
Proceedings Paper:
Radoglou-Grammatikis, P., Liatifis, A., Dalamagkas, C. et al. (2023) ELECTRON: An architectural framework for securing the smart electrical grid with federated detection, dynamic risk assessment and self-healing. In: ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES 2023: The 18th International Conference on Availability, Reliability and Security, 29 Aug - 01 Sep 2023, Benevento, Italy. Association for Computing Machinery (ACM), p. 51. ISBN: 9798400707728.

https://doi.org/10.1145/3600160.3605161

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

Panagiotis Radoglou-Grammatikis
pradoglou@uowm.gr
University of Western Macedonia
Kozani, Greece

Athanasios Liatifis
University of Western Macedonia
Kozani, Greece
aliatifis@uowm.gr

Christos Dalamagkas
Innovation Hub of Public Power Corporation S.A.
Attica, Greece
c.dalamagkas@uowm.gr

Alexios Lekidis
Innovation Hub of Public Power Corporation S.A.
Attica, Greece
A.Lekidis@dei.gr

Konstantinos Voulgaridis
Department of Computer Science, International Hellenic University
Kavala, Greece
kwboulg@cs.ihu.gr

Thomas Lagkas
Department of Computer Science, International Hellenic University
Kavala, Greece
tlagkas@cs.ihu.gr

Nikolaos Fotos
UBITECH Limited
Limassol, Cyprus
nfotos@ubitech.eu

Sofia-Anna Menesidou
UBITECH Limited
Limassol, Cyprus
smenesidou@ubitech.eu

Thomas Krousarlis
UBITECH Limited
Limassol, Cyprus
tkrousarlis@ubitech.eu

Pedro Ruzafa Alcazar
Department of Information and Communications Engineering, University of Murcia
Murcia, Spain
pedro.ruzafaa@um.es

Juan Francisco Martinez
Department of Information and Communications Engineering, University of Murcia
Murcia, Spain
juanfrancisco.martinezg@um.es

Antonio Fernando Skarmeta Gomez
Department of Information and Communications Engineering, University of Murcia
Murcia, Spain
skarmeta@um.es

Alberto Molinuevo Martín
TECNALIA, Basque Research and Technology Alliance (BRTA)
Derio Bizkaia, Spain
alberto.molinuevo@tecnalia.com

Inaki Angulo
TECNALIA, Basque Research and Technology Alliance (BRTA)
Derio Bizkaia, Spain
inaki.angulo@tecnalia.com

Jesus Villalobos Nieto
ATOS Spain SA
Madrid, Spain
jesus.villalobosnieto@atos.net

Hristo Koshutanski
ATOS Spain SA
Madrid, Spain
hristo.koshutanski@atos.net

Rodrigo Diaz Rodriguez
ATOS Spain SA
Madrid, Spain
rodrigo.diaz@atos.net

Ilias Siniosoglou
MetaMind Innovations P.C.
Kozani, Greece
isiniosoglou@metamind.gr

Orestis Mavropoulos
Exalens
London, UK
orestis.mavropoulos@exalens.com

Konstantinos Kyranou
Sidroco Holdings Ltd
Nicosia, Cyprus
kkyranou@sidroco.com

Theocharis Saoulidis
Sidroco Holdings Ltd
Nicosia, Cyprus
hsaoulidis@sidroco.com

Allon Adir
IBM Research - Israel
Haifa, Israel
ADIR@il.ibm.com

Ramy Masalha
IBM Research - Israel
Haifa, Israel
Ramy.Masalha@ibm.com

Pablo Gallegos Jimenez
IDENER
Sevilla, Spain
pablo.gallegos@idener.es

Emanuele Bellini
LOGOS
Firenze, Italy
emanuele.bellini@logos-ri.eu

Nikolaos Kolokotronis
Department of Informatics and Telecommunications, University of Peloponnese
Tripolis, Greece
nkolok@uop.gr

Stavros Shiaeles
University of Portsmouth
Portsmouth, UK
stavros.shiaeles@port.ac.uk

Jose Garcia Franquelo
Isotrol
Sevilla, Spain
jgfranquelo@isotrol.com

George Lalas
Netcompany-Intrasoft
Luxembourg, Luxembourg
George.LALAS@netcompany-intrasoft.com

Andreas Zalonis
Netcompany-Intrasoft
Luxembourg, Luxembourg
Andreas.ZALONIS@netcompany-intrasoft.com

Angelina Bintoudi
Centre of Research & Technology Hellas
Thessaloniki, Greece
bintoudi@iti.gr

