Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results

Author(s): Berg, Petra; Berlijn, Sonja Monica; Eltahawy, Bahaa; Hilber, Patrik; Karimi, Mazaher; Klepper, Karina Barnholt; Turtola, Linda; Ulshagen, Andrea; Xu, Qianwen

Title: Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results

Year: 2024

Version: Accepted manuscript

Please cite the original version:

Berg, P., Berlijn, S. M., Eltahawy, B., Hilber, P., Karimi, M., Klepper, K. B., Turtola, L., Ulshagen, A., & Xu, Q. (2024). Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results. In *2024 International Workshop on Artificial Intelligence and Machine Learning for Energy Transformation (AIE)*, 1-6. IEEE. https://doi.org/10.1109/AIE61866.2024.10561312

Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid – Review and Workshop Results

Petra Berg
School of Marketing and Communication and VEBIC
University of Vaasa
Vaasa, Finland
petra.berg@uwasa.fi

Sonja Monica Berlijn
Electrical Power Engineering
KTH Royal Institute of Technology
Stockholm, Sweden
berlijn@kth.se

Bahaa Eltahawy
Digital Economy Research Platform
University of Vaasa
Vaasa, Finland
bahaa.eltahawy@uwasa.fi

Patrik Hilber
Electromagnetic engineering and fusion science
KTH Royal Institute of Technology
Stockholm, Sweden
hilber@kth.se

Mazaher Karimi
School of Technology and Innovations
University of Vaasa
Vaasa, Finland
mazaher.karimi@uwasa.fi

Karina Barnholt Klepper
The Norwegian Defence Research Establishment (FFI)
Kjeller, Norway
karina-barnholt.klepper@ffi.no

Linda Turtola
Industrial management
University of Vaasa
Vaasa, Finland
linda.turtola@uwasa.fi

Andrea Ulshagen
The Norwegian Defence Research Establishment (FFI)
Kjeller, Norway
Andrea.ulshagen@ffi.no

Qianwen Xu
Electrical Power Engineering
KTH Royal Institute of Technology
Stockholm, Sweden
qianwenx@kth.se

***Abstract*— The energy system, including the electrical power system, is currently undergoing major changes to meet increased demands and climate target plans, and to stand against potential malicious activities and all sorts of disruptions. Specifically, the electrical power system is drastically changing with regards to consumption, production, transmission, control, monitoring, markets, and digitalization. Such a change, however, makes the power system an attractive and vulnerable target to all kinds of disruptive events and social-cyber-physical attacks since the system is crucial for the functioning of the society and economy. In this work, to act against such events and to study the future power system's susceptibility and resilience towards social-cyber-physical attacks, the Resilient Digital Sustainable Energy Transition (REDISET) project has shown the need for a new model that is able to describe the future electrical power system in a way that reflects the future reality. In this paper, existing power system models, the changing landscape of power systems, the drivers for a new model, the suggested model that comprises 7 building blocks instead of today's 3, and finally a direction of future related work are presented.**

Keywords—Power Grid, Resilience, Social-cyber-physical Threats.

I. Introduction and Background

With the current unprecedented global changes, the energy system, including its subdomains, such as the electrical system, is undergoing a substantial transition into a fully digitalized, cyber-physical system. These changes are driven by the increased demands and shifts in the market, the need to meet climate target plans, achieve sustainable development goals, and enhance resilience against potential malicious activities and other disruptive events. Specifically, due to digitalization, the electrical system is currently witnessing changes in monitoring, protection, and control systems across generation, transmission, and distribution plants. While these changes bring about new opportunities, products, added services, expanded markets, and an improved user experience, they also increase the complexity and vulnerability of the power system. This accordingly renders the power system susceptible to various disruptive events, ranging from minor malfunctions to large-scale cyber-physical attacks, resulting in significant social and economic impacts. Existing smart energy models, e.g., National Institute of Standards and Technology (NIST) [1] and Smart Grid Architecture Model (SGAM) [2], could provide guidance on the structure of the power system's components and interaction in a hierarchical manner. However, they lack a thorough consideration of the "human risk" factor, as in organizational cybersecurity-culture [3] and policy implications [4]. Recent attempts, e.g., [5] and [6], have partially addressed this gap by introducing integrated and interdisciplinary gird models, considering different domains, levels, and interactions, holistically, rather than separately, as previously done. This work acknowledges these efforts, and as a part of the Resilient Digital Sustainable Energy Transition (REDISET) project – which is a research project combining academic institutions and energy providers in Finland, Sweden, and Norway – it continues in the same direction.

