Cyber Security and Its Vulnerabilities in Hydro Power Companies, Plants, Other Energy Resources, and Power Stations

Yunus Emre Aydar
(40110411)
Concordia University

Akash Shrivastava
(40110131)
Concordia University

Shah Md Shahalam
Shawon(40105749)
Concordia University

Abstract

This survey aims to figure out which kind of methods can be observed during cyber security attacks in hydro power companies, plants, renewable energy resources and power stations. Methodologies, attack scenarios, challenges and solutions, study cases, models and architectures of hydro power plants and other renewable energy resources, detection and prevention systems will be analyzed to understand the concept of cyber security in smart grid structures. Systems such as Industrial Control Systems (ICS)[13], Programmable Logic Controller (PLC)[2], Supervisory Control and Data Acquisition (SCADA), Automated Process Control Systems (APCS)[10], and tools such as SPEAR[14] Forensic Readiness Framework (SPEAR – FRF)[14], open source Security Information and Event Management (SIEM)[14] will be mentioned in our survey. The study cases which are Brazilian – Paraguay Blackout, Norsk Hydro Incident and Venezuelan Blackouts as hydro power plant incidents will be discussed in the survey. Also, SCADA-based and Industry 4.0-based failures such as Deriner Hydro Electric Plant[7], and Maroochy Water Service [13] will be discussed briefly.

Keywords - Cyber-attacks, Risk assessment methods, Hydropower, Hydro electricity, Risk management, Renewable energies, Cyber security, Hydro plant hack, Security in hydro plant, Smart Grid.

1.INTRODUCTION

We are in a period where the development of electrical technology is becoming more and more present in our world and making life easier. For many years, traditional electricity grids have been built for the production and provision of electricity to the society. Electric grids designed in traditional ways have started not to meet the desired capacity due to the increase in the population density and individual energy needs today. In addition, these traditional networks have started to become important but cumbersome structures where the growing and complex energy we need is produced and distributed over time. In line with this energy demand, an efficient, safe and environmentally friendly solution had to be brought. Moreover, it was necessary to provide automation within the information technologies, to solve problems in terms of troubleshooting and efficiency, and to charge production and distribution in detail. For this reason, traditional electrical grids took a different form with the possibilities provided by technology. As a result of technology, these grids transformed into smart grids. This smart grid system has been used in the production of various energy sources. Among these energy resources, these smart grids started to be used in the hydro energy sector. However, although the use of these smart grids has great advantages, it has also started to bring some disadvantages. The use of internet technology by smart networks has increased the risk of security dimension with the emergence of cyber threats. When we look at hydro-based smart grids and other renewable energy-based smart grids, we see that various cyber attacks have been carried out. This situation has become more visible to the public with the power outages for unknown reasons or the self-disclosure of hacker groups. It has become an international duty to take action against these cyber

security attacks. There are various elements for planning the system in these measures.Considering these factors, methodologies, attack scenarios, challenges and solutions, study cases, models and architectures, detection and prevention systems play an important role for cyber security in smart grid structures. These factors will play an effective role in the development of hydro power companies, plants and other renewable energy resources with power stations and in the protection of smart grids within the framework of cyber security.

On this paper, use of technology to prevent cyber-attacks in hydro power companies, plants, creation of a safe environment for use of the renewable energies, protection of the confidential information in hydro power plants, evaluation of risk and exposures, and the control of network security will be discussed. The paper summarizes systems such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Automated Process Control Systems (APCS), and tools such as SPEAR Forensic Readiness Framework (SPEAR – FRF), open source Security Information and Event Management (SIEM). Also, attack scenarios such as Norsk Hydro [1], [13], [19], [20] , Brazilian – Paraguay Blackout [4], [5], [9], [21] and Venezuelan Blackouts [17], [18], [22] will be studied as study cases. There will be comparative tables related to scenarios. Suggested and stimulative ideas will be proposed in the end of the survey regarding security solutions for smart grid in hydro power companies, plants and other renewable energy resources with power stations.

2. SURVEYED WORK

As can be seen from the figure 1 below, the working principle of hydro plant power was briefly mentioned in this survey. The systems used by combining hydro energy with smart grid technology was discussed in the survey.

