A Review of Cybersecurity Attacks on Bulk Power System: Assessing Risks

Muhammad Faisal Nadeem khan, *Senior Member, IEEE* and Francisco de León, *Fellow, IEEE*

[1]***Abstract*—Cyber security for power systems is becoming a concern for many researchers. However, the impact of cyber-attacks on actual power systems is unclear. This paper discusses analytically the significance of cyber security for power systems and evaluates whether cyber-attacks are a real threat, or are just a hypothetical concept. First, this paper categorizes the different types of power system attacks and then systematically reviews the cyber-attack modeling, detection, and mitigation approaches for bulk power systems. This paper also discusses prominent cyber and physical attacks on actual power systems and draws a comparison among them based on economical and societal impacts. Based on the facts uncovered in the paper, when compared to physical attacks, cyber-attacks on power systems have had negligible economic and societal impacts. In fact, there is only one documented case (the Ukrainian cyber-attack by Russia) that successfully caused customer disconnections.**

***Index Terms*— Cyberattacks, cyber-physical systems, power transmission lines, security of smart grids.**

List of Acronyms

AMI	Advanced Metering Infrastructure
BDD	Bad Data Detector
CCPA	Coordinated Cyber–Physical Attack
CIA	Command Injection Attack
CPA	Cyber–Physical Attack
CPI	Cyber Physical Infrastructure
CPPS	Cyber Physical Power System
DDA	Dummy Data Attack
DFR	Digital Fault Recorder
DoS	Denial of Service
DoE	Department of Energy
EVs	Electric Vehicles
FDI	False Data Injection
FDIA	False Data Injection Attack
HIL	Hardware in Loop
ICT	Information and Communication Technology
ISO	Independent System Operator
MITM	Man-in-the-Middle
MTD	Moving Target Defense
PMU	Phasor Measurement Unit
RIA	Relay Injection Attack
SA	Sequential Attack
SCADA	Supervisory Control and Data Acquisition
TDA	Time Delay Attack

I. Introduction

POWER system security has become a subject of paramount importance as electric grids evolve into more convoluted structures to supply the ever growing electricity demand. Based on a comprehensive literature review, this paper categorizes the security threats of power grids into four types: (1) naturally generated physical attacks such as relay maloperation, large frequency variations, and insulation failure; (2) externally organized physical attacks that create forced transmission line and transformer outages; (3) cyber-attacks that cause corruption of measurements or data transfer in the supervisory control and data acquisition (SCADA) systems [4]; and, (4) coordinated cyber–physical attacks (CCPAs) such as tripping transmission lines as a result of false data injection, for example [6].

The major causes of natural physical attacks are switching surges, lightning strikes, damage to transmission lines, and sudden change in load or generation. External physical attacks involve terrorist attacks such as gun fire at the substation equipment or loss of transmission lines through explosive devices [8]. Power systems have largely been affected by natural physical attacks. The 2003 northeast blackout which affected 45 million people in 8 states of the USA is an example of natural physical attacks and it occurred because overloaded transmission lines hit untrimmed trees and the alarm did not sound to warn maintenance workers [10]. Similarly, many other large blackouts happened globally (such as 2012 Indian and 2023 Pakistan blackouts) which affected even more people [12].

External physical attacks are mounting globally, and the US power grid is suffering a decade-high surge as extremists and vandals increasingly take aim at the nation's critical infrastructure. According to the US Department of Energy (DOE) [13], 164 external physical attacks have been reported in 2022, while the previous peak was 97 attacks in 2021. Fig. 1 summarizes the cumulative number of reported external physical attacks on power grid infrastructure of the past five years. Cyber-attacks are considered a serious concern for the power grid by some studies [14-16] due to the deep integration of information and communication technologies (ICT) into grid operations. Reference [4] stated that cyberattacks in the form of

Muhammad Faisal Nadeem khan is with the Electrical Engineering Department at University of Engineering and Technology Taxila, Taxila, Pakistan and also with the Department of Electrical and Computer Engineering at New York University, Five Metro-tech Center, Brooklyn, NY, 11201 (E-mail: faisal.nadeem@uettaxila.edu.pk).

F. de León is with the Department of Electrical and Computer Engineering at New York University, Five Metro-tech Center, Brooklyn, NY, 11201 (E-mail: fdeleon@nyu.edu).

false data injections (FDIs) can have irrecoverable consequences in SCADA operations.

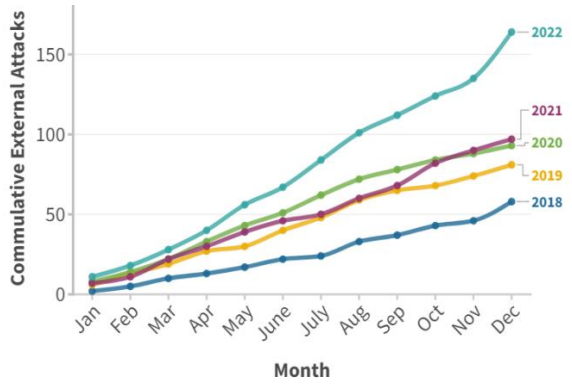

Fig. 1. Power grid attacks [13].

In recent years, there has been an attempt to modernize the present grid by securely building cyber-physical infrastructure (CPI) to increase grid robustness and efficiency [17, 18]. This concept is generally known as cyber physical power system (CPPS) and its conceptual view is presented in Fig. 2 [19]. Since CPPSs depend upon cyber system information, CPPS's sophisticated communication capabilities for monitoring and control applications are extremely sensitive to cybersecurity threats, as demonstrated in Fig. 2. Therefore, the authors of [20] believe that CCPAs can be dangerously covert. In CCPA the naturally generated or external created physical attack disconnects a transmission line, transformer or generator, and a simultaneous cyber-attack masks the natural or external physical attack by manipulating the sensor measurements.

The authors of [15] stated that cyberattacks may cause power system security and sustainability concerns in the CPPS. Numerous types of equipment such as Electric Vehicles (EVs), Power System Stabilizers (PSS), Intelligent Electronic Devices (IED), Advanced Metering Infrastructure (AMI), Digital Fault Recorder (DFR), SCADA, Phasor Measurement Units (PMUs), connected with the CPPS and their communication nodes can be vulnerable to cyberattacks and must be protected [15]. Therefore, the authors of [21] believe that, for CPPS, the priority research theme should be security against cyberattacks. Moreover, with the emergence of various types of cyberattacks such as False Data Injection (FDI) attacks, Man-in-the-Middle (MITM) attacks Time Delay Attacks (TDAs), and Denial of Service (DoS) attacks, the cybersecurity of CPPS has emerged as a hot research topic among power system researchers due to high possibility of security breach [22, 23]. However, researching real-world contexts is challenging, i.e. verifying security and performance assessments is costly [22]. Large-scale modeling and simulation could be an option, but it needs a comprehensive mathematical model of the system, which is time-consuming and may result in errors when simulating the interaction mechanism between the physical and the cyber systems in the CPPS [21, 24]. Furthermore, although there are many claims of potential cyber physical attacks, their actual impact on real power systems has not been scientifically measured and it is still unclear if it is real or a hoax.