Antonios Voulgaridis
Centre of Research & Technology Hellas
Thessaloniki, Greece
antonismv@iti.gr

Konstantinos Votis
Centre of Research & Technology Hellas
Thessaloniki, Greece
kvotis@iti.gr

David Pampliega
Schneider Electric
Seville, Spain
david.pampliega@se.com

Panagiotis Sarigiannidis
University of Western Macedonia
Kozani, Greece
psarigiannidis@uowm.gr

ABSTRACT

The electrical grid has significantly evolved over the years, thus creating a smart paradigm, which is well known as the smart electrical grid. However, this evolution creates critical cybersecurity risks due to the vulnerable nature of the industrial systems and the involvement of new technologies. Therefore, in this paper, the ELECTRON architecture is presented as an integrated platform to detect, mitigate and prevent potential cyberthreats timely. ELECTRON combines both cybersecurity and energy defence mechanisms in a collaborative way. The key aspects of ELECTRON are (a) dynamic risk assessment, (b) asset certification, (c) federated intrusion detection and correlation, (d) Software Defined Networking (SDN) mitigation, (e) proactive islanding and (f) cybersecurity training and certification.

CCS CONCEPTS

• **Security and privacy → Intrusion detection systems**; **Malware and its mitigation**; **Domain-specific security and privacy architectures**; *Security requirements*; *Denial-of-service attacks.*

KEYWORDS

Cybersecurity, Dynamic Risk Assessment, Energy, Smart Electrical Grid, Self-healing, Software-Defined Networking

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605161

ACM Reference Format:
Panagiotis Radoglou-Grammatikis, Athanasios Liatifis, Christos Dalamagkas, Alexios Lekidis, Konstantinos Voulgaridis, Thomas Lagkas, Nikolaos Fotos, Sofia-Anna Menesidou, Thomas Krousarlis, Pedro Ruzafa Alcazar, Juan Francisco Martinez, Antonio Fernando Skarmeta Gomez, Alberto Molinuevo Martín, Inaki Angulo, Jesus Villalobos Nieto, Hristo Koshutanski, Rodrigo Diaz Rodriguez, Ilias Siniosoglou, Orestis Mavropoulos, Konstantinos Kyranou, Theocharis Saoulidis, Allon Adir, Ramy Masalha, Pablo Gallegos Jimenez, Emanuele Bellini, Nikolaos Kolokotronis, Stavros Shiaeles, Jose Garcia Franquelo, George Lalas, Andreas Zalonis, Angelina Bintoudi, Antonios Voulgaridis, Konstantinos Votis, David Pampliega, and Panagiotis Sarigiannidis. 2023. ELECTRON: An Architectural Framework for Securing the Smart Electrical Grid with Federated Detection, Dynamic Risk Assessment and Self-Healing. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3600160.3605161

1 INTRODUCTION

In the era of digital economies, the electrical grid has evolved significantly over the last few years, providing multiple benefits, such as increased load balancing, consumer empowerment and the integration of renewable and distributed energy resources. However, this evolution raises critical cybersecurity issues due to the necessary presence of legacy Electrical Power and Energy Systems (EPES) and the involvement of new technologies. Well-known Advanced Persistent Threats (APTs) campaigns against the energy sector were Indostroyer, Dragonfly and Sandworm. According to the International Energy Agency (IEA), cyberthreats against energy infrastructures could result in a loss of up to $1.4 trillion globally by 2025.

Based on the aforementioned remarks, it is evident that the smart electrical grid should be enhanced with advanced cyber detection,

mitigation and prevention solutions. In this paper, the ELECTRON architectural framework is presented. 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. According to them, the following sections present the ELECTRON architectural components in a collaborative manner.

Therefore, the rest of this paper is organised as follows. Section 2 discuss some relevant works in this field. Section 3 provides an overview of the ELECTRON architecture. In section 4, the dynamic risk assessment and certification mechanisms are presented. Similarly, in section 5, the components related to intrusion detection and correlation are described. Next, in section 6, the energy defensive mechanisms are discussed. Section 7 presents the cybersecurity training and certification mechanisms. Finally, section 8 concludes this paper.

2 RELATED WORK

Several works have investigated the security issues of the smart electrical grid. Some of them are listed in [1, 2, 4, 5, 7]. In [2], P. Gope and B. Sikdar provide a private and reconfigurable key exchange scheme for securing the communications in the smart grid. In [4], the authors study how blockchain can protect future smart grid ecosystems. In [7], J. Shi et al. provide a distributed intrusion detection mechanism against false data injection attacks in the smart grid. In [1], the authors provide a detailed survey about the use of honeypots and honeynets in the smart grid. Finally, in [5], the authors investigate the data protection and certification activities in the energy domain.