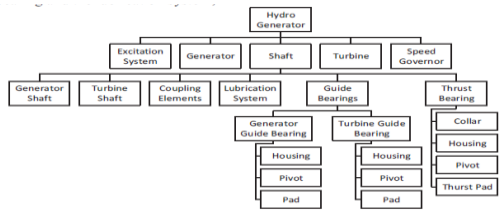

Figure 1 : Part of The Hydro Generator Functional Tree[4]

The infrastructure of the cyber physical system (Figure 2) in hydro plants and the network connection within the system was mentioned in the survey. The security systems and methodologies created against the security problems that may be caused by smart grid technology in hydro plants was tried to be explained in this survey. Also, other renewable energy resources such as wind and solar energy surveyed as well.

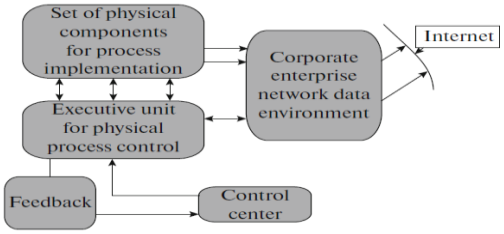

Figure 2 : Logical Structure of The Cyber Physical System [10]

Attack scenarios such as Norsk Hydro [1], [13], [19], [20], Brazilian – Paraguay Blackout [4], [5], [9], [21] and Venezuelan Blackouts [17], [18], [22] were studied as study cases. According to the scenarios, the reasons for the emergence of security vulnerabilities depending on the scenarios and the ways of their prevention also was included in the survey separately. The one possible scenario can be seen in the figure 3 below.

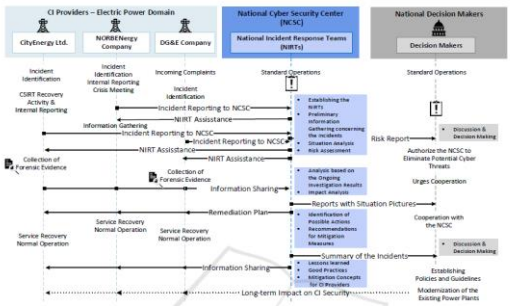

Figure 3 : Information Sharing Scenario [3]

To conduct this survey, we have taken the reference of research papers from various sources such as journals from various countries related to attacks or hydro companies and plants infrastructure (Brazil, Venezuela, Turkey, etc.) Google Scholar, Concordia University Compendex and INSPEC via Engineering Village, IEEE Xplore, ResearchGate, etc.

3. OVERVIEW AND LIMITATIONS

According to long-term malfunctions in the SCADA and various problems ICS pose a great risk for the operation of the hydro power plants. It is anticipated that the operation of the unit may be prevented and the availability and total energy production may decrease in case of any subcomponent failure or cyber attack or both. Security plans against those problems aimed to eliminate these anticipated risks by developing protection methods for the control systems of the power plants. that SCADA and various ICS can suffer from various attacks such as DoS(Denial of Service), MITM(Man in The Middle), Delay, Replay, and malicious files related attacks(Ransomware). Especially the case of Norsk Hydro shows that attachment like malicious email attachment may trigger huge atrocity in the whole operation of the systems. We have proposed a few solutions such as strict firewall planning, application of listing methods (whitelisting, greylisting, blacklisting), access control, antivirus, control network security provision measures, security provision arrangements, etc. Firewall restrictions to detect the attacks can be one of the best solutions among suggested protections to keep the system safe and functional. Moreover, this could be considered as a scope for future studies.

4. RELATED WORKS

During the survey, we came across the paper [14], which compared 3 different cyber attacks in Industry 4.0. This paper shows us step by step the security breaches in detail that occur in the SCADA systems used in the various services (Maroochy Water Services, German Steel Mill, and Norsk Hydro Aluminum and renewable energy company). The paper [14] that contains Norsk Hydro, one of our study cases, helped our survey during its development. Separately, the paper [16] made a great contribution to the surveillance regarding the predicted possible attacks due to the blackout cases. Methods of cyber attacks against Venezuela Blackout which is one of our study cases, and Ukraine Blackout are discussed in one of our papers have also guided our survey in understanding of the SCADA system, the probability of failures in ICS and the security methods in cyber physical structure. Finally, the survey papers gave some ideas about the working principle of the Itaipu hydroelectric system that we tried stimulating ideas about Brazilian - Paraguay Blackout.

