American Journal of Electrical Power and Energy Systems
2022; 11(6): 118-122
http://www.sciencepublishinggroup.com/j/epes
doi: 10.11648/j.epes.20221106.12
ISSN: 2326-912X (Print); ISSN: 2326-9200 (Online)

The Impact of Cyber Attack on Emergency Energy System

Ghaeth Fandi, Miroslav Müller, Martin Čerňan, Zdeněk Müller, Josef Tlusty

Department of Electrical Power Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Prague, Czech Republic

Email address:

fandigha@fel.cvut.cz (Ghaeth Fandi)

To cite this article:

Ghaeth Fandi, Miroslav Müller, Martin Čerňan, Zdeněk Müller, Josef Tlusty. The Impact of Cyber Attack on Emergency Energy System. *American Journal of Electrical Power and Energy Systems*. Vol. 11, No. 6, 2022, pp. 118-122. doi: 10.11648/j.epes.20221106.12

Received: June 22, 2022; **Accepted**: July 14, 2022; **Published**: January 10, 2023

Abstract: An emergency energy system is a backup power system used in critical situations with the aim of protecting lives and property from the consequences of energy loss, as is the case in hospitals (heart monitors, Ventilator,…etc), and also in sensitive facilities (military industries and government buildings). The emergency power system can contain batteries of all kinds, in addition to solar and wind energy equipment and other cheap types of energy. The concept of cyber security arose several decades after the invention of the computer. At first, there was no need for cyber security, as it was difficult for electronic attacks to occur, because access to computers was limited to specific numbers of users, as the devices were giant confined to a room with certain specifications and were not Linked to networks at the time, Energy sectors expose themselves to a range of cyber threats that can damage control systems. So management, engineering, and IT must adhere to a comprehensive approach that includes threat prevention, detection, and elimination. In this research we will try to mitigate the effects of the cyber attack on these systems by applying some algorithms in order to detect, identify and prevent such attacks, and we will see through the results we obtained that we have made remarkable progress in this field.

Keywords: Cyber Attack, Emergency System, Standby System, Solar Power

1. Introduction

Energy shortages can lead to several risks to any society. This can affect the standard of living of individuals, it can also endanger the lives of patients in hospitals, and so on. In developed countries, we do not face such risks because they countries have well-organized electrical systems and high energy security [1]. A model for integrating autonomous emergency power systems with the micro-grid is proposed in order to improve the reliability of power supply in a more economical way. Simulated by the Monte Carlo method [2]. With renewable energy sources, like solar, wind, dropping in price by 85% in the last 8 years and energy storage seeing drastic cost reductions of more than 20% year over year since 2012 [3, 4]. The harmful effects of carbon and carbon dioxide emissions from excessive dependence on oil is a global issue, currently being addressed by encouraging the contribution of renewable energy resources (RE) to the energy mix. Encouraging renewable energy is important in order to solve the unsustainable nature of electricity generation [5]. Information and Communication Technology (ICT) plays a major role in the modern energy system. A cyber attack may lead to the complete collapse of the energy system, which may result in disasters at the human and physical level. Cyber attack, which works on cyber system of the Cyber–physical system (CPS), could trigger even larger loss in power systems. In order to guarantee cyber security of the system, technologies such as access control, firewall, intrusion detection, cryptography and key management are utilized [6]. Traditionally, the causes of power system fault are generally supposed to distribute as Poisson process and the fault due to these factors should follow exponential distribution in given time interval. If the scale of blackout is proportional to the number of line outage [7]. Integrated Energy System (IES) constitutes a new type of cyber-physical system combined with advanced information and communication technology. The coupling of a cyber system and an IES improves energy efficiency while introducing a cybersecurity threat. The importance of IES cybersecurity is highlighted and cybersecurity weaknesses in IES heating systems are exposed [8]. The telecommunication infrastructure of power grids was analyzed to elicit the main challenges arising from power grids with regard to cyber