In this work, we thoroughly examine the power grid system from the threats angle to answer the following question: *"How to assess the effects of social-cyber-physical threats on the future power grid?"*. The aim of this multidisciplinary research is to counter social-cyber-physical threats affecting the grid, adding the third, 'social' layer that represents the integration of cyber-physical systems with social networks such as smart technologies and Internet of Things (IoT) [7] . Also, we aim to assess the future power system's susceptibility and resilience against such vulnerabilities. Here, we use the term resilience to describe the ability of the system to withstand and recover from different threats [8].

The remainder of this paper is organized as follows: Section II describes the research approach. Section III highlights existing models of power systems, workshop results, and the changing landscape. Section IV follows with our proposed model for assessing the effects of social-cyber-

physical threats on the future power grid, are presented. Section V concludes and suggests future work directions.

II. Research Methods

To comprehensively address our research question from both the conceptual and practical sides, two research approaches were employed in this research. First, a rapid review method [9] was used to gather information on existing energy models. Second, qualitative research in the form of workshops [10] was conducted, to discuss these models, the challenges they face, and gain insights and suggestions on filling the identified gaps. For the latter, two workshops were held, involving multidisciplinary experts from academia and industry, focusing on exploring power models and their social aspects. Figure 1 shows a schematic diagram of the research methodology employed. Table 1 presents a description of workshops and participants.

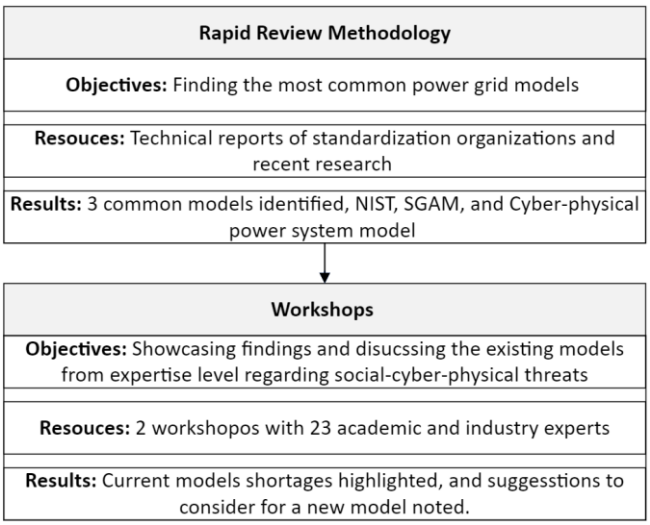

Figure 1. Research method

TABLE I. Workshops Descriptions

Attribute	Description
Dates	October 27th, 2022, and February 17th, 2023
Location	KTH, Royal Institute of Technology, Stockholm, Sweden
Countries involved	Sweden, Finland, and Norway
Research institutions involved	4: KTH from Sweden, University of Vaasa from Finland, and FFI and NTNU from Norway
Companies involved	7: Ellevio, Svenska Kraftnät, Vattenfall, Statnett, Fingried, Hitachi Energy, and Sintef
Total number of participants, present or online	23
Academic participants	14
Industrial participants	9

In the following section, the most common energy models from selected articles as well as workshop results on these models and the evolving landscape, are presented.

III. Review and Workshops Results

A. Review summary on existing power system models

Initially, although there are various power system models that describe power systems from different perspectives, this review has identified three common models as being particularly noteworthy: the ISO/IEC Smart Grid Architecture Model (SGAM), the NIST framework, and the Cyber-physical power system model. These are outlined as follows:

1) SGAM Model

The ISO/IEC SGAM [2], as shown in Figure 2, is a hierarchical layered representation of smart grids, consisting of five interactive layers that represent different domains and their associated objectives. The model encompasses the business, function, information, communication, and component layers, in which the latest encompasses the domains of the energy sector, i.e., generation, transmission, distribution, Distributed Energy Resources (DER), and customer premises. Furthermore, the component layer is also divided into different zones, i.e., process, field, station, operation, enterprise, and market, depending on the function to be performed. With such a structure and flexibility, the SGAM model is well-suited to showcase, simulate, and implement various use cases and scenarios covering different aspects of smart grids [11].