Recent review papers [16, 25-27] have discussed distinct aspects of cyber security for distribution systems or microgrids. However, to the best of our knowledge there is no comprehensive review available in the literature discussing cyber-attacks in bulk power systems. This paper discusses for the first time the concept of cyber-attack in bulk power systems, including their critical components, attack strategies, and mitigation measures. Furthermore, the authors of this paper are interested in assessing the economic and social impacts of cyber-attacks on large power systems. Although there are many studies available in the literature that have simulated different scenarios of cyber-attacks on standard and practical power systems, there are dearth of incidents reported in literature, news, and government reports regarding cyber-attack on real power systems and its impact on society. This motivated the authors to conduct a study on whether cyber-attacks affect real bulk power systems, or if this is simply an idea that has had no major economic consequences or caused human suffering.

The major contributions of this paper are:

1) Present the concept of cybersecurity for bulk power systems, providing a detailed explanation of how various types of attacks operate and outlining defense strategies.
2) Assess whether cybersecurity poses an actual threat to bulk power systems or remains a theoretical concept.

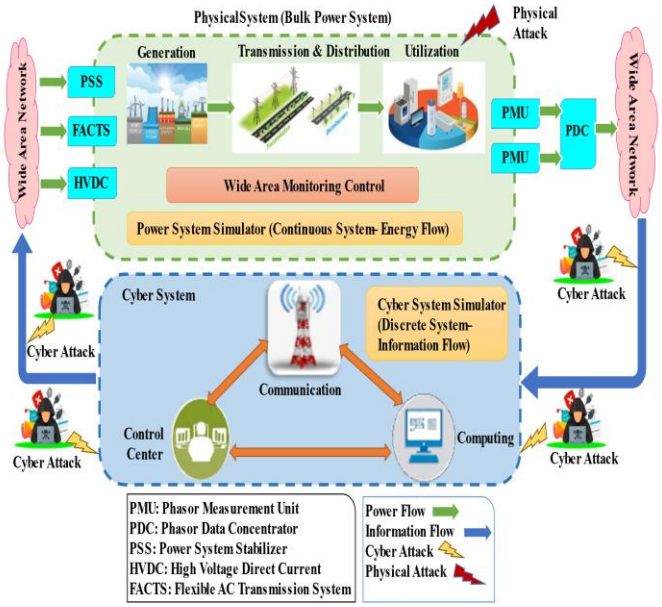

Fig. 2. Cyber Physical Power System.

II. Literature Review of Cyber-attacks on Bulk Power Systems

Many recent studies have discussed the concept of cyber security for bulk power systems. Most of these studies deal with modeling, detection, and mitigation of cyber-attacks while others discuss reliability indices and co-simulation platforms for analysis of CPPSs. Table I outlines different types of cyber-attacks (i.e., FDI, DoS, MITM, and TDA), as investigated by various studies and discussed in this section.

A. False Data Injection (FDI Attacks

False data injection attacks are often launched against the controlling channels and metering systems of power systems. They can potentially destroy the real-time measurements of voltage and frequency, which may mislead the process of state estimation [12], [13]. The modeling, detection, and mitigation

of FDI attacks for bulk power systems are discussed in many studies [28-38]. Reference [28] reports a FDI-based attack made against the physical parameters and control center of bulk power system. References [29, 30] proposed neural network based approaches for accurate detection of FDI attacks. A stream learning approach is proposed in [31] for real-time detection of FDI attacks in CPPS. A deep learning approach is presented in [32] to identify the new form of FDI attacks. In [34], a dynamic three stage FDI attack is developed first and then a new encoding scheme is introduced to identify the attack location. To understand the attacker behavior, a multi-objective stealthy FDI attack model is introduced in [35]. A new robust linear regression-based data driven strategy is proposed in [36] for design of FDI attacks that make them difficult to be detected by Bad Data Detector (BDD) algorithms. Mixed-integer linear programming is used in [37] to model the FDI attacks that can cause simultaneous congestion in different transmission lines. A bilayer game theory-based approach is presented in [38] for modeling attack and defense architecture of FDIs.

B. Denial of Service (DoS) Attacks

Although most studies in literature have considered FDI attacks to understand the concept of cyber security for bulk power systems, there are other cyber-attacks as well that may affect the power system. For Example, DoS attacks are launched against the transmission channels of CPPS and may affect its dynamic performance. An early-stage DoS attack detection mechanism based on the irregularities in the communication system is presented in [14]. Reference [39], presented two effective compensation strategies (one used the reference value and other information of previous time step) to secure multi-terminal high voltage direct current systems against DoS attacks.

C. Time Delay Attacks (TDA)

In TDAs, the attacker injects time delays in control signals and system components. This delays the information exchange between the nodes of bulk power system that can result in stability loss [16]. Reference [40] and [41] proposed a data driven approach and partial spectral discretization method to evaluate the delay in communication signals and ensure the stability of bulk power systems.

D. Man-in-the-Middle (MITM) Attacks

In MITM attacks, the hacker intrudes in the communication between two devices to steal information or mimic the characteristics of one device. In this way, it appears that the information is transferring in a normal mode. However, the hacker can now launch an FDI attack [16]. For detection and mitigation of MITM in bulk power systems, [50] and [42] presented a dynamic assessment model and cross-layered strategy respectively.

E. Coordinated Cyber-Physical Attacks (CCPA)

A three level CCPA is modeled in [43] to initiate the cascaded tripping and analyze its impact on *N*-1 secure power systems. In [20], the moving target defense (MTD) approach is presented to identify the CCPA in power grids. Reference [44] proposed a technique to identify fixed and variable CPAs and it is observed that variable CPAs are more deceptive. Based on a discrete-time dynamic model a new detector is proposed in [45] for simultaneous identification of CCPAs and FDIAs. Reference [46] first designed two types of FDI based CCPAs i.e., optimized attacks and replay attacks and then proposed suitable countermeasures for detection.

F. Reliability Indices

Other than modeling, detection, and mitigation of cyber-attack there are studies available in literature that focus on formulation of reliability indices, finding suitable co-simulation software, and implementation of testbeds for CPPSs. Reference [47] considered two reliability indices for determining the performance of CPPS at substation level. Similarly two reliability indices considered in [48] for reliability assessment of CPPSs using a Bayesian attack graph and Markov model-based technique. Reference [49] constructed a cross space model and proposed different impact indices for numerical risk assessment of cyber-attacks. Reference [50] proposed a comprehensive mechanism to quantify the resilience of power system using four stability index and two performance indexes. The co-simulation platforms have recently gain much attention of the researchers because until now there is no reliable software that can handle the differences in the mathematical model of communication and power systems [51]. A co-simulation platform is proposed with hardware in the loop (HIL) in [51] to perform real time analysis of CPPS for MITM and distributed DoS cyber-attacks using OPNET and RT-LAB software. Reference [52] tested various cyber-attack detection and defense methodologies in virtual environment and then based on cost-benefit and risk reduction tradeoff suggested that wind farm operators, grid operators, and OEMs should install the proposed technologies for reducing the chances of destructive attacks.

