Defense against cyber-attacks on the Hydro Power Plant connected in parallel with Energy System

Valeri Mladenov
Techical University of Sofia
Faculty of Automatics
Sofia, Bulgaria
valerim@tu-sofia.bg

Veselin Chobanov
Techical University of Sofia
Faculty of Mechanical Engineering
Sofia, Bulgaria
vesselin_chobanov@tu-sofia.bg

Panagiotis Sarigiannidis
University of Western Macedonia
Department of Electrical and Computer Engineering
Kozani, Greece
psarigiannidis@uowm.gr

Panagiotis I. Radoglou-Grammatikis
University of Western Macedonia
Department of Electrical and Computer Engineering
Kozani, Greece
pradoglou@uowm.gr

Anton Hristov
MVETS Lenishta Ltd
Managing Director
Sofia, Bulgaria
anton.h@geo-source.eu

Pencho Zlatev
University of Ruse
Department of Heat Engineering
Hydraulics & Engineering Ecology
Ruse, Bulgaria
pzlatev@uni-ruse.bg

***Abstract*— In today’s modern energy sector, driven more and more towards decentralization, which includes many smaller energy producers rather than huge government projects, security against cyber-attacks is becoming more crucial for the energy grid. Since many small energy plants do not have the resources to finance very expensive existing cyber-security systems, they often have no security system in place at all. Although with small energy producers, the risks of being under attack are not as devastating as in a huge power plants, they still pose a serious threat to the energy system and to the supply of electricity to whole regions. Moreover, in the era of technology, such cyber-attacks could be carried out simultaneously at many locations, thus risking the lack of electricity to larger areas. Since there was a clearly identified need for such an instrument, the SPEAR consortium, started to develop tailor made solution for different types of actors in the energy sector, to prevent such occurrences and help secure the energy system. One of the use cases, investigated in the project, is a real operating hydro power plant in the mountain area of Bulgaria called Leshnitsa, which will be one of the four sites to first test the functionality of the finished product. The plant had no previous cyber-security system in place and had already experienced one attack, where one of the computers in the plant was hacked and a ransom was demanded from the attackers to unlock it. Exactly events like this one are proof, that the energy sector has a need to protect the growing number of small independent actors in the energy system..**

Keywords—Energy System, Hydro Power Plant, Cyber security, Smart grid, Grid infrastructure

I. Introduction (*Heading 1*)

The energy sector and its infrastructure have significantly improved with the integration of information technologies, which has increased the efficiency of generation, transmission and distribution of electricity services. Various use cases of the digitalization have been highlighted [1], indicating a more advanced, data-driven energy system. Smart cities and homes are also emerging where IoT is integrated with the energy provisioning. However, these advances also have their downside. The probability of attacks on the smart grid has increased[2],[3], [9].These attacks also put at risk personal data that may be associated with these smart technologies, including the Internet Protocol (IP) addresses and smart meters used to reach individual consumers [10], [11], [12], [13], [14].

A platform to overcome these problems will be used.

It will collect and deal the following types of data: network traffic, operating system shell commands, keystrokes, communications and syslogs collected from the devices in smart grid, sensors, gateways, etc.; quantitative data related to day-to-day activity (event data produced after processing collected raw data); and cyber attacks and threats data for information sharing through an anonymous channel/repository.

The tools proposed by platform aim to provide effective detection, response and countermeasures against advanced cyber threats and attacks targeted at the smart grids. Such tools are important from a user perspective, as the ability to detect different kinds of attacks concerning confidentiality, integrity and availability, as well as timely detection of these attacks are key to their business model. If the settings of the smart grid are “manipulated with malicious intent, it can pose a serious threat to the business operations, plant equipment and grid equipment, safety of power plant personnel as well as safety of the local population” [61].This poses a threat of significant concern, requiring a thorough understanding of the needs of the energy operators in designing the proposed tools.

