Major Blackouts of the Decade: Underlying Causes, Recommendations and Arising Challenges

Nirupma Sharma [1], Aparna Acharya[1], Irene Jacob[1], Sumanth Yamujala[2], Vikas Gupta[1], Rohit Bhakar[1*]
[1]*Department of Electrical Engineering,* [2] *Centre for Energy and Environment*
Malaviya National Institute of Technology Jaipur, India
Email: rbhakar.ee@mnit.ac.in

***Abstract*— Large disturbances in electric grids lead to severe load-generation imbalances, thus resulting in power outages or blackouts. Blackout is a phenomenon that occurs not because of a single cause, but due to multiple cascading disturbances. A critical review of such events can help in drawing preventive strategies and ensures readiness to mitigate the risk of blackouts. In this context, the work reviews the causes and severity of blackouts of various geographical locations in the past decade. An attempt has been made to summarize major blackouts and their effects. Some recommendations are also presented to provide strategies for grid protection and to mitigate the severity of blackouts. Further, an index to identify potential category of events that may cause a blackout in a geographical location is formulated. Finally, the work highlights few challenges arising due to transition in power systems. This work helps system operators and planners to develop grid technologies, electricity market models, and grid codes for improving system resilience.**

Keywords*— *Blackout analysis, blackout causes, blackout prevention, potential challenges, power system blackout.

I. Introduction

Power systems should be able to provide continuous electricity supply to consumers in all conditions. However, as the networks cover a large geographical area, they are vulnerable to various faults and weather conditions [1]. Any disturbance in supply-demand balance affects reliability and security of the power grid. This is even more important when consumer expectancy from the grid and the need for reliable power are increasing consistently. Therefore, priorities have invariably been given by utilities to emphasize grid security and reliability even in the event of disturbances. If the power system is subjected to disturbances like overloading, generator failure, equipment malfunction, tripping of transmission lines, or cyber threats, it would experience cascading failures resulting in a blackout [2]. Cascading failures are the sequence of events that occur in a power system after the disruption of a single element, leading to its global breakdown (blackout). Considering this fact, a blackout can be defined as a scenario that consists of a series of events resulting in temporary interruption of power supply from few hours to several days in a specific area. As power grids have been failing due to a variety of factors, it is important to review historic blackouts, analyze the causes and effects of such events, and investigate certain prevention strategies or measures taken by utility companies to avoid the risk of blackouts.

Further, various challenges have been evolving in the grids over a decade due to higher renewable penetration, climatic stresses, etc. [3]. Maintaining reliable, robust, and stable grid operations has become more complex with expansion in Renewable Energy Sources (RES) integration and de-commitment of conventional power plants. This is due to variable cross-border power trades, operating systems closer to their technical limits, and intermittent nature of RES [4]. Moreover, the shift towards power electronics interface poses a risk to the power system's dynamic stability [5]. These conditions further aggravate the grid operating conditions and may result in frequent and severe outages. This paper is concerned with these potentially growing challenges faced by system planners and operators in framing policies and market models to mitigate the impact of blackouts while ensuring smoother transition in power systems. In this context, the paper contributes to providing-

1. A refined classification of blackouts
2. Recommendations to mitigate blackouts and
3. Potential challenges in power system security

The remainder of this paper is structured as follows: The underlying causes of blackouts are investigated in Section II. Some recommendations from regulators and system operators to mitigate the adverse impacts of blackouts are presented in Section III. The challenges posed by recent transitions in power systems are studied in Section IV and Section V concludes the paper.

II. Blackout Causes

Generally, the causes of power system blackouts include inappropriate load shedding, voltage collapse, voltage instability in transmission networks, dynamic or static stability loss, multiple tripping of overloaded lines, and others. Historical surveys show major blackouts occurred due to these causes and affected massive population worldwide [6]. Blackout can be classified into five major categories based on the major source of the event, as shown in Table I. Although most blackouts do not occur because of only one cause, there exists a series of events called cascading causes that comes after all those major causes. A thorough audit of significant blackouts and their causes that have occurred within the last decade is presented henceforth [7].

