MINDS

ARES conference

ELECTRON: An Architectural Framework for Securing the Smart Electrical Grid with Federated Detection, Dynamic Risk Assessment and Self-Healing

P. Radoglou-Grammatikis et al.

University of Western Macedonia

Contact: pradoglou@uowm.gr

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

Introduction

Industrial Internet of Things and Smart EPES

In the era of hyper-connected digital economies, the smart technologies play a vital role in the operation of the electrical grid, transforming it into a new paradigm.

Legacy Systems

The presence of legacy systems, such as ICS/SCADA remains a crucial issue, raising multiple threats and vulnerabilities.

Insecure Communication Protocols

Both smart and legacy EPES assets use insecure communication protocols that do not comprise essential authentication and authorization mechanisms.

Existing Countermeasures

Despite the effectiveness of existing cybersecurity solutions they cannot mitigate coordinated EPES cyberattacks, such as Advanced Persistent Threats (APTs)

Lack of Datasets & Privacy

The existing countermeasures are not certified dynamically, ensuring their sufficiency.

ELECTRON

ELECTRON refers to an integrated platform which is capable of detecting and mitigating potential cyberattacks in a timely manner, combining a set of cybersecurity and energy defensive mechanisms. The key characteristics of ELECTRON are: (a) dynamic risks assessment, (b) cybersecurity certification, (c) federated intrusion detection and correlation, (d) Software Defined Networking (SDN) mitigation, (e) proactive islanding and (f) cybersecurity training and certification

ELECTRON

Business Logic & Architecture

ELECTRON

ELECTRON Business Logic

Main Innovation Points

- Post Quantum Privacy Preserving in EPES
- Honeypot as a Service
- 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

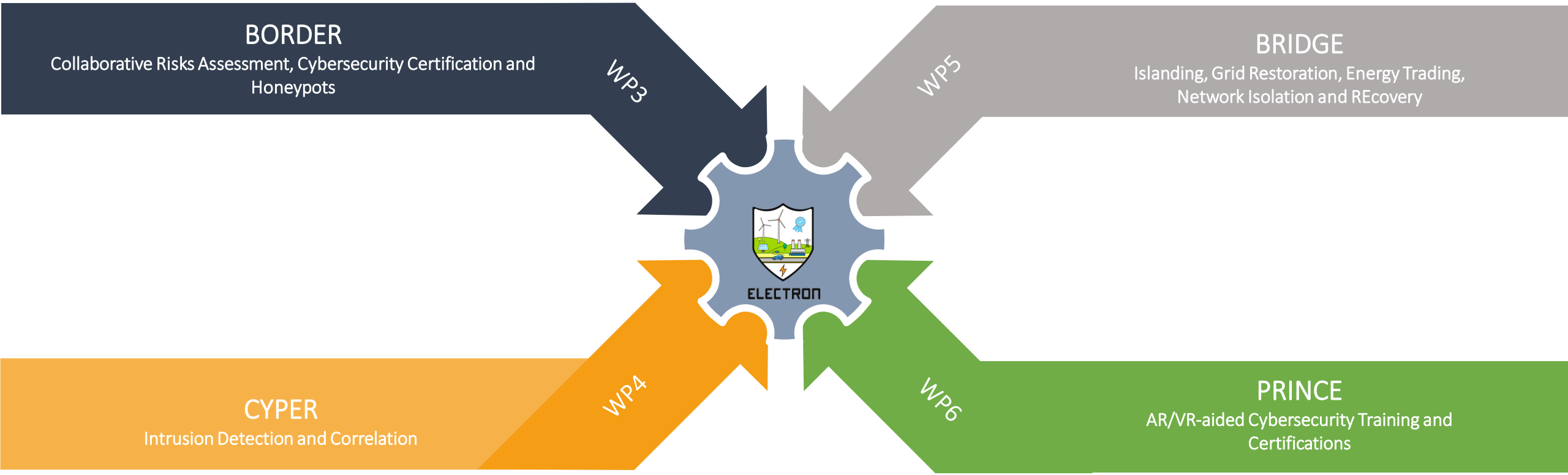
PRINCE

ELECTRON 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 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