G. Summary of Cyber Attack Studies in Bulk Power Systems

Table I presents the overview of some significant studies that discussed cyber physical security for bulk power systems. Each study is summarized according to its focus of research, cyberattack discussed, test system utilized, proposed methodology, and outcomes of the research work. Most of these studies considered FDI attacks while other DoS attacks, MITM attacks, Data Injection Attacks (DIAs), Sequential Attacks (SAs), TDAs and CCPAs to investigate the cyber physical security for bulk power system. This is because FDI cyber-attacks are extremely covert and difficult to detect through BDDs [53]. According to different studies, in FDIA an attacker can tamper with power system component measurements [54], overload multiple transmission lines [55], and mask line tripping [56]. Furthermore, Table I demonstrates that most of the studies considered IEEE 39 and 118 bus systems while the rest considered other tests systems and practical systems for testing of proposed frameworks.

TABLE I
SUMMARY OF THE SIGNIFICANT RESEARCH STUDIES ON CYBER SECURITY FOR BULK POWER SYSTEMS

Refs	Focus of the research	Cyber attack	Test system	Proposed strategy	Main results
[14]	CPPS situational awareness	DoS	IEEE 39 bus	Hybrid deep learning model	Cyber-attacks can be localized and identify in near real-time
[57]	Modeling, detection and mitigation of cyber attack	FDIA	IEEE 118 bus and Chinese 132 bus	Decomposition algorithm-based detection and mitigation strategy	Stealthy cyber-attacks can be prevented by constructing a feasible attack vector
[28]	Cyber-attack modeling	DIA	IEEE 118 and 30 bus	Attack against measurements of physical infrastructure and control center.	Attack against physical infrastructure and control center indirectly and directly affects the state estimation.
[29]	Cyber Attack detection	FDIA	IEEE 14 and 118 bus	Graph neural network	Improved detection accuracy
[47]	Power system reliability assessment	CCPA	IEEE 24 bus & practical system	CPPS performance is assessed via two indices	Power system usually fails due to failure of physical components
[30]	Cyber-attack Detection	FDIA	IEEE 30, 118 and 2848-bus	Graph convolutional network	Efficient detection of FDI attacks
[58]	Power system robustness	SA	IEEE-118 bus	Deep Q-network Algorithm	Increased robustness
[33]	Power system resilience	MITMA	IEEE 14 and 118 bus	Dynamic risk assessment model	Uncover network security risks and highlights high-risk nodes
[31]	Detection and mitigation of cyber attack	FDIA	Central New York power system	SLA	Accurate detection and mitigation of FDI attacks aligned with a disturbance in the system
[59]	Attack detection	FDIA	IEEE 39 bus	Voting-Based Machine Learning Strategy	Accurate detection of FDIA
[60]	Power system resilience	FDIA	IEEE 30 Bus system	Dynamic risk propagation evaluation approach	Accurate attack prediction and risk analysis
[42]	Attacks Detection	FDIA, DoS, MITM	IEEE-118 bus	Cross-layered strategy	Accurate detection of cyber attacks
[32]	Attack modeling and detection	Distributed FDIA	IEEE 14-bus	Deep learning-based algorithm	Accurate detection of FDIA
[61]	Attack modeling and detection	FDIA	IEEE 24 bus and 39 bus	Ensemble based Learning	Improved modeling and detection of FDIAs.
[34]	Attack modeling and detection	FDIA	IEEE standard 14-, 30-, and 118-bus	Interval state forecasting-based countermeasure	Improved modeling and detection of FDIAs.
[35]	Attack Modeling	FDIA	IEEE 14-bus, 30-bus, and 118-bus	NSGAII-based FDIA (NSGAII-FDIA) scheme	Sparse and stealthy FDIA are modeled.
[62]	Power system reliability assessment	FDIA	IEEE 30 bus	GA based risk-averse routing model	System resilience of routing model is better than other techniques.
[43]	Power system reliability assessment	CCPA	IEEE 14, 57, and 118 bus	Three-level CCPA attack is modeled for transmission line cascading failure.	Proposed CCP attack can cause N-1-1 contingency
[63]	Attack detection and mitigation	FDI and DoS	IEEE 39 bus system	Saturation defense method based on an active cut set	Accurate detection and mitigation of attack
[64]	Attack detection	FDIA	IEEE 39 bus	Sliding mode observer	Accurate detection of unknown attacks
[65]	Attack Detection and mitigation	MDIA	IEEE 14-bus and 57-bus	Dynamic time wrapping	Reduce the MDIA threats
[49]	Attack modeling and detection	FDIA	160-node CPPS test	Markov processes	Improved method for attack modeling and detection
[66]	Attack modeling	FDIA	IEEE 14, 39, and 118 bus	AC state estimation based CCPA	Maximize financial loss
[40]	Attack detection	TDA	IEEE 39 bus	Data driven time delay evaluation approach.	Accurate detection of time-delay attacks.
[67]	Attack detection	FDIA	IEEE 14 bus	Dynamic weight ensemble isolation forest algorithm	Improved attack detection accuracy.
[68]	Power system cascading failure modeling	CCPA	IEEE 39 bus	Stochastic modeling technique	Effective approach for evaluating robustness of multistate CPPS.
[69]	Power system vulnerability analysis	FDIA	IEEE 118-bus	Nonlinear optimization model	Developed model successfully overflow single and multiple lines
[20]	Attack detection	Coordinated FDI	IEEE 39 bus and Virtual European Grid	Moving target defense (MTD) strategy	Successfully detected coordinated FDI
[70]	Attack detection	FDIA	IEEE standard 14-, 57- and 118-bus	Multivariate ensemble classification	Successfully detected FDIA
[71]	Detection and mitigation of cyber attacks	FDIA	New England 39-bus system	Multi-agent-based hierarchical detection and mitigation scheme	Successfully detected and mitigated FDIA