3 ELECTRON ARCHITECTURE

As illustrated in Fig. 1, the ELECTRON architecture relies on the SDN architectural model [6]. The SDN model encompasses four main planes: the Data Plane, Control Plane, Application Plane, and Management Plane. The Data Plane comprises EPES entities/devices connected to hardware or software SDN switches, which are indispensable components of the ELECTRON architecture due to their widespread use in many ELECTRON components. The Control Plane is characterized by the presence of the SDN Controller (SDN-C), which manages the network elements of the Data Plane through a southbound Application Programming Interface (API) using various protocols, such as OpenFlow, Network Configuration Protocol (NETCONF), Open Policy Framework for Exchange (OpFlex), and the Simple Network Management Protocol (SNMP). The Application Plane involves applications that interact with the SDN-C to apply effective policies for the entities of the data plane using northbound APIs, such as REpresentational State Transfer (REST), which is adopted in the context of ELECTRON. Lastly, the Management Plane is a cross-layer block responsible for the deployment, configuration, and management of the various entities/devices and components of the other planes.

Considering the previously mentioned points, the Data Plane in the ELECTRON architecture will comprise software and hardware SDN switches that will establish interconnections among EPES entities/devices such as Programmable Logical Controllers (PLCs), Remote Terminal Units (RTUs), smart meters, Phasor Measurement Units (PMUs), and others with the SDN controller. OpenFlow protocol will be utilized as the southbound protocol for ELECTRON, while the hardware SDN switches from Aruba and Open vSwitch (OVS) will be employed based on the particular characteristics and requirements of the ELECTRON use cases/pilots.

To ensure the security of SDN networks against potential Distributed Denial of Service (DoS) attacks, the ELECTRON architecture will deploy multiple SDN-Cs within the Control Plane. This approach will eliminate the possibility of a single point of failure. To maintain synchronization and coordination among the SDN Controllers, the Management Plane will incorporate the Synchronizations and Coordination Service (SCS).

The ELECTRON core is located within the Application Plane and consists of multiple cybersecurity and energy protection components designed to ensure the security and resilience of the EPES infrastructure/organization. These components are classified into four main logical frameworks: the Collaborative Risk and Certification Framework (BORDER), the Cybersecurity and Privacy-Preserving Framework (CYPER), the Nanogrid-based Prevention and Mitigation Scheme (BRIDGE), and the Personnel Training and Certification Environment. Each framework is composed of several functional components that work together to safeguard against cyber-physical risks in the energy sector. BRIDGE includes three components that focus on collaborative and dynamic risk assessment and cybersecurity certification, while CYPER includes eight components that focus on intrusion/anomaly detection and correlation. BRIDGE comprises four primary components that concentrate on intrusion/anomaly mitigation by leveraging SDN technology and electricity-related mitigation actions. Lastly, Personnel tRainINg & Certification Environment (PRINCE) is responsible for cybersecurity evaluation and certification educational and training activities for EPES personnel.

The Management Plane of the ELECTRON architecture comprises services that manage the orchestration, deployment, interconnection, and security of the components within each logical framework. Additionally, this layer includes penetration testing services that assess the security level of the ELECTRON components themselves.

Finally, it is noteworthy that ELECTRON architecture is characterised by eight functional layers: (a) SDN-Layer, (b) Electrical Layer, (c) Islanding and Restoration Layer, (d) Intelligence Layer, (e) Resilience Layer, (f) Information Layer, (g) Platform Layer and (h) Authority Layer. The functionality behind these layers relies on the components of the logical frameworks (i.e., BORDER, CYPER, BRIDGE and PRINCE) and the SDN solution. In particular, the SDN Layer refers to the presence of the SDN controller managing and controlling the SDN network. The Electrical Layer refers to the EPES entities/devices interconnected with the SDN switches. Next, the Islanding and Restoration Layer denotes the functionality of the BRIDGE components that can form autonomous microgrids/nanogrids and restore the main electrical grid. The Resilience Layer refers to the capabilities of the ELECTRON components to

