This is a peer-reviewed, accepted author manuscript of the following paper:
Vozikis, D., Dara, E., Kuusk, T., Kavallieros, D., Reintam, A., & Bellekens, X. (2020).
On the importance of cyber-security training for multi-vector energy distribution system operators.
In M. Volkamer, & C. Wressnegger (Eds.), ARES Proceedings of the 15th International
Conference on Availability, Reliability and Security [114] ACM Press. https://doi.org/10.1145/3407023.3409313

On the Importance of Cyber-Security Training for Multi-Vector Energy Distribution System Operators

Dimitrios Vozikis
dimitrios.vozikis@strath.ac.uk
University of Strathclyde
Glasgow

Eleni Darra
e.darra@kemea-research.gr
KEMEA-Center for Security Studies
Athens, Greece

Tanel Kuusk
tanel.kuusk@cybexer.com
CybExer Technologies
Tallinn, Estonia

Dimitris Kavallieros
d.kavallieros@kemea-research.gr
Center for Security Studies
Athens, Greece
University of the Peloponnese
Tripolis, Greece

Aare Reintam
aare.reintam@cybexer.com
CybExer Technologies
Tallinn, Estonia

Xavier Bellekens
xavier.bellekens@strath.ac.uk
University of Strathclyde
Glasgow

ABSTRACT

Multi-vector Energy Distribution Systems (EDS) are increasingly connected to provide new services to consumers and Distribution Network Operators (DNO). This exponential growth in connectivity, while beneficial, tremendously increases the attack surface of critical infrastructures, demonstrating a clear need for energy operator cyber-security training. This paper highlights the cyber-security challenges faced by EDS operators as well as the impact a successful cyber-attack could have on the grid. Finally, training needs are contextualised through cyber-attack examples.

KEYWORDS

cyber-security, energy distribution system, training

ACM Reference Format:
Dimitrios Vozikis, Eleni Darra, Tanel Kuusk, Dimitris Kavallieros, Aare Reintam, and Xavier Bellekens. 2020. On the Importance of Cyber-Security Training for Multi-Vector Energy Distribution System Operators. In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3407023.3409313

1 INTRODUCTION

Critical Infrastructures (CI) present an ideal target for state actors and crime groups due to their large attack surface composed of intertwined Information Technology (IT) and Operational Technology (OT) networks. Over the last decade, numerous innovations have spawned in the energy sector strengthening the reliance of society on these infrastructures by providing new services such as smart-meters, micro-grids, etc. While these services provide numerous advantages to DNO and end-users, they rely heavily on the technologies underpinning them. This reliance on technology was further exacerbated during the COVID-19 pandemic when key-workers were required to work from home, managing CI remotely [15]. The increased connectivity has also allowed the automation of energy infrastructures for both manufacturers and producers. While these advances are beneficial, this new paradigm requires operators to understand new cyber-attacks and threat vectors underpinning remote-working and the advances in multi-vector energy distribution systems. Training is therefore essential to differentiate a fault from a cyber-attack, as the course of action will be different based on the issue at hand. The remainder of this paper is organised as follows; Section 2 provides an overview of multi-vector energy systems. Section 3 defines the structure and architecture of EDS, Section 4 provides a list of cyber-attacks aimed at EDS, Section 5 identifies the future of EDS systems, Section 6 discusses the training requirements for EDS operators, Section 7 highlights EU policies for EDS security while Section 8 concludes the paper.

ARES 2020, August 25–28, 2020, Virtual Event, Ireland

ACM ISBN 978-1-4503-8833-7/20/08…$15.00
https://doi.org/10.1145/3407023.3409313

2 MULTI-VECTOR ENERGY DISTRIBUTION SYSTEMS

Multi-Vector Energy (Electricity, Gas, Heat, and Water) provides vital services to developed societies and cyber-attacks will have a growing negative economic and societal impact, thus representing a major and global risk [3].

Historically, the various sectors constituting the UK energy system (electricity, gas, water) have operated independently, with interactions limited to, for example, the provision of gas to power stations, or liquid fuel to service the transport sector. The requirement to support the low-carbon transition has driven an increasing interest in strengthening the integration between stakeholders operating within the mix of energy

provisions such that new value streams can be mined across domains. The evolution is most often referred to as multi-energy vector integration, the goal being the provision of new or enhancement of existing services using multiple energy providers (electricity, heat, gas, hydrogen).