A. Natural Calamity

Natural Calamities like heavy storms, earthquakes, hurricanes, lightning strikes, and temperature fluctuations have caused large power blackouts worldwide. About 8 million individuals were affected due to lightning strikes in Thailand's power system. In 2017, Hurricane Maria hit Puerto Rico, resulting in a power loss to the entire island. It took 326 days to restore the entire system. Azerbaijan had a

This work is supported by the DST grant for UKICERI project, DST/RCUK/JVCCE/2015/02.

2021 9th IEEE International Conference on Power Systems (ICPS) | 978-1-6654-2873-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICPS52420.2021.9670166

major power outage due to unexpected high temperatures which lasted for more than 6 hours, affecting 8 million people. A serious ice storm has left New Mexico without electricity for 10 days. Recently in 2021, a severe winter storm caused a power outage in Texas that lasted for 17 days affecting 2 million households without power. Findings show that below freezing temperature has caused power plants to shut down as equipment frozen/fuel ran out. Thereby, consumers were cut off to keep the grid itself operating and avoid a catastrophic failure [8].

TABLE I. CLASSIFICATION OF BLACKOUTS

Blackout Classification	Causes
Natural calamity	1) Storms, Earthquakes, Cyclones 2) Lightning strikes 3) Temperature fluctuation
Transmission failure	1) Line tripping due to excessive sag and congestion 2) Short-circuit fault 3) Protection device failure 4) AC tie-line failure 5) Tripping of CV transformer 6) Tree contact
Generation failure	1) Loss of generation or load shedding 2) Substation failure 3) Voltage collapse 4) Transient instability 5) Voltage and frequency deviation
Cyber issues	1) Malware 2) Security breach 3) Denial of Service 4) Communication failure 5) Control system failure
Human/equipment/unknown error	1) Operator error 2) Mechanical failure 3) Animal misbehavior

B. *Transmission Failure*

Extreme transmission failures resulting in blackout are caused by tripping of transmission lines due to congestion and overloading, insufficient load shedding schemes, short-circuit faults, protection device failures in lines, AC tie-lines failure, and physical contact of lines to structures. Some of the blackouts due to these causes were - a) Power outages that occurred in Pacific Southwest (San Diego, California, Arizona, and Mexico.), lasted for about 12 hours affecting 2.7 million residents. In this event, tripping of a major transmission line during peak load led to system collapse. At that time, San Diego experienced a complete power outage because of deficient load shedding that prompted falling impacts. b) A power outage happened in Brazil because of transmission lines failure which went on for around 16 hours affecting 53 million individuals. c) In 2012, power outage due to tripping of a transmission line affected almost 350 million people in northern and eastern parts of India [9]. The power outage was experienced due to overloading of one of the 400 kV Gwali–Binar transmission lines while another line was under scheduled maintenance. Although the system was partially restored in 15 hours, it experienced another outage again on the next day due to demand-generation imbalance. Around 680 million individuals were affected when almost 32 GW of energy was interrupted. An overloaded transmission line caused a cascading failure in the Turkish power grid, affecting about 75 million people. In Vietnam, a 500 kV line tripped, isolating the northern and southern region of Vietnam's power system. In 2021, a transmission line trip at Guddu power plant due to a technical fault has caused the entire power system to shut down for 18 hours and affected 200 million people in Pakistan [10]. Investigations have found that National Transmission & Despatch Company has failed in isolating fault, resulting in cascading effects that plunged the nation into darkness. Also, transmission line tripping is found to be the major cause for 05 biggest grid collapse events till now.

C. *Generation Failure*

Blackouts due to generation failure are caused by the overloading of generators that results in loss of generation, substation failures, voltage, and frequency instabilities. In the Philippines 14 power plants were shut, affecting their capital city Manila and almost 40 % of the Luzon islands. The tripping of generators and voltage instability in transmission lines led to overall voltage collapse in the system and affected around 8 million individuals. Bangladesh Power System (BPS) experienced a complete system breakdown in 2014, which went on for around 24 hours. As indicated by findings, this was because of an unplanned High Voltage Direct Current (HVDC) station outage. Unresponsive reserves and scheduled maintenance of some generators have worsened the situation. The aggregated load shed with activation of all under-frequency load shedding stages was less than the disturbance experienced by the system, and this led to the blackout. Historically, generation side failure affected a larger population compared to any other causes. Recently in 2021, a grid failure resulted in massive power outages which lasted for 2 hours in some areas and 10-15 hours in other areas of Central Mumbai. Findings show that overloading of lines and lack of contingency planning are the major causes of the power outage. A load loss of 2.6 GW and generation loss of 840 MW occurred due to system failure.

