CONTRIBUTED PAPER

Toward Resilient Modern Power Systems: From Single-Domain to Cross-Domain Resilience Enhancement

This article presents a systematic review of power system resilience enhancement techniques that aim to harden the infrastructure and proactively defend against threats.

By Hao Huang, *Member IEEE*, H. Vincent Poor, *Life Fellow IEEE*, Katherine R. Davis, *Senior Member IEEE*, Thomas J. Overbye, *Fellow IEEE*, Astrid Layton, *Member IEEE*, Ana E. Goulart, *Member IEEE*, and Saman Zonouz, *Member IEEE*

ABSTRACT | Modern power systems are the backbone of our society, supplying electric energy for daily activities. With the integration of communication networks and high penetration of renewable energy sources (RESs), modern power systems have evolved into a cross-domain multilayer complex system of systems with improved efficiency, controllability, and sustainability. However, increasing numbers of unexpected events, including natural disasters, extreme weather, and cyberattacks, are compromising the functionality of modern power systems and causing tremendous societal and economic losses. *Resilience*, a desirable property, is needed in modern power systems to ensure their capability to withstand all kinds of hazards while maintaining their functions. This article presents a systematic review of recent power system resilience enhancement techniques and proposes new directions for enhancing modern power systems' resilience considering their *cross-domain multilayer* features. We first answer the question, "what is power system resilience?" from the perspectives of its definition, constituents, and categorization. It is important to recognize that power system resilience depends on two interdependent factors: *network design* and *system operation*. Following that, we present a review of articles published since 2016 that have developed innovative methodologies to improve power system resilience and categorize them into *infrastructural resilience enhancement* and *operational resilience enhancement*. We discuss their problem formulations and proposed quantifiable resilience measures, as well as point out their merits and limitations. Finally, we argue that it is paramount to leverage higher order subgraph studies and scientific machine learning (SciML) for modern power systems to capture the interdependence and interactions across heterogeneous networks and data for holistically enhancing their infrastructural and operational resilience.

Manuscript received 7 June 2023; revised 18 November 2023 and 8 April 2024; accepted 17 May 2024. Date of current version 14 June 2024. This work was supported in part by the National Science Foundation under Grant 1916142, Grant 2039716, Grant 2220347, and Grant 2231651; in part by the C3.ai Digital Transformation Institute; in part by the U.S. Department of Energy under Award DE-OE0000895 and Award DE-CR0000018; in part by the School of Engineering and Applied Science (SEAS), Princeton University; in part by the Andlinger Center for Energy and the Environment, Princeton University; and in part by Texas A&M Engineering Experiment Station (TEES) Smart Grid Center. *(Corresponding author: Hao Huang.)*

Hao Huang and **H. Vincent Poor** are with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: hh6219@princeton.edu).

Katherine R. Davis and **Thomas J. Overbye** are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA.

Astrid Layton is with the J. Mike Walker' 66 Department of Mechanical Engineering, Texas A&M University, College Station, TX 77843 USA.

Ana E. Goulart is with the Department of Engineering Technology and Industrial Distribution, Texas A&M University, College Station, TX 77843 USA.

Saman Zonouz is with the School of Cybersecurity and Privacy (SCP) and the School of Electrical and Computer Engineering (ECE), Georgia Institute of Technology, Atlanta, GA 30332 USA.

Digital Object Identifier 10.1109/JPROC.2024.3405709

KEYWORDS | Enhancing resilience; higher order subgraph analyses; modern power systems; power system resilience; scientific machine learning (SciML).

I. INTRODUCTION

Power systems are the backbone of modern society as they generate, transfer, and deliver electric energy from different energy resources to end users. With more than a century of development, modern power systems are evolving into a wide-area weather-dependent c-physical complex system of systems. Their modern configurations are more efficient and flexible and have better economic allocation of energy resources than their predecessors. Their interactions exist among different sectors of generation, transmission, distribution, and customers. The increasing penetration of renewable energy sources (RESs), including solar and wind energy, is changing traditional grid configurations in the quest to reduce the emission of greenhouse gases and create a cleaner and more sustainable environment [1], [2]. Leveraging these benefits, power systems, including the distribution networks and microgrids (MGs), have been increasingly integrated with other energy infrastructures, including thermal and gas networks. This integration turns power systems into multienergy systems that help better manage energy sources, contributing to the development of decarbonized and sustainable energy ecosystems [3]. All these benefits are owed in part to the digitalization of power systems with the integration of communication networks. Operational power system data can be more efficiently transferred over wide areas, improving operators' understanding and control for security and economics. It also gives end users the ability to schedule their energy consumption according to weather and price. These data have also enabled recent advancements in distributed automatic control algorithms and machine learning techniques that control local devices more efficiently and reliably. As a result, modern power systems have evolved into a cross-domain multilayer complex system of systems with heterogeneous networks and data from physical, cyber, weather, and societal domains.