The multi-vector energy systems allow fast transactions allowing multi-energy grids, without the necessity of a centralised energy dispatch. One of the main spines that facilitate the migration to a fully integrated operational environment are frameworks that provide trusted interactions, guarantee resilience, and in turn long-term stability of the large-scale infrastructure. The integration of multi-vector energy systems necessitates a secure and reliable implementation of essential control, protection, scheduling, and monitoring systems. Nevertheless, to achieve robust and agile control, it is expected that the low-level communication layer will be directly linked between the various sources of energy.

3 STRUCTURES OF MULTI-VECTOR EDS

Multi-vectors EDS systems are based on 4 distinct layers namely; I) Process and Control, II) Operations and Management Zone, III) Enterprise Zone, and IV) External zone as depicted in Figure 2. Layer 2, 3, and 4 are common to most energy sectors as they focus essentially on the control, monitoring, and reporting aspects. While Layer 1 is dedicated to specific energy sectors. Furthermore, it is possible for the low-level layers to interact directly which various energy sectors, to achieve resilience, fast responses and overall enhanced stability of the system. Figure 1 is an adapted Purdue Models, as defined in IEC 62443, demonstrating the reference levels and security zone applicable to EDS.

Digitisation of the energy sector provides significant operational benefits. However, the widespread use of digital communications and inter-connectivity between organisations and systems induces a significant risk from cyber-attack. This risk further increases as the energy sectors move towards smart grid and Distribution System Operations (DSO), resulting in an increased attack surface[9] Furthermore, each zone should have its own security boundary and requirements should meet the desired security attributes to support the desired level of security for that zone. This means that the assets, systems, and services within the zone need to be examined and key features identified. Also it is necessary to realise that the assets, systems or services may have interactions with other equipment or information systems both internally or external to the system, increasing the security risk.

4 EDS CYBER-ATTACKS

4.1 Types of cyber-attacks

A wide range of cyber- attacks have been identified in the literature but the most common types that targeted the energy sector include the following [6] [10]:

- *Malicious software (Malware)*: is a program or file that is designed to harm a device or user. The existing types of malware include:

  Virus: It replicates itself when it is executed on a computer.

  Worm: It replicates itself to spread to computers through the network. It relies on security failures of the other computers in the network.

  Trojan horse: provides a backdoor to malicious users.

  Ransomware: threatens a victim to publish data or block access to the system for a ransom

  Spyware: It gathers information from the system, stealing, internet usage and sensitive data, trying to hack another entity.

  Adware: It generates unwanted advertisements on a device.

- *Denial of Service (DoS)*: aims at denying the usage of a service or machine to a legitimate user or set of users. The attack typically involves flooding the services or resources with more requests than they can handle, or sending specially crafted requests that crash the application. A subset of DoS attacks is the *Distributed Denial of Service (DDos)*, in which case the requests originate from numerous different computers throughout.

- *Social engineering*: in this type of attack the users can be tricked into divulging confidential information. The social engineering attacks mainly rely on the human interaction with the most common examples include phishing and spear phishing.

  Phishing: it includes deceptive emails, websites and text message.

- *Advanced Persistent Threats (APTs)*: is a type of attack where an unauthorised party gains an extended access to a system. APT require extensive experience of the systems [11].

4.2 Cyber-attacks in the energy sector

Over the last decade, numerous cyber-attacks have been conducted against energy companies throughout the world. Most of them have targeted electricity production and distribution.

One of the first widely-known attacks that was targeted against an energy company was the Stuxnet worm, that was discovered in 2010. It was originally aimed at Iran's nuclear facilities, targeting the Programmable Logic Controllers (PLCs) used to automate machine processes, eventually damaging the centrifuges required by the nuclear plant. It was the first known virus to be capable of crippling hardware. In the following years, Stuxnet and its descendants have affected every fourth power company in the world [16].

Another significant attack occurred on December 23, 2015, but this time against the electricity distributors of Ukraine. Using the BlackEnergy 3 malware the attackers gained access into the network and systems of multiple energy distributors. The malware was initially distributed through spear phishing attacks, while the malware itself was disguised (infected MS Word attachment) [14], [29]. That was the first part of the attack while the second part of the attack targeted the restoration efforts though the usage of the KillDisk attack.