[6]	Detection and mitigation of cyber attacks	FDIA	IEEE 118-bus	Mixed-integer linear programming model	Effectively detected and mitigated FDIA
[72]	Attack detection	CIA and RIA	Practical system	Bilateral-information-based cyber-attack identification method	Successfully detected cyber attack
[51]	Co-simulation platform	DDOS and MITM	7-bus system	Real-time co-simulation platform with HIL based on RT-LAB and OPNET	Successfully simulate the proposed approach
[73]	Detection and mitigation of cyber attacks	FDIA	IEEE 14-, 57-, and 118	Classifier development using extreme learning machines.	Successful system restoration
[74]	Power system Vulnerability Analysis	DoS	New England 39 nodes system	Minimum load reduction model	Attack on the cyber layer cause more loss.
[75]	Power system resilience	DoS, FDI	IEEE 57-bus	MILP based optimized algorithm	Successfully improves the system resilience
[76]	Attack detection	FCIA	IEEE 39-bus	Sequential search strategy	Successfully detected attack pattern
[45]	Attacks detection	FDIA	IEEE 39 bus	Adaptive nonparametric cumulative sum detector	Successfully detected attack pattern
[77]	Co-simulation	CCPA	IEEE 9-bus system	State-caching-based synchronization mechanism	The advantages of the proposed platform in terms of simulation accuracy and calculation speed are demonstrated
[78]	Attack detection and mitigation	FDIA	IEEE 30-bus and IEEE 118-bus	Graphical detection techniques	Proposed method can detect FDI attacks accurately
[79]	Attack modeling	FDIA	IEEE 4-bus, 118-bus	Multiple cooperative attacking	Proposed strategy reduces the attack cost.
[80]	Power system resilience	TDA and DoS	IEEE 39 bus	Distributed finite-time frequency control framework	Successfully quantified the cyber physical resilience
[81]	Attack detection	DDIA	IEEE 30, 57, and 118-bus	Dynamic cyberattack model with local network information	proposed solution is capable of anomaly detection.
[41]	Attack detection	TDA	Practical transmission network	Partial spectral discretization	Proposed method reduces the computation time.
[82]	Attack detection	TDA	Practical transmission system	Delayed differential algebraic equations	Accurate detection of time delay attack
[83]	Attack modeling and detection	FDIA	IEEE 14, 30 and 57 bus	Dynamic attack model	Accurate modeling and detection of attack
[84]	Attack detection	FDIA	IEEE 39 bus	Matrix perturbation theory	Accurately track targeted interarea oscillation
[38]	Modeling, detection and mitigation of attack	FDIA	IEEE 14-bus	Two-layer game theoretical attack model	Better understanding of attackers and defenders' behavior
[85]	Power system security assessment	FDIA	IEEE 118 test system	Distributed blockchain-based protection framework	Promising solution for the data security
[86]	Detection of cyber attack	FDIA	IEEE 39 bus	Distributed host-based collaborative detection	Accurate detection of FDIA

III. Major Cyber Attacks on Global Power Systems

Over the years a few cyber-attacks on power grids have been reported. The summary of those cyber-attacks is given in Table II. The Idaho National laboratory conducted a generator test against a cyber-attack in 2007 [1]. For this purpose, a 27-ton, 2.25 MW diesel generator was procured and connected with the substation. A 30 lines computer program rapidly performs out of synchronization switching of the circuit breaker associated with the diesel generator. Consequently, the generator loses its synchronism with the grid and then the generator's engine experienced unusual torque which eventually exploded the generator. This was only a test against cyber-attack, therefore this experiment had no impact on the customers and the quality of electricity supply [1]. In 2010 the US and Israel intelligence agencies attacked the Iran nuclear power plant facilities with a malicious worm named Stuxnet [2]. The Stuxnet was injected in the target facility through an infected USB flash drive which then proliferated to other industrial control processes. It is reported that Stuxnet disrupted approximately one-fifth of the nuclear power plants in Iran. However no major impact on the power system was recorded [2]. In December 2015 the Ukrainian power grid was attacked by a malware which affected almost thirty substations. Overall 225,000 people of three distribution companies lost power for a time period from one to six hours [3]. This is the first publicly acknowledged successful cyberattack on a power grid. The US and Ukrainian intelligence agencies attributed this attempt to a Russian cyber-attack. Approximately one year later, Ukraine power grid was attacked with further advanced cyber-attack on December 17, 2016, resulting in an outage of one transmission substation [3]. Because of this 200 MW of load remain unsupplied for a few hours. In March 2019 the power grid

TABLE II
CYBER PHYSICAL ATTACKS

Ref.	Year	Location	Attack object	Attack type	Impact
[1]	2007	Idaho National Laboratory, USA	Aurora attack manipulated a circuit breaker of a diesel generator	FDIA	Exploded generator
[2]	2010	Iran	Stuxnet worm penetrated the nuclear power plant SCADA system	Malware Injection	At least 14 industrial locations in Iran were infected, including a uranium enrichment plant.
[3]	2015	Ukraine	Attack on the breaker's settings in 3 distribution companies	FDIA	For a few hours, 225 k customers were without service.
[3]	2016	Ukraine	Malware industroyer intrudes into transmission substation control systems	Malware Injection	It amounted to a one-fifth reduction in power use at that time of night. (200 mw load was unaddressed)
[5]	2017	Ireland	Copied all the firmware and files on the compromised routers	MITM	Information of sensitive components was breached
[7]	2019	Power Utilities @ California & Wyoming, USA	Communication network bombarded with network traffic	DoS	For a short time, electrical system operations would be disrupted, but this would not result in a blackout.
[9]	2019	Kudankulam Nuclear Power Plant, Tamil Nadu, India	Virus infected the systems at the power plant	MITM	The infected systems were segregated from the vital internal network, and the rest of the system's functionality was unaffected.
[11]	2020	Mumbai, India	Malware affected safety systems of the power grid	Malware Injection	For a few hours, customers were without service.

operation was interrupted by the distributed DoE attack in the Los Angeles and Salt Lake counties of US [7]. The power delivery to the consumers was not disrupted due to the attack, however, it caused few operational interruptions. These operational interruptions may include computer hacks, data loss, or unexpected errors. The Ireland power grid was targeted by foreign actors through MITM type of cyber-attack in 2017 [5]. The attack was first detected and reported by Vodafone; a company which provides telecommunication services to the Irish grid. The attack on the internet router remained for seven hours and the attackers gained access to all the information that passes through strategical routers. Fortunately, there was no blackout or power interruption reported but authorities are still unclear how much data was compromised because of the attack [5]. In September 2019 the Kudankulam nuclear power plant in India was targeted by a malware attack [9]. According to the investigation report only one personal computer connected with the administrative network through an internet server was targeted. However, no electricity interruption was reported due to this attack. In another incident, the cyber-attack was made on the power grid of Mumbai which is the business hub of India [11]. As per the reports most of the city remained without power for 8 to 10 hours. According to the US based company *Recorded Future* malware was injected by the Chinese attackers. However, the Indian authorities denied these reports and stated that there is no proof that cyber-attack was behind the October 2020 blackout, and it was totally due to human error. Furthermore, China also categorically denied any connection with suspected cyber-attack on the Indian power grid [11].

