Digitalization in Power Energy Sector: Principles of Cybersecurity

Valentina Timčenko[1], Slavica Boštjančič Rakas[1], Milenko Kabović[1] and Anka Kabović[1]

[1] Institute Mihajlo Pupin, University of Belgrade, Belgrade, Serbia

valentina.timcenko@pupin.rs; slavica.bostjancic@pupin.rs; milenko.kabovic@pupin.rs; anka.kabovic@pupin.rs

***Abstract*— This paper deals with the digitalization of the power energy system, with the introduction of future internet technologies, such as Internet of Things, cloud and fog computing. We have also presented an overview of cybersecurity issues in such environment, with special reference to intrusion detection systems and digital twin technologies.**

***Index Terms*—smart grid, energy efficiency, cybersecurity, digital twins**

I. INTRODUCTION

Smart Grid, the intelligent electric power (EE) network, represents a reliable and secure electricity and power infrastructure capable of the enhanced use of the available digital information and control data, in order to improve the security, availability, reliability and overall efficiency of the electric grid systems. It integrates the operational technologies (OT) and information technologies (IT), making a specific combination of the traditional energy networks and the Future Internet (FIN) technologies, such as Cloud Computing, Fog Computing, Internet of Things (IoT), Big Data analytics, etc. It was designed to be consistent with the needs of the deployment of the distributed resources and integration of different energy resources, including the renewable and green energy resources. Other aspects of its implementation rely on the requirement for the development of special purpose on-demand resources, and resources that can be treated as fully energy efficient. Additionally, the continuous development and deployment of diverse smart technologies, now even combined with the artificial intelligence (AI) and machine learning (ML) techniques and features, provide possibilities of real-time, automated, and highly interactive technologies that can improve the metering results, the automation of the system distribution and also the communication that is necessary for proper smart grid operations. Above all these features and aspects, one of the rising importance is the dynamic optimization of the smart grid operation and resource management, while providing a high level of cybersecurity. Combined with the needs of flexibility, scalability and sustainability, this technological concept is at the moment at one of its peak research and development phase, where many new technologies such as intelligent systems, Internet of Energy (IoE), Internet of Things (IoT), Industrial IoT (IIoT) and distributed energy generations via smart grids (SG) coexist.

The work is funded by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, as well as EU H2020 funded project SINERGY (GA No. 952140).

The most recent studies claim that by the 2035, the world energy demand will rise by more than two-thirds [1]. If not being awaken till now, this is the right moment to make an effective situation analysis and current positioning of the smart grid as a concept. Being an electricity network that relies on a set of different electricity transfer monitoring and management technologies for responding to the varying electricity demands of the end users, the smart grids apply mechanisms for coordination of capabilities and needs for proper functioning of the network generators, operators, and end users.

The strict requirements, now more than ever, stimulate the growth of the energy market relying on efficient operation of all the parts of the system, minimal costs and highest standards for system reliability, resilience, flexibility and stability. Still, this system has to keep with the minimal environmental impact, to improve the amount of sustainable generation in power systems, promote energy-saving, enable the effective and intelligent management of renewable energy and enforce the sustainability development goals agenda policies [2].

Recent development directions cover the means for distribution network upgrade possibilities, while raising digitalization levels of its grids. Some recent research efforts cover the development of the specific smart grid digital twins, as well as a range of the flexibility services [3].

This paper is structured as follows. In the second section we have discussed the issues related to the digitalization in power energy sector, while in section III we focus to the issue of providing time sensitive networking for the energy-based environments. Section IV discusses the cybersecurity in smart greed environment, considering intrusion detection and digital tween approaches. Section V summarizes the main points of the paper and provides an overview of the potential directions for further development of the smart grid solutions.

II. DIGITALIZATION OF POWER GRIDS

In general, the energy sector consists of four different electricity sectors, namely: production, transmission, distribution and consumption. The introduction of FIN technologies has transformed the one-way energy systems into the two-way smart, efficient, safe, flexible, personalized and sustainable energy system. For ensuring such a two-way electricity flow, there was a need to provide adequate storage

capabilities, thus enabling the consumer to become a prosumer, an entity with an active role in selling and buying electricity [4], [5]. The digitalization of all the system sectors came with the introduction of IIoT technology, having noticeable impact to the energy efficiency, cost reductions, supply and demand for electricity optimization, along with parallel improvement in the aspects of the interoperability, reliability and scalability. [5], [6].