5.COMMON TYPE OF ATTACK

Man in the middle attack can be referred to as the most common type of attack that happens in a cyber security system. Usually done when two networks are interconnected to transfer the data hacker intercept in between the communication and take advantages. In March 2000, Maroochy Shire Council experienced problems with its new wastewater system Communications which at first glance thought as a normal technical problem on further investigation came out as a hacker who was trying to get the internal information by hacking the radio signals which were used to transmit signals.best method. In which the SCADA control system can be used to control and limit the hackers gaining access to the main system, a sample figure shown below.

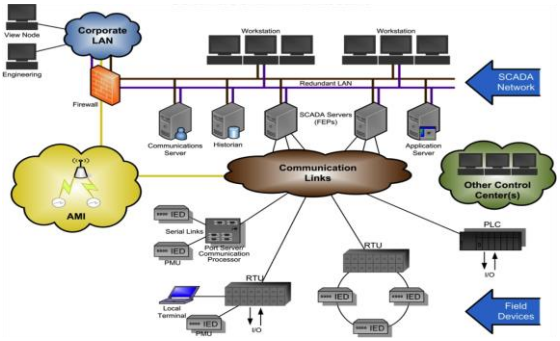

Figure 4:SCADA Control System [23]

It consists of one main control system and one or more RTU (remote terminal units) completely dependent on the requirement of the system.Taking

SCADA system security in account it makes it hard for the attacker to infiltrate the central control system.

A similar type of incident happened in the German Steel Mill incident in which the attackers entered in the central corporate system using spear-phishing attack by getting the full control plant authority was unable to shut down the plant in time due to excess heat in blast furnace it leads to property damage as a result. Another similar attack was on the Norsk Hydro attack in which the attacker used a virus called LockerGoga which was another form of ransomware which encrypted the files in the system and asked for payment in order to access those files[13].These types of attacks can be divided into two main categories[27].

1) ARP spoofing

In which the attackers interfere in between the communication of sender and receiver to get the confidential data.

2) DNS spoofing

In this type of attack the attacker changes the DNS value of the main DNS server which changes the name the domain name to the another domain name which send the data packet into the attackers server

3) Delay attack

This type of attack is a new version of DoS attack. The attacker or hacker can insert delay into the signal which is transmitted in the communication channel, which affects or can delay the stability of the entire stable system.

6. DIFFERENT ATTACK SCENARIOS

There can be many different scenarios in which an attacker or hackers can use to take control over the successful running hydro power system. In the early stages of SCADA system security in general or if we talk about cyber security also were not the main concern in early stages security was only considered as a physical attribute to successfully transfer the data packet successfully to the right address. Due to the introduction of cyber security over the past decade it made it an important feature or tool for the successful running of the system.Therefore the modern and updated SCADA system needs to be modernization and self updating real time system according to the present day challenges.

Firstly attackers can intercept the information from master sender to slave receiver and can send wrong information which can lead to opening of the hydro power plant canal which can lead to vast destruction and total failure of the hydro power plant. The main motive behind these types of attackers can be personal or just a motive to cause destruction.

Secondly an attacker with the wrong intentions can also perform man in the middle attack where he can interpret the communication of sender hub and receiver hub to cause disruption by sending wrong information or changing the commands as well. The communication methods or protocols used for communication redundant are DNP3, Ethernet-based Local Area Network (LAN), IEC 60870-5, RS232 series of connections to other third party data receivers mentioned; all are not very safe ways to communicate or transfer the data and information. These attack scenarios can lead to many cyber threats like False Data Injection Attack (FDIA), Denial-of-Service (DoS) Attack, man in the middle attack and some other attacks like GPS Spoofing Attack (GSA), Load Altering Attack（LAA） etc.