security. Accordingly, a wide range of attack vectors and the resulting attack scenarios that threaten the security of power grids have been identified. To meet these challenges, it has been proposed to rely on an in-depth defensive strategy, which includes measures for device and application security, network security, and physical security, as well as policies, procedures, and awareness [9]. Prof. Bompard and colleagues from universities and companies across the EU have come up with a system that gives grid operators the information they need to make decisions in the face of a potentially devastating cyber attack [10]. Big data and machine-learning framework were implemented by using crime data collected from social media platforms. The data were gathered through Volunteered Geographic Information, web and mobile crime reporting applications. Crime predictions were produced from the collected data using the NB algorithm. The purpose of these predictions is to determine the location of possible crimes and prevent them [11], some research's present a conceptual framework for assessing systemic cyber risk to individual countries. This involves analyzing cyber risk exposures, assessing cybersecurity and preparedness capabilities, and identifying buffers available to absorb cyber risk–induced shocks [12], Smart Home Energy Management Systems (HEMS) have been proposed as a way of reducing energy consumption in households and for better utilization of grid resources. therefore we investigates the impact of cyber-attacks on a smart HEMS. Thereafter, possible ways of detecting the attacks and how to mitigate these are examined. Attack on price is the main focus of the simulations. The results obtained from the simulations and detection methods are presented and conclusions are drawn [13]. To detect cyber-attacks on smart grids, S. Khan et al. [14], propose a UPnP technology networking between the Home Energy Gateway (HEG) and household appliances. ECC-based secure HTTP communication framework is also used (elliptic curve cryptography), In order to evaluate the cyberattack, a simulation test rig is developed in four phases: Model development and optimization, simulation of attack, detection of attack and mitigation. In order to validate the simulations, data from Austin, Texas was used [15]. In this paper, we will closely examine current approaches to address physical cybersecurity in power systems with a focus on microgrids.

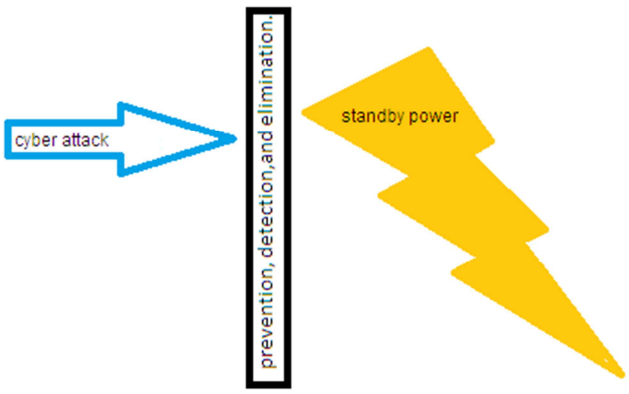


Figure 1. *Prevention and location.*

2. Methodology

There are several key strategies that are recommended to use to protect An small energy system and enterprise from cyber attacks, such as data backup, install firewall and other antiviruse, contol access to system and using passwords.

The most important step is to detect the cyberattack. Before we can figure out how to spot cyber threats, it is important to first identify the most common threats. According to the National Institute of Standards and Technology (NIST), the five most common threats are:

1) Identity theft: One of the most famous attacks is that some hackers access system databases and steal information.
2) Phishing: In this type of attack, a disguised email is sent to the employee by the cyber criminal, which begins with a phrase like “Dear valued customer”, and it targets a large number of people with the purpose of stealing the password.
3) Spear phishing: This type targets only one person or people within a specific department, the messages are more specific, for example, a person working in the sales department receives an email about a specific invoice.
4) Spam: Spam messages greatly reduce productivity, and cause great inconvenience, as it takes a lot of time and effort to sort such messages, and for this purpose, certain programs were used to detect and remove these messages, but it is not easy to do so, as we always need the human element to achieve this.
5) Compromised web applications and web pages: Hackers target websites, fill them with misleading content or turn them off, and they can also install malicious programs on visitors' computers without their knowledge.

One of the most important tools to use is antivirus software. Most antivirus mechanisms can detect malware, spyware, and malicious email attachments. Then, when you are alerted about a high-risk incident, you can quickly identify the threat and treat it before it causes any damage.

Another way to monitor potential cyber threats is to use a threat detection log. Most cybersecurity platforms offer advanced logging capabilities that will help you detect suspicious activity on your networks and systems. By keeping and reviewing these logs, you will have access to a detailed assessment of the security of your network.

Other key threat detection strategies include:

1) Penetration Testing: By thinking the way a cybercriminal would do it, security experts can scan their IT environments for vulnerabilities, such as unpatched software, authentication errors, and more.
2) Automated monitoring systems: Besides manual processes, organizations can enhance cybersecurity by integrating automated threat detection systems. These platforms can help organizations by tracking device performance and activity, monitoring web traffic, and notifying the cybersecurity team when irregularities are detected.

3) User behavior analytics: By analyzing user behavior, the organization can better understand what normal employee behavior would look like. This includes the type of data they access, the time of day they log in, and their physical location. This way, any external behavior will appear as unusual, and it will be easier for the security analyst to know what behavior to investigate.