The digitalization of modern EE system include the integration of wireless sensor networks, actuators, intelligent measuring devices and other components of the EE network with FIN technologies in order to provide a more detailed insight into the production and consumption of energy and predict future actions with the aim of increasing energy efficiency and reducing total costs. The application of IoT improves visibility of EE system objects, optimizes the management of distributed sources of electricity, reduces electricity losses and total costs [4].

A. Digitalization in the energy production sector

The distributed sources of electricity tend to become the dominant electricity production infrastructure, including smart grids. In order to improve the electricity production efficiency, the sources should be a part of the IIoT procedures for sources location selection, implementation, maintenance and optimization. It is necessary to provide conditions for real-time data collection from the transmission and distribution networks, which are further used by the network load forecasting algorithms, and thus providing efficient and balanced electricity production, monitoring of the distributed parts of the system along with the overall management of a smart grid. This way, the digitalized power generation can obtain valuable information related to the behavior of the power generation resources, the standard values of the frequency, voltage and power factor, and learn about different patterns, which can further aid the power production optimization [7]. In smart grids combined with IIoT, the collected data will encompass the additional information related to the metrics collected from the smart meters, intelligent feeders, current phasor data, and relying on the edge/cloud-based analytics the system can be aware of the real-time operation of the smart grid. This data can enhance the operation, the sustainability of electricity production, and its maintenance.

B. Digitalization in the energy transmission and distribution sector

These energy system sectors face a number of potential issues, stating from the power loses, stealing of the power resources, inaccurate and delayed response to potential outages, while still having to smoothly integrate to the operations and management of the distributed power sources. By adjusting the values of electricity parameters, digitalization of these sectors enables intelligent monitoring and management of network, while permitting the operators to proactively react to the issues in electricity supply, track the source of electricity theft, deal with the consumer issues and smooth integration of distributed energy sources.

C. Digitalization in the energy consumption sector

The digitalization tendencies have enabled the consumer to take an active part in the smart production of energy, reduction of losses, control of the costs and consumption of the renewable energy sources, while also having possibility to sell some part of its production to the EE companies. The digitalization provided the collection of a large amount of data, which can be used as the basis for the use of AI/ML data analysis algorithms which can help system learn, optimize and react to energy consumption patterns of different consumers, in different geographical areas (urban, suburban, rural) [6].

III. FIN TECHNOLOGIES AS A FOUNDATION FOR SMART GRID

Traditional information technologies cannot satisfy requirements for data analysis, latency, mobility, security, privacy and bandwidth; therefore, FIN technologies are increasingly integrated in the whole EE system. These technologies help with the optimization, personalization and efficiency enhancement of power generation and consumption systems.

A three-layered communication architecture of the smart grid, encompassing IoT devices at the lowest level (end users), fog computing and cloud computing, as the middle and top level, respectively, is presented in Figure 1 [8].

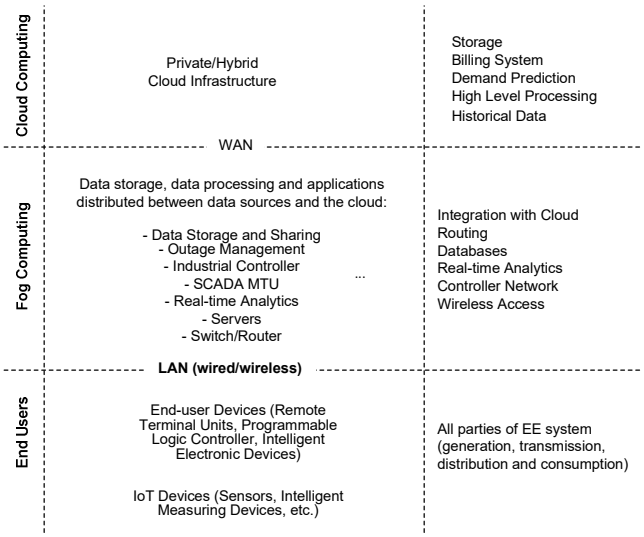

Fig. 1. Three-layered communication architecture for smart grid.