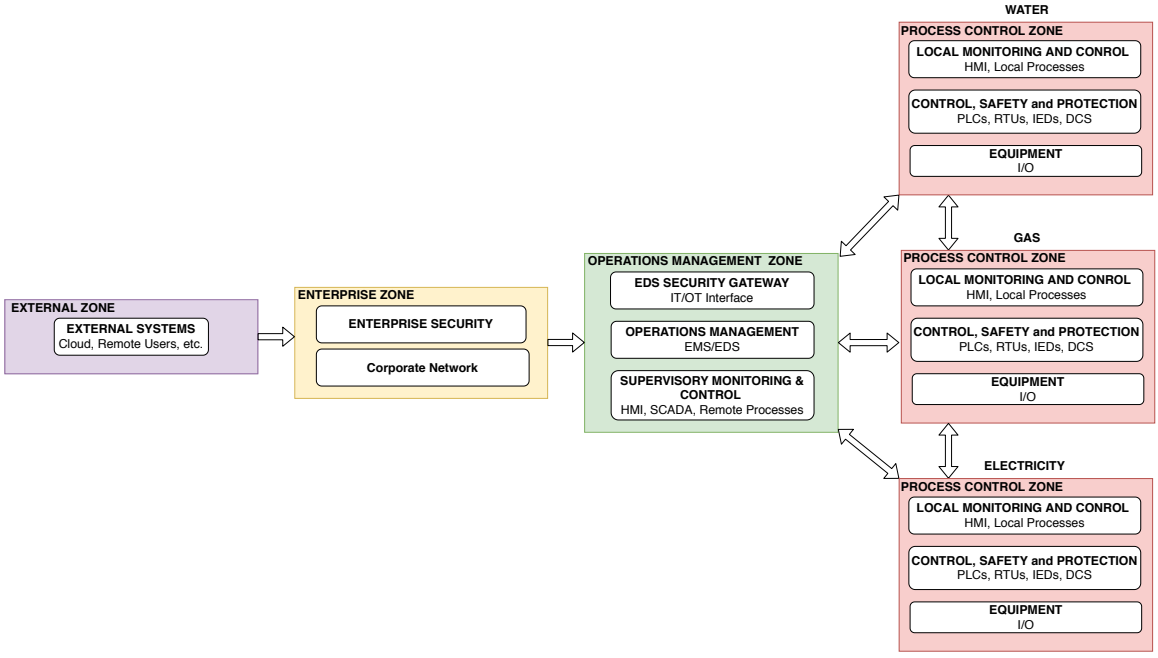


Figure 1: Multi-Vector CPS Energy System

The impact of the attack was tremendous as it caused a blackout for six-hours for over 250.000 citizens [17], [24].

One year later, a second attack targeted the power grid of Ukraine which caused a blackout for one hour in a fifth of Kiev [13].

The attackers used a malware called Industroyer, capable of controlling substation switches and circuit breakers via standardized industrial communication protocols. Later, research indicated, that the intent of the attackers might have been to cause physical damage to the power transmission systems at the time of recovery, not just shut it down for an hour [4], [8], [13].

The U.S.A. energy generation provider, sPower, was hit by a DoS attack in 2019. The attack disrupted the communication between the control center of the company and the field devices. The disruption was not continuous but was happening every five minutes while lasting for twelve hours [5], [28].

Energy companies have also been suffering attacks against their billing and automated meter reading (AMR) systems. In 2018, the AMR system of Uttar Haryana Bijli Vitran Nigam (UHBVN) has been hacked and their billing data encrypted with ransomware. The hackers demanded $153,800 in Bitcoin from government of Haryana for decryption of the files and restoring access to the system [1]. There is at least one open-source tool called Termineter available for communicating to the smart-meters via their optical interface [23].

There are reports of attacks against oil production companies in Saudi Arabia. In 2012, Armaco, was hit by the disk-wiping malware Shamoon, also known as W32.Distrack. Tens of thousands of computers were infected, displaying a burning U.S. flag [20]. The hackers were believed to be working for the Iranian government [2]. In 2017, a rare and dangerous type of malware dubbed Triton was spotted in Middle East. It was targeting safety systems commonly used by oil companies [7]. No damage were reported, but the idea of crippling safety systems of an industrial process without hindering the process itself is extremely dangerous, as it can remain unnoticed for a long period of time. [26].