In addition to detecting potential cyber threats, strengthening our system's cybersecurity will also help us to keep our comunication protected.

Some of the tools we can use to bolster our system's cybersecurity:

1) Multi-factor authentication: Having more than one form of authentication in place significantly reduces the chance of a cyber attack. There are a lot of authentication options available, including passwords, fingerprints, authenticator apps, facial recognition, voice recognition, and more.
2) Identity and access management: This ensures that the right people have the tools they need to do their jobs. Identity and access management (IAM) strengthens our system's security by controlling who can access which information, but it also increases productivity.
3) Vulnerability management: Keeping your software and operating systems up to date can prevent malicious actors from leveraging any vulnerabilities within our network. And the best part is that most of these updates can be automated.
4) Data loss prevention: Implementing backup and disaster recovery solutions will help us safeguard our company's data, even in the event of a cyber attack.

Suggested algorithm:

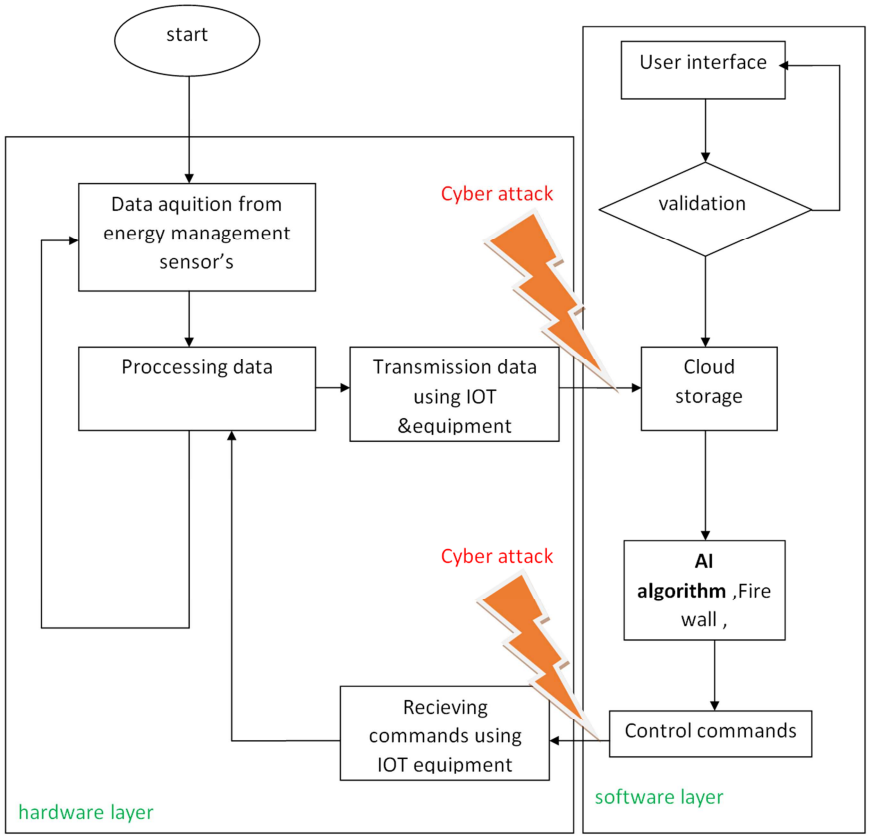


Figure 2. *Flowchart of data flow.*

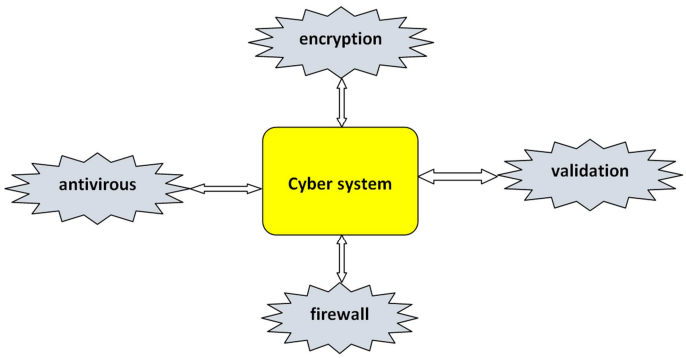


Figure 3. *Cyber security controls for the energy system.*

The involvement of AI in cybersecurity has four primary goals:

1) Big Information Management: AI prioritizes which situations and attacks have administrative priority and which are false threats, eliminating the workload on systems.
2) Real-time response: AI allows immediate action in response to attacks to reduce risks, based on endless data and context.
3) Automation: Automate the response to multiple threats and reduce their cost in terms of detection and response.
4) Prediction: AI helps improve the forensic analysis of previous attacks, which translates to improved defenses.