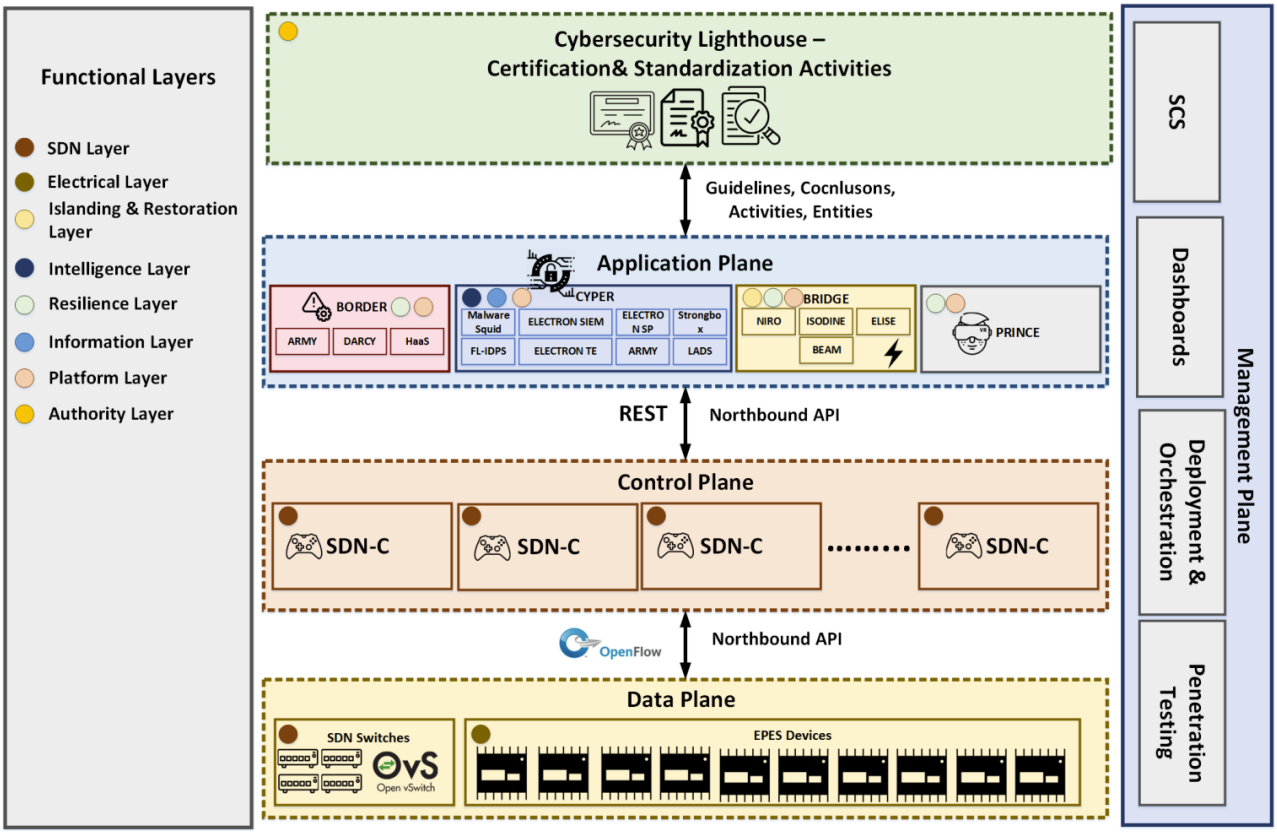

Figure 1: Conceptual View of the ELECTRON Architecture

ensure the normal operation of the electrical grid in case of critical cyberattacks. This is achieved through the dynamic and collaborative risk assessment of BORDER and the mitigation and prevention services of BRIDGE and the SDN-C. The Information and Intelligence Layers refer to the CYPER components that use and handle various kinds of data in order to detect and disseminate timely potential intrusions and anomalies. The Platform Layer implies the capability of the ELECTRON components to be provided and used as a Software as a Service (SaaS) model, thus showing the ELECTRON scalability. Finally, the Authority Layer refers to the creation of a cybersecurity lighthouse based on the certification and standardization mechanisms and guidelines that will be extracted by the outcomes of the project.

4 COLLABORATIVE RISK ASSESSMENT AND CERTIFICATION

BORDER is composed of three components: (a) collAborative Risk assessMent sYstem (ARMY), (b) Dynamic Asset ceRtifiCation sYstem (DARCY) and (c) Honeynet as a Service (HaaS). ARMY is responsible for the dynamic and collaborative risk assessment procedures. DARCY is responsible for the dynamic certification of the EPES assets, combining three visions: (a) the vision of the certification authority, (b) the vision of the manufacturer and (c) the vision of the EPES end-user. For this purpose, DARCY relies on the Manufacturer Usage Description (MUD) and its variant, the Threat Manufacturer Usage Description (Threat MUD). Finally, HaaS is in charge of deploying EPES honeypots `as a Service` in a cloud environment, keeping in parallel the local features of the EPES entities/devices, such as the Internet Protocol (IP) addresses of the EPES production/internal network.