BORDER

BORDER: collaBOrative Risk anD cErtification fRamework

ARMY: collAborative Risk assessMent sYstem

Collaborative Risk Assessment: Asset Identification, Threat Identification, Vulnerability Identification, Analysis of existing security resources, determining vulnerability likelihood, imact analysis, risk identification and risk treatment

DARCY: Dynamic Asset ceRtifiCation sYstem

Dynamic cybersecurity certification system for the EPES assets, which combines three visions: a) the vision of the certification authority, b) the vision of the manufacturer and c) the vision of the EPES-end user thus certifying continuously whether an EPES asset (e.g., RTU, PLC, MTU, smart meters, etc.) can enter or not into the production network of the EPES infrastructure

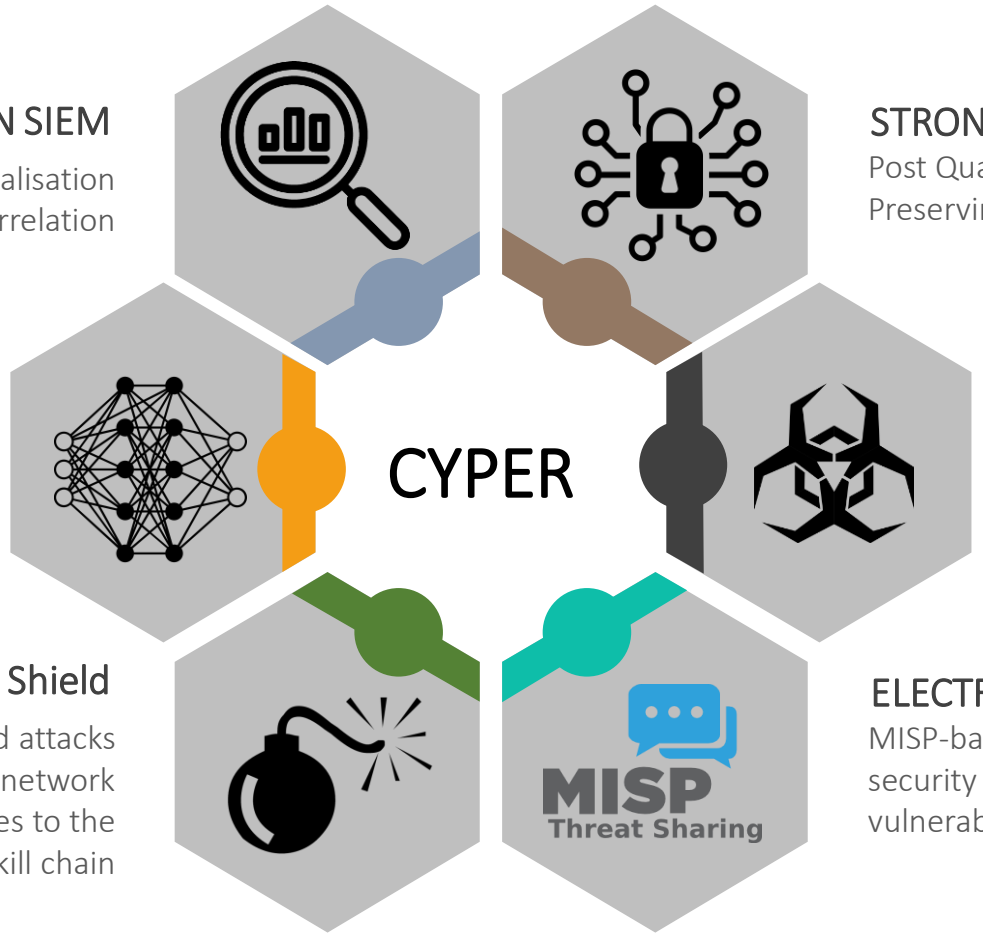
HaaS: Honeypot as a Service

EPES honeypots and honeypot orchestration

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

CYPER

CYPER: CYbersecurity and Privacy prEserving fRamework



ELECTRON SIEM
Intrusion detection, normalisation and correlation

STRONGBOX
Post Quantum Privacy Preserving in EPES

FL-IDPS
Intrusion/Anomaly detection utilizing federated learning

ELECTRON Threat Explorer
A cyberthreat intelligence mechanism, which will explore and mine significant information from various web sources regarding the EPES threats and vulnerabilities, thus updating continually the ELECTRON SharePoint