IV. CYBERSECURITY IN SMART GRIDS

The main challenges for the implementation of smart grid are operation complexity, and a need for high efficiency, availability and reliability. With the integration of FIN technologies into all parts of the energy system, it becomes prone to cyber security risks, demanding stable and sophisticated security solutions. Unlike public and corporate information and communication systems, in which the protection of information and infrastructure has reached a certain level of maturity, industrial systems require different and new solutions that can be used in this environment. In such environment, information security becomes really important. In that sense, a guide for users is provided that can

be used for evaluating the level of a cloud/fog computing environment security, through 10 basic corporate/user level steps [9].

Integration of FIN technologies brings a range of cybersecurity challenges, starting from the internal intrusions, the poor integration of provider and user protection systems, technological interoperability issues, troubles related to the access control, the issues with the authorizations for technologies sharing, the failures of the security measures at the provider side, non-secure applications, rise of services for hijacking the accounts, and the loss/theft of data.

The main requirements of the cybersecurity solutions are [10]:

- **Confidentiality**, for preserving authorized restrictions on information access and disclosure.
- **Availability**, for ensuring the authorized user timely and reliable access.
- **Integrity**, for preventing malicious modification of information.
- **Authorization**, for giving users the permission to access specific resources.
- **Non-repudiation**, for proving that the specific user performed specific action.

Also, the trustworthy and reliable cybersecurity solution that could be applied in energy networks, must meet several strict criteria:

- continuous and real-time monitoring;
- updated security techniques;
- data encryption;
- secure user access;
- isolation of the flow of information originating from different users, services and applications;
- automatic distribution of software patches;
- continuous collection and analysis of events;
- ncidents, suspicious activities and anomalies;
- creation and analysis of log files in order to detect attacks in real-time and proceed with adequate response measures;
- consistent and reliable customer service.

A. Cyber-Attacks in Smart Grid

Cybersecurity requirements in smart grids have the following priority: availability, integrity and confidentiality.

There are two basic types of cyber-attacks in smart grid environment, passive and active attacks that violate the AIC triad. Passive attacks aim to get in possession of transmitted data in order to get information on the system configuration, architecture, normal behavior, etc. They are hard to detect, since they only acquire data, and are not changing the data. Examples of such attacks are eavesdropping and traffic analysis attacks. Passive attacks influence data confidentiality. On the other hand, active attacks modify transmitted data, thus affecting the operation of EE system. Active attacks mostly influence before all the availability and integrity, but can also affect data confidentiality [11].

Table I represents classification of cyber-attacks according to influencing the AIC triad in smart grid.

Table I. Cyber-attacks classification according to AIC [11]

Availability	Integrity	Confidentiality
- Wormhole - Flooding - Puppet Attack - DoS/DDoS - Jamming - Buffer Overflow	- Tampering - Wormhole - Replay - Spoofing - Data Injection - Time Synchronization - Data Modification	- Man in the Middle - Password Pilfering - Spoofing - Unauthorized Access - Traffic Analysis - Eavesdropping

B. Smart Grid Intrusion Detection Systems

Fog computing enables the use of the Intrusion Prevention and Detection Systems (IPS/IDS), at both the user and the network sides, thus providing double protection, from internal attacks and attacks coming from the cloud itself. Thus, there is a possibility to prevent the further impact of the attack to the sensitive data and to the internal, critical parts of the system infrastructure, as they stay blocked at the fog premises.