4.1 ARMY - Collaborative Risk Assessment System

ARMY realises ELECTRON's collaborative risk assessment using novel mathematical modules, interdependency graphs and quantification techniques on various levels. ARMY is considered the backbone of the ELECTRON framework since it applies the necessary risk assessment procedures required by the platform components to enforce security policies. In particular, ARMY performs a detailed and combined risk assessment approach consisting of asset, threat and vulnerability identification and management towards providing impact and risk assessment per asset, per attack path and the EPES infrastructure as a whole. To realise the aforementioned services ARMY receives topology information from the underlying SDN-based infrastructure, asset vulnerability details, and MUDs, offering several advantages against traditional risk assessment approaches [3].

4.2 DARCY - Dynamic Asset Certification System

DARCY aims to offer dynamic certification of EPES assets by focusing on two visions, (a) the vision of the certification authority and (b) the vision of the manufacturer. The main work of DARCY is to monitor the MUD and Threat MUD Files and their updates to ensure the normal operation and status of the EPES assets. DARCY is composed of local premises (i.e., Threat MUD Manager) and manufacturer premises (i.e., MUD File server). In the first case, DARCY focuses on pulling Threat MUD files and translating them to policies, whereas in the second case, it focuses on generating MUD files on EPES devices and offering these descriptors to any stakeholder related to the certification process by receiving continuous updates in the MUD and Threat MUD by updating the description files allocated in the MUD File Servers and Threat MUD file server.

4.3 HaaS - Honeypot as a Service

ELECTRON HaaS is tasked with the provisioning of proactive EPES honeynets without the need to deploy them in the real premises of the EPES organisation, thus minimising the deployment, configuration and maintenance costs. Following the *-as-a-Service cloud model ELECTRON HaaS allows the configuration of honeynets as a group of honeypots deployed in the Cloud. ELECTRON HaaS incorporates a specific component to act as a gateway between the Cloud honeynet and the EPES network. HaaS consists of three submodules, namely the Honeypot Manager Core Backend (a) providing administration and orchestration functionalities to the HaaS, the Honeypot Manager Core Frontend (b) offering a rich graphical interface and the Honeypot Manager Agent (c) acting as the gateway between the cloud honeynet network and the local EPES infrastructure.

5 INTRUSION DETECTION AND CORRELATION

CYPER provides a decentralized solution for detecting and correlating various threats and attacks against EPES. CYPER consists of (a) ELECTRON Security Information and Event Management System (SIEM), (b) Federated Intrusion Detection and Prevention System (FIDPS), (c) Malware Squid, (d) Lightweight Anomaly Detection System (LADS), (e) APT Shield, (f) STRONGBOX, (g) ELECTRON Threat Explorer (TE) and (h) ELECTRON SharePoint (SP). Each of them is further discussed below.

5.1 ELECTRON SIEM - Security Information and Event Management

The main role of the ELECTRON SIEM is twofold: (a) recognition of attacks and malicious activities across different layers of an EPES infrastructure; and (b) normalisation of heterogeneous security logs and events coming from different ELECTRON components and third-party security tools at EPES operator premises for uniform processing and alarms generation. The ELECTRON SIEM will also provide an EPES-wide correlation of security events for a range of attacks and threats through association rules.

5.2 FIDPS - Federated Intrusion Detection and Prevention System

FIDPS is responsible for detecting intrusions against the EPES assets, using AI models that have been trained through a federated learning procedure. Thus, during the training procedure, the data privacy of the EPES organisations/infrastructures is ensured. In particular, FIDPS will be able to detect particular cyberattacks against industrial communication protocols, such as Modbus/Transmission Control Protocol (TCP), International Electrotechnical Commission (IEC) 61850, IEC 60870-5-104, IEC 60870-5-102 and Profinet based on the characteristics and the requirements of the ELECTRON end users. To this end, FIDPS uses network flow statistics from TCP/IP and the attributes of the application-layer protocols. Moreover, based on the detection results, FIDPS is able to indicate appropriate firewall and SDN rules in order to prevent timely the various cyberattacks.