IV. MAJOR NATURAL AND EXTERNAL PHYSICAL ATTACKS ON GLOBAL POWER SYSTEMS

Over the years, power systems have faced many naturally generated and externally created physical attacks due to various reasons. These physical attacks caused widespread blackouts and huge economic loss. There is no proper list of external physical attacks available in literature and news. However a list of naturally generated physical attacks is available in [12]. The details about some of the prominent natural and external physical attacks are mentioned in Table III. The table clearly demonstrates that each incident affected many people for a long time. The 2003 North American and Canadian power breakdown is the prominent one and most discussed blackout in the history that affected 55 million people, resulted in 11 deaths and an economic loss of $6 billion [12]. For many consumers power returned in three days, however it took 14 days to completely recover the system. The 2012 Indian blackout affected approximately 620 million people (this is the largest number of people affected due to any blackout) for around 2 to 3 days [87]. The blackout started from a breakdown in the northern grid and then proliferated to half of the country [12]. Similarly, the 2023 Pakistan blackout due to naturally generated physical attack affected 230 million people (90% population of country) for one day. The breakdown started because of chronic frequency fluctuations in the southern part of the country that resulted in cascade tripping [12]. Another example of power breakdown because of naturally generated physical attack is the 1999 southern Brazil blackout that affected 97 million people. The breakdown started due to a lightning strike at an electrical substation in Sao Paulo state and then proliferated to the entire power system. The power started returning after 10 hours, however it took 103 days to completely reinstate the entire system [12].

In 2015 Pakistan power system was hit by a massive external physical attack that caused blackout in almost 80% of the country [87]. Terrorist attacked the 220 kV transmission line in Baluchistan province that initiated the cascaded tripping. It took around one day to completely recover the system. Similarly, terrorists attacked the Iran to Iraq transmission line through

explosive device that caused a blackout in one third of Diyala province [88]. In another incident a shooting attack was made at two electrical substations in North Carolina on Dec 5, 2022, that left thousands of people without power for almost 5 days [89].

TABLE III
MAJOR INTERNAL AND EXTERNAL PHYSICAL ATTACKS ON GLOBAL POWER SYSTEMS

Ref	Attack	Location	Year	People Affected (Million)	Time Duration
[12]	Natural	India	2012	620	36 hours
[12]	Natural	Pakistan	2023	230	22 hours
[12]	Natural	Bangladesh	2022	140	10 hours
[12]	Natural	Java	2019	120	8 hours
[12]	Natural	Southern Brazil	1999	97	103 days
[10]	Natural	Canada, USA	2003	55	48 hours
[87]	External	Pakistan	2015	200	1 day
[88]	External	Iran-Iraq	2021	0.54	2 days
[90]	External	North Carolina	2022	0.1	3 days
[89]	External	California	2013		
[91]	External	Washington state	2022	0.014	8 hours

V. DISCUSSION AND RECOMMENDATIONS

Over the years significant advancement has been made in the infrastructure and operation of power systems via integration of modern generation sources and inclusion of latest control and protection technologies. Accurate operation of these technologies may require control signals and measurements of power system components transferred over high-speed communication networks. Although the interaction between power systems physical infrastructure and communication networks (generally known as CPPS) offer numerous benefits, many researchers believe that they may subject to cyber-attacks. Therefore, this concept has been addressed in many studies that assume various attack scenarios and different attack modeling techniques (see Table I). However, if we look at Table II, only a few cyber-attacks are reported against practical power systems. Most of these attacks have not had any significant impact on power system stability. For example, the Idaho national laboratory cyber-attack was confined to a lab experiment. The Stuxnet attack against the nuclear power plants in Iran had no impact on the power system. The cyber-attack against the Irish power system resulted in the stealing some data but no customer lost power. The cyber-attack against power utilities of California and Wyoming caused some interruptions but not a blackout. As mentioned in Table II, until today only three incidents of cyber-attacks have made significant impact on powers systems around the globe. The 2015 cyber-attack against Ukrainian power grid affected about 225 thousand people with the respective social and economic consequences. Similarly, due to another cyber-attack against Ukrainian power grid in 2016 almost 200 MW of load remain unsupplied for few hours. However, one can argue that both Ukrainian attacks are special cases comprising unusually dilapidated infrastructure, a high level of corruption, and exceptional possibilities for Russian infiltration due to the historical links between the two countries [92]. The Ukrainian power grid was built when it was part of the Soviet Union. It has been upgraded with Russian parts and still not been fixed. The Russian attackers are as familiar with the software as insider operators [92]. According to *Recorded Future*, a Massachusetts based cyber security company, the 2020 Mumbai blackout occurred due to malware injected by China. However, this is still not clear as both Indian and Chinese authorities do not admit it as a successful cyber-attack.

A. Comparison of Physical and Cyber Attacks

Globally, power systems have experienced both physical attack and cyber-attacks. Since the development of modern power systems numerous physical attacks occurred on the power grid that resulted in long blackouts and massive financial loss. The details of all the major cyber-attacks on power systems are mentioned in Table II. The information regarding a few prominent physical attacks against the global power systems is mentioned in Table III. The comparison of physical and cyber-attacks in terms of frequency of occurrence, economic and social impact on society reveals that physical attacks are far more dangerous than cyber-attack. For example, the 2003 North American blackout left 50 million people without power for almost two days. It caused a minimum of 11 deaths and an estimated loss of $6 billion. Similarly, the 2012 Indian blackout affected 670 million people (half of country population) for almost one and a half days. The 2023 Pakistan blackout affected 230 million people (90% of country population) for almost 22 hours. The 2022 Bangladesh blackout affected 140 million people (80% of country population) for at least 10 hours. On the other hand, there is merely one example of cyber-attack (2015 Ukraine cyberattack) that affected only 20 substations in the service area of three distribution companies. This demonstrates that, as compared to physical attacks, cyber-attacks on power systems have had negligible economic and societal impacts. Furthermore, physical attacks are easy to initiate and requires less effort as well such as a gun fire at substation transformer or remote transmission line can cause line outage that overloads other lines which are then tripped by protective relays resulting in cascading failure.

B. Why Power Systems are Less Affected by Cyber Attacks?

Cyber security for power systems has recently emerged as a buzz word but it has not significantly affected the power system. Even a few energy security experts have now started to say that although grid assets and utilities are bombarded by cyber-attacks, there is little possibility that attackers will cause an extensive blackout [93]. Most of these attacks are financially motivated and the hackers try to steal the information that grants them financial gains such as credentials of company employees or customers and financial information of company or customers.

Widespread grid breakdown requires in-depth understanding of power systems and expertise in complex attack modeling. This level of expertise may be possessed by a

group backed by some nation or state. The blackout caused by a state backed actor will probably be considered as an act of war and there is a possibility that it will result in electronic or kinetic response or maybe both after the identification of the actors [94].

Power systems are usually designed in such a way that even if the cyber attackers were successful in taking out the largest power generating unit from the grid (for example, 6.8 GW Grand Coulee Dam in Washington) a blackout will not occur [94]. Many modern utilities and ISO's have started installing cyber secure synchrophasor platforms that store the system parameters and measurements on multiple computers. In case of any contingency the least loaded computer offer the fastest response [95]. Furthermore, to reduce such risks, effective preventive, and corrective measures, such as generation redispatch, line switching and load shedding, have been implemented to alleviate the post-contingency overload and prevent false line tripping [96-98]. In general, if these protective measures are properly implemented, the system will remain post-contingency stable and secure.