In all, this paper highlights the specific requirements methodologies of the platform software requirements—the process of determining the potential users’ needs, the requirements to ensure that the requisite privacy and security controls are embedded into the architecture of the system to be developed using “data protection and security by design” approach.

The paper is outlined as follows. In the next chapter an overview of the developed platform is presented. In chapter III a methodology to capture the user, privacy protection, and data security requirements of the platform are given. Then in Chapter IV the concluding remarks for a multi-component tool that allows for detection and signalization, forensic investigation and possibly prevention of cyber-attacks are given in the last chapter.

II. Overview of the Platform

The Platform aims to support energy operators with a tool that could be deployed for detecting, responding and taking countermeasures against advanced cyber threats and attacks

978-1-7281-9439-4/20/$31.00 ©2020 IEEE

targeted at modern smart grids. This platform is proposed as a three-tier system, where each part has a different yet complementary role: the first tier builds an advanced all-in-one, open source Security Information and Event Management (SIEM) tool. This is designed for timeously detecting threats and attacks in smart environments. The second tier provides a rigorous forensic framework (SPEAR Forensic Readiness Framework (SPEAR-FRF), aiming to assure forensic readiness in the sense that the applied network forensic strategies are deployed before a cyber-attack incident takes place. Innovative techniques employed in this tier include an Advanced Metering Infrastructure (AMI), and honeypots for attracting attackers and capturing the necessary attacks traces for forensic procedures that will secure a detailed and complete report of the launched attack for legal purposes. The third tier is designed in line with two major requirements of all security-oriented organizations: increasing the trust between smart grid operators and facilitating EU consensus towards confronting cyber-attacks. In this respect, platform not only proposes standalone solutions but goes beyond by inaugurating an anonymous and secure communication channel between all energy operators in the EU. To this end, all platform SIEM tools are interconnected via a common and distributed incident database, called platform Repository of Incidents (RI), where updates, patches and best practices are anonymously exchanged, in real time, without risking an organization's reputation or exposing weak parts of the grid.

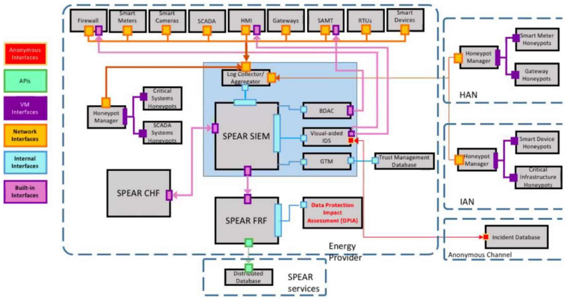

Fig. 1. The platform diagram

III. Methodology

The objective of this task is to capture the user, privacy protection, and data security requirements of the SPEAR platform given the project's objectives. In general, the design of the SPEAR project is based on the ARCADE methodology framework[8]. For the tasks described in this report, desktop research, questionnaires and consultations with relevant project partners have been utilized to complete them. According to the common rules for the internal market in electricity, entities engaging in "electricity undertaking" include any natural or legal person carrying out at least one of the following functions: generation, transmission, distribution, supply, or purchase of electricity. This assisted in identifying and defining the SPEAR end-users, including consumers.

A. *User requirements investigation*

This section describes only the user requirement investigation based on the viewpoint requirement extraction of the ARCADE framework. Three complementary methods were applied in parallel in order to achieve better results in the collection of the SPEAR user requirements. As follows, these methods are quantitative and qualitative methods:

- Observation and field visit: These are types of correlational methods in which an analysis team observes users (i.e., energy providers) as they work and takes notes of the activities that occur during the execution of their job tasks. In the SPEAR project, each use case partner and end-user partner conducted this user observation and field visit in its own premises in order to collect and extract user requirements. Some academic partners (e.g.UOWM) more familiar with the concept of Quality Assurance and Project Management technics visited the use case partners (e.g.,VETS) premises as the analysis team.
- Interview: This is the most common technique for gathering requirements. The users are interviewed by the requirements analysis team, to receive information about their needs and requirements in relation to the new system. In the SPEAR project, the interviews were conducted in a form of teleconferences among the use case partners, the end-users in order to understand and detect user requirements.