5.3 Malware Squid

This component is a custom plugin in `Zeek`. It monitors the network traffic data and converts them into meaningful pictures. Then, these pictures are fed to the ML engine to classify the incoming traffic as normal or malware. Detected malware traffic will be used to train the classifier to enhance its detection accuracy continuously. In order not to overwhelm the resource with the image analysis, before moving to this step, the plugin is using what is called digital fingerprinting, which is the process of identifying devices based on unique characteristics that can be observed as the biometric counterpart to detect malware wrapped in Transport Layer Security (TLS). Network-based TLS fingerprinting has been researched as a reaction to data encryption, using observable TLS parameters exchanged before a secure session has been established.

5.4 LADS - Lightweight Anomaly Detection System

This component is a dedicated anomaly detector specialised for the analysis of EPES protocols. Several protocols have been profiled under LADS (such as Modbus, Distributed Network Protocol 3 (DNP3), IEC 60870-5-104). A number of advanced and persistent activities are subject to detection, such as false data injection, unauthorised access and DoS. Finally, LADS aims also at resource optimisation to operate in environments with possibly constrained computing resources.

5.5 APT Shield - Advanced Persistent Threat Shield

ELECTRON APT Shield is a detection sensor for detecting APTs in the target smart electrical grid. The ELECTRON APT Shield monitors the assets of the infrastructure by analysing network information and security logs. In particular, the APT Shield will be able to detect malicious activity on hosts through anomalies in their behaviour and determine their place in the `MITRE ATT&CK` knowledge base. The APT Shield will make use of ML and DL techniques to optimise the detection of threats.

5.6 STRONGBOX - Postquantum Cryptography and Signature Toolbox

STRONGBOX component is a cryptographic toolbox implementing post-quantum cryptography to ensure strong resilience against quantum cryptanalysis attacks. In particular, STRONGBOX will provide two main functions: (a) a privacy-preserving audit mechanism designed to alert potential security events based on post-quantum resistant Fully Homomorphic Encryption (FHE) and signature and (b) a secure toolbox to secure internal communications of the ELECTRON integrated platform against quantum cryptanalysis attacks. STRONGBOX is composed of four components: (a) Aggregator, (b) FHE Anomaly Detector, (c) PQC Digital Signature Solution and (d) Secure Communication Toolbox. The Aggregator receives plaintext event logs from the facility, aggregates, encrypts and signs the aggregated logs and sends the signed-encrypted logs to the FHE Anomaly Detector component. For this purpose, the Aggregator creates the necessary FHE keys and enrols to PQC Digital Signature Solution to receive the necessary signature keys and to perform the signature step. The FHE Anomaly Detector receives signed encrypted logs from the Aggregator, authenticates the signature and then performs anomaly detection analysis over the encrypted data using FHE computations. The anomaly detection analysis also updates and uses an encrypted behavioural model of the monitored devices, which is used to detect deviations from normal behaviour. The result of the analysis is an encrypted alert report (which is produced but cannot be read by the FHE Anomaly Detector – since it does not have the secret decryption key). This encrypted report is signed and sent to the alert decryptor on the client side, which does have access to the decryption key. For this purpose, the FHE Anomaly Detect or receives the necessary FHE keys from the Aggregator and enrols to PQC Digital Signature to receive the necessary signature keys and to perform the signature step. The PQC Digital Signature is a hardware security device that implements a hybrid digital signature. Finally, the Secure Communication Toolbox t provides a way to create a quantum-resistant communication channel by using a post-quantum algorithm. The post-quantum client of this component exchanges a secure symmetric key with the post-quantum server. Once the key is shared, any data transfer between client and server is encrypted.

5.7 ELECTRON Threat Explorer

The ELECTRON TE is a software component that automatically checks different sources (such as databases and web pages) to discover if a new vulnerability has been discovered that could affect the energy domain. In particular, ELECTRON TE is composed of the following sub-components: (a) Scheduler, (b) Crawler and (c) Filter. The Scheduler is in charge of processing a list of Uniform Resource Locator (URLs) of Web resources and scheduling (executing) a number of crawler instances according to the list of priorities (and any performance settings). The Crawler is a software module (Internet bot) that browses or reads World Wide Web (WWW) resources and collects and indexes results according to a predefined setup. Finally, the Filter determines the relevance of the collected data according to a predefined list of keywords specific and relevant for a given EPES instance. It stores cybersecurity indicators from the vulnerabilities and/or threats to the ELECTRON SP.