The referred attacks against electricity and oil production are mostly denial of critical services. Although disruption of such services can have a vast effect on the economy, not only for the energy companies, but also to all the affected consumers, the implications of cutting off supplies can be lowered by implementing redundancy or backup. In March 2016, Verizon reported attacks against an undisclosed water treatment plant, identified by the fake moniker "Kemuri Water Company" (KWC). The report described how hackers initially targeted public-facing web server of KWC, that were running on an outdated platform, with the intent of stealing customer data. The hackers later pivoted through the systems that were interconnected, eventually gaining access to PLCs that managed the amount of chemicals used to treat the water in order to make it drinkable, as well as the water flow rate. It was considered likely, that the attackers didn't realize their opportunity to poison the tap water [27].

5 DEVELOPING FUTURE CYBER-PHYSICAL ENERGY SYSTEMS

In most of the cyber-physical studies the effect of a cyber-attack on the physical domain is represented as a faulty

operation. This can only provide information on the severity of the attack, without exposing the propagation of the attack [31]. Therefore, future studies may need to observe the interaction between the cyber and physical domains in order to identify, detect or even prevent attacks.

Future operators need to consider cyber-security into the energy system design. This may be achieved by increasing the redundancies on three different aspects; protection, hardware, and control. Also, as some business models allow only separate contracts among services it may be crucial to provide independent investigation on forensics post analysis whether the equipment failures are due to faults, mismanagement or cyber-attacks.

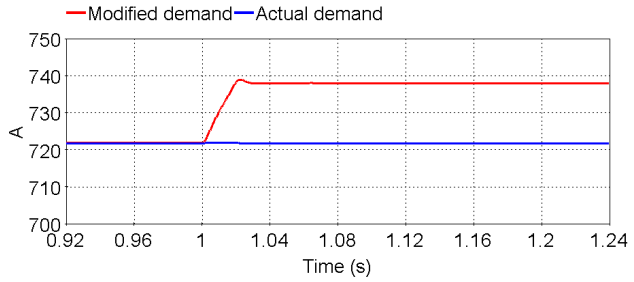
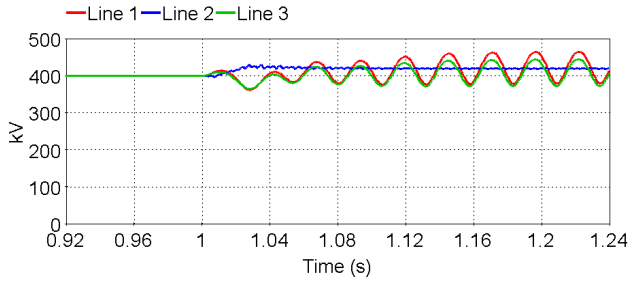
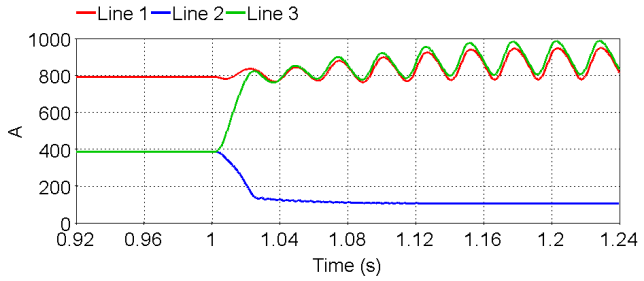


Figure 2: Simulations waveforms of an HVDC transmission system, when a cyber-attack modifies the measurements by 2%



(a) Line voltages



(b) Line currents

Figure 3: Simulations waveforms of a three sources transmission system when a cyber-attack enables one of the protection relays during normal operation.

Energy system operators are reluctant on modifying the protection system, as it may jeopardise the discrimination and the sensitivity performance as any change of the proprietary settings may jeopardise the system's stability. Moreover, the widely-used industrial communication standards don't have security features built into their original versions [12]. Upgrading can be costly and complicated, as special-purpose devices have limited computing power that can't handle e.g. modern cryptography, they might also lack options for upgrading their firmware. Increasing the redundancies on the hardware equipment, such as energy paths, energy hubs etc, is a straightforward solution. However, the extra cost of investment may not be justified by the risk. The most inexpensive adjustment is that of adopting new control methods which react upon a cyber-attack detection [25]. Also, implementing reactive controllers may reduce the cost of the aforementioned equipment redundancies. However these controls will highly depend on the speed and discrimination of cyber-attack detections.

