIs: Detection accuracy > 90%, 2 Detection False Positive Rate < 20%, Intrusion Mitigation Time < 1 min, Certification accuracy > 90%

Scenario #4 – APTs against Transelectrica and Electrica SA

Detecting and Mitigating Advanced Persistent Threats

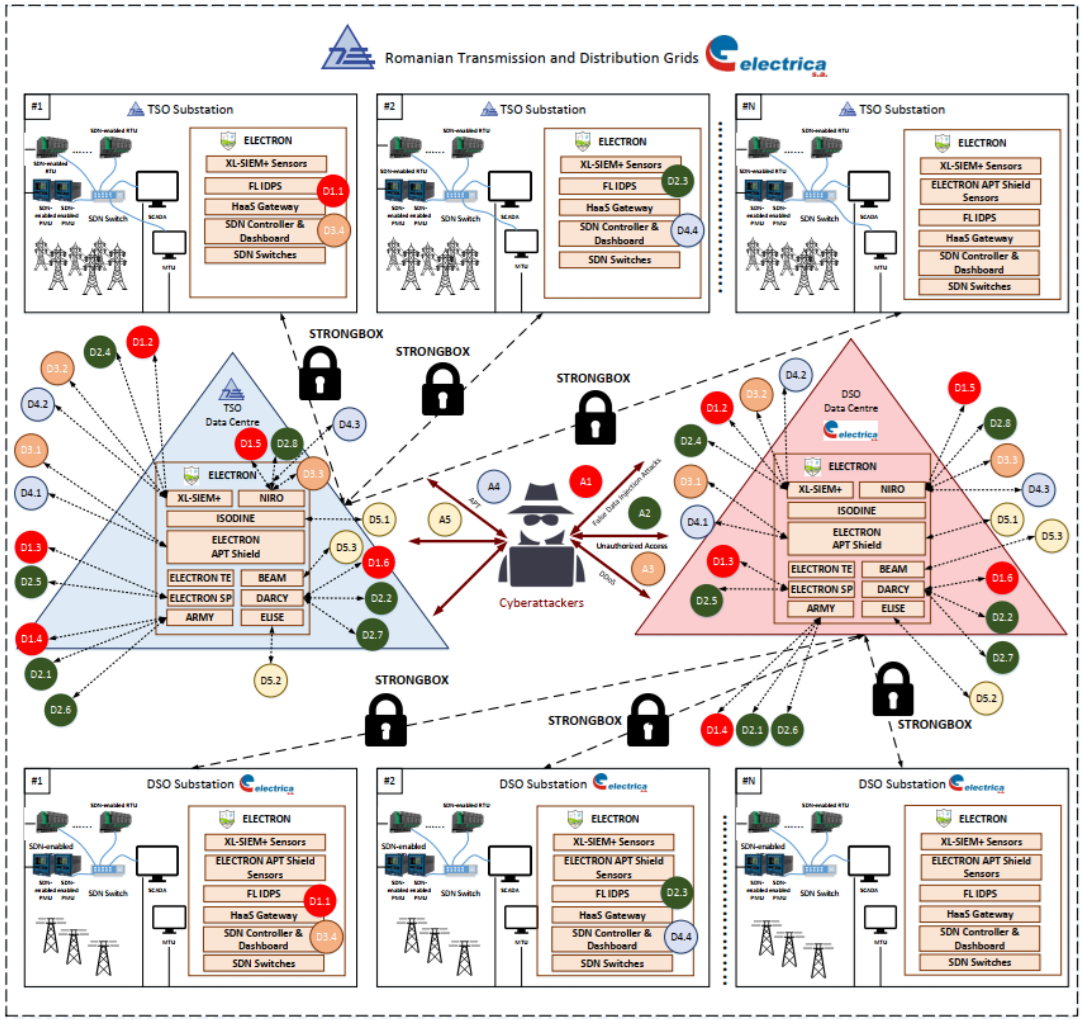
ELECTRON Components: APT Shield, ELECTRON SP (MISP), ELECTRON SIEM, ELECTRON Threat Explorer, NIRO, SDN-C, STRONGBOX

KPIs: Detection accuracy > 90%, 2 Detection False Positive Rate < 20%, Intrusion Mitigation Time < 1 min, Certification accuracy > 90%

Scenario #5 – Islanding Schemes and Nanogrid Management Actions - Electrica SA

Applying Islanding Schemes and Nanogrid Management Actions

ELECTRON Components: ISODINE, ARMY, ELISE, BEAM, STRONGBOX, KPIs: Intrusion Mitigation Time < 1 min, Verifiability of the data integrity up to 100% due to the smart contract mechanism, Traceability, accountability, and non-repudiation of the critical actions in the system will increase up to 80%, Support of turing completeness as regards the business logic of the Information Sharing mechanism will reach 90%



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

IOTWeek | Dublin
June 20-23, 2022

Thank You & Q/A

ELECTRON

Contact us

psarigiannidis@uowm.gr

https://ithaca.ece.uowm.gr/

https://gr.linkedin.com/in/panagiotis-sarigiannidis-7636901a

https://www.researchgate.net/profile/Panagiotis-Sarigiannidis

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Thank You

Q/A ?

https://electron-project.eu/