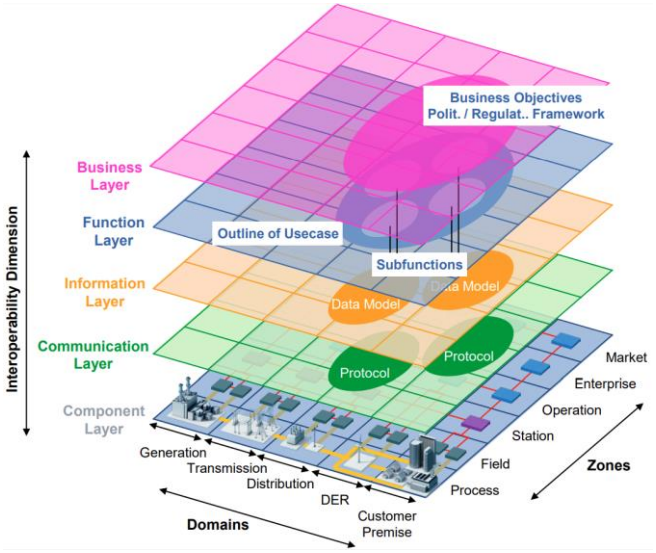

Figure 2. SGAM model (adopted from [2])

2) Smart Grid Conceptual Model

NIST's framework, the Smart Grid Conceptual Model (SGCM) [1], is a high-level framework that illustrates the roles and responsibilities, as well as the interactions between the different domains within the power grid. The model, as shown in Figure 3, encompasses the operations, service provider, customer, generation, transmission, markets, and distribution planes, delineating the lines needed for information exchange from the direct energy exchange ones, forming the actual grid. With its distinct detailed roles, SGCM acts as a guideline for understanding the grid by different stakeholders and is used for developing standards that ensure interoperability and seamless communication among the grid's components, thus enhancing the efficiency, reliability, sustainability, and resilience of the power system.

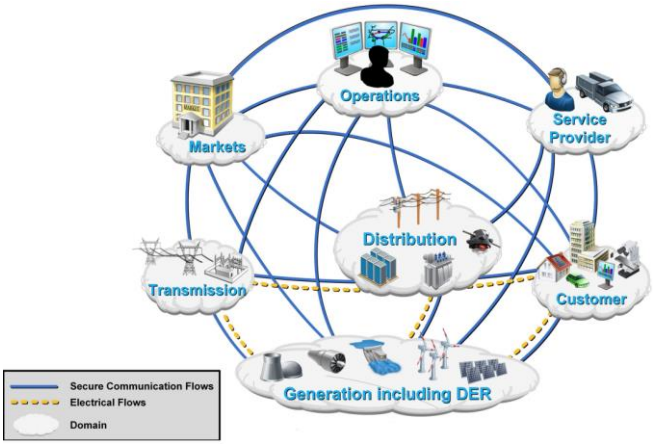

Figure 3. NIST's SGCM model (adopted from [1])

3) Cyber-Physical Power Model

In the Cyber-Physical Power Model [12], power systems are modelled as cyber-physical systems, combining a physical power system, a control center (cyber layer), and communication between the two. As shown in Figure 4, the model's physical power system comprises a generation system including various DER, a transmission and distribution system, and customers. The cyber system, i.e. the control center, performs monitoring, operation, optimization, and control functions. Finally, the communication network handles sensors' measurements and control commands between the two systems. With its structure, the model effectively separates the actual grid and explicitly adds a cyber layer, where all information flow and control functions are executed.