D. *Cyber Issues*

Arising cyber issues like cyber-attack of various kinds including data/security breaches, malware, denial of services, man in middle attacks, etc., and their further impact on communication systems and operation & control of power systems can lead to blackouts. In the past decade, several countries around the world have faced various cyber issues, for example, cyberattacks on Ukraine's power grid, hydropower generation in New York, Korea Hydro and Nuclear Co. Limited, security breach in Iran's nuclear plant. Even blackout in three cities of USA is also suspected to be a cyber-attack. Out of all such attacks, the Ukraine grid attack is considered to be the first known large-scale power outage caused by a cyber-attack [11]. This was a spear-phishing attack with BlackEnergy malware; later distributed denial of service attacks and KillDisk were used by attackers to further stop the operators from problem resolving. It affected more than 0.23 million population and 73 MWh of energy supply. Though power was recovered after 1-6 hours, it took more than 2 months for system control and operation restoration, till then operators had to do manual operations.

E. Human/Equipment/Unknown Error

Some of the blackouts have also occurred due to human error like system operators' error, equipment failure like mechanical failure in large machines, and some unknown causes like animal misbehavior with equipment. Though these failures may sound small enough to cause damage, the cascading failures resulted in a larger blackout. A power outage was reported when a monkey fell on transformer located at Gitaru hydropower station in Kenya. Findings show that subsequent tripping of transformer interrupted 180 MW of power supply affecting 10 million people for more than 4 hours. Uncontrolled events following the 180 MW power loss worsened the situation and led to system breakdown. In 2016, the areas of Argentina, Uruguay, and Paraguay were affected by a power outage because of operator mistake, leaving approximately 48 million individuals without electrical supply [12].

Some statistical analysis has also been presented in this paper by considering some work analyzed in [13]. A statistical summary of blackouts that occurred over the last decade is presented in Table II. In this, the total average population affected by a specific cause of blackout with its average occurrence per year is highlighted. Fig. 1 depicts the severity of blackouts considering the population affected for each year. This shows that natural calamities, transmission, and generation side failures are the major sources of blackouts. In addition, the impact of each category of blackout is shown in Fig. 2 in terms of average power outage duration (in hours). Duration of blackouts due to natural calamity is more, compared to other causes with respect to system restoration time.

TABLE II: STATISTICS OF BLACKOUTS (2011-2021)

Blackout	Average population affected per year (in millions)	Average occurrences per year
Natural calamity	50	4.2
Transmission failure	70	1.9
Generation failure	100	1.8
Cyber issues	5	1
Human/equipment/ unknown error	20	1.5

Based on the critical review of historic blackout events, the most plausible cascading faults that are resulting in a blackout under each classification are highlighted in Table III.

III. Recommendations for Blackout Prevention

To prevent and deal with the causes of blackouts and consequent failures, it is crucial to make the system robust and limit the cascading failures. This section presents the key recommendations for each classification of blackouts that can be considered to mitigate their consequences.

A. Failure due to Natural Calamities

Restoration of damaged transmission lines has been a tedious task in case of natural calamities like storms, hurricanes, cyclones, earthquakes, lightning strikes, etc. For this, forming microgrids can be a way towards improving grid resilience. Integration of distributed energy sources and RES could be an alternative due to their self-sufficient nature. In geographic locations, that are prone to natural disasters, a more comprehensive energy assurance plan is