3. Results

It is difficult to measure and track risks and impacts. The first barrier is the lack of comprehensive publicly available data on cybersecurity incidents. The second is that many incidents may not be reported at all - even to the relevant authorities - and some attacks may go undetected. The third is the difficulty to overcome major differences in scope and definitions, such as what constitutes an "incident" or "attack". For example, a global database to track “major” cyber incidents shows that the number of incidents has increased significantly in recent years, including in the electricity sector.

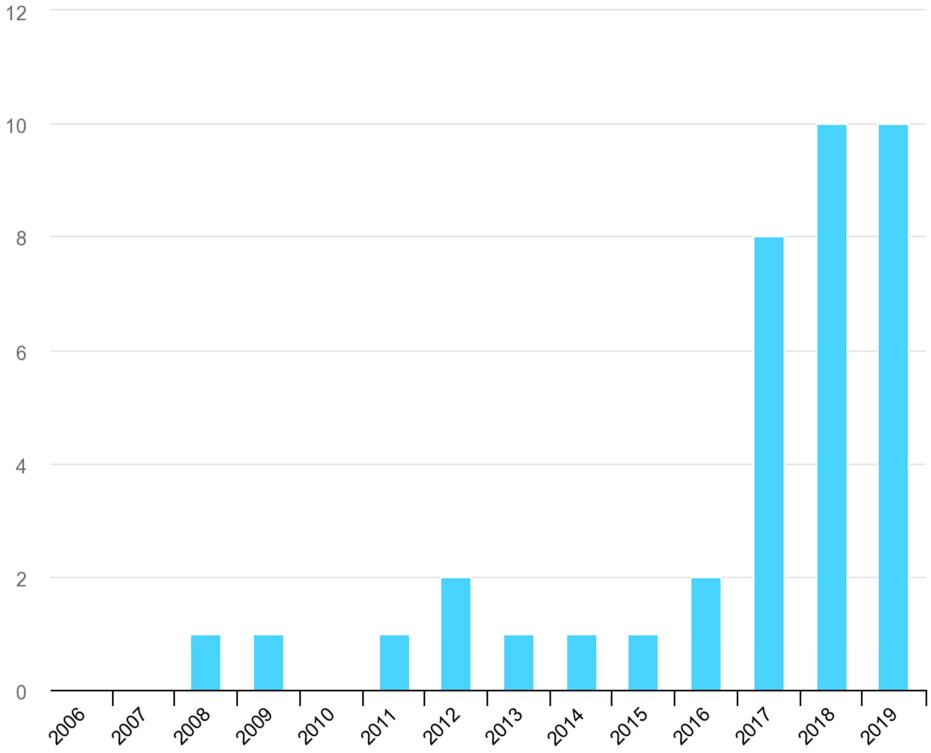
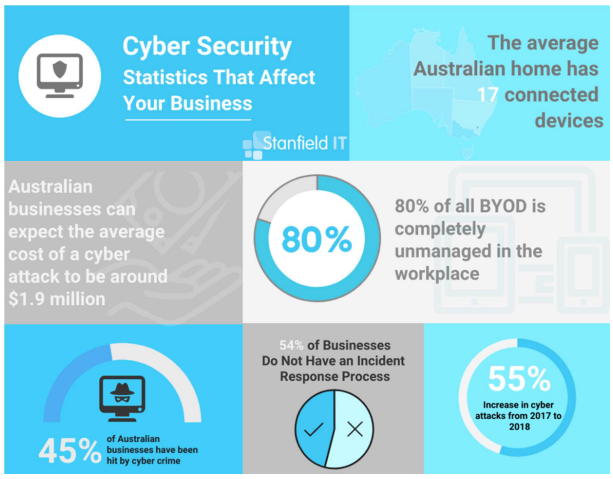


Figure 4. *Electricity-related incidents worldwide, 2006-2019.*



Figur 5. *Damage of cyberattack.*

Cyber security analysts are overwhelmed by the massive volume of information units they must monitor to combat intrusions, and the volume and complexity of cyber attacks has grown considerably in recent years. For this and other reasons, the Markets and Markets report “Artificial Intelligence in the Cyber security Market: Global Forecast to 2026” concludes that the artificial intelligence sector in cybersecurity will reach $38.2 billion by 2026, representing an average annual growth of 23.3%.