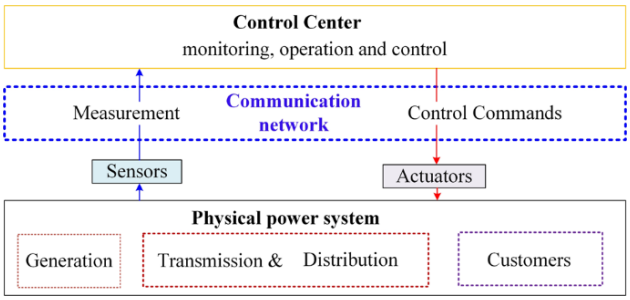

Figure 4. Cyber-physical power model (adopted from [12])

B. Applicability and deficiencies of the existing models – Workshop results

Although the given models provide comprehensive views on modeling the grid, they also exhibit several deficiencies. First, SGAM model suffers from complexity and lacks flexibility due to its segmented layered approach. Furthermore, issues [2] highlighted in the literature include formal functional description, the need for a well-defined interfacing tool for the architectural structure, and difficulties with automatic testing and configurations. Second, SGCM model faces similar complexity, flexibility, and interoperability limitations. In addition [13], the model faces concerns related to confidentiality, privacy, and compliance with anti-trust laws; hindrance in deployment due to being voluntary in the private sector; and human error, including user awareness in the customer domain and user errors in the operations domain. Finally, the cyber-physical power model's control center is oversimplified, considering that many Transmission System Operators (TSOs), Distribution System Operators (DSOs), producers, and larger consumers, have multiple control and monitoring centers, infrastructure monitoring centers, dispatch centers, and cyber surveillance centers, alongside switch centers. Moreover, the model lacks clarity addressing the market system.

Other notes that were emphasized during the workshops include: 1) The existing models are highly technical and lack on addressing the human factor adequately; 2) Building on the preceding point, the models neglect behavioral aspects such as social-cultural matters and their impact on the energy sector; 3) There is a lack of emphasis on privacy and cybersecurity issues; 4) Additionally, they fail to incorporate emerging technologies, e.g., Artificial Intelligence (AI) and blockchain.

C. Changing landscape

The abovementioned concerns, along with ongoing changes in the energy system, make it vulnerable and more susceptible to cyber and physical attacks. As modern society is more reliant on electricity, hostile actors can exploit weaknesses such as outages and instabilities to pose threats to our communities. Grid operators, i.e. TSOs and DSOs, have already witnessed a significant increase in cyberattacks. Additionally, the interdependencies within the current energy system can be exploited in international conflicts and hybrid warfare, as seen in Russian cyberattacks in 2015 [14], [15] and attacks on Ukrainian power infrastructure since February 2022 [16], to cause major disruptions and blackouts. These conflicts have led to what is called the "energy war", where energy resources are manipulated for political purposes. Alongside cyber threats, issues like the maintenance of nuclear reactors in France and the decommissioning of German nuclear power plants, shed light on the interdependencies within the European energy system, highlighting the risk of energy shortages and poverty. Given the vital role of energy supply and delivery in modern society, they have become a target for adversaries. Thus, ensuring the security and resilience of the energy infrastructure is crucial for the functioning of our society.

IV. Proposed Model for Future Power System

A. Social-Cyber-Physical grid model

Based on the reviews conducted and the workshop results, a system-of-systems energy model that explicitly emphasizes social-cultural aspects and disruptions, is proposed. The model, as shown in Figure 5, encompasses seven system domains, as follows: 1) supply system; 2) demand system; 3) transmission/distribution infrastructure system; 4) market system; 5) control system; 6) disruption system; 7) and, the social-cultural system. As the name indicates, every system of the proposed model encompasses its own sub-systems, which might vary depending on many factors and the types of DERs used, for example. Here and for simplicity, we present the proposed model from an abstract high-level view.

1) Supply System

The main purpose of the supply system is to generate and supply electricity and create revenue for investors and producers of electricity. Key functions of the supply system are:

- Generating electricity from different resources through energy conversion processes.
- Providing inertia, frequency reserves, and ancillary services to support grid stability.