VI. Conclusion

Power system security is a fundamental concern as power systems around the world are prone to different types of attacks. This paper explained different types of power system attacks and critically discussed the significance of cyber security for power systems i.e., whether it is important or just an idea. Historically, there have been many naturally generated and externally created physical attacks that have occurred on the system. These attacks affected millions of people and caused massive economic loss. On the other hand, merely one authenticated significant cyber-attack (2015 Ukraine cyber-attack) occurred on the system that affected only 20 substations in the service area of three distribution companies. Thus, so far, only one successful attack was carried out and the attackers had substantial inside information. This demonstrates that maybe cyber security is required for the system, but it is not a matter of serious concern. This is because until today the cyber-attacks have not caused any blackout or power breakdown that has significantly impacted the lives of the people.

VII. References

[1] A. GREENBERG. "How 30 Lines of Code Blew Up a 27-Ton Generator." https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/ (accessed.

[2] Gregg-Keizer. "Iran admits Stuxnet worm infected PCs at nuclear reactor." https://www.computerworld.com/article/2749187/iran-admits-stuxnet-worm-infected-pcs-at-nuclear-reactor.html (accessed.

[3] D. P. a. M. WALSTROM. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ (accessed.

[4] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 1, pp. 478-487, 2020.

[5] G. CLULEY. "Attack on Ireland's state-owned power provider blamed on state-sponsored hackers." https://www.bitdefender.com/blog/hotforsecurity/attack-on-irelands-state-owned-power-provider-blamed-on-state-sponsored-hackers/ (accessed.

[6] J. Khazaei, "Cyberattacks with limited network information leading to transmission line overflow in cyber–physical power systems," *Sustainable Energy, Grids and Networks*, vol. 27, p. 100505, 2021.

[7] L. Franceschi-Bicchierai. "A 'Cyber Event' Disrupted the Power Grid in California and Wyoming, But Don't Panic Just Yet." https://www.vice.com/en/article/9kxb85/cyber-event-california-wyoming-utah-dont-panic (accessed.

[8] J. Pagliery. "Sniper attack on California power grid may have been an insider. ." https://money.cnn.com/2015/10/16/technology/sniper-power-grid/ (accessed.

[9] M. Robbins. "Cyberattack Hits Indian Nuclear Plant." https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant (accessed.

[10] J. Barron. "THE BLACKOUT OF 2003: The Overview." https://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html (accessed.

[11] R. Staff. "Mumbai power outage could have been cyber sabotage." https://www.reuters.com/article/us-india-power-china/mumbai-power-outage-could-have-been-cyber-sabotage-says-minister-idUSKCN2AT31Q (accessed.

[12] W. contributors. "List of major power outages." https://en.wikipedia.org/w/index.php?title=List_of_major_power_outages&oldid=1148983637 (accessed.

[13] D. o. Energy, "Electric Disturbance Events (OE-417) Annual Summaries," Department of Energy, Cyber security, Energy security and Emergency response. [Online]. Available: https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

[14] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack Graph Model for Cyber-Physical Power Systems using Hybrid Deep Learning," *IEEE Transactions on Smart Grid*, 2023.

[15] R. V. Yohanandhan *et al.*, "A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid," *International Journal of Electrical Power & Energy Systems*, vol. 136, p. 107720, 2022.

[16] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, 2023.

[17] C. Gavriluta, C. Boudinet, F. Kupzog, A. Gomez-Exposito, and R. Caire, "Cyber-physical framework for emulating distributed control systems in smart grids," *International journal of electrical power & energy systems*, vol. 114, p. 105375, 2020.

[18] P. Yang *et al.*, "Hierarchical multiple time scales cyber-physical modeling of demand-side resources in future electricity market," *International Journal of Electrical Power & Energy Systems*, vol. 133, p. 107184, 2021.

[19] K.-D. Lu and Z.-G. Wu, "Genetic algorithm-based cumulative sum method for jamming attack detection of cyber-physical power systems," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1-10, 2022.

[20] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense against cyber-physical attacks in power grids via game theory," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5244-5257, 2021.

[21] M. Govindarasu and C. Liu, "Cyber physical security testbed for the smart grid: fidelity, scalability, remote access, and federation," in *National CPS Energy Workshop*, 2013.

[22] H. Holm, M. Karresand, A. Vidström, and E. Westring, "A survey of industrial control system testbeds," in *Secure IT Systems: 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19–21, 2015, Proceedings*, 2015: Springer, pp. 11-26.

[23] R. V. Yohanandhan, "Rajvikram Madurai Elavarasan, Premkumar Manoharan, and Lucian Mihet-Popa. 2020. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications," *IEEE Access*, vol. 8, pp. 151019-151064, 2020.

[24] R. Vikhram Yohanandhan and L. Srinivasan, "Decentralised wide-area fractional order damping controller for a large-scale power system," *IET Generation, Transmission & Distribution*, vol. 10, no. 5, pp. 1164-1178, 2016.

[25] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, 2022.

[26] T. Berghout, M. Benbouzid, and S. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *International Journal of Critical Infrastructure Protection*, p. 100547, 2022.

[27] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications*, vol. 209, p. 103540, 2023.

[28] D. An, F. Zhang, F. Cui, and Q. Yang, "Toward Data Integrity Attacks Against Distributed Dynamic State Estimation in Smart Grid," *IEEE Transactions on Automation Science and Engineering*, 2023.

[29] X. Li, Y. Wang, and Z. Lu, "Graph-based detection for false data injection attacks in power grid," *Energy*, vol. 263, p. 125865, 2023.

[30] E. Vincent, M. Korki, M. Seyedmahmoudian, A. Stojcevski, and S. Mekhilef, "Detection of false data injection attacks in cyber–physical systems using graph convolutional network," *Electric Power Systems Research*, vol. 217, p. 109118, 2023.

[31] E. Hallaji, R. Razavi-Far, M. Wang, M. Saif, and B. Fardanesh, "A Stream Learning Approach for Real-Time Identification of False Data Injection Attacks in Cyber-Physical Power Systems," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 17, pp. 3934-3945, 2022.

[32] M. Mohammadpourfard, Y. Weng, A. Khalili, I. Genc, A. Shefaei, and B. Mohammadi-Ivatloo, "Cyber-Physical Attack Conduction and Detection in Decentralized Power Systems," *IEEE Access*, vol. 10, pp. 29277-29286, 2022.

[33] K. Yan, X. Liu, Y. Lu, and F. Qin, "A Cyber-Physical Power System Risk Assessment Model Against Cyberattacks," *IEEE Systems Journal*, 2022.

[34] K.-D. Lu, Z.-G. Wu, and T. Huang, "Differential Evolution-Based Three Stage Dynamic Cyber-Attack of Cyber-Physical Power Systems," *IEEE/ASME Transactions on Mechatronics*, 2022.