5.8 ELECTRON SharePoint

ELECTRON SP is based on the Malware Information Sharing Platform (`MISP`) technology. It composes a `MISP`-based interface for allowing the intercommunication of all EPES entities in a decentralised and anonymous way. The ELECTRON TE will explore a variety of sources and existing vulnerability databases and feed the ELECTRON SP with relevant to EPES operator threats and vulnerabilities. A Threat Intelligence Engine (TIE) will be developed and integrated with the `MISP` instance that will rank and score vulnerabilities shared by other EPES operators according to their relevance to an EPES operator ´s specific infrastructure assets and software/hardware components. Anonymisation will be based on the encryption of selected data fields (of cybersecurity indicators) by each EPES operator when sharing Cyber Threat Intelligence (CTI) data. The anonymisation will be according to the `MISP` standard object notations.

6 INTRUSION MITIGATION AND RESPONSE

BRIDGE focuses on prevention and mitigation mechanisms capable of blocking cascading effects. Thus, BRIDGE combines energy and ICT components, taking full advantage of the SDN technology. BRIDGE consists of: (a) Network Isolation and Recovery mOdule (NIRO), (b) Intentional iSOlation anD IslaNding modulE (ISODINE), (c) ElectricaL grId reStoration modulE (ELISE) and (d) Blockchain Energy transaction systeM (BEAM). NIRO undertakes to instruct the SDN controller with respect to the mitigation policies that can be applied in the EPES SDN network. ISODINE and ELISE are responsible for the proactive islanding and grid restoration processes, respectively. Finally, BEAM provides and blockchain-based energy trading centre supporting the functions of ISODINE and ELISE. The following subsections provide more details about the BRIDGE components.

6.1 NIRO - Network Isolation and Recovery Module

NIRO is a data analysis engine, focusing on EPES, that undertakes to guide the SDN-C in order to implement the appropriate mitigation actions that would protect the SDN-based EPES network. NIRO processes the security alerts generated by ARMY as well as the potential mitigation actions from DARCY. Depending on the identified cybersecurity threat, NIRO may redirect the malicious network flow to a security application (e.g., a honeypot) or completely drop the communication. Moreover, NIRO considers the sensitivity and criticality of the EPES communications. Therefore, it re-arranges the network flows between hosts through constrained optimisation with genetic algorithms to ensure the appropriate Quality of Service (QoS). Finally, for cybersecurity incidents involving Phasor Measurement Units (PMUs), NIRO applies a smart Decision Support System (DSS) that is based on a matchmaking algorithm in order to restore the observability and preserve the communication links between PMUs and Phasor Data Concentrators (PDCs).

6.2 ISODINE – Intentional Islanding and Isolation Module

ISODINE undertakes to calculate and apply islanding schemes in a proactive manner, thus forming microgrids and nanogrids that can ensure the continuous operation of the electrical grid in cases of critical cyberattacks or critical faults. ISODINE employs Artificial Intelligence (AI) methodologies in order to detect abnormalities that are signs of impending faults and subsequently isolates the affected segments of the grid to avoid blackouts and other cascading effects.

6.3 ELISE – Electrical Grid Restoration Module

After an islanding operation takes place, ELISE undertakes to restore and ensure that the formed microgrids and nanogrids are operating normally in terms of voltage and frequency stability. In more detail, ELISE employs a Multi-Agent System (MAS) that coordinates and implements a three-hierarchy control, where the primary and secondary control uses a hybrid centralised/distributed architecture to eliminate single-point-of-failures, while a centralised optimal dispatch agent residing on the tertiary control level, asserts the economical operation of each microgrid. Moreover, other subcomponents of ELISE evaluate the real-time operation and based on deviations, the various asset agents are instructed in order to alter their attitude.

6.4 BEAM – Blockchain Energy Transaction System

BEAM aims to provide a blockchain-based energy trading framework implemented as a private fabric network to enable peer-to-peer energy trading amongst prosumers. BEAM will employ a permission blockchain-based system in which a collection of deployed smart contracts will manage data sharing by encoding data with relevant data references and commonly shared standards. BEAM is compatible with the Vickrey-type e-auction, where each participant will either buy or sell energy based on their current amount of energy. Vickrey auction mechanism is a sealed bid type of auction where each bidder submits a bid without knowing the amount everyone else submitted to encourage each participant to bid their true valuations for the energy they request.