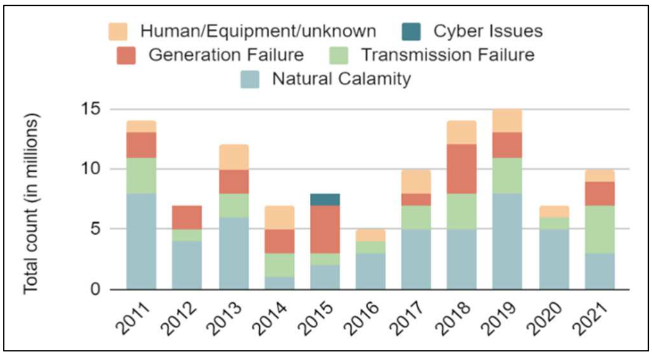

Fig. 1. Severity of Blackout considering population affected

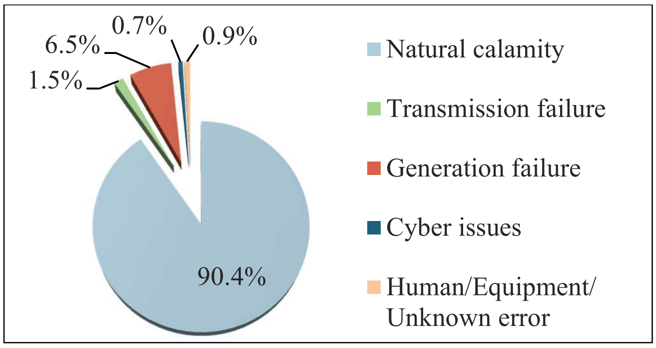

Fig. 2. Blackout Impact based on average power outage duration

TABLE III: MAJOR CASCADING EVENTS

Blackout Classification	Major Cascading Events
Natural calamity	1) Damage of Transmission corridors 2) Generators loss of synchronism 3) Undervoltage and under frequency load shedding
Transmission failure	1) Overloading of transmission lines 2) Generators loss of synchronism 3) Power angle instability and under frequency load shedding
Generation failure	1) Unresponsive spinning reserves 2) Subsequent generator tripping 3) Transmission line tripping due to Undervoltage
Cyber issues	1) Communication failure 2) Generators loss of synchronism 3) Insufficient time for backup supply
Human/equipment/unknown error	1) Transmission line tripping 2) Generators loss of synchronism 3) Undervoltage and under frequency load shedding

needed for restoration planning inclusive of pre-established contracts for transporting material, human resources, and having sufficient spares [14]. For failures due to temperature fluctuations, adapting new policies along with existing energy policies, reducing system loads during peak hours of summers through demand response mechanisms [15], augmenting existing infrastructure to prevent overloading, and weatherizing power system equipment can be some measures. Along with these, grid interconnections should be considered to reduce the severity of blackouts. Transmission lines should be maintained timely by insulator washing during winter [12].

B. Transmission System Failure

Operational planning and real-time situational awareness, scheduled outage and maintenance planning, and improved tools for accelerating the process of on-line (N-1) contingency analysis are useful to avoid overloading of transmission corridors [16]. The blackouts due to protective device failure can be prevented using protective systems auditing and analyzing automatic protection equipment by comparing with real data in different critical conditions. Ensuring standard operating procedures in critical conditions and training people with realistic simulations to deal with cascading failures are also necessary [17]. Other transmission failure causes like line tripping due to overloading, sag, or congestions and tripping of any equipment like transformers can be prevented by coordinated outage planning for transmission system and system equipment. Synchrophasor-based wide area monitoring systems for real-time monitoring, protection, and control of systems should be employed. In case of short circuit faults, proper telemetry and communication to load dispatch centers, islanding schemes for all regions of the grid for faster recovery in case of disruptions are needed [18]. Optimal utilization of grid assets like HVDC, thyristor-controlled series capacitor, static voltage compensators, and giving more autonomy to all load dispatch centers in taking and implementing decisions regarding operations and security of grid should be considered. Furthermore, a separate task force should be formed for analysis of present grid to avoid future disturbances [19]. For tripping due to tree contacts, regular trimming of vegetation should also be carried out.