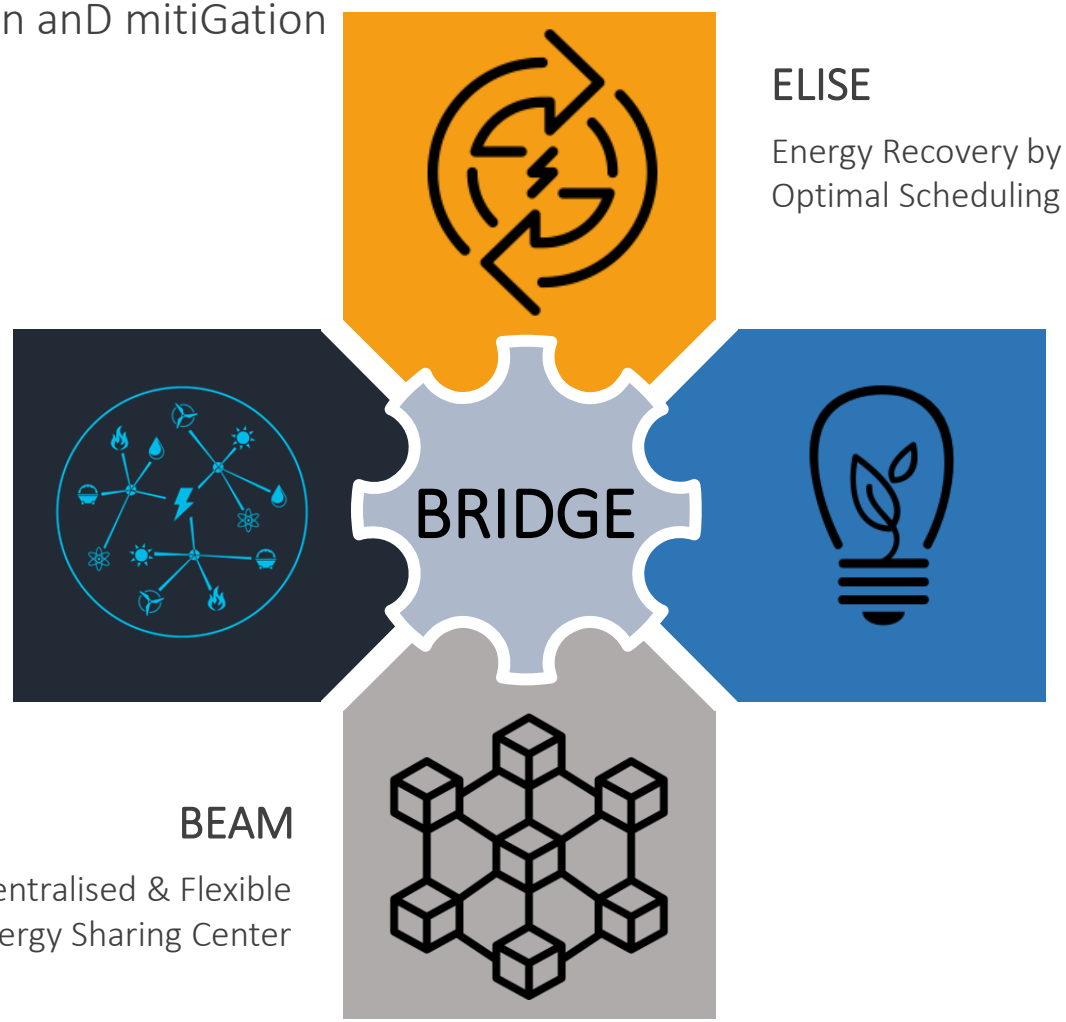
APT Shield
Detecting sophisticated attacks and threats by mapping network and host-related activities to the APT kill chain