New threats come with new technologies and development. As a cyber–physical system, the resilience and security of power systems are threatened by natural disasters [4], cyberattacks [5], mis-operations [6], geomagnetic disturbances [7], and even high-altitude electromagnetic pulses (HEMPs) [8], [9]. The widespread presence of power networks exposes them to natural disasters, such as hurricanes, earthquakes, and floods. The increasing frequency of extreme weather events is disrupting the energy supply, thereby jeopardizing the economy and putting public health and safety in danger, which can devastate affected communities [10]. Furthermore, the power grid is aging, becoming increasingly susceptible to threats that lead to infrastructure damage and blackouts for end users [4], [11]. The integration of RESs can impact the grid's voltage and frequency stability, causing power quality issues [12]. Meanwhile, the intermittency of RESs introduces further uncertainties to power system operation [13], [14]. The increasing reliance on communication networks also introduces cyber threats to the security and reliability of power system operations. Examples can be found from [15], [16], and [17], demonstrating that adversaries can exploit the vulnerabilities in communication networks to obtain the control of power systems and create disturbances. Other threats, including energy theft [18] and false data injections (FDIs) [5], can compromise the situational awareness and reliability of the system. Overall, there is a pressing need to enhance power systems' resilience to ensure their security, reliability, and functionality of consistently supplying electric energy, particularly in light of the increasing prevalence of unexpected disturbances across different domains.

This article presents a systematic review of power system resilience enhancement techniques that aim to harden the infrastructure and proactively defend against threats. Unlike existing works that primarily review resilience enhancements in the physical domain, namely the functionality and resilience of transmission, distribution, and generation systems, our aim is to broaden the perspective on modern power systems, considering their interconnected cross-domain multilayered architecture encompassing physical, cyber, weather, and human networks. We select articles published since 2016 that have developed innovative methodologies to provide a timely review, and we discuss their merits and limitations regarding problem formulation and quantifiable resilience measures. As modern power systems have evolved into a *cross-domain multilayer complex system of systems*, it is essential to consider the interdependence and interactions across heterogeneous networks and data to holistically enhance the system's inherent resilience. Doing so, let us operators and stakeholders holistically design and operate modern power systems with improved resilience against increasing unexpected events from physical, cyber, weather, and societal domains. However, there is a lack of consensus on how to holistically analyze these interconnected heterogeneous networks, characterize their interdependence and interactions regarding their network structures and data, and enhance modern power systems' inherent resilience. In order to address these issues, we propose new directions of using higher order subgraph analyses and scientific machine learning (SciML) for enhancing modern power system resilience. The main contributions of this article include the following.

1) We present data on the U.S. electric disturbance events from 2011 to 2022, including the annual number of events, loss of load, and affected customers. By categorizing these events into *natural disasters*, *physical attacks*, *system issues*, and *cyber/suspicious events*, we observe that natural disasters are the most disastrous factors compromising power grids, while cyberattacks are emerging threats that directly affect customers. These facts call for a holistic approach to enhancing the resilience and security of modern power systems, considering the interdependence and

interactions across different networks from cyber, physical, weather, and societal domains.