C. Generation System Failure

For causes like substation failure, development of mandatory reliability standards is essential [17]. Deployment of under-frequency and under-voltage load shedding systems is sufficient to prevent uncontrollable cascading. Along with this, operation of defense mechanisms like under-frequency and df/dt based load shedding should be ensured to stop running generators from tripping in case of faults. For instabilities due to voltage or frequency deviations, there should be enhanced research in automatic emergency control systems to relieve overloads and prevent instabilities. Establishing regulations for frequency control through generator reserves/ancillary reserves and unscheduled interchange mechanism should also be reviewed [19]. System planners must ensure the availability of sufficient black-start capable units in the generation mix for quick grid restoration. In case of inverter dominated power systems where grid restoration is achieved by renewables and energy storage systems [20], resources should provide voltage support along with power generation for system restoration. Load segregation strategies to reduce the burden on system must be implemented to achieve this. Proper testing of primary response of generators and maintaining critical operating inertial reserves for existing frequency response schemes are some of the measures as recommended by countries affected with such blackouts, for example, BPS [21].

D. Cyber Threats

Evolving smart grid technologies would provide advanced communication, monitoring, control, and digitized systems, but along with this comes a great challenge of cybersecurity. There should be proper cybersecurity regulations and guidelines to which the electricity sector should adhere to. Secure configuration of industrial control systems, demilitarized zone set up for emails/web server, as well as a separate set up for control system networks are required. All unused protocol ports and services should be locked down or turned off to reduce the points for attackers to enter into the system and cause damage. All remotely accessed services should be monitored and operator-controlled. Credential's monitoring should be there for any unusual activity so that system administrators would be well alerted before any attack. Use of properly trained intrusion detection systems and strong multi-factor authentication in the system for network security should be considered. Use of signed firmware drivers to have protection against malicious drives and application whitelisting to detect any malware can be some prevention measures. Moreover, vulnerability assessment and penetration testing should be done through approved agencies [22]. These are some of the recommendations provided with respect to the Ukraine cyberattack, which can be utilized as precautionary measures by other countries too.

E. Failure due to Human/Equipment/Unknown Error

To prevent blackouts from equipment error, regular maintenance of equipment and their timely replacement is required. Overall grid infrastructure upgradation viz., remote terminal unit to phasor measurement units is needed. Moreover, for relay systems, coordinated relay protection scheme along with over-current, over-excitation limiter, distance protection, out-of-step, and under-frequency load-shedding relays is needed. Apart from equipment upgradation, schemes for protection and grid codes should also be revised [6]. To prevent blackouts due to human error, human interventions should be reduced through automated monitoring and control of systems. Along with this, there should be regulations for control center operator training. Staff certification procedures should also consider proficiency test approval to certify capability of control center operators in handling reliability issues. Furthermore, there should be considerations regarding the use of tools such as operator training simulators to train them to face any critical conditions and use of simulator models that match real-time conditions [23].

F. Discussions

Though it is well understood that blackouts may happen due to diverse primary causes, their intensity is determined by weak points of the grid. Geographical location, operating conditions, and robustness of grid play a key role on frequency and intensity of blackouts. Hence, a detailed analysis considering various grid paraments is required to highlight a critical category of events that have the potential to drag a severe disturbance into a blackout for a geographical location, either as primary or cascading failure.

An attempt has been made to quantify such categories. This requires extensive data of historical events under each category given in Table 1. For each category, data on frequency of occurrence of an event and number of times it affected grid operations, population affected due to such event are recorded. For category of events related to transmission and generation, peak demand, installed capacity and average line loading can give additional inference. Based on the data, indices like Reliability Affect Factor (RAF) and Population Affect Factor (PAF) are estimated for each category, $c \in C$, and year, $n \in N$, as given in (1) and (2).

$$RAF = \sum_{n}^{N} \left[\frac{no.\ of\ times\ event\ affected\ syst.\ operations}{no.of\ times\ event\ occured} \right] \forall c \quad (1)$$

$$PAF = \sum_{n}^{N} \left[\frac{Population\ affected\ due\ to\ event}{total\ population} \right] \forall c \quad (2)$$

RAF and PAF give indices between zero and one. Aggregating both indicators with appropriate weights, say 0.5, highlights the index of each type of category. Categories with a higher index could become the potential sources of blackouts for a geographical location.