7. VIRUSES, MALWARES USED FOR CYBER ATTACK HYDRO POWER PLANTS

The most number of cyber attacks recorded were performed with the help of virus and malwares. Attackers can inject these viruses with wrong intentions in the system to collect information and cause disruption. For example Norsk Hydro company was attacked with the help of ransomware[1],slammer worm and virus named Sobig is used to attack nuclear plant in Ohio [2],unscheduled power outage in ukraine hydro power plant was caused by malware which was found in various important systems[3]. similarly in the Norsk Hydro aluminum and renewable energy company cyber attack in which a new stream of ransomware was used called lockergogo which encrypted all the files in the plant system and was asking for payment to access them.

8. PROTECTING THE HYDRO SYSTEM

In order to protect the systems from these commonly known attacks there are several techniques which can be a great asset to protect the system.

Antivirus: It is most widely used and seen very effective in detecting malwares and other harmful viruses which help to a great extent to keep the system in a hydro power plants virus free Firewall - in order to control and monitor the incoming and outgoing data in a network system and to monitor the attacker and stop them from sending malicious packets by blocking them permanently is the main reason why firewalls are widely used .

Hydro power plants take a lot of time and capital to run . Control systems in modern plants and high tech. hydro power plants are responsible for high levels of power generation and water supply which can affect the lives of millions of people directly and indirectly.. Protecting these critical assets with software (firewalls or other IT security measures) is not enough as all software by nature can be compromised[6].

On the basis of industrial APCS (SCADA) protocols used in APCSs in all critical production sectors, where real-time process control by the operator is required.

Spear phishing related incidents with ICS facilities can be easily handled by Awareness and Training, Security Assessment Management ,Configuration Management, Planning Management PS Personnel Security by the employee.

In Deriner Hydro Electric Plant project[7], the power plant hardware of control systems with no backups, SCADA long-term experience in the system malfunctions and data archiving issues, great risk for the operation of the power plant was forming. Any sub component corruption disabled the unit's operation may be prevented if it is left, the availability and total energy production It was predicted that it could fall. The software of the control systems of the power plant has to eliminate these anticipated risks by developing. To sum up, some deficiency in SCADA may lead to cyber security issues and the risks have to need advanced cyber attack protections.

PLC(Programmable Logic Controller)[2] can be a good monitoring system to observe various control systems, such as valves, solenoids and other actuators. THe system interacting with human operators that track and manage the system from a control center. The SCADA system uses WAN(Wide Area Network) that communicates with the controller like PLC.

SIEM(Security Information and Event Management) which is proposed in the paper[14], is an efficient detection tool against cyber threats and attacks in many environments. The tool can be part of vital protection for any system.

SPEAR Forensic Readiness Framework (SPEAR-FRF), aiming to assure forensic readiness in the applied network forensic strategies are deployed before a cyber-attack incident took place.

9. ATTACKS ON OTHER RENEWABLE SOURCES

Apart from hydro-electric plants, there are other types of electricity plants where smart-grid and use of automated technologies is prominent. Therefore, enhanced cybersecurity is a vital part of these plants. In our survey, we studied and summarized two different research papers on Solar Energy [11],[15], where they discuss different possible attacks such as cyber attack on Solar Photovoltaic and propose solutions to mitigate those cyber attacks. Solar panels can be installed in homes and industries to meet the additional power needs that the existing power grid may lack, but sometimes home solar panels may produce and supply extra energy to the grid that the grid does not actually need, therefore destabilizing the power supply. Apart from that, nowadays there are sophisticated solar power plants in many countries of the world as Solar Energy is the most easily available source of renewable energy regardless of the location. Other renewable energy sources such as Hydro electricity, wind turbines require specific locations to set up the plant which may be far from the cities or serving areas, since the availability varies by location.

If we talk about solar energy, Solar Photovoltaic(PV) plays an important role. Photovoltaic cells are used to establish solar panels in households and industries. Photovoltaics is the process of converting heat (from sunlight) to energy or electricity using semiconductor materials, based on the principle in physics called photovoltaic

effect. One of the papers[15] we studied, discusses the issues of cybersecurity of PV systems.

The security vulnerability of PV systems are, most of the PV panels are privately-owned and the users are not aware of the security risks. Therefore, the PV panels connected to the main supply grid may be vulnerable to attacks that give the attacker control over voltage regulations.