B. *Privacy and security requirements investigation*

The privacy and security requirements investigation comprise both the identified requirements of the users, as well as the general system requirements of SPEAR (during the system's development and actual use in a real environment). The users' aspect was obtained with the method above

- Questionnaire: To identify whether personal data will be processed in the development and actual use of the platform, a questionnaire was also sent by to all the other project partners to describe the nature of the data they intend to process in the project. The questionnaire introduces the meaning of personal data as well as records the intention of the partners to collect and process personal data within the scope of platform.

- System architecture analysis: The description of the SPEAR system's input and output data was analyzed to obtain the privacy and security requirements for the system. Privacy and security experts in the project collaborated in this task of which the use case scenarios afforded the opportunity to imagine some of the input and output data of the system.

- Desktop research: The legal and ethical framework—laws, guidelines, standards, etc., relevant for privacy and security in the smart energy systems was investigated through desktop research and analyzed using a doctrinal approach.

C. *Requirements specification model and link with the system's specification and architecture*

1) *User requirements elicitation*

As mentioned earlier, a user-oriented approach [62] has been adopted to identify the SPEAR user requirements. In their responses to the questionnaire circulated by LUH asking for requirements, the SPEAR end-users represented by the Use Case partners (VETS, Schneider/Enel, PPC, and CERTH) highlighted a number of key aspects, even though some of them are beyond the scope of SPEAR. First, these users stressed the need for a quick response time, in which the SIEM would detect and allow responses to cyber-attacks, preferably near real-time; the time interval for the forensic analysis to be ready was seen as less critical, with 3-7 days suggested by one respondent as a reasonable margin. Second, as regards the type of threat users regarded as most requiring protection against, this varied to some extent according to the nature of their enterprise. Thus VETS, in the context of running its hydro-electrical power station, flagged as critical the risk a cyber-intruder might gain access to the main control unit and manipulate the parameters or settings of the unit; this could involve direct physical means (malware on a USB stick). In the Smart Home scenario, CERTH noted the specific added risk of eavesdropping and extortion attacks that aim to steal information from the occupants as a basis for committing fraud or even extortion against the latter.

For their part, Schneider/ENEL, and PPC from the perspective of large utility providers, stressed the need for their Smart Grid to be safeguarded from DDOS attacks. However, they also flagged as important that the SIEM send an alert (including by email or SMS to key offsite personnel) in case a cyber-attacker seeks to take over remote control of devices and communications: this presupposed that the SIEM would be able to identify attacker behavior that deliberately mimics the real behavior of the system. PPC identified the IAN and HAN scenarios in its Testing, Research and Standards Centre as especially central to its security needs.

A further suggestion of VETS was that the system could allow for the disconnection of elements under attack, while maintaining just the most critical components for the essential plant functioning. It was also deemed important that, in visually presenting attack information, the Visual-based IDS should employ a chronological dimension that allows the user quickly to understand the way different incidents unfold and relate to each other across time. Ideally, this information should be layered, with the user able to click on a given incident to see further details for it presented in an 'expert mode'. In relation to cyber-hygiene issues, the partners identified the need for the SPEAR system to reflect and support information security standards and frameworks, such as the ISO 27000 specifications, IEC 62351 and IEC 62443, as well as the data protection requirements of the GDPR as best as possible to assist them in achieving them.

1) *The Hydro Power Plant Scenario*

a) *Description of the Hydro Power Plant*

Hydro power is an essential part of the electricity mix and is the biggest contributor to the renewable energy production worldwide, constituting more than 50% of the global RES production[64].Hydro power plants vary in size and technology and have a different impact on the local or regional grid. The hydro power plant scenario includes real testing of the developed SPEAR tools and components in an operational electricity production facility. HPP Lenishta is located in the mountain area of Bulgaria (near the city of Razlog) and has an installed capacity of 500kW. The plant is connected to the distribution grid via 370 meters long 20 kV transmission line. The SPEAR components will be running to detect attacks. Types of attacks will vary in order to confirm the SPEAR ability to differentiate between a cyber-attack and anomalies caused by extreme weather conditions.