ELECTRON SharePoint
MISP-based anonymous repository hosting security events, alerts, threats and vulnerabilities

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

BRIDGE

BRIDGE: nanogrid-Based pRevention anD mitiGation schEme



ELISE

Energy Recovery by Curtailment Allocation & Optimal Scheduling

ISODINE

Generates and applies proactive islanding schemes in case of emergency

NIRO

NIRO introduces an automated cybersecurity mitigation level based on the network automations provided by the SDN controller and the SDN-enabled EPES devices, based on EDAE.

BEAM

Blockchain-based Decentralised & Flexible Energy Sharing Center

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

PRINCE

PRINCE: Personnel tRainINg & Certification Environment

Spear Phasing Scenario

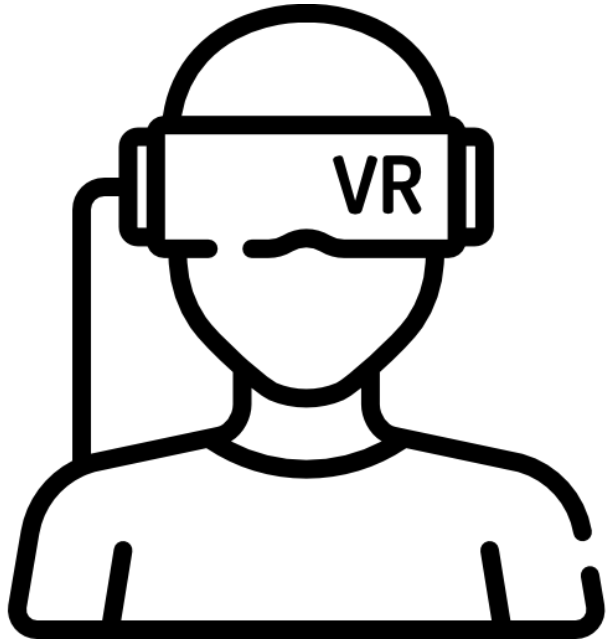
Training scenario about phishing and spear phishing attacks

DDoS Scenario

Training scenario about DoS and DDoS attacks

Unauthorized Access Scenario

Training scenario about unauthorized access attacks



Physical Threats

Training scenario about natural disasters, environmental threats

False Data Injection Scenario

Training scenario about false data injection attacks

MITM Scenario

Training scenario about MITM attacks

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

ELECTRON

ELECTRON Use Cases

Use Case #1: Addressing and Mitigating Cyberattacks and Data Leaking in Ukraine and Azerbaijan

ELECTRON

5 Scenarios: The following scenarios will be executed in both Ukrainian and Azerbaijanis end-users.

Involved Actors

CSDFC (Technology Provider), JSC (Ukrainian DSO), PIMEE (Ukrainian End User & Technology Provider) and ADNSU (Technology Provider)