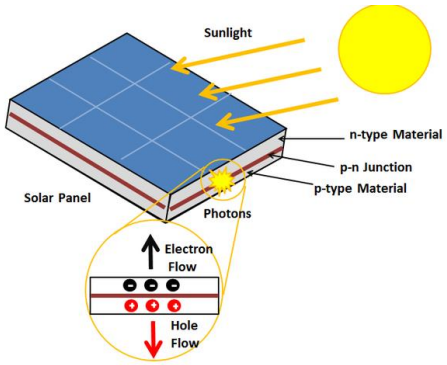

Figure 5: Photovoltaic Panel [24]

10. RESPONSE AND MEASURES ATTACKS,STUDY CASE

To determine or audit the risk factors in SCADA systems, the companies and the authorities may consider implementing several risk assessment systems[2]. To assess the cyber security risk factors, several methods can be used according to our survey paper [2]. Assessing the risks will give us the opportunity to identify any potential vulnerability and come up with the solution for that vulnerability before any actual damage is done.

For SCADA system, risk can be stated as follows, "a function between the possibility of a probable vulnerability exploited by a known threat, and the outcome or impact of an actual attack on this known vulnerability"[2]

In general term, risk can be presented in a mathematical form stated below[2]:

$R = \{s_i, p_i, x_i\}$, i = 1 , 2 , 3 ... N (Kaplan and Garrick)

Where,

R = risk, {} = set,

s = a scenario (undesirable event) description,

p = the probability of a scenario;

x = the measure damage instigated by a scenario and

N – the number of scenarios that may lead to damage of a system.

And in SCADA system, the risk assessment equation would be[2]:

$R = tvx_{tv}$ Where,

t – threat;

v – vulnerability; and

x_{tv} – the outcome of the cyber threat which leads to successfully attacking the weakness.

There are several risk assessment methods used by organizations and governments over the years. Though there are so many risk assessment methods implemented, here are some of the risk assessment methods used in Renewable Energy Systems:

Real-Time Monitoring, Anomaly Detection, Impact Analysis and Mitigation Strategies (RAIM)

1. Risk Assessment, Attack Detection for Sensor Networks
2. CORAS based risk assessment, CORAS is a framework for risk assessment
3. PMU (Phasor Measurement Unit) based risk assessment protocol for power control systems
4. Smart Grid Information Security Analysis based on game models or game theory

For solar electricity, the scope for the attacker is to target the sensors. If they have an attack on the solar supply and they are able to gain illegal access to the electricity, they can target the sensors of the power supply and PV panel to disable them so that the system becomes unable to detect any changes in the voltage. The measures that can prevent these attacks is a voltage detection system proposed in one of the papers[13]. This scheme is a multi-stage scheme that can detect any change in the voltage, it also identifies if the voltage is normal or beyond the normal level.

Our main three study cases include Norsk Hydro case, According to the Norsk Hydro case, Brazilian-

Paraguay Blackout(2005, 2007, and 2009), and Venezuela Blackout(2019).

At the Norsk Hydro case, Norwegian agency, the national agency of cybersecurity, confirmed that the attacker had used a virus known as LockerGoga, which is multiple strains of ransomware, which encrypts files in the system and requires or demands payment to unlock them. In Brazilian Blackout case which is one of the biggest hydroelectric plant in the world with (14,000 MW capacity) reason given was heavy rains and strong winds caused three transformers on a key high-voltage transmission line to short circuit in which the fire overheated the connecting lines, triggering load rejection mechanisms that protect the lines connected to the dam. Still the cause of damage was not clear and it was blamed on the rain and cyber attack and lastly in case of Venezuela Blackout corporation indicated a vegetation fire occurred on series of three lines each of around of 765 kV connecting the dam and Malena and San Gerónimo B stations .On further study by multiple Engineering department and cyber security agencies by the Central University of Venezuela, the consistent loss of power and reduce in intensity of electric voltage over the period of time at the Dam of Gurí caused the turbines which increased their speed, which created an overload on crucial fragile machines and electrical on systems which could have been caused by cyber attack.