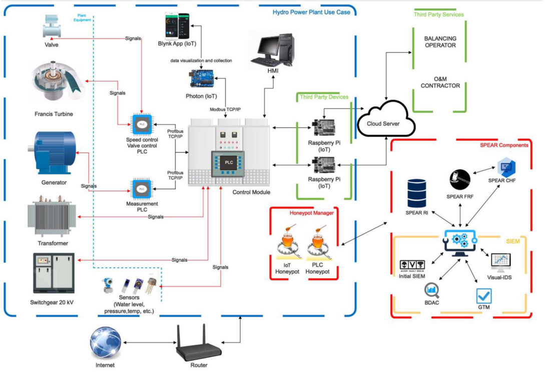

Fig. 2. The hydro powerplant scenario

b) *Components and related data for the Hydro Power Plant scenario*

The components existing in the Hydro Power Plant are as follows:

- Plant equipment–(valve, turbine, generator, transformer, switchgear, sensors) -all power plant components generate signals and communicate them to the PLC units. A set of sensors perform measurements of pressure, temperatures, water levels and other critical parameters for operation.
- Control Module PLC–gathers data from the plant equipment either directly, or through additional PLC units and makes decisions about the plant operation based on the received values and the preset limits.
- HMI–visualizes information from the control module and allows for monitoring and operating the power plant. This can also be done through remote control of the HMI.
- Particle Photon (IoT)–an open source product, which communicates through Modbus TCP/IP with the Control module and collects data, which it then visualizes on an IoT application. The Blynk application is used for remote monitoring of the PLC visualization module. Currently, control functions are also being developed
- Raspberry Pi (IoT)–two separate devices that collect data about the plant performance from the Control module. The first one sends data to the balancing operator which is necessary for correct forecasting of production and grid stability. The other one collects information about operational data and sends it to the O&M operator for continuous monitoring of the power plant status and enables timely preventive maintenance measures.

The potential SPEAR components to be integrated and the required functionalities from them are the following:

- SPEAR SIEM–the detection tool with its related components will detect and warn about any suspicious activities, which may constitute a cyber-attack. The platform will use state of the art analytics tools, graphical-aided visualization techniques and trust management mechanisms in order to detect anomalies and disruptions in the data traffic and alert about it in real time.

- Honeypots –that simulate the vulnerable hydro power plant PLCs and IoT devices, and capture as much information about the attack and attacker, including IP addresses, timestamp, access ports and communication protocols and other.

Data collected during the deployment of the use case and the lifespan of the project:

- Communication Data–data communication between the plant equipment, PLC and smart devices includes strictly industrial measurement data regarding operational readiness. Metrics like equipment temperatures, water levels, voltage and other hydro power related measures do not include any personal information.
- Data from the Honeypots-Honeypots simulating the PLC controller and the IoT devices will collect detailed information regarding the attack and attacker which may include personal data.

Outputs:

- Visual-based IDS shall provide a visual representation of the SPEAR SIEM functionalities in the hydro power plant architecture.
- PLC Honeypot shall store logs and generated network traffic.

c) Hydro Power Plantuse case scenario definition

Table 2 describes the Hydro Power Plant scenarios while figure 3 shows the roles of the actors identified for this use case.