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

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

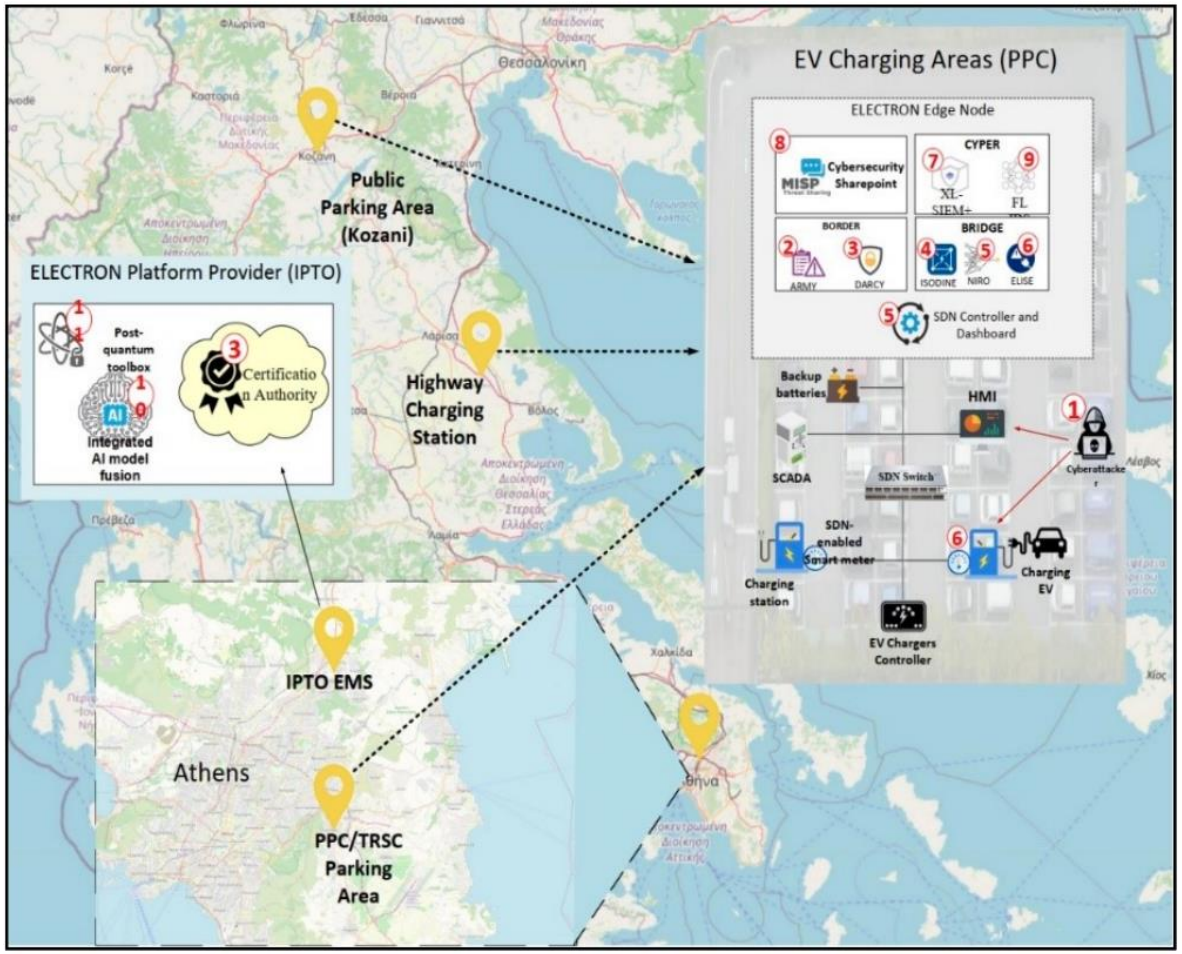
KPIs: Accuracy of ELECTRON to identify the vulnerabilities of the HMI: > 99%, Time needed to determine the certification status of the HMI: < 10 ms

