This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787011.

SPEAR NEWSLETTER

7th newsletter **October 2021**

Dear reader,

You are reading the 7th issue of our newsletter, published by the SPEAR project, a Horizon 2020 program funded by European Union under grant agreement No. 787011.

This issue summarises the latest scientific publications and dissemination activities of the SPEAR consortium.

You can always stay up-to date about our latest news and publications by visiting our website:

https://www.spear2020.eu/

SPEAR Publications

The SPEAR consortium continuously updates the SPEAR website about new publications, which are also uploaded to Zenodo. You can find bellow our latest publications:

- I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "**A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments**," IEEE Trans. Netw. Serv. Manage., pp. 1–1, 2021: https://zenodo.org/record/5565354
- P. Radoglou-Grammatikis et al., "**SPEAR SIEM: A Security Information and Event Management system for the Smart Grid**," Computer Networks, p. 108008, Apr. 2021: https://zenodo.org/record/4668407
- T. Kotsiopoulos, P. Sarigiannidis, D. Ioannidis, and D. Tzovaras, "**Machine Learning and Deep Learning in smart manufacturing: The Smart Grid paradigm**," Computer Science Review, vol. 40, p. 100341, May 2021: https://zenodo.org/record/4661095
- M. Charalampos-Rafail, K. Thanasis, V. Vasileios, I. Dimosthenis, T. Dimitrios, and S. Panagiotis, "**Cyber Attack Detection and Trust Management Toolkit for Defence-Related Microgrids**," in Artificial Intelligence Applications and Innovations. AIAI 2021 IFIP WG 12.5 International Workshops, Springer International Publishing, 2021, pp. 240–251: https://zenodo.org/record/5566931

Project Details

- **Project no.** 787011
- **Research and Innovation Action:** Co-funded by the Horizon 2020 Framework Programme of the European Union
- **Call identifier:** H2020-DS-2016-2017 (Digital Security Focus Area)
- **Topic: DS-07-2017:** Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
- **Project Start date:** May 1st, 2018 (42 months duration)

Communication

Website
https://www.spear2020.eu

LinkedIn
https://www.linkedin.com/company/spear2020

YouTube
https://www.youtube.com/channel/UCw6-d5G01ToBhCmaUnHIcpw

Project Coordinator:
Prof. Panagiotis Sarigiannidis
University Of Western Macedonia, Greece

E-mail: psarigannidis@uowm.gr

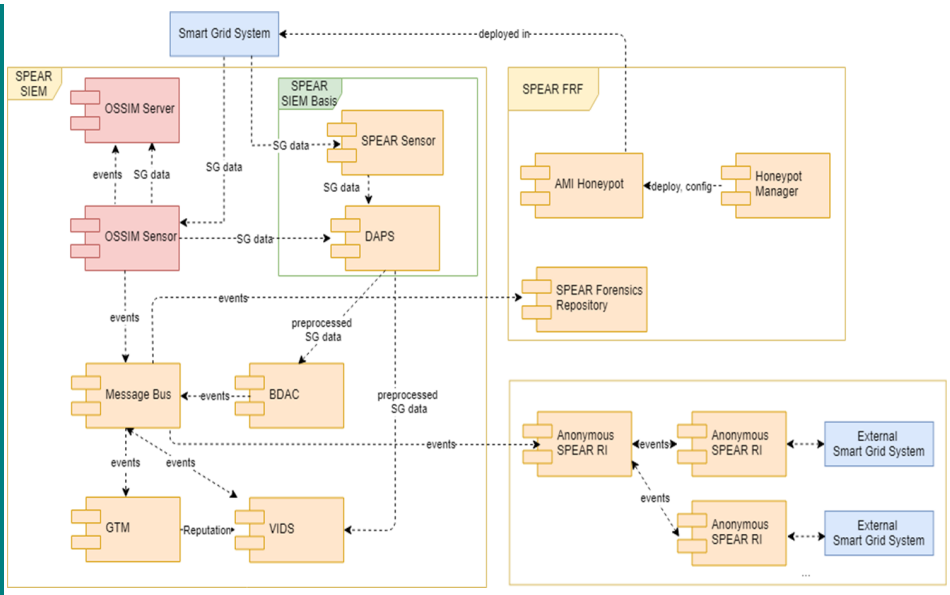
SPEAR Architecture

The SPEAR project aims to introduce a three-tier platform architecture that is able to ensure confidentiality, integrity and availability of smart-grid oriented data and services. The SPEAR architecture consists of the following major layers:

SPEAR SIEM: The SPEAR system information and event management framework aims at detecting and illustrating anomalies on operational data and network traffic that could indicate a cyber-attack or any kind of anomaly that needs immediate action.