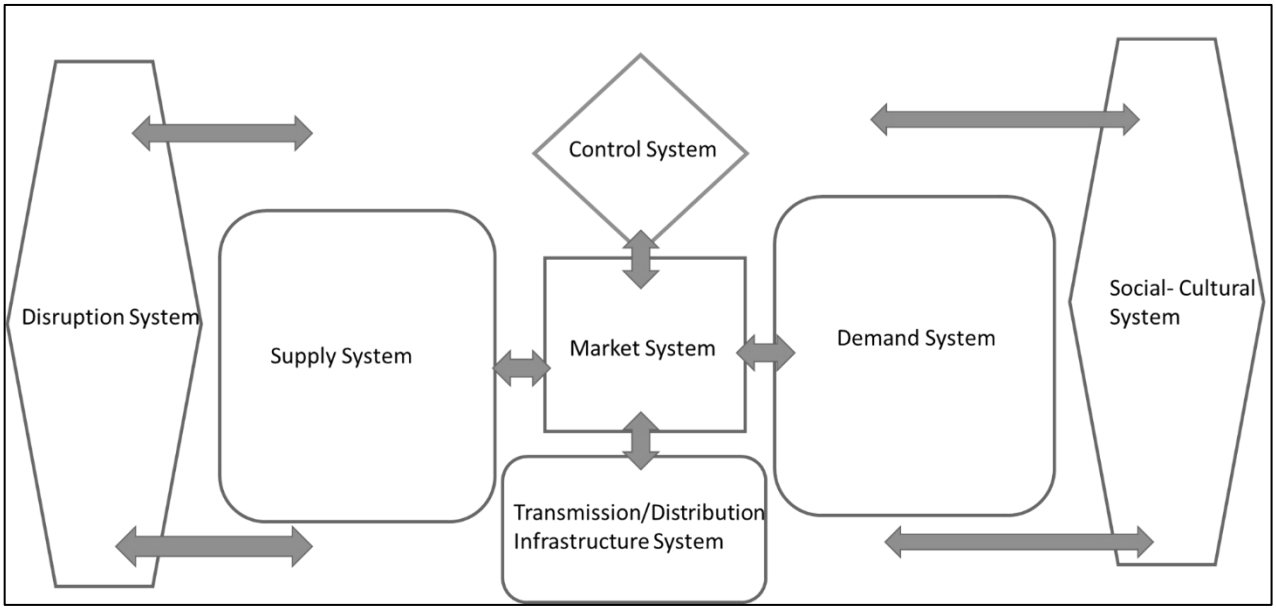

Figure 5. Proposed Social-Cyber-Physical Grid Mode, Version 1.0

- Connecting different electricity resources to the grid
- Generating financial returns for investors and stakeholders.
- Securing energy demands.
- Monitoring and controlling voltage and frequency conditions to maintain grid reliability.

2) Demand System

The main task of the demand system is to use electricity, compensate for services delivered, and to transmit data to the system for further analysis. Key functions of the demand system are:

- Utilizing the supplied energy for purposes, such as generating motion or alternative types of energy.
- Implementing own monitoring and control.
- Generating value or fulfilling functions for the consumer.
  - Heating
  - Industrial processes
  - Data storage
  - Transportation
- Responding to price signals through demand-response mechanisms.

3) Transmission / Distribution Infrastructure System

The primary objective of the grid system is to facilitate the transportation of electricity and information, while measuring parameters necessary for optimizing grid capacity utilization. Key functions of the transmission/distribution infrastructure system are:

- Transmitting electricity across various points of the grid.
- Facilitating the transmission of data necessary for grid operations.
- Incorporating demand and supply domains, thus forming the operational grid network.
- Performing data measurement tasks to monitor grid performance.
- Implementing control and protection measures to safeguard infrastructure equipment.

4) Market System

The primary objective of a well-functioning market system is to promote a secure supply of energy produced sustainably and at affordable prices. Key functions of the market system are:

- Integration of markets.
- Supporting decarbonization initiatives.
- Continuous intraday trading (market).
- Performing balancing actions (balancing market, end-user market).
- Enabling flexibility through aggregators.
- Collecting data on grid capacity.
- Gathering market data (demand, supply, capacity).
- Providing market data services as needed.
- Maintaining trading platforms for both intraday and day-ahead markets.
- Facilitating price settlements.
- Achieving balance between supply and demand.