11. FUTURE WORK

As we have learned from the study and the papers that Smart Grid and Interactive Control Systems are vulnerable to Cyber Attacks from outsiders and insiders, we look forward to developing an AI based solution to detect and prevent cyber attacks on ICS and smart grid. Security is a general term, which applies to various entities in digital technology, including networks, operating systems, blockchain, websites, softwares, tools that help software development such as git and containers, servers, IOT devices, Control Systems and so on. This project helped us think and analyze from a security point of view. Since Artificial intelligence is the emerging technology which can detect even slightest of changes, we believe that AI can play a big role in future Intrusion Detection in case of Smart Grids. It is possible to train the machine with both normal data and CVE (Common Vulnerability and Exposure) data so that the machine can identify real attacks on these vulnerabilities.

12. INDIVIDUAL WORK

Yunus Emre Aydar (40110411) - Work

In my part, I searched for the articles on study cases and hydro plant security, which will be selected during the survey report, and I determined these articles as survey papers. I brought and proposed the study cases(Norsk Hydro, Brazilian – Paraguay Blackout, and Venezuelan Blackouts) to our survey. In addition, I played a role in researching, determining, and including the articles that were found by every group member that the articles will be the backbone of our survey. I wrote the parts of Abstract, Introduction, Surveyed Work, Overview and Limitations, Related Work, Discussion, References, and some part of Protecting The Hydro System in our survey paper. I gave ideas to my teammates on the study cases during our survey progress and I gave direction to each group member about how to include the found articles in our survey. In addition, I searched for the articles, which are about Hydro electric plants in Turkey that have cyber security issues due to usage of the SCADA system to bring different perspectives to our survey. Finally, I tried to improve the effectiveness and work of each team member in our survey by carrying out various meeting activities. To sum up, each team member completed their parts, and the survey has been completed successfully at the end.

13. DISCUSSION

In the survey, It had been understood that some other hydro plants such as Guri Dam were established before internet/WAN technology. Even though those establishments seem to be secure against cyberattack, later integration of the WAN technology and other smart, modern technology might cause misadaptation of structure in the smart grid because the technology was not meant to be designed for original and traditional infrastructure of the hydro plants. So, integration of modern technology causes cyber security gaps compared to other traditional power plants and power stations.

According to the Itaipu plant, the IT network is entirely secluded from the open Internet that it might not assure protection against cyber attacks because insider attackers or regular employees can cause security problems like It had been seen in the Norsk Hydro case.

14. CONCLUSION

Due to increase in the usage of latest technology and internet usage there is a sudden increase of cyber attacks and cyber threats for many organizations and to the many IT industries as well. The number of service disruptions and cyber attacks against essential systems like hydro power plants and other networks is constantly rising too. In our survey we gathered 18 papers including articles and some other different resources with different attack scenarios in hydro power plants and compared the security protocol used by them against cyber attack and threats. As a result of that, we listed security protocols, such as RAIM, CORAS based risk assessment, SPEAR-FRF, SIEM, SCADA system etc. which can be great assets against cyber attack on hydro power plants.

REFERENCES

[1] N. Bloxsome, "Towards Cyber Resilience In Aluminium Manufacturing," *Aluminium International Today,* vol. 33, no. 1, pp. 6-7, Jan/Feb 2020.

[2] Y. Cherdantseva et al., "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Computers & Security,* vol. 56, pp.1-27, February 2016.

[3] T. Pahi, M. Leitner and F. Skopik, "Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers," in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, Porto, Portugal, 2017.

[4] A. H. A. Melani et al., "Updating a Hydro Power Plant Monitoring System Through Failure Modes and Symptoms Analysis," in *29th European Safety and Reliability Conference*, Hannover, 2019.

[5] J. P. Conti, "The Day The Samba Stopped," *Engineering & Technology,* vol. 5, no. 4, pp. 46-47, 06-26 March 2010.

[6]Waterfall,"Cybersecurity For Hydropower," Waterfall,[Online].Available:https://waterfall-security.com/industries/power/hydropower/.

[7]TÜBİTAK MAM, "Santral Kontrol Teknolojileri,"[Online].Available:https://ee.mam.tubitak.gov.tr/sites/images/ee_mam/derinerhes_proje_bilgi.pdf.