Scenario #2 – FDI Attacks against EV Charging Stations

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

4 Scenarios

Involved Actors

PPC, IPTO

Scenario #3 – DoS Attacks against EV Charging Stations

Detecting and Preventing DoS attacks

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

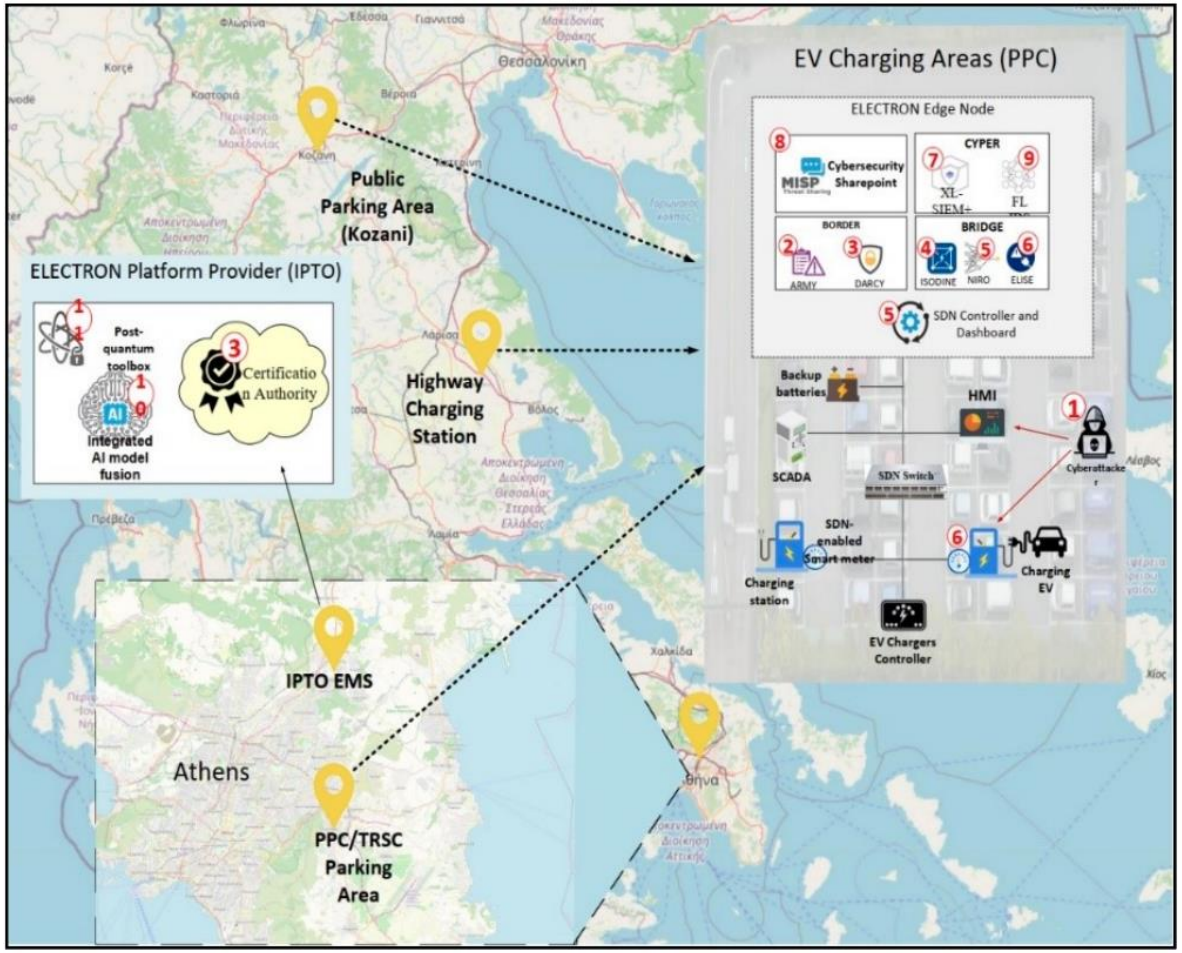
KPIs: Malware threat detection and prevention: 99.9%, Time needed to detect and prevent the malware threat: < 10 ms

Scenario #4 – MITM Attacks against EV Charging Stations

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.