TABLE I. THE HYDRO POWER PLANT SCENARIO DEFINITION

Use case	Scenario ID and Title	Priority level	Related requirements
UC1. Hydro Power Plant	SC1.1. Detection and reaction to cyber-attack on the PLC controller in the hydro power plant	High	UR-01, UR-02
	SC1.2 Detection and reaction to cyber-attack on the IoT devices in the hydro power plant	High	UR-01, UR-02
	SC1.3. Differentiation between cyber-attack and anomalies caused by extreme weather conditions	Medium	UR-13
	SC1.4. Honeypots operation in the hydro power plant	High	UR-12, ER-02

- Platform Security Engineer–a person responsible for installation, monitoring and operation of the SPEAR platform in the hydro power plant. Since the Lenishta power plant is fully automated and does not require human presence full time, the security engineer would be accessing the plant and platform software remotely. He is responsible for receiving notifications from the platform and taking the necessary measures to react to the cyber-attack.
- Hydro power plant operator–a person with technical and operational knowledge of the plant, who when necessary physically controls the facilities through the control module or the HMI inside the control room.
- Cyber-attacker–a person conducting the cyber-attack either remotely or by physically connecting a hard drive with malicious software to the control module or HMI

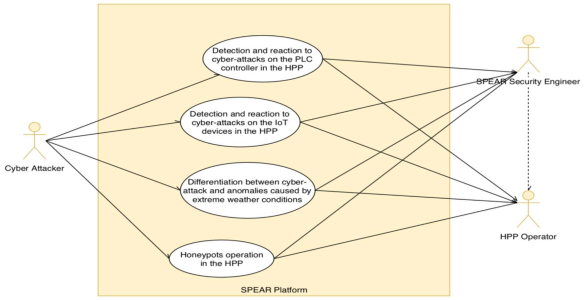
Detection and reaction to cyber-attacks on the PLC controller in the HPP
Detection and reaction to cyber-attacks on the IoT devices in the HPP
Differentiation between cyber-attack and anomalies caused by extreme weather conditions
Honeypots operation in the HPP
Cyber Attacker
SPEAR Security Engineer
HPP Operator
SPEAR Platform

Fig. 3. High-level description of the Hydro powerplant use case roles in theuse case scenarios

d) Scenarios description

Tables 3, 4, 5 and 6 describe the use case scenarios for the Hydro-Power Plant in Bulgaria. These tables showcase what each scenario of the use case is targeted at as well as the evaluation criteria.

TABLE II. DETECTION AND REACTION TO CYBER-ATTACK ON THE PLC CONTROLLER IN THE HYDRO POWER PLAN

Scenario Name	SC1.1. Detection and reaction to cyber-attack on the PLC controller in the hydro power plant
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	The automated hydro power plant has a PLC Control module connected to the internet, which monitors all operational parameters and takes decisions regarding the behaviour of the plant. This is the most critical component to protect in this use case, since it manages all aspects of the power plant and poses a threat to plant and grid equipment, but also third party property damage and physical health. This scenario showcases how the SPEAR platform detects and reacts to a cyber-attack on the most critical plant device.
Challenges	1. Ability to detect a breach in the security of the PLC as quickly as possible 2. Short alert and response time
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The security engineer is monitoring the system remotely via the visual IDS.
Goal (Successful End Condition)	The attack has been successfully identified by the output of the SPEAR SIEM tool, the BDAC, or the Visual IDS or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart Grid Database, the reputation of the attacked node is being updated in the GTM and the attack has been recorded in the SPEAR-RI.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Cyber attacker
Scenario Initiation	An attacker launches an attack against the Profibus TCP/IP protocol used by the PLC devices.
Main Flow	1. The attacker launches a (D)DoS attack against the controller and inundates it with traffic. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the security engineer monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the inverters/chargers is updated in GTM component. The incident is being recorded in SPEAR-RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