2) By answering the question, "what is power system resilience?", from the perspectives of its definition, constituents, and enhancement categorization, we argue that it is important to recognize that infrastructural resilience lays the foundation for operational resilience, and operational resilience guides the hardening of infrastructural resilience. These two aspects of power system resilience are interdependent and mutually promote the development and enhancement on each other. In particular, it is essential to value the compounded impact across interconnected heterogeneous networks from physical, cyber, weather, and human domains to enhance both infrastructural and operational resilience for modern power systems.
3) We present a comprehensive review of articles that have developed innovative methodologies to enhance power system resilience. We categorize the reviewed articles into infrastructural resilience enhancements and operational resilience enhancements and classify their contribution to resilience enhancement at different phases. We also discuss their merits regarding their problem formulations and proposed quantifiable resilience measures as well as the gap between research and realization.
4) In order to enhance modern power systems' inherent resilience, it is essential to consider their cross-domain multilayered architectures. We believe that it is significant to incorporate heterogeneous networks and data across physical, cyber, weather, and human domains to develop holistic criterion and approaches. It is necessary to emphasize the value of heterogeneity in physical, cyber, and social networks along with granular modeling to derive new standards and requirements for designing and operating modern power systems.
5) We propose two new research directions: higher order subgraph analyses and SciML, to understand the interdependence and interactions across different networks and data, facilitating trustworthy decision-making to enhance the inherent resilience of modern power systems. This article includes preliminary case studies using higher order subgraph analyses to disclose key local structures contributing to power networks' resilience as well as to identify critical connections in cyber–physical power networks. In addition, we also propose a SciML-based framework to process large amounts of heterogeneous data across different networks and provide explainable and trustworthy decision-making for system operations.

This article is organized as follows. Section II analyzes 12-year data of U.S. power grid disturbances. Section III discusses the definition, constituents, and enhancement categorization of power system resilience. Sections IV and V review enhancement techniques on infrastructural resilience and operational resilience at different phases regarding the development of disturbances on power systems, respectively. Section VI discusses the merits and limitations of reviewed approaches regarding their problem formulation and proposed quantifiable resilience measures. Section VII presents new opportunities to enhance modern power systems resilience considering heterogeneous networks and data. Section VIII concludes this article.

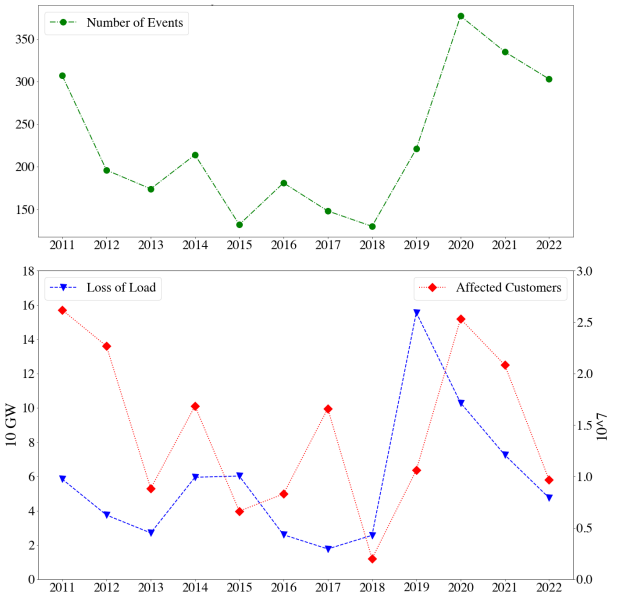


Fig. 1. ***Annual U.S. power grid events, loss of load, and affected customers (2011–2022) [19].***

II. 2011–2022 U.S. POWER GRIDS EVENTS

The data on the U.S. electric disturbance events (Form DOE-417)[1] is available in [19], which provides valuable insights into the reliability and resilience of the country's power systems. With a 12-year dataset spanning 2011 to 2022, Fig. 1 shows the annual statistics of grid events, loss of load, and affected customers in the U.S. power systems. Notably, from 2011 to 2018, there was a decreasing trend of reported grid events and associated loss of load, although the number of affected customers fluctuated. However, from 2019 to 2020, there was a dramatic increase in grid events, loss of load, and affected customers, due to several unexpected extreme events, including hurricane, floods, and wildfire [20], [21]. Stakeholders and operators learned valuable lessons from these events, resulting in improvements in the system's performance in the past two years. Nevertheless, despite these improvements, the overall condition of the U.S. power grid appears to be worse than in the earlier years of this decade.

We have categorized the events into four groups: *natural disasters*, *physical attacks*, *system issues*, and

[1]The Electric Emergency Incident and Disturbance Report (Form DOE-417) collects information on electric incidents and emergencies.