SPEAR FRF: The SPEAR Forensic Readiness Framework encompasses tools that process forensic data and prepare evidences which can be used in courts. In addition, FRF realizes the optimal deployment of honeypots to trap attackers and collect precious evidences.

Anonymous SPEAR-RI: The SPEAR Anonymous Repository of Incidents enables communication and transaction of security incidents among energy providers and operators in Europe. Anonymisation techniques guarantee that the participating organisations will not get exposed.



SPEAR Architecture

SPEAR Publications

A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments

IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT

I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," IEEE Trans. Netw. Serv. Manage., pp. 1–1, 2021. [Online] Available: https://zenodo.org/record/5565354

This paper introduces an Intrusion Detection System (IDS) for Smart Grids, called **MENSA (anoMaly dEtection aNd claSsificAtion)**, which adopts a novel **Autoencoder-Generative Adversarial Network** (GAN) architecture for (a) detecting operational anomalies and (b) classifying Modbus/TCP and DNP3 cyberattacks. MENSA combines the aforementioned Deep Neural Networks (DNNs) in a common architecture, taking into account the adversarial loss and the reconstruction difference. The proposed IDS is validated in **four real smart grid evaluation environments**, namely (a) smart grid lab, (b) substation, (c) hydropower plant and (d) power plant, solving successfully an outlier detection (i.e., anomaly detection) problem as well as a **challenging multiclass classification problem** consisting of 14 classes (13 Modbus/TCP cyberattacks and normal instances). Furthermore, MENSA can discriminate five cyberattacks against DNP3.

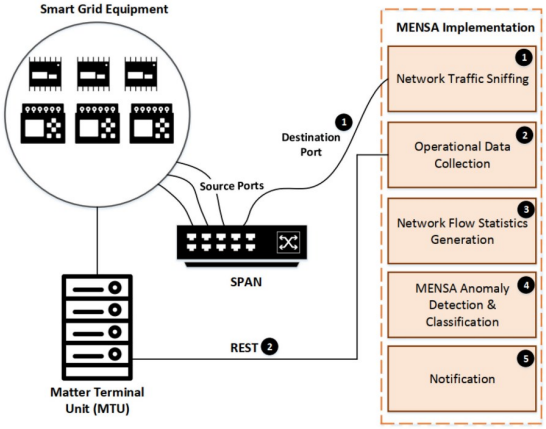


Figure: The proposed architecture

SPEAR SIEM: A Security Information and Event Management system for the Smart Grid

Computer Networks

P. Radoglou-Grammatikis et al., "SPEAR SIEM: A Security Information and Event Management system for the Smart Grid," Computer Networks, p. 108008, Apr. 2021. [Online] Available: https://zenodo.org/record/4668407

The Security Information and Event Management (SIEM) systems constitute an emerging technology in the cybersecurity area, having the capability to detect, normalise and correlate a vast amount of security events. They can **orchestrate the entire security** of a smart ecosystem, such as smart grids. Nevertheless, the current SIEM systems do not take into account the unique smart grid peculiarities and characteristics like the **legacy communication protocols**. This paper presents the **Secure and PrivatE smArt gRid (SPEAR) SIEM**, which focuses on smart grids. The main contribution of this work is the design and implementation of a SIEM system capable of detecting, normalising and correlating cyberattacks and anomalies against a plethora of smart grid application-layer protocols. It is noteworthy that the detection performance of the SPEAR SIEM is demonstrated with real data originating from **four real use cases** (a) hydropower plant, (b) substation, (c) power plant and (d) smart home.