IV. Arising Challenges

The power industry is in a stage of transition and becoming market-driven. Along with the integration of renewables into the grid, restructuring of power systems and adoption of smart grid technologies are paving their way to make systems resilient. These technologies can meet the increasing electricity demand, however, they pose many challenges in maintaining grid conditions. Thus, it is a prime responsibility of electricity market participants and utilities to underline certain challenges for grid failure to maintain uninterrupted power supply and security at an adequate level. Some of these challenges are addressed in this paper.

A. High RE Integration

RES such as solar and wind are being increasingly deployed for power generation. The integration of renewables and Distributed Generations (DGs) leads to voltage and frequency variations, harmonic distortions, etc. Also, non-dispatchable nature of such resources may cause power shortages and congestion [24]. The asynchronously connected RES to the grid can make it insensitive to system frequency changes due to lack of rotational inertia. By displacing conventional power plants, these interfaces reduce grid strength to disturbances, thus making grids unstable and may lead to cascade blackouts. Also, most of the existing wind turbine generators lack fault ride-through capability. This makes a large-scale generation loss in case of any short circuits. However, retrofitting such units to make them Low Voltage Ride Through (LVRT) compliant incurs additional investments in generation. Further, higher renewable penetration into the grid makes weather forecasting important for scheduling resources to cater netload variations [25].

B. System Operations and Resiliency

Power industry is driven towards deregulated and restructured environment. The deregulation in market forces has significant impacts on functions like economic dispatch, unit commitment, etc. Therefore, instead of performing these functions system operators have to manage the network according to market requirements, deliberated by supply contracts, bids for available generation, and location of the load [26]. In a restructured industry, reserve margins tend to be lower as compared to that in traditional power systems and the probability of blackout is higher [26]. Power sector utilities tend to perform operational and economic planning to prevent supply-demand imbalances due to intermittent generation sources. Further, restoration of blackout involves black start, network reconfiguration, and load restoration [27]. Strategies to use RES along with energy storage systems for grid restorative services must be explored. Large-scale black start capability of RES needs a detailed investigation [28]. Also, present utility-scale Li-ion batteries are not ideal for bulk storage of electricity. Switching to alternative batteries is highly capital intensive. Estimation of appropriate energy storage portfolio is essential to ensure system-wide security and enhance black start capability. Microgrids along with distributed energy resources are advantageous in grid restoration due to self-healing property to serve local loads in fault conditions. But they face load-generation balance in islanded mode, feeder design, etc. which directly impacts its resiliency. In addition to this, microgrids with limited generation capacity are not allowed to participate in grid services. This impedes in making microgrid clusters to protect system in extreme events [29]. Some of these conditions aggravate the situation in event of a blackout, if not addressed properly.

C. System Security

The conventional power systems are getting upgraded to smarter grids which would be advantageous in terms of efficient integration of renewable energy sources, and overall improved grid operations and services. However, the smart grid is highly dependent on advanced communication infrastructure since a large amount of data is needed to be exchanged for proper operation of such a complex system. Also, wide-area controls are being used; the design, simulation, on-line testing, and cyber protection of such controls are expensive and time-consuming. Smart grid architecture is vulnerable to numerous security threats and challenges including thefts, physical and cyberattacks, terrorism, natural disasters, etc. Possible repercussions of these issues would be - increased operation costs, infrastructure failures, incorrect visualization of system's actual condition due to false data, derailed consumer devices, disorganized energy market, cascading failures, and power system blackouts [30]. In case of natural disasters, there are advanced automation technologies available in the smart network infrastructure which would provide faster data access and system restoration but, their cost of deployment remains a barrier, particularly the challenges lie in monetizing the benefits of such installations. There is a need to critically analyze these issues [31]. To ensure safe and proper operation of the smart grid, operators should have cyber resilient monitoring of physical and cyber states of power system. The complexity faced by power system operators should be addressed through detailed procedures. Moreover, assistance of artificial intelligence and improved man-machine interfaces for system operators can be an aid for enhanced reliability and security.