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

5 Scenarios

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

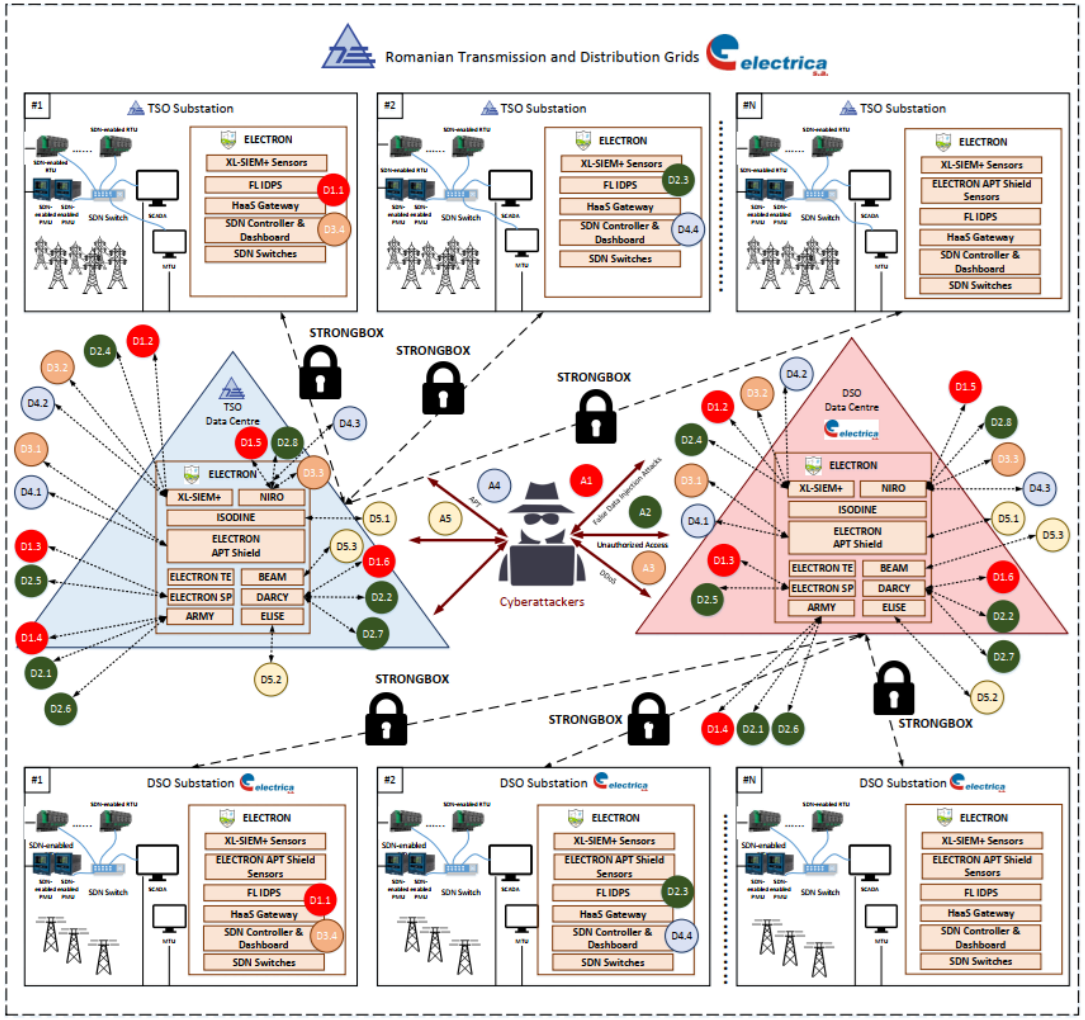
KPIs: Detection accuracy > 90%, 2 Detection False Positive Rate < 20%, Intrusion Mitigation Time < 1 min, Certification accuracy > 90%