The inability of traditional equipment to cope with IT risks shows that only with AI can companies strengthen their defence systems and cyber security can become smarter than cyber attacks. This need is opening the way to platforms that manage industrial systems in an integrated manner and ensure the cyber security of their customers.

4. Conclusion and Implications

Due to the strong economic expansion, significant population growth and new uses of energy, there has been a rapid growth in the demand for energy in recent years and this has posed a major challenge requiring the implementation of policy measures to ensure that reliable, affordable and safe energy supplies reach energy users. In countries that do not have large sources of energy, this is a real problem and therefore they are forced to rely on energy imports. However, these countries can pursue individual or joint strategies to ensure their energy security. first, Animal and plant wastes such as corn and rice can be used to produce methane gas that can be used for cooking or heating. This method gives a positive return in terms of energy security because it gives new resources and reduces the demand for traditional types of energy. Second, countries can benefit from renewable energies such as wind and solar energy and connect them to their electric grids. These types of energy are considered promising in the future, especially in the Middle East and North Africa regions. Third, by setting strict laws regarding investment in this field, and starting to manufacture electric cars that reduce fuel consumption and current electricity prices. Fourth, improving the performance of energy markets is an important factor in enhancing energy security through fundamental reforms. Proper implementation of these measures will significantly reduce waste and stimulate investment in the energy sector by private companies and reduce prices for consumers. Fifthly, at the international level It is possible to achieve cooperation between countries in the field of energy trade and give a profit to exporters and importers.

Acknowledgements

This work was supported by Ministry of the interior of the Czech Republic through the grant (number: VI20192022124).

References

[1] Ghaeth Fandi, Vladimír Krepl, Ibrahim Ahmad, Famous O. Igbinovia, Tatiana Ivanova, Soliman Fandie, Zdenek Muller and Josef Tlusty. “Design of an Emergency Energy System for a City Assisted by Renewable Energy, Case Study: Latakia, Syria”, Energies 2018, 11, 3138.

[2] Liting Zhang, Yongwen Yang, Qifei Li. “Reliability and cost analysis of the integrated emergency power system in building complex”, SAGE journals October 20, 2021.

[3] IRENA, "Renewable Power Generation Costs," International Renewable Energy Agency, Abu Dhabi, 2019.

[4] D. Frankel, S. Kane and C. Tryggestad, "The new rules of competition," McKinsey & Company, 2018.

[5] Abubakar Mas’ud, A., Wirba, A. V., Muhammad-Sukki, F., Albarracín, R., Abu-Bakar, S. H., Munir, A. B., & Bani, N. A. (2016).” A review on the recent progress made on solar photovoltaic in selected countries of sub-Saharan Africa. Renewable and Sustainable “ Energy Reviews, 62, 441–452.

[6] Su Sheng, Wang Yingkun, Long Yuyi, Li Yong, Jiang Yu, “Cyber attack impact on power system blackout”, IET Conference on Reliability of Transmission and Distribution Networks (RTDN 2011), November 2011.

[7] B. A. Carreras, David E. Newman, I. Dobson, A. Bruce Poole. “Evidence for self-organized criticality in a time series of electric power system blackouts”, IEEE Trans. Circuits Systems I, Vol. 51, No. 9, pp: 1733-1740, Sept. 2004.

[8] Shixing Dinga, Wei Gu, Shuai Lu, Ruizhi Yu, Lina Sheng, “Cyber-attack against heating system in integrated energy systems: Model and propagation mechanism”, Applied Energy, Volume 311, 1 April 2022.

[9] T Krause, R Ernst, B Klaer, I Hacker, M Henze, “Cyber security in Power Grids: Challenges and Opportunities”, - Sensors, 2021 - mdpi.com.

[10] Jon Cartwright, “Europe's power grids readied against cyber attack”, horizon-magazine, 18 September 2015.

[11] Jha, Pranay, Raman Jha, and Ashok Sharma. "Behavior analysis and crime prediction using big data and machine learning." International Journal of Recent Technology and Engineering 2019.

[12] Lincoln Kaffenberger, Emanuel Kopp, “Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment”, Carnegie Endowment, SEPTEMBER 30, 2019.

[13] Aksha Sajeev; Haile-Selassie Rajamani, “Cyber-Attacks on Smart Home Energy Management Systems under Aggregators” 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI).

[14] S. Khan, R. Khan and A. H. Al-Bayatti, "Secure Communication Architecture for Dynamic Energy Management in Smart Grid," in IEEE Power and Energy Technology Systems Journal, vol. 6, no. 1, pp. 47- 58, March 2019.

[15] Pecan street data, https://dataport.pecanstreet.org/, 2020.