V. Conclusion

Blackouts are major catastrophic failures leading to the shutdown of electricity in almost every area of modern society. This paper has investigated the causes and impacts of various power outages. Analysis of various blackouts has brought out the need for certain remedial measures that constitute recommendations that can help power system operators and equipment upgradation to prevent blackouts to some extent. With the new transitions in power systems, security and reliability have paved their way along with certain complexities and challenges. This paper highlights such arising challenges that must be addressed to prevent frequent blackouts/power outages and make the system more robust and resilient. The work can be extended to highlight the major causes and cascading events of a blackout in a given geographical region through extensive historical data and system characteristics. Also, various scenarios of power outages can be studied to understand the strategies that can be adopted in different regions to mitigate the impact of blackouts.

REFERENCES

[1] Mark Dyson and Becky Li, "Reimagining grid resilience," *Rocky Mountain Institute*, 2020. [Online]. Available: http:// www.rmi.org/insight/reimagining-grid-resilience. [Accessed: Sept. 2021].

[2] M. Behnert and T. Bruckner, "Causes and effects of historical transmission grid collapses and implications for the German power system," *Institute for Infrastructure and Resources Management, University of Leipzig*, March 2018. [Online]. Available: https://www.econstor.eu/bitstream/10419/190501/1/1043587349.pdf . [Accessed: Sept. 2021].

[3] M. S. Alam, F. S. Al-Ismail, A. Salem and M. A. Abido, "High-level penetration of renewable energy sources into grid utility: Challenges and solutions," *IEEE Access*, vol. 8, pp. 190277-190299, Oct. 2020.

[4] IEA-ETSAP and IRENA, "Renewable energy integration in power grids", *Technology Brief*, April 2015, [Online]. Available: https://www.irena.org//media/Files/IRENA/Agency/Publication/2015/ IRENA-ETSAP_Tech_Brief_Power_Grid_Integration_2015.pdf. [Accessed: Sep. 2021].

[5] A. Jain, "Blackstart and Islanding capabilities of wind turbines", *DTU Wind Energy*, 2020. [Online]. Available: https://windenergy. dtu.dk/english/education/phd/phd-projects/anubh av-jain. [Accessed: June 2021].

[6] Y-K. Wu, S. M. Chang and Y-L. Hu, "Literature review of power system blackouts", *Energy Procedia*, Vol. 141, pp. 428-431, 2017.

[7] H. Haes Alhelou, M. Hamedani-Golshan, T. Njenda, and P. Siano, "A survey on power system blackout and cascading events: Research motivations and challenges," *Energies*, vol. 12, no. 4, p. 682, Feb. 2019.

[8] J. W. Busby, K. Baker, M. D. Bazilian, et. al, "Cascading risks: Understanding the 2021 winter blackout in Texas," *Ene. Res. & social science*, vol. 77, p. 102106, 2021.

[9] R. Anubhav, "India's blackouts of July 2012: What happened and why?", Dec. 2016. [Online]. Available: https://medium.com/clean-energy-for-billions/indian-blackouts-of-july-2012-what-happened-and-why-639e31fb52ad 2013. [Accessed: June 2021].

[10] NEPRA, "Inquiry report regarding total power system collapse on Jan 2021", *National Electric Power Regulatory Authority*, Pakistan, Feb. 2021. [Online]. Available: https://www.nepra.org.pk. [Accessed: June 2021].

[11] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks", *IEEE Trans. Power Syst.,* vol. 32, no. 4, pp. 3317-3318, July 2017.

[12] P. Yuan *et al*., "Analysis and enlightenment of the blackouts in Argentina and New York," *Chinese Automation Congress (CAC)*, pp. 5879-5884, 2019.

[13] K. M. J. Rahman, M. M. Munnee and S. Khan, "Largest blackouts around the world: Trends and data analyses," *IEEE Int. WIE Conf. on Electrical and Computer Engineering (WIECON-ECE)*, pp. 155-159, 2016.

[14] A. Kwasinski, F. Andrade, M. J. Castro-Sitiriche and E. O'Neill-Carrillo, "Hurricane maria effects on puerto rico electric power infrastructure," *IEEE Power and Energy Tech. Systems J.*, vol. 6, no. 1, pp. 85-94, March 2019.