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%



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

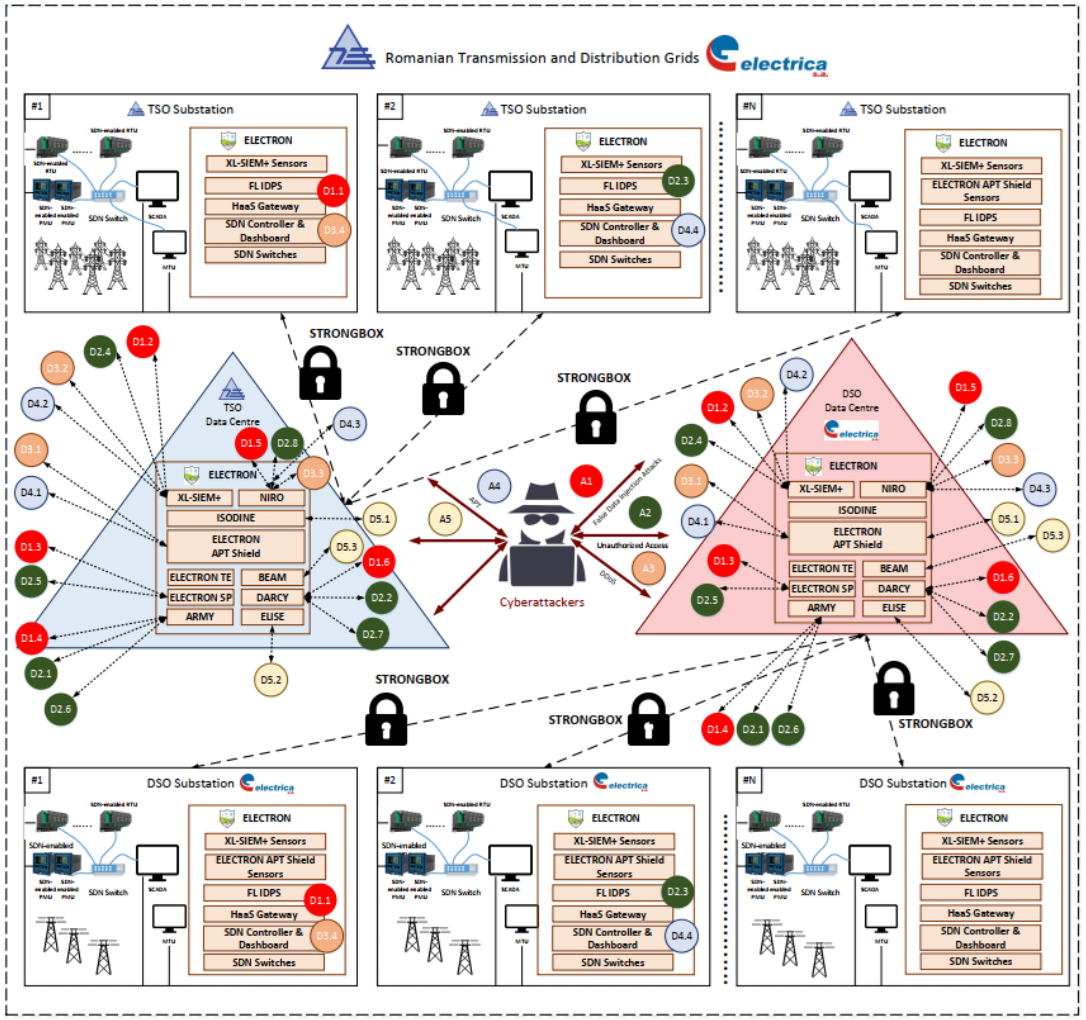
ELECTRON Components: APT Shield, ELECTRON SP (MISP), ELECTRON SIEM, ELECTRON Threat Explorer, NIRO, SDN-C, STRONGBOX

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

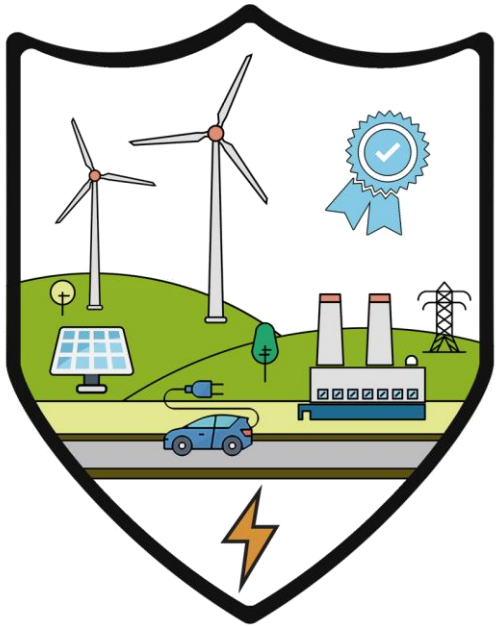
Scenario #5 – Islanding Schemes and Nanogrid Management Actions - Electrica SA

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



Thank You

Q/A ?

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