5) Control System

The primary function of the control system is to maintain a balance between electricity demand and supply in accordance with market dynamics, ensuring the quality of supply, and communicating signals to the market regarding grid capacity. Key functions of the control system are:

- Maintaining a stable 50 Hz frequency.
- Regulating voltage levels.
- Controlling power generation for stable operation
- Ensuring grid stability and security
- Monitoring key parameters, such as frequency, voltage, power, and overall system stability.
- Responding to disruptions and anomalies.
- Collecting data for investigation and analysis purposes.

6) Disruption System

The main task of the disruption system is to create disturbances that disrupt the smooth functioning of the energy system. In response, the energy system needs to demonstrate resilience to withstand such disruptions, employing strategies

like n-1 redundancy, manual operation, island operation, etc. Key functions of the disruption system are:

- Weather events and climate change impacts
- Cyberattacks targeting the system or its components.
- Equipment malfunctioning.
- Social disruptions affecting operations [17].
- Natural disasters causing system disturbances.
- Political conflicts or wars affecting energy infrastructure.
- Market interruptions affecting energy supply.
- Frequency fluctuations impacting system stability.
- Disrupting the balance between functionality, security, and economic considerations.

7) Social-Cultural System

The main purpose of the social-cultural system is to establish a stable framework for the energy system, integrating social, economic, and environmental aspects. It recognizes individual's integration into broader social structures shaped by collective beliefs and agreements [18]. This system interacts closely with socio-technical institutions, reflecting the culture of a society [19]. It examines drivers of energy behavior [20] and vulnerabilities, including cyber ones. Key functions of the social-cultural system are:

- Governance, including policy and legal frameworks.
- Influencing security interests and decisions.
- Shaping the business climate and culture.
- Driving economic and financial considerations.
- Influencing energy consumption behaviors.
- Influencing production behaviors, including prosumer activities.
- Providing relevant services.
- Adapting and shaping the global landscape in response to international structures and dynamics.

B. Feedback on the model

As part of REDISET project Work-Package 3 development, the proposed model was presented during two project workshops held in Vaasa, Finland, in June and September 2023. The model generated positive feedback from both industrial and academic experts, although some points were raised. Below are the main concerns and responses to them.

- Issue 1: Control system is positioned solely above the market system.
  Response: In this model, which represents a system-of-systems, each system possesses its own control mechanism. Therefore, in this proposed model, the control system serves as the most centralized control system.
- Issue 2: Arrows only connect certain domains.
  Response: Since every domain is interconnected with other domains, the connections can occur directly or indirectly. The current model shows only direct connections for simplicity, with future iterations emphasizing interconnectedness.
- Issue 3: Arrows from the social-cultural and disruption systems are directed solely towards the control and transmission - distribution infrastructure systems.
  Response: The arrows of the social-cultural and disruption systems are inclusive, indicating their influence extends these systems.

V. CONCLUSIONS AND FURTHER WORK

This paper critically evaluates the most prominent existing power systems in light of the changing landscape, emphasizing the need for developing a model capable of meeting future grid demands. It is clear that existing models lack consideration of the human and social-cultural factors, which are critical for the future grid. Moreover, they also fail to address some of the most recent critical issues, such as security and privacy. Accordingly, the paper presents a model that provides a comprehensive framework for mapping the interdependencies among various infrastructure environments within the Nordic power system. By considering the disruption system, supply system, market system, control system, transmission/distribution infrastructure system, demand system, and social-cultural system, the proposed model enables a holistic understanding of the system-of-systems perspective.

Moving forward, our future research will delve deeper into exploring both intra- and inter-dependencies within and between these infrastructure environments. This analysis will provide valuable insights into the vulnerabilities present in the power system. We will specifically focus on simulating and studying the potential cascading consequences of failures in critical components at both the component and the executive levels. By conducting such analysis, we aim to enhance our understanding of the system's overall resilience. To facilitate further development, we recognize the importance of providing more detailed descriptions and discussions of the individual sub-systems within the power system. This additional level of refinement and development will allow for a more comprehensive exploration of the system's intricacies. The model approach outlined in this paper provides a solid foundation for investigating the dependencies and vulnerabilities within the Nordic power system. Through future research, we aspire to advance our understanding of the system's behavior and contribute to the development of strategies for ensuring its robustness and reliability.