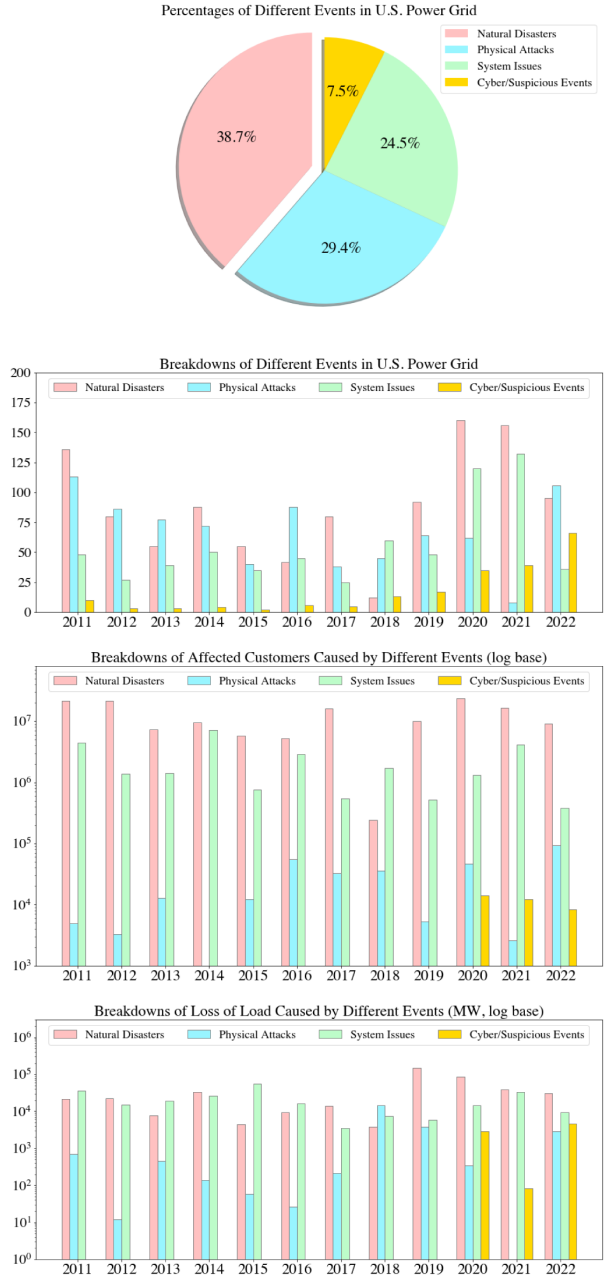


Fig. 2. ***U.S. power grid events distribution (2011–2022) [19].***

cyber/suspicious events based on the events' description. *Natural disasters* include all events such as severe weather, flood, storm, extreme temperature, and earthquake; *physical attacks* include all vandalism, sabotage, and attacks on physical network; *system issues* include all disturbances on physical systems, such as physical faults, energy deficiency, equipment failure, relay mis-configuration, and mis-operations; and *cyber/suspicious events* include all suspicious activities on communication networks and unidentified activities. Fig. 2 provides the percentages of each type of disturbance with respect to all grid events and the breakdowns of all grid events based on these categories for a number of events, a number of affected customers, and the amount of loss of load.

It can be seen that *natural disasters* have happened the most, accounting for 38.7% of all events, followed by *physical attacks* (29.4%) and *system issues* (24.5%). *Cyber/suspicious events* only account for 7.5% of all events. *Natural disasters* and *physical attacks* are responsible for most power grid disturbances and outages because they directly compromise the system's functionality and are easy to be caught and reported. *System issues* are mainly because of insufficient situational awareness for system planning, operation, and protective relay configuration. *Cyber/suspicious events* are less frequent than other types of disturbances due to the following reasons. On the one hand, cyberattacks do not directly compromise physical system operations, and cyber threats can remain dormant until triggered and inflict whatever physical impact on the system might be. On the other hand, communication networks have the mechanism to detect and defend cyber threats to avoid compromise of the physical system, and only the sophisticated threats that bypass intrusion detection systems have the capability of interrupting the system's operation and compromising power systems' security and resilience. However, the annual statistics for each category exhibit an urgent need to protect power systems against cyberattacks. The annual number of *cyber/suspicious events* has increased from 5 to 66 since 2017. Meanwhile, these events have been reported as the cause for compromising power systems' operation and resulting in loss of load from 2020 to 2022 but were not reported or identified as the cause before those dates. At the same time, the number of *system issues* has also increased. It is plausible that more cyberattacks happened in power systems recently, and they compromised the system with insufficient situational awareness, leading to system issues, such as mis-operations and misconfigurations on industry controllers. While discovering the true cause of *system issues* is not the objective of this work, we emphasize the importance of identifying the *real* cause of system disturbances and the need for designing resilient cyber and physical networks for secure and resilient modern power systems. It is of great interest to understand the underlying relationship of interdependence and interactions across different domains in modern power systems for sustainable and resilient electricity service [22].