7 CYBERSECURITY TRAINING AND CERTIFICATION

Cybersecurity training and certification are achieved through the PRINCE framework. PRINCE is based on the utilization and combination of Augmented Reality (AR)/ Virtual Reality (VR) mechanisms, e.g., `ARTutor`, `KYROX`, and `PROCESS-AR`, for the education, training, and consciousness of EPES on Cyber Hygiene. `ARTutor` is an AR-based educational platform that transforms the submitted educational material into an immersive experience that can be accessed through the trainee's personal mobile device. `KAYROX` is a digital platform that enables the creation of VR environments by non-experienced individuals through their browser or VR headset, while supported by cloud deployment. `PROCESS-AR` is a platform utilizing eXtended Reality (XR) characteristics, with the capability of integrating real-time sensory data in a Mixed Reality (MR) environment. PRINCE consists of Training and Certification process. Starting with the Training Process, once key requirements on educational material and required skills are identified, a collection of cybersecurity practices and immersive tasks are designed and developed, which are transitioned into didactic pills and evaluation quizzes while utilizing `ARTutor`, `KAYROX`, and `PROCESS-AR`. These components are hosted in the ELECTRON Portal and interconnected with the Cyber Range Facility for the creation of interactive training environments that are accompanied by the ELECTRON Avatar virtual coach throughout the completion of the exercises. The Certification Process consists of the Cyber Hygiene Certification schema, which is based on the global standard International Organization for Standardization (ISO)/IEC 17024, aiming toward the identification of requirements, processes, and standards, and the Cyber Hygiene Certification Process that is related to the identification of required activities that need to be implemented. The ELECTRON Portal is also interconnected with the Certification Process for the conduction of the evaluation exams.

8 CONCLUSIONS

In the digital era, the electrical grid is evolving continuously, integrating harmonically multiple advanced technologies. However, this progression creates severe cybersecurity concerns. For this purpose, in this paper, the ELECTRON architectural framework is presented, providing in a collaborative manner detection, mitigation and prevention mechanisms. In particular, ELECTRON consists of four frameworks: (a) BORDER, (b) CYPER, (c) BRIDGE and (d) PRINCE. BORDER is responsible for the dynamic risk assessment and asset certification. CYPER focuses on federated intrusion detection and correlation. BRIDGE includes energy defence measures. Finally, PRINCE refers to cybersecurity training and certification mechanisms.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Javier Franco, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. 2021. A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2351–2383. https://doi.org/10.1109/COMST.2021.3106669

[2] Prosanta Gope and Biplab Sikdar. 2021. A Privacy-Aware Reconfigurable Authenticated Key Exchange Scheme for Secure Communication in Smart Grids. *IEEE Transactions on Smart Grid* 12, 6 (2021), 5335–5348. https://doi.org/10.1109/TSG.2021.3106105

[3] Athanasios Liatifis, Pedro Ruzafa Alcazar, Panagiotis Radoglou-Grammatikis, Dimitris Papamartzivanos, Sofianna Menesidou, Thomas Krousarlis, Molinuevo Martin Alberto, Iñaki Angulo, Antonios Sarigiannidis, Thomas Lagkas, Vasileios Argyriou, Antonio Skarmeta, and Panagiotis Sarigiannidis. 2022. Dynamic Risk Assessment and Certification in the Power Grid: A Collaborative Approach. In *2022 IEEE 8th International Conference on Network Softwarization (NetSoft)*. IEEE, Milan, Italy, 462–467. https://doi.org/10.1109/NetSoft54395.2022.9844034

[4] Muhammad Baqer Mollah, Jun Zhao, Dusit Niyato, Kwok-Yan Lam, Xin Zhang, Amer M. Y. M. Ghias, Leong Hai Koh, and Lei Yang. 2021. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet of Things Journal* 8, 1 (2021), 18–43. https://doi.org/10.1109/JIOT.2020.2993601

[5] Iheanyi Nwankwo, Marc Stauch, Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis, George Lazaridis, Anastasios Drosou, and Dimitrios Tzovaras. 2022. Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector. *Electronics* 11, 6 (2022), 965.

[6] Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis, Christos Dalamagkas, Yannis Spyridis, Thomas Lagkas, Georgios Efstathopoulos, Achilleas Sesis, Ignacio Labrador Pavon, Ruben Trapero Burgos, Rodrigo Diaz, et al. 2021. Sdn-based resilient smart grid: The sdn-microsense architecture. *Digital* 1, 4 (2021), 173–187.

[7] Jiayu Shi, Shichao Liu, Bo Chen, and Li Yu. 2021. Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids. *IEEE Transactions on Circuits and Systems II: Express Briefs* 68, 3 (2021), 993–997. https://doi.org/10.1109/TCSII.2020.3020139