[8] E. L. Ratnam et al., "Electricity system resilience in a world of increased climate change and cybersecurity risk,*The Electricity Journal,* vol. 33, no. 9, p. 106833, November 2020.

[9] F. M. Ribeiro and G. A. Silva, "Life-cycle inventory for hydroelectric generation: a Brazilian case study," *Journal of Cleaner Production,* vol. 18, no. 1, pp. 44-54, January 2010.

[10] Y.S.Vasiliev, P.D. Zegzhda, and D.P. Zegzhda, "Providing security for automated process control systems at hydropower engineering facilities," *Thermal Engineering,* vol. 63, no. 13, p.948–956, 01 December 2016.

[11] A. A. Abdulkadir and F. Al-Turjman, "Smart-grid and solar energy harvesting in the IoT era: An overview," *Concurrency and Computation Practice and Experience,* vol. 33, no. 4, August 2018.

[12] M. Balat, "Security of energy supply in Turkey: Challenges and solutions," *Energy Conversion and Management,* vol. 51, no. 10,pp. 1998-2011, October 2010.

[13] N. E. Oueslati, H. Mrabet, A. Jemai and A. Alhomoud, "Comparative Study of theCommon Cyber-physical Attacks in Industry 4.0," *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, Tunis,Tunisia,2019,pp.17,doi:10.1109/IINTEC48298.2019.9112097.

[14] V. Mladenov, V. Chobanov, P. Sarigiannidis, P. I. Radoglou-Grammatikis, A. Hristov and P.

Zlatev, "Defense against cyber-attacks on the Hydro Power Plant connected in parallel with Energy System," *2020 12th Electrical Engineering Faculty Conference (BulEF)*,Varna, Bulgaria, 2020, pp.1-6,doi:10.1109/BulEF51036.2020.9326016.

[15] A. Teymouri, A. Mehrizi-Sani and C. Liu, "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, 2018,pp.28722877,doi:10.1109/IECON.2018.8591583.

[16] F. Li, X. Yan, Y. Xie, Z. Sang and X. Yuan, "A Review of Cyber-Attack Methods in Cyber-Physical Power System," *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, Xi'an, China, 2019, pp.1335 1339,doi:10.1109/APAP47170.2019.9225126.

[17] L. Viscidi and N. Graham, "Blackouts in Venezuela: why the power system failed and how to fix it," 22 April 2019. [Online]. Available:http://www.realinstitutoelcano.org/wps/wcm/connect/24d62196-f891-4b5e-a5da-0cd2443d3298/Commentary-Viscidi-Graham-Blackouts-Venezuela-why-power-system-failed-and-how-to-fix-it.pdf?MOD=AJPERES&CACHEID=24d62196-f891-4b5e-a5da-0cd2443d3298.

[18] E. Colmenares, D. Rubinstein, and M. Florez, "ABB Review," March 2006. [Online]. Available: https://library.e.abb.com/public/f27f769220adaeaac12571d9004169c6/32-36%203M647_ENG72dpi.pdf.

[19] "What Can We Learn From The Norsk Hydro Hack?" Athens Group, 26 June 2019. [Online].Available:https://athensgroup.com/what-can-we-learn-from-the-norsk-hydro-hack/.

[20] B. Briggs, "Hackers hit Norsk Hydro with ransomware. The company responded with transparency," Microsoft, 16 December 2019. [Online].Available:https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/.

[21] "2009 Brazil and Paraguay Blackout," Wikipedia, 22 February 2021. [Online]. Available:https://en.wikipedia.org/wiki/2009_Brazil_and_Paraguay_blackout.

[22] "2019 Venezuelan Blackouts," Wikipedia, 18 January 2021.[Online]. Available: https://en.wikipedia.org/wiki/2019_Venezuelan_blackouts.

[23] "SCADA System," Electronics Hubs, 19 October 2015. [Online]. Available: https://www.electronicshub.org/scada-system/.

[24] B. Afework et al., "Energy Education," University of Calgary, 25 June 2018. [Online]. Available:https://energyeducation.ca/encyclopedia/Photovoltaic_cell.

[25] Y. Yang et al., "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems," International Conf. Sustainable Power Generation and Supply (SUPERGEN 2012), pp. 1-8.