[35] K.-D. Lu and Z.-G. Wu, "Multi-Objective False Data Injection Attacks of Cyber–Physical Power Systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 9, pp. 3924-3928, 2022.

[36] H. Liu, X. Chen, L. Huo, Y. Zhang, and C. Niu, "Impact of inter-network assortativity on robustness against cascading failures in cyber–physical power systems," *Reliability Engineering & System Safety*, vol. 217, p. 108068, 2022.

[37] B. Ti, G. Li, M. Zhou, and J. Wang, "Resilience assessment and improvement for cyber-physical power systems under typhoon disasters," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 783-794, 2021.

[38] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 169-177, 2019.

[39] Y. Zhang, L. Wei, W. Fu, X. Chen, and S. Hu, "Secondary frequency control strategy considering DoS attacks for MTDC system," *Electric Power Systems Research*, vol. 214, p. 108888, 2023.

[40] G. Zhang, J. Li, O. Bamisile, D. Cai, and Q. Huang, "A novel data-driven time-delay attack evaluation method for wide-area cyber–physical smart grid systems," *Sustainable Energy, Grids and Networks*, vol. 32, p. 100960, 2022.

[41] Q. Mou, H. Ye, and Y. Liu, "Enabling highly efficient eigen-analysis of large delayed cyber-physical power systems by partial spectral discretization," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1499-1508, 2019.

[42] N. Aljohani *et al.*, "Cross-Layered Cyber-Physical Power System State Estimation towards a Secure Grid Operation," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, 2022: IEEE, pp. 1-5.

[43] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, "Revealing vulnerability of n-1 secure power systems to coordinated cyber-physical attacks," *IEEE Transactions on Power Systems*, 2022.

[44] W. Bi, K. Zhang, Y. Li, K. Yuan, and Y. Wang, "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2859-2868, 2019.

[45] T. Zhou, K. Xiahou, L. Zhang, and Q. Wu, "Real-time detection of cyber-physical false data injection attacks on power systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 6810-6819, 2020.

[46] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420-2430, 2017.

[47] M. Gholami, A. Gholami, and M. Mohammadtaheri, "Cyber-physical power system reliability assessment considering multi-state independent components," *Electric Power Systems Research*, vol. 217, p. 109141, 2023.

[48] A. Rostami, M. Mohammadi, and H. Karimipour, "Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities," *International Journal of Electrical Power & Energy Systems*, vol. 147, p. 108892, 2023.

[49] B. Qin, D. Liu, and G. Chen, "Formal modeling and analysis of cyber-physical cross-space attacks in power grid," *International Journal of Electrical Power & Energy Systems*, vol. 141, p. 107790, 2022.

[50] S. Talukder, M. Ibrahim, and R. Kumar, "Resilience indices for power/cyberphysical systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 4, pp. 2159-2172, 2020.

[51] Z. Liu, Q. Wang, and Y. Tang, "Design of a cosimulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems," *IEEE Access*, vol. 8, pp. 95997-96005, 2020.

[52] M. Mccarty *et al.*, "Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment," *IEEE Access*, vol. 11, pp. 15297-15313, 2023.

[53] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1-33, 2011.

[54] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 720-729, 2015.

[55] S. Pazouki and A. Asrari, "Attacking Energy Hubs via Manipulating Demand Response Program," in *2021 IEEE PES/IAS PowerAfrica*, 2021: IEEE, pp. 1-5.

[56] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1592-1602, 2016.

[57] M. Du, X. Liu, Z. Li, and H. Lin, "Robust Mitigation Strategy against Dummy Data Attacks in Power Systems," *IEEE Transactions on Smart Grid*, 2023.

[58] H. Tu, F. Gu, X. Zhang, and Y. Xia, "Robustness analysis of power system under sequential attacks with incomplete information," *Reliability Engineering & System Safety*, vol. 232, p. 109048, 2023.

[59] A. Jafari, H. Ergun, and D. Van Hertem, "A Voting-Based Machine Learning Strategy to Detect False Data Injection Attack in Cyber-Physical Power Systems," in *2022 57th International Universities Power Engineering Conference (UPEC)*, 2022: IEEE, pp. 1-6.

[60] B. Hu, C. Zhou, Y.-C. Tian, X. Du, and X. Hu, "Attack Intention Oriented Dynamic Risk Propagation of Cyberattacks on Cyber-Physical Power Systems," *IEEE Transactions on Industrial Informatics*, 2022.

[61] H. Goyel and K. S. Swarup, "Data integrity attack detection using ensemble based learning for cyber physical power systems," *IEEE Transactions on Smart Grid*, 2022.

[62] B. Ti, J. Wang, G. Li, and M. Zhou, "Operational risk-averse routing optimization for cyber-physical power systems," *CSEE Journal of Power and Energy Systems*, vol. 8, no. 3, pp. 801-811, 2022.

[63] T. Yang, S. Cai, P. Yan, W. Li, and A. Y. Zomaya, "Saturation defense method of a power cyber-physical system based on active cut set," *IEEE Transactions on Smart Grid*, 2022.

[64] M. Adeli, M. Hajatipour, M. J. Yazdanpanah, H. Hashemi-Dezaki, and M. Shafieirad, "Optimized cyber-attack detection method of power systems using sliding mode observer," *Electric Power Systems Research*, vol. 205, p. 107745, 2022.

[65] X. Liu, P. Chang, Z. Wu, M. Jiang, and Q. Sun, "Malicious data injection attacks risk mitigation strategy of cyber–physical power system based on hybrid measurements attack detection and risk propagation," *International Journal of Electrical Power & Energy Systems*, vol. 142, p. 108241, 2022.

[66] P. K. Jena, S. Ghosh, E. Koley, D. K. Mohanta, and I. Kamwa, "Design of AC state estimation based cyber-physical attack for disrupting electricity market operation under limited sensor information," *Electric Power Systems Research*, vol. 205, p. 107732, 2022.

[67] Z. Wu, Q. Wang, X. Cai, J. Dai, X. Liu, and Q. Tian, "Methods of anomaly state detection for power systems based on bilateral cyber-physical information," *IET Generation, Transmission & Distribution*, vol. 16, no. 7, pp. 1449-1459, 2022.

[68] G. Wu, M. Li, and Z. S. Li, "A stochastic modeling approach for cascading failures in cyberphysical power systems," *IEEE Systems Journal*, vol. 16, no. 1, pp. 723-734, 2021.

[69] J. Khazaei, M. Alkaf, and J. Zhao, "Convex Optimization of Cyberattacks Overflowing Multiple Lines in Cyber-Physical Power Systems," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5224-5233, 2021.

[70] Y. Li *et al.*, "Intrusion detection of cyber physical energy system based on multivariate ensemble classification," *Energy*, vol. 218, p. 119505, 2021.