Therefore, operators may need to implement cyber-attack detection algorithms which allow their equipment, control and protection to act accordingly. These algorithms may detect the cyber-attacks through proxies (e.g. measurements of voltage, pressures etc) to identify an abnormal operation. This may appear to be challenging for cyber-attacks that targeting fast transient events e.g. opening a protection relay. Nonetheless, for long-term events this may be a viable solution for saving equipment's lifespan, reduce the maintenance costs and avoid costly investment on redundant equipment. FigureA2 shows the possible effect of a long term undetected cyber-attack, where a negligible change on the measurements may affect the lifespan of the equipment by increasing the current stresses. In addition as the current increases, the thermal losses increase proportionally, hence additional operational costs are billed to the operator [30]. Figure 3 shows a fast transient event, when a cyber-attack disables a protection relay. The system may consider this operation as a fault, activating the protection systems. This kind of event may jeopardise the stability of the energy systems and equipment may be damaged, with likelihood of blackout.

6 TRAINING NEED

The high level of accessibility and integration of different power systems, the advent of distributed energy resources, smart metering and ICT-based grid observability has raised new challenges for the power sector. The power systems are being digitised and face advanced cyber-security threats regularly. Cyber-risks can emerge out of a great variety of operations, focused on the technical functionalities of EDS, data breach of market participants and customers, or a combination of both, that could initiate adverse security threats. Cyber security in multi-vector energy distribution environment requires skilled personnel and well-prepared administrators to take proactive choices of teaming up with partners to train at the cutting-edge. Employees will have to keep their skills up to date with the new security solutions for Smart

Grids as well as understand the impact of cyber-attacks and fault on multiple systems.

Their theoretical background must be enriched and supported through hands-on training exercises. Realistic training enhances the preparedness of personnel at all hierarchical levels either horizontally or vertically depending on the role of the personnel. Such roles may include, but are not limited to administrative or technical cyber-security professionals at all levels. The need for cybersecurity expertise has increased in an exponential manner, a fact that increases the importance of educating personnel. Highly skilled operators are needed by the industry as the number of cyber-threats and ingenuity of attackers grows. To be able to meet the increasing requirements, the synergies of education must be considered along with professional training and certification programs to establish the basics of cyber-security. This can be addressed by new teaching and knowledge transfer methods that rely on technical exercises.

The attacks described in section 4.2 express certain common properties. In the modern era, malware do not spread on their own, like classical computer viruses used to. Instead, they are delivered within a compromised software (update) package, phishing e-mails, malicious links, USB flash drives, or other means that involve social engineering or require human interactions. This means, that attackers often gain initial footprint in the target network with the help of an unaware employee. Another common pattern is that it is easy for attackers to pivot through the internal network of the victim from publicly accessible systems, like homepage or self-service portal, to most critical parts of the infrastructure, that are controlling the production processes. These attacks indicate a lack of network segregation and other security measures. Emerging trends of implementing multi-vector EDS greatly enhance the risk, allowing attackers to pivot not only within a single company or domain, but move laterally to other dimensions of EDS. This raises the need for new type of awareness training - e.g. how an operator can prevent its equipment and facilities from being used as a proxy to attack other parts of EDS. The topics include learning to identify patterns that could be used to attack someone else's systems, monitoring and blocking outgoing traffic. These types of attacks are often overlooked in training.

Energy distribution systems are often made up of very different devices, that can vary even within a single company or small geographic area [18]. The roots of European power grids are in the 19th century. Most power stations and substations are decades old and contain legacy hardware and software. Substations built in 1970-s initially had manual control, or simple automation based on mechanical relays with electrical control. When the relays reached end of life, or broke down, they were replaced with more modern ones. Better-lasting items could have some add-ons installed to allow connecting them to computer-driven control systems. Such replacements and upgrades don't take place all at once due to high cost, but on a necessity basis. This leads to a situation where substations can contain equipment from different eras and different manufacturers increasing the the training need of multi-vector energy distribution operators.