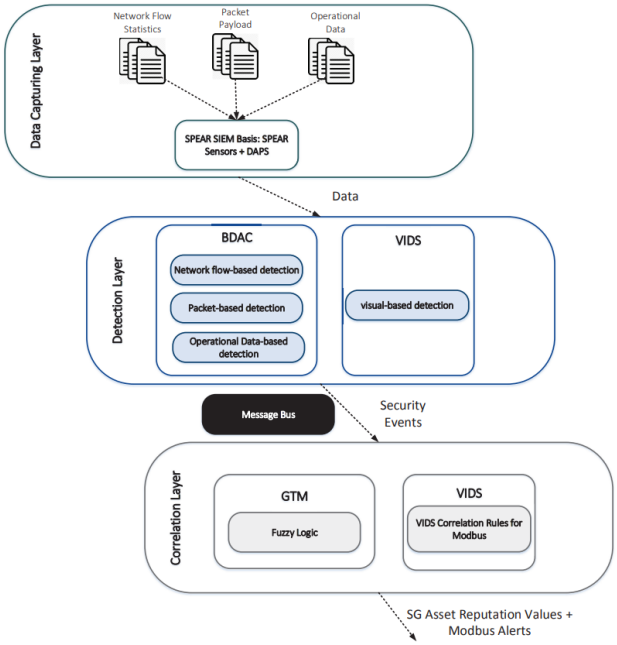


Figure: The SPEAR SIEM architecture

Machine Learning and Deep Learning in smart manufacturing: The Smart Grid paradigm

Computer Science Review

T. Kotsiopoulos, P. Sarigiannidis, D. Ioannidis, and D. Tzovaras, "Machine Learning and Deep Learning in smart manufacturing: The Smart Grid paradigm," Computer Science Review, vol. 40, p. 100341, May 2021. [Online] Available: https://zenodo.org/record/4661095

Machine Learning (ML) and **Deep Learning** (DL) are two subsets of Artificial Intelligence (AI), which are used to evaluate the generated data and produce valuable information about the manufacturing enterprise, while introducing in parallel the **Industrial AI** (IAI). In this paper, the principles of the **Industry 4.0** are highlighted, by giving emphasis to the features, requirements, and challenges behind Industry 4.0. In addition, **a new architecture for AIA** is presented. Furthermore, the most important **ML and DL algorithms** used in Industry 4.0 are presented and compiled in detail. Each algorithm is discussed and evaluated in terms of its features, its applications, and its efficiency. Then, we focus on one of the most important Industry 4.0 fields, namely the **smart grid**, where ML and DL models are presented and analyzed in terms of efficiency and effectiveness in smart grid applications. Lastly, **trends and challenges** in the field of data analysis in the context of the new Industrial era are highlighted and discussed such as scalability, cybersecurity, and big data.

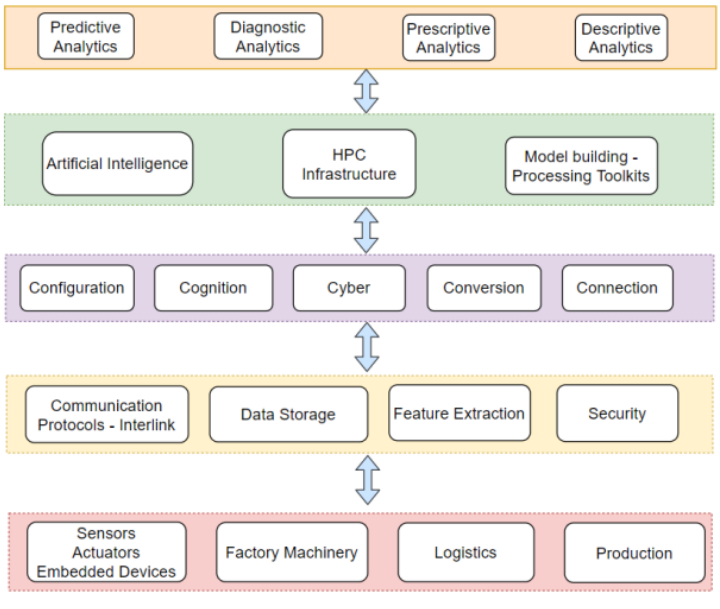


Figure: The proposed architecture

Cyber Attack Detection and Trust Management Toolkit for Defence-Related Microgrids

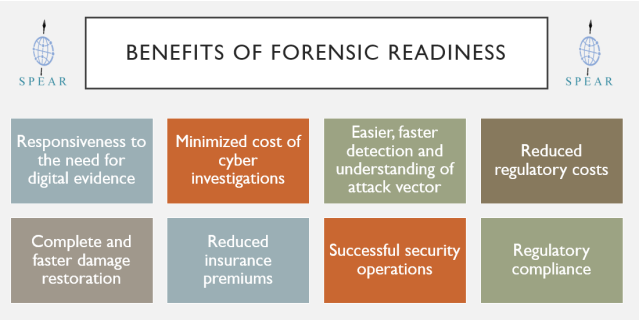
Artificial Intelligence Applications and Innovations (AIAI) Conference, Springer