[71] T. Zhou, K. Xiahou, L. Zhang, and Q. Wu, "Multi-agent-based hierarchical detection and mitigation of cyber attacks in power systems,"

International Journal of Electrical Power & Energy Systems, vol. 125, p. 106516, 2021.
[72] Q. Wang, X. Cai, Y. Tang, and M. Ni, "Methods of cyber-attack identification for power systems based on bilateral cyber-physical information," *International Journal of Electrical Power & Energy Systems*, vol. 125, p. 106515, 2021.
[73] T. Wu *et al.*, "Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1892-1904, 2020.
[74] H. Pan, H. Lian, C. Na, and X. Li, "Modeling and vulnerability analysis of cyber-physical power systems based on community theory," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3938-3948, 2020.
[75] S. N. Edib, Y. Lin, V. M. Vokkarane, F. Qiu, R. Yao, and D. Zhao, "Optimal PMU restoration for power system observability recovery after massive attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1565-1576, 2020.
[76] Z. Zhang, S. Huang, F. Liu, and S. Mei, "Pattern analysis of topological attacks in cyber-physical power systems considering cascading outages," *IEEE Access*, vol. 8, pp. 134257-134267, 2020.
[77] Q. Wang, Z. Liu, and Y. Tang, "SCCO: a state-caching-based coagulation platform for cybor-physical power system evaluation," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1615-1625, 2020.
[78] Y. Li and Y. Wang, "Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system," *Journal of systems architecture*, vol. 105, p. 101705, 2020.
[79] J. Yan, F. Guo, and C. Wen, "False data injection against state estimation in power systems with multiple cooperative attackers," *ISA transactions*, vol. 101, pp. 225-233, 2020.
[80] Z. Wang and J. Wang, "A practical distributed finite-time control scheme for power system transient stability," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 3320-3331, 2019.
[81] H. Wang *et al.*, "Dynamic data injection attack detection of cyber physical power systems with uncertainties," *IEEE Transactions on Industrial informatics*, vol. 15, no. 10, pp. 5505-5518, 2019.
[82] H. Ye, K. Liu, Q. Mou, and Y. Liu, "Modeling and formulation of delayed cyber-physical power system for small-signal stability analysis and control," *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 2419-2432, 2019.
[83] H. Wang, A. Meng, Y. Liu, X. Fu, and G. Cao, "Unscented Kalman Filter based interval state estimation of cyber physical energy system for detection of dynamic attack," *Energy*, vol. 188, p. 116036, 2019.
[84] Q. Mou, H. Ye, Y. Liu, and L. Gao, "Applications of matrix perturbation theory to delayed cyber-physical power system," *International Journal of Electrical Power & Energy Systems*, vol. 107, pp. 507-515, 2019.
[85] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162-3173, 2018.
[86] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 32-41, 2017.
[87] I. G. S. Baloch. "Attack on power lines in Balochistan causes nationwide blackout." https://tribune.com.pk/story/827139/parts-of-punjab-sindh-balochistan-left-without-power-after-guddu/ (accessed.
[88] G. Media. "IRAQ...AN ATTACK CUTS THE ELECTRICITY TRANSMISSION LINE FROM IRAN." https://www.gulanmedia.com/en/story/262084/iraq...an-attack-that-cuts-the-electricity-transmission-line-from-iran (accessed.
[89] M. Memmott. "Sniper Attack On Calif. Power Station Raises Terrorism Fears." https://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears (accessed.
[90] F. Morris. "North Carolina attacks highlight the vulnerability of power grids." https://www.npr.org/2022/12/09/1141937948/north-carolina-attacks-highlight-the-vulnerability-of-power-grids (accessed.
[91] A. Press. "Vandalism at 3 Washington state electric substations cuts power." https://www.pbs.org/newshour/nation/vandalism-at-3-washington-state-electric-substations-cuts-power (accessed.
[92] R. M. L. M. J. A. T. Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case." https://www.sans.org/webcasts/analyzing-ukrainian-power-grid-cyber-attacks-102007/ (accessed.
[93] R. Walton. "Sophisticated hackers couldcrash the US power grid, butmoney, not sabotage, is theirfocus." https://www.utilitydive.com/news/sophisticated-hackers-could-crash-the-us-power-grid-but-money-not-sabotag/603764/#:~:text=Deep%20Dive-,Sophisticated%20hackers%20could%20crash%20the%20US%20power%20grid%2C%20but%20money,and%20Preparedness%20Scott%20Aaronson%20said. (accessed.
[94] R. Walton. "Sophisticated hackers could crash the US power grid, but money, not sabotage, is their focus." https://www.utilitydive.com/news/sophisticated-hackers-could-crash-the-us-power-grid-but-money-not-sabotag/603764/ (accessed.
[95] L. OSIsoft, "Redundancy and Reliability of Wide-Area Measurement Synchrophasor Archivers."
[96] Y. Wang, L. Huang, M. Shahidehpour, L. L. Lai, H. Yuan, and F. Y. Xu, "Resilience-constrained hourly unit commitment in electricity grids," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5604-5614, 2018.
[97] X. Zhang, Y. Liu, H. Gao, L. Wang, and J. Liu, "A bi-level corrective line switching model for urban power grid congestion mitigation," *IEEE Transactions on Power Systems*, vol. 35, no. 4, pp. 2959-2970, 2019.
[98] Y. Wang, L. Huang, M. Shahidehpour, L. L. Lai, and Y. Zhou, "Impact of cascading and common-cause outages on resilience-constrained optimal economic operation of power systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 590-601, 2019.

VIII. Biographies

Muhammad Faisal Nadeem Khan (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from Air University, Islamabad, Pakistan, and the M.Sc. and Ph.D. degree in electrical engineering from the University of Engineering and Technology, Taxila, Pakistan, in 2012 and 2019 respectively. He has held several academic positions in Pakistan and is an Associate Professor of electric power systems at Department of Electrical Engineering, University of Engineering and Technology, Taxila, Pakistan. He is currently a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, New York University, New York, NY, USA. He has authored or coauthored more than 50 refereed journals and conference papers. His research interests include power system resilience assessment, DER integration with power systems and smart grids.

Francisco de León (S'86 - M'92 - SM'02 - F'15) received the B.Sc. and M.Sc. (Hons.) degrees in electrical engineering from National Polytechnic Institute, Mexico City, Mexico, in 1983 and 1986, respectively, and the Ph.D. degree in electrical engineering from the University of Toronto, Toronto, ON, Canada, in 1992. He has held several academic positions in Mexico and has worked for the Canadian Electric Industry. He is currently a Professor with the Department of Electrical and Computer Engineering, New York University, New York, NY, USA. His research interests include the analysis of power phenomena under non-sinusoidal conditions, the transient and steady-state analyses of power systems, the thermal rating of cables and transformers, and the calculation of electromagnetic fields applied to machine design and modeling. Prof. de León is currently (2020-2025) the Editor-in-Chief of the IEEE Transactions on Power Delivery