These heterogeneous systems composed of legacy devices create extra challenges on developing protections. Different devices have different features and glitches, leading to compatibility issues and limitations. Every firmware has its own set of bugs, creating a wide attack footprint - if an attack doesn't succeed on one device, it can be tried on another. The training methodologies and content should take this into account. Training should have options that raise general awareness of cyber-attacks, how to identify them and react upon incidents. Such type of training would help in developing effective cyber-attack detection algorithms and systems. There should also be hands-on training options for personnel, who work daily with the energy distribution equipment and supporting infrastructure. This is challenging, as the devices from different manufacturers or different eras don't share the same user-interfaces and may have different functionality. Conducting training in an over-simplified lab will take the trainees too far from their usual working environment and they might lose focus, as operating a unfamiliar device requires too much attention and the obtained knowledge cannot be easily transferred back to everyday job. It is therefore essential to simulate and emulate environments that are as close as the real ones.

7 ENERGY SPECIFIC EU POLICY

Cyber-security in the energy sector has become of utmost importance in European Commission (EC). In that way, EC has promoted key strategic documents outlining the EU policies in the domain of energy:

- *European Energy Security Strategy*: it has been laid down by the EC in May 2014. This document identifies the status quo and points out the immediate and long term actions to ensure the energy security in the EU [21].
- *Energy Union Package*: its aim is to propose specific measures mainly focusing on the secure and sustainable energy for the Europe. The document focuses on providing an integrated and unified strategy for the security of supplies, the sustainability of energy as well as for the competitiveness of the sector [22].
- *European Programme for Critical Infrastructure Protection*: The Council of the European Union established a procedure for the identification and designation of European Critical Infrastructures (ECI). The policy aims at improving the protection of ECI. In the adopted Directive three energy critical sub-sectors were identified, namely; electricity, oil and gas [19].

8 CONCLUSION

In this paper we highlighted the need for critical EDS operators to understand the attack-vectors and threats faced by multi-vector energy systems to improve their response time, as well as providing them with the ability to differentiate between faults and cyber-attacks. We also provided an

overview of cyber-attacks faced by EDS and highlighted the need for the integration of security and privacy at the core of the development of future cyber-physicial systems. The future work will concentrate on the development of a training methodology aimed at multi-vector energy distribution system operators.

9 ACKNOWLEDGEMENTS

This paper has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 833673. The work reflects only the authors' view and the Agency is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] Uzair Amir. 2018. Hackers take over power billing records of Indian state; demand ransom. https://www.hackread.com/hackers-demand-ransom-indian-power-billing-records/. Accessed: July 1, 2020.

[2] Al Arabiya. 2017. What is the Shamoon virus that has returned to hack Saudi networks? https://english.alarabiya.net/en/media/digital/2017/01/24/What-is-the-Shamoon-virus-that-has-returned-to-hack-Saudi-networks-.html. Accessed: July 1, 2020.

[3] Xavier Bellekens, Amar Seeam, Kamila Nieradzinska, Christos Tachtatzis, Alison Cleary, Robert Atkinson, and Ivan Andonovic. [n. d.]. Cyber-physical-security model for safety-critical iot infrastructures.

[4] Anton Cherepanov and Robert Lipovsky. 2017. Industroyer: Biggest threat to industrial control systems since Stuxnet. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/. Accessed: July 1, 2020.

[5] Catalin Cimpanu. 2019. Cyber-attack hits Utah wind and solar energy provider. https://www.zdnet.com/article/cyber-attack-hits-utah-wind-and-solar-energy-provider/. Accessed: July 1, 2020.

[6] ENISA. 2019. ENISA Threat Landscape Report 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018. Accessed: July 3, 2020.

[7] Andy Greenberg. 2017. Unprecedented Malware Targets Industrial Safety Systems in the Middle East. https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/. Accessed: July 3, 2020.

[8] Andy Greenberg. 2019. New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/. Accessed: July 3, 2020.

[9] Hanan Hindy, Ethan Bayne, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, and Xavier Bellekens. 2020. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study. *arXiv preprint arXiv:2006.15340* (2020).

[10] H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens. 2020. A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. *IEEE Access* 8 (2020), 104650–104675.