[15] N. Komendantova, D. Kroos, D. Schweitzer, C. Leroy, E. Andreini, B. Baltasar, et al., "Protecting electricity networks from natural hazards," *Organization for Security and Cooperation in Europe (OSCE)*, 2016. [Accessed: June 2021].

[16] ENTSOE, "Report on blackout in Turkey on 31st March 2015," *Project group Turkey,* Belgium, Sept. 2015. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/SOC%20 documents/Regional_Groups_Continental_Europe/20150921_Black_Out_Report_v10_w.pdf. [Accessed: July 2021].

[17] Md. Rokonuzzaman, "Blackouts in South Asia - Perspective of Bangladesh: Observation and Recommendation", *J. Bangladesh Electron. Society (JBES)*, vol. 14, pp 21-27, 2014.

[18] S. Soman, S. Tom, P. Thomas, and J. George, "Forced islanding and restoration scheme to prevent blackout for improving power system security," *IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, pp. 1-6, 2015.

[19] M. Vaiman *et al*., "Mitigation and prevention of cascading outages: Methodologies and practical applications," *IEEE Power & Energy Society General Meeting*, pp. 1-5, 2013.

[20] B. Zohuri and P. McDaniel, "*Introduction to energy essentials,*" 1st ed., Academic Press, 2021.

[21] M. A. Kabir, M. M. H. Sajeeb, M. N. Islam and A. H. Chowdhury, "Frequency transient analysis of countrywide blackout of Bangladesh Power System on 1st November 2014," *Int. Conf. on Advances in Elect. Engg. (ICAEE)*, pp. 267-270, 2015.

[22] A. Shehod, "Ukraine power grid cyberattack and US susceptibility: Cybersecurity implications of smart grid advancements in the US," *Cybersecurity Interdisciplinary Systems Laboratory, MIT*, 2016-22, Dec. 2016. [Onine]. Available: http://web.mit.edu/smadnick/ www/wp /2016-22.pdf. [Accessed: July 2021].

[23] O. P. Veloza and R. H. Cespedes, "Regulatory mechanisms to mitigate the vulnerability of power systems to blackouts," *IEEE/PES Trans. & Dist. Conf. and Expo: Latin America*, pp. 1-6, 2006.

[24] N. Holjevac, T. Baškarad, J. Đaković, M. Krpan, M. Zidar, and I. Kuzle, "Challenges of high renewable energy sources integration in power systems - The case of Croatia," *Energies*, vol. 14, no. 4, p. 1047, Feb. 2021.

[25] A. K. Alsaif, "Challenges and benefits of integrating the renewable energy technologies into the AC power system grid," *American J. Engg. Res*., vol. 6, no.4, pp. 95-100, 2017.

[26] E. Androulidakis, A. Alexandridis, H. Psillakis, and D. Agoris, "Challenges and trends of restructuring power systems due to deregulation," *5th WSEAS Int. Conf. on Power Systems and Electromagnetic Compatibility*, pp. 49-54, 2005.

[27] Y. Liu, R. Fan and V. Terzija, "Power system restoration: A literature review from 2006 to 2016," *J. Modern Power Systs. and Clean Energy*, vol. 4, no. 3, pp. 332-341, July 2016.

[28] S. Saleem, "Black-start using renewable energy resources," *IEEE Smart Grid Resource Centre*, April 2021. [Online]. Available: https://smartgrid.ieee.org/newsletters/april-2021/black-start-using-renewable-energy-resources. [Accessed: July 2021].

[29] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab and Y. Al-Turki, "Networked microgrids for enhancing the power system resilience," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1289-1310, July 2017.

[30] A. O. Otuoze, M. W. Mustafa, R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *J. Elect. Systems and Info. Tech*., vol. 5, no. 3, pp. 468-483, 2018.

[31] M. Waseem and S. D. Manshadi, "Electricity grid resilience amid various natural disasters: Challenges and solutions", *The Electricity J.*, vol. 33, no. 10, pp. 106864, 2020.