IDS systems applied in smart grid environments should be adaptable to the specific characteristics and limited computer resources of intelligent smart grid devices (e.g. RTU, Remote Terminal Unit) and intelligent meters. It is also important to distinguish different types of IDS according to the part of smart grid that has to be protected. In the case of the centralized overall protective solution, there is need to keep with a number of heterogeneous information communication technologies that can cause certain security problems and dispose some vulnerabilities, thus increasing the probability of exposure to cyber attacks. Also, the smart devices tend to be limited in resources, thus any complex conventional security solution would be difficult for the implementation and use [12]. The use of the advanced metering infrastructure (AMI) relies on the two-way communication between the energy system and consumer, which is based on the use of the application built upon a number of information and communication technologies, and as such, they can be further vulnerable to hijacking, the false data injection (e.g. into SCADA which enables monitoring and management of processes different energy or industrial environments) and similar malware activities, resulting in additional system vulnerabilities. In that kind of the environments and systems, the protection should be aware of the use of the unreliable and insufficiently secure protocols (Modbus, DNP3), with no integrated the identity confirmation and access control mechanisms. The system substations rely on the controlled and fully automated Substation Automation Systems (SAS), encompassing the specific industrial based information and communication components, the Intelligent Electronic Devices (IED), RTUs and user/operator devices. The standard

communication is realized according to the IEC 61850 standard, which lacks any protection or security mechanisms. Still, the use of the IEC 62351 can provide certain level of safety and counts on proper mechanisms for authentication, authorization, and data encryption [12].

C. Digital Twin for Cybersecurity

Digital Twins (DTs) concept assumes provisioning of high-fidelity digital representation of some physical system. It integrates available data and simulations, providing the possibility to mimic the entire life-cycle of the system, and thus obtain the most up-to-date information related to the physical entity. As an accurate virtual representation of the operational environment, it can provide multi-layer decision making. It also provides referent outputs that can be further applied in the real system under the evaluation.

DT represent a special purpose training tool, with a goal to enhance the system cyber resilience, by providing additional experience to the engineers and operators to detect, recognize, diagnose the type of the compromise of the control system, and to react accordingly. Its purpose is to simulate the security attack, and based on the set of parameter values, it should apply its decision-making features resulting in providing a set of potential responses.

The main idea is to feed both the system and the twin with the identical environmental data (e.g. temperature, power, frequency of operation, etc.) and operational data (metrics values, measurements, states). The users of this information (prosumers, operators, intelligent meters, sensors, controllers) uses this information to perform as the system would (e.g., changing the system parameters and behavior, closed loop controls). In parallel with this, the DT system is being operated in the same manner, controlled by a DT controller, and producing the results of the operations such as the initialization, pausing, stopping, or other more complex operation, and based on the obtained results and experience, the DT can develop a decision making tree which aids in determining the extent of an attack and thus provides accurate response for each case. Important benefit of the TD development and application is the possibility of obtaining the real-time responsive environment, which can be used for the simulation of a range of energy system vulnerabilities and compromises [13]. Figure 1 presents a general overview of the DT implementation.

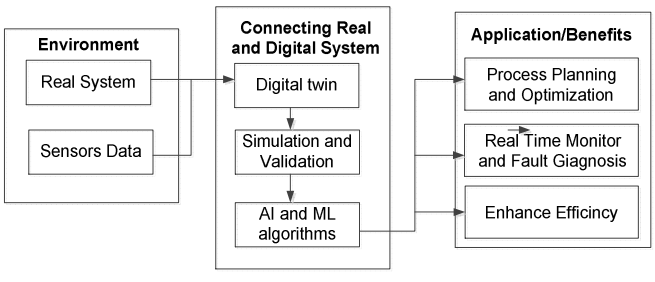

Fig. 2. Digital Twins implementation (Adapted form [14]).

As a result, based on the DT, it is possible to simulate systemic and operational failures, which further enables the development, analysis and application of feasible troubleshooting and procedures for real time decision-making in different virtual environments and conditions.

V. CONCLUSION

The modern tendencies in energy system sector indicate an increase in number of prosumers, while still having some limitations of memory, CPU and computing capacities of the end devices and highly distributed systems consisting of heterogeneous entities. Contrary to the traditional power grid systems, the SGs can provide more efficient fault diagnosing, based on collection of data and activities of many different sources of energy and information. Such an environment is a fertile landscape for a range of different security and privacy concerns. The smart grid utilities should develop a forward-looking approach to resilience against existing and newly developed intrusions, with a special focus to the cybersecurity risks. There, a number of intelligent intrusion prevention and detection solutions, combined with the sophisticated AI/ML algorithms can be of major help.