ACKNOWLEDGMENT

The authors would like to acknowledge the following financers: Nordic Energy Research, Business Finland, The Swedish Energy Agency, The Norwegian SmartGrid Centre, Statnett, Svenska Kraftnät, Fingrid. The authors would like to acknowledge the following project participants and technical and scientific reference group: Elevio, Hitachi, Vattenfall, Statkraft, F-secure, Wärtsila, Traficom, ABB and Recorded Future.

REFERENCES

[1] Gopstein, Avi, et al. NIST framework and roadmap for smart grid interoperability standards, release 4.0. Gaithersburg, MD, USA: Department of Commerce. National Institute of Standards and Technology, 2021.

[2] Uslar, Mathias, et al. "Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A European perspective." Energies 12.2 (2019): 258.

[3] Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. Computers & Security, 129, 103199.

[4] Krkoleva Mateska A, Krstevski P, Borozan S. (2021) Overview and Improvement of Procedures and Practices of Electricity Transmission System Operators in South East Europe to Mitigate Cybersecurity Threats. Systems. 9(2):39. https://doi.org/10.3390/systems9020039

[5] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

[6] Sun C., Hahn A., Liu, C. (2018) Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems. Vol. 99. p.45-56, ISSN 0142-0615. https://doi.org/10.1016/j.ijepes.2017.12.020.

[7] Yevseiev, Serhii, et al. "Development of a Sociocyberphysical Systems Cyber Threats Classifier." 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). IEEE, 2023.

[8] Jasiūnas, Justinas, Peter D. Lund, and Jani Mikkola. "Energy system resilience–A review." Renewable and Sustainable Energy Reviews 150 (2021): 111476.

[9] Hamel, Candyce, et al. "Defining rapid reviews: a systematic scoping review and thematic analysis of definitions and defining characteristics of rapid reviews." Journal of Clinical Epidemiology 129 (2021): 74-85.

[10] Thoring, Katja, Roland Mueller, and Petra Badke-Schaub. "Workshops as a research method: Guidelines for designing and evaluating artifacts through workshops." (2020).

[11] Hooshyar, Hossein, and Luigi Vanfretti. "A SGAM-based architecture for synchrophasor applications facilitating TSO/DSO interactions." 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2017.

[12] Aravinthan, Visvakumar, et al. "Reliability modeling considerations for emerging cyber-physical power systems." 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS). IEEE, 2018.

[13] Kotut, Lindah, and Luay A. Wahsheh. "Survey of cyber security challenges and solutions in smart grids." 2016 cybersecurity symposium (CYBERSEC). IEEE, 2016.

[14] Jim Finkle, "U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage", Reuters, published January 8, 2016. Retrieved 22 May 2023

[15] N. Kostyuk and Y. M. Zhukov, “Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?”, J. Conflict Resolution, 63(2), pp. 317-347, 2019. Available: https://doi.org/10.1177/0022002717737138

[16] Human Rights Watch, “Ukraine: Russian Attacks on Energy Grid Threaten Civilians”, published December 6, 2022. Retrieved 22 May 2023.

[17] Ten Brinke, Wilfried BM, et al. "Social disruption by flooding, a European perspective." International journal of disaster risk reduction 21 (2017): 312-322.

[18] A. Stirling, “Transforming power: Social science and the politics of energy choices,” Energy Research & Social Science, vol. 1, pp. 83-95, 2014.

[19] M. Sarrica, S. Brondi, P. Cottone and B.M. Mazzara, “One, no one, one hundred thousand energy transitions in Europe: The quest for cultural approach,” Energy Research & Social Science, vol. 13, pp. 1-14, 2016.

[20] L. Steg, R. Shwom, and T. Dietz, “Engaging People in a Sustainable Energy Transition,” IEEE Power & Energy Magazine, vol. 16(1), pp. 20-28, 2018.