M. Charalampos-Rafail, K. Thanasis, V. Vasileios, I. Dimosthenis, T. Dimitrios, and S. Panagiotis, "Cyber Attack Detection and Trust Management Toolkit for Defence-Related Microgrids," in Artificial Intelligence Applications and Innovations. AIAI 2021 IFIP WG 12.5 International Workshops, Springer International Publishing, 2021, pp. 240–251. [Online] Available: https://zenodo.org/record/5566931

This paper presents a cyberattack detection and cyber attack severity calculation toolkit, with the aim to provide an end-to-end solution to the cyberattack detection in defence IoT/microgrid systems. Concretely, in this paper the **SPEAR Visual Analytics AI Engine** and the **SPEAR Grid Trusted Module** (GTM) of the SPEAR H2020 project are presented and evaluated. The aim of the Visual Analytics AI Engine is to detect malicious action that intend to harm the microgrid and to assist the security engineer of an infrastructure to easily detect abnormalities and submit security events accordingly, while the GTM is responsible to calculate the severity of each security event and to assigns trust values to the affected assets of the system. The accurate detection of cyber-attacks and the efficient reputation management, are assessed with data from a **real smart home infrastructure** with an installed nanogrid, after applying a 3-stage attack against the **MODBUS/TCP** protocol used by some of the core nanogrid devices.

SPEAR Blog Posts

Forensic Readiness in Critical Infrastructures



According to various studies, UK companies **losses** reach up to **37 billion euro per year** (27 billion pounds), which is comparative to the European Commission's budget in Innovation, Research and Development over a three-year period for the entire Horizon 2020 program. Across the European Union, the "average cost of cybercrime in Europe has risen steeply to **$57,000 (€50,000) per incident**", while recent figures also show that the median cost to companies that suffered cyber incidents and breaches jumped to €50,000 over the past 12 months (2019-2020), representing a near six-fold increase on the previous year's €9,000.

Currently, the approach of the majority of organisations to cyber-incidents focuses on business continuity and disaster recovery. However, this approach often includes actions that contradicts the principles of **forensic investigations**. Organizations tend to be reactive to cyber-incidents, meaning that once a security incident or data breach occurs their first course of action is to try to handle it and perform forensic investigations, followed by actual evidence collection.

Read more about forensic readiness: https://www.spear2020.eu/News/Details?id=123

A review of cascading events in the panEuropean electricity network

Energy infrastructures are complex systems which have physical, geographical, logical and, finally, cyber **interdependencies** with other critical infrastructures, e.g. transport, telecommunications, water, agriculture, health, finance, chemical industry and networks supporting the government, central and territorial entities, emergency services, as well as military- and civil defense. A disruption in the normal operation of critical energy infrastructures can have a **negative cascading effect** on other infrastructures, as well.

Read more about relevant incidents: https://www.spear2020.eu/News/Details?id=126

Visual analytics for Anomaly Detection in IoT networks

Internet of things (IoT) is defined as the embodiment of various physical devices or objects to Internet. Due to the frequency of utilization of such connected devices in our daily activities and the unattended and open operations of the network, numerous inherent security challenges in IoT systems have emerged. Treatment of these challenges could be achieved both via using **anomaly detection algorithms** and monitoring of different types of data produced by devices within an IoT network via **visual analytics techniques**.

Read more about the visual analytics methods employed in SPEAR: https://www.spear2020.eu/News/Details?id=124

Figure: The SPEAR Visual Analytics Framework

SPEAR Anonymization Techniques

The insurance of user privacy is of utmost importance in the context of SPEAR. Therefore, in order to achieve anonymity of the exchanged data three well-known anonymization techniques are being reviewed for usage. These three techniques are **k-anonymity**, **ℓ-diversity** and **group signatures**. Group signatures enable the anonymous upload of data, while k-anonymity is used to verify the anonymity of the data and ℓ-diversity is used for group anonymization.

Read more about the anonymisation techniques used by SPEAR: https://www.spear2020.eu/News/Details?id=125