At the other hand, there is the digitalization in energy sector, mostly seen through the use of the advanced metering infrastructure which empowers the use of smart grids combined with IoT. It thus enables the EE distribution systems the detection of a range of energy generated by different system users, and aid in most effective further distribution of that energy. The digitalization has also brought the integration of the renewable energy sources while enabling the increase in system reliability, stability, operational efficiency, leading to the potential cost decreases for consumers. Among other, it enhanced the utilities management capabilities in peak demand periods and more active cooperation of the utilities and customers. With additional consideration of the United Nations Sustainable Development Goals achievements and regulations, these measures can increase safety, and rise of the awareness for saving the normal and balanced environmental characteristics.

The development and application of different versions of DT can further aid in obtaining more secure and reliable systems, where these solutions besides being a perfect training tools can provide additional useful services, such as the forecasting of the product performances in the upcoming period of time and under certain specific operational conditions.

The promising directions for further development of the smart grid correspond to the development of the techniques for the energy system efficiency and sustainability optimization, along with adequate analysis of the recommendations related to the integration and application of each individual technology within such a complex system. The future SG applications should provide enhanced computational capabilities, and smarter, real-time responding security algorithms, keeping a high level of intrusion detection accuracy.

REFERENCES

[1] IEA (2018), Energy Efficiency 2018: Analysis and outlooks to 2040, IEA, Paris, https://doi.org/10.1787/9789264024304-en.

[2] Agenda for Sustainable Development, United Nations, Online: https://sdgs.un.org/2030agenda

[3] M. M. H. Sifat, et al. "Towards electric digital twin grid: Technology and framework review," Energy and AI, 2022, ID: 100213.

[4] S. Bostjancic Rakas, V, Timccenko, M. Kabovic, A. Kabovic, M. Stojanovic, „Energy Internet: Architecture, Characteristics and Security Issues", Proceedings of the CIGRE 2019. [In Serbian]

[5] G. Bedi, G. Kumar Venayagamoorthy, R. Singh, R. R. Brooks, K.-C. Wang, "Review of Internet of Things (IoT) in Electric Power and Energy Systems", *IEEE Internet of Things Journal,* vol. 5, no. 2, 2018.

[6] H. Boyes, B. Hallaq, J. Cunningham, T. Wtson, "The Industrial Internet of Things (IIoT): An analysis framework", *Computers in Industry*, 2018, vol. 101, pp. 1-12.

[7] B. Arslanagić, A. Damadžić, A. Gosto, S. Mešić, I. Mušanović, „Present and Future of Smart Electrical Energy Networks", Proceedings of the INFOTEH 2018, pp. 506-511. [In Serbian]

[8] S. Bostjancic Rakas, "Energy Internet: Architecture, Emerging Technologies and Security Issues", In Cyber Security of Industrial Control Systems in the Future Internet Environment, edited by Mirjana D. Stojanović and Slavica V. Boštjančič Rakas, 248-266. Hershey, PA: IGI Global, 2020.

[9] Security for Cloud Computing Ten Steps to Ensure Success Version 3.0, Copyright © 2017 Cloud Standards Customer Council

[10] Saleem, Y., Crespi, N., Rehmani, M. H., & Copeland, R. (2017). Internet of Things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions. *IEEE Accesss,7*, 62962-63003.

[11] M. Z. Gunduz, R. Das, "Analysis of cyber-attacks on smart grid applications", *Proceedings of the 2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, Malatya, Turkey, September 2018.

[12] A. Patel, H. Alhussian, J. M. Pedersen, B. Bounabat, J. C. Júnior, and S. Katsikas, "A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems", Computers & Security, vol. 64, pp. 92–109, 2017.

[13] P. Palensky, M. Cvetkovic, D. Gusain, and A. Joseph, "Digital twins and their use in future power systems," Digital Twin, vol 1, no.4, 2022, version 2; peer review: 2 approved. Unpublished. Doi: https://doi.org/10.12688/digitaltwin.17435.2

[14] C. Ghenai, L. A. Husein, M. A. Nahlawi, A. K. Hamid, M. Bettaye, "Recent trends of digital twin technologies in the energy sector: A comprehensive review", *Sustainable Energy Technologies and Assessments*, No. 54, 2022, Artcile No. 102837.