[11] Hanan Hindy, Christos Tachtatzis, Robert Atkinson, David Brosset, Miroslav Bures, Ivan Andonovic, Craig Michie, and Xavier Bellekens. 2020. Leveraging Siamese Networks for One-Shot Intrusion Detection Model. *arXiv preprint arXiv:2006.15343* (2020).

[12] Junho Hong. 2014. *Cyber Security of Substation Automation Systems.* Ph.D. Dissertation. Washington State University. Accessed: July 4, 2020.

[13] N. Kshetri and J. Voas. 2017. Hacking Power Grids: A Current Problem. *Computer* 50, 12 (2017), 91–95.

[14] AO Kaspersky Lab. 2020. BlackEnergy APT Attacks in Ukraine. https://www.kaspersky.com/resource-center/threats/blackenergy. Accessed: July 1, 2020.

[15] Harjinder Singh Lallie, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2020. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *arXiv preprint arXiv:2006.11929* (2020).

[16] R. Langner. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy* 9, 3 (2011), 49–51.

[17] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong. 2017. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Transactions on Power Systems* 32, 4 (2017), 3317–3318.

[18] K Nieradzinska, C MacIver, S Gill, GA Agnew, O Anaya-Lara, and KRW Bell. 2016. Optioneering analysis for connecting Dogger Bank offshore wind farms to the GB electricity network. *Renewable Energy* 91 (2016), 120–129.

[19] Council of the European Union. 2008. European Programme for Critical Infrastructure Protection. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN. Accessed: July 4, 2020.

[20] Charlie Osborne. 2012. Kaspersky: Shamoon malware nothing more than 'quick and dirty'. https://www.zdnet.com/article/kaspersky-shamoon-malware-nothing-more-than-quick-and-dirty/. Accessed: July 1, 2020.

[21] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT and THE COUNCIL. 2014. European Energy Security Strategy. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52014DC0330. Accessed: July 4, 2020.

[22] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT and THE COUNCIL. 2015. Energy Union Package. https://ec.europa.eu/energy/publications/energy-union-package_en. Accessed: July 4, 2020.

[23] Emil Protalinski. 2012. Smart meter hacking tool released. https://www.zdnet.com/article/smart-meter-hacking-tool-released/. Accessed: July 1, 2020.

[24] Tereza Pultarova. 2016. News Briefing: Cyber security-Ukraine grid hack is wake-up call for network operators. *Engineering & Technology* 11, 1 (2016), 12–13.

[25] P. Rault, O. Despouys, A. Petit, H. Saad, D. Vozikis, S. Gao, J. Freytes, M. Narayanan, M. Ramet, M. Zeller, and P. Askvid. 2019. Implementation of a dedicated control to limit adverse interaction in multi-vendor HVDC systems. In *15th IET International Conference on AC and DC Power Transmission (ACDC 2019)*. 1–6.

[26] Nayla Razzouk and Javier Blas. 2019. Saudi Oil Output Cut in Half After Drones Strike Aramco Site. https://www.bloomberg.com/news/articles/2019-09-14/saudi-aramco-contain-fires-at-facilities-attacked-by-drones. Accessed: July 1, 2020.

[27] Mary-Ann Russon. 2016. Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned. https://www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility/-company-was-using-1988-server-1551266. Accessed: July 1, 2020.

[28] sPower. 2019. Electric Emergency Incident and Disturbance Report. https://www.eenews.net/assets/2019/10/31/document_ew_03.pdf. Accessed: July 4, 2020.

[29] Adam Vincent. 2018. BlackEnergy Malware: How Hackers May Tackle our Infrastructure. https://www.infosecurity-magazine.com/opinions/blackenergy-malware-infrastructure/. Accessed: July 1, 2020.

[30] D Vozikis, GP Adam, P Rault, D Tzelepis, D Holliday, and S Finney. 2018. Steady-state performance of state-of-the-art modular multilevel and alternate arm converters with DC fault-blocking capability. *International Journal of Electrical Power & Energy Systems* 99 (2018), 618–629.

[31] D. Vozikis, P. Rault, D. Holliday, and S. Finney. 2019. Fault blocking converters for HVDC transmission: a transient behaviour comparison. *The Journal of Engineering* 2019, 17 (2019), 3825–3830.