TABLE III. DETECTION AND REACTION TO CYBER-ATTACK ON THE IOT DEVICES IN THE HYDRO POWER PLANT

Scenario Name	SC1.2 Detection and reaction to cyber-attack on the IoT devices in the hydro power plant
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	The hydro power plant equipment includes 3 IoT devices. A Photon Particle, which sends data to a mobile application for monitoring and 2 Raspberry Pi's, which send data to a cloud service to be accessed by third parties. This scenario showcases how the SPEAR system reacts to a cyber-attack against the IoT devices.
Challenges	1. Ability to detect anomalies in the data transfer from the IoT devices. 2. Timely detection of the anomalies.
Assumptions & Pre-Conditions	1. The IoT devices are functioning properly and sending adequate data. 2. The SPEAR system is up and running. 3. The security engineer is monitoring the system remotely via the visual IDS.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool or SPEAR BDAC or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM and the attack has been recorded in the SPEAR-RI.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Cyber attacker
Scenario Initiation	An attacker launches an attack against the Modbus TCP/IP protocol used by the IoT devices
Main Flow	1. The attacker sends TCP packets exceeding the maximum length to the Modbus client and server trying to succeed a buffer overflow attack. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the security engineer monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the inverters/chargers is updated in GTM component. The incident is being recorded in SPEAR-RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer, allowing him to take appropriate remedial actions.

TABLE IV. DIFFERENTIATION BETWEEN CYBER-ATTACK AND ANOMALIES CAUSED BY EXTREME WEATHER CONDITION

Scenario Name	SC1.3. Differentiation between cyber-attack and anomalies caused by extreme weather conditions
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	The hydro power plant may experience anomalies in traffic and communication with the grid or between devices due to extreme weather conditions. Such incidents may include lack of internet connectivity caused by the provider's equipment or absence of electrical power to the router. This scenario showcases the ability of SPEAR components to differentiate between a cyber-attack and a naturally caused anomaly.
Challenges	1. Ability to differentiate the cause of the detected anomaly
Assumptions & Pre-Conditions	1. All plant components are working properly before the extreme weather event 2. The SPEAR system is up and running. 3. The security engineer is monitoring the system remotely via the visual IDS.
Goal (Successful End Condition)	The anomaly has been successfully identified by the SPEAR SIEM tool or the SPEAR BDAC or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM and the anomaly has been recorded in the SPEAR-RI.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Weather conditions
Scenario Initiation	Extreme weather causes anomalies in the communication between the plant components and smart devices.
Main Flow	1. The communication between the plant components and devices is disrupted. 2. The SPEAR BDAC anomaly detection algorithms identify the incident as not-malicious and caused by a cyber-attack or the security engineer monitoring the system notices the internet connection or the power is down. 3. System logs and network packets are securely stored in the Smart grid Database for a non-malicious example. 4. The incident is being recorded in the SPEAR-RI without the need to protect personal information.
Evaluation Criteria	SPEAR detects the anomaly and notifies the security engineer allowing him to take appropriate remedial actions.

TABLE V. HONEYPOTS OPERATION IN THE HYDRO POWER PLAN

Scenario Name	SC1.4. Honeypots operation in the hydro power plant
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	Honeypots are a cyber-security system which acts as a decoy for attackers and captures information about the attacker and the incident. This scenario showcases how the SPEAR honeypots operate and record data from cyber-attacks on the PLC and IoT devices in the power plant.
Challenges	1. Honeypots should mimic the PLC or IoT devices realistically to attract the attacker and hide the original device 2. SPEAR SIEM should be able to detect anti-honeypot techniques and overcome them
Assumptions & Pre-Conditions	1. Honeypots are installed and connected to the Local Area Network of the hydro power plant 2. Honeypots will simulate a PLC controller and an IoT device
Goal (Successful End Condition)	The execution of this scenario is considered successful when the honeypot has attracted a simulated cyber-attack on the simulated devices and has recorded information regarding attacker and incident.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Cyber attacker
Scenario Initiation	An attacker launches an attack against the Modbus TCP/IP protocol used by the IoT devices
Main Flow	1. Initialize and start the execution of the honeypot software. 2. Verify that the honeypot records the cyber-attacker actions. 3. Execute the steps of a cyber-attack against the simulated Hydro power equipment or service. 4. Collect system logs and network packets. Interpretation and assignment of the registered information in the log-files with the cyber-attack actions.
Evaluation Criteria	SPEAR honeypot records the attack and notifies the security engineer allowing him to take appropriate remedial actions.

IV. CONCLUSION

In order to address the growing concern for cyber-security in the modern decentralized energy sector, the SPEAR consortium has developed a state of the art security product, which can be deployed at many different actors in the energy sector. The SPEAR platform is a multi-component tool, that allows for detection and signalization, forensic investigation and possibly prevention of cyber-attacks. The consortium has included end users from for very different actors in the energy sector to ensure the platform is accessible and applicable to any stakeholders. In the presented hydro power plant Leshnica, the SIEM component of the platform will monitor the network traffic between all components in the hydro power plant and using its advanced analytic tools will detect any anomalies or discrepancies almost instantly. Once it has detected it, the platform will immediately send signals to the security operator of the plant, who can assess the information from the visualization screen of the platform and take the necessary measures to minimize the possible risks and damages. Additional components of the platform, such as the AMI honey pots and the SPEAR-RFR will try to "distract" the attacker from the actual components and record as much information about the attack/attacker, as possible and also as permitted by personal data regulations. Overall, the SPEAR platform will provide security and improve productivity not only in hydro power plants, but all energy stakeholders, including power generating plants, substations, smart homes and more.

ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787011, Secure and PrivatE smArt gRid (SPEAR)

REFERENCES

[1] P. Vingerhoet, M. Chebbo, and N Hatziargyriou, "The digital energy system 4.0,"Smartgridsproject 2016. [Online]. Available: https://www.etip-snet.eu/wp-content/uploads/2017/04/ETP-SG-Digital-Energy-System-4.0-2016.pdf. [Accessed Jan. 13, 2019]

[2] Directorate General for Internal Policies, “Cyber Security Strategy for the Energy Sector”, October 2016. Available: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf. [Accessed Jan. 13, 2019].

[3] P. Paganini“Smart meters in Spain can be hacked to hit the National power network” Security Affairs, October 17, 2014. Available:http://securityaffairs.co/wordpress/29353/security/smart-meters-hacking. [Accessed Jan. 13, 2019].

[4] Directive 2009/72/EC of the European Parliament andof the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[7] Smart Grid Task Force 2012-14, “Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems,” v. 2 of 13 September 2018.Available: https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf. [Accessed Jan. 10, 2019].

[8] E. Stav, S. Walderhaug, and U. Johansen, ARCADE -An Open Architectural Description Framework. December 2013, SINTEF ICT. Available at: http://www.arcade-framework.org/wp-content/uploads/2013/12/ARCADE-Handbook.pdf. [Accessed Jan. 10, 2019]

[9] C. Vallance, “Ukraine cyber-attacks 'could happen to UK',” BBC News, February 29, 2016. Available: https://www.bbc.com/news/technology-35686493. [Accessed Jan. 10, 2019]

[10] V. Dattana, K. Gupta and A. Kush, "A Probability based Model for Big Data Security in Smart City," 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 2019, pp. 1-6, doi: 10.1109/ICBDSC.2019.8645607

[11] S. Tanimoto, S. Yamada, M. Iwashita, T. Kobayashi, H. Sato and A. Kanai, "Risk assessment of BYOD: Bring your own device," 2016 IEEE 5th Global Conference on Consumer Electronics, Kyoto, 2016, pp. 1-4, doi: 10.1109/GCCE.2016.7800494.

[12] M. Oleg and P. Ekaterina, "Security and privacy risk estimation for personal data stored on mobile devices aposteriori statistical approach to risk estimation," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 730-736, doi: 10.1109/ICITECH.2017.8079935

[13] M. M. H. ONIK, C. KIM and J. YANG, "Personal Data Privacy Challenges of the Fourth Industrial Revolution," 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South), 2019, pp. 635-638, doi: 10.23919/ICACT.2019.8701932.

[14] A. Stefanov and C. Liu, "Cyber-power system security in a smart grid environment," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, 2012, pp. 1-3, doi: 10.1109/ISGT.2012.6175560.