In addition to the U.S. power outages, the studies in [23], [24], [25], and [26] also document historical worldwide major blackouts and analyze their sources and impacts. Overall, there are increasing contingencies in both cyber and physical domains that threaten the security and resilience of power systems.

The U.S. National Academies' grid resilience report specifically calls for enhanced power system abilities to prepare for, endure, and recover from severe hazards [27]. Such abilities are recognized as the nature of *resilience* [28]. Even though there are various procedures and guidelines for power systems operation [29], the abruptness of unexpected contingencies is hard to predict, especially considering cyber events and cascading failures [30].

In addition, modern power and energy systems have integrated more RES to address the increasingly severe climate crisis. This integration of RES necessitates the incorporation of climate, weather, and energy system models to support infrastructure planning, real-time operation, and recovery toward climate-resilient power systems [31]. It is important to acknowledge that there is no way to make power systems completely invulnerable to physical or cyber disruptions and to the effects of extreme weather events [22]. In order to ensure the security and resilience of power systems, it is crucial to minimize (if not eliminate) the feasibility and impact of threats [32].

III. WHAT IS POWER SYSTEM RESILIENCE?

A. Definition of Power System Resilience

The word *resilience* originates from the Latin word "resiliere," which means to "bounce back." In the scientific arena, this meaning of *resilience* can date back to the 1970s, where Holling [33] defined *resilience* in ecology as a measure of the ability to absorb changes of variables and parameters in systems. The common use of resilience is to imply the ability of an entity or system to return to normal condition after the occurrence of an event that disrupts its state. It is a general concept that has multiple dimensions and definitions in different specialized fields such as psychology, economics, biology, and engineering [34].

For power systems, different authorities have provided their definitions of resilience. Both the National Infrastructure Advisory Council (NIAC) and North America Electric Reliability Corporation (NERC) view power system resilience as preparing and planning, absorbing, recovering, and adapting to adverse events [35], [36]. The U.K. Energy Research Center (UKERC) has defined resilience as "the capability of an energy system to tolerate disturbance and to continue to deliver affordable energy service to consumers" [37]. The U.S. Power Systems Engineering Research Center (PSERC) has recognized resilience as a system's capability to gradually deteriorate under increasing exertion and rapidly recover to its previous secure status [7], [38]. The Electric Power Research Institute (EPRI) has defined power system resilience with three elements: prevention, recovery, and survivability with respect to the development of disruptions [39]. The U.S. National Association of Regulatory Utility Commissioners (NARUC) has described resilience in terms of robustness and recovery characteristics of the power system during and after disasters [39]. The U.S. Presidential Policy Directives-21 (PPD-21) has defined resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [40]. As a cyber–physical system, the U.S. Department of Energy (DOE) has defined power system cyber–physical resilience as the ability to avoid or withstand grid stress events without suffering operational compromise or to adapt to and compensate for the resultant strains so as to minimize compromise via graceful degradation [41].

Based on the above definitions, it is evident that the key characteristic that describes power system resilience is its ability to anticipate, absorb, and recover from external disruptions, especially with respect to the high-impact low-frequent (HILF) events in power systems. To be more specific, the *anticipation* refers to the system's ability to avert any deterioration from the disturbances, the *absorption* is the system's ability to tolerate the disturbances and minimize deterioration, and the *recovery* is the system's ability to restore the compromised system. As power systems evolve into smart grids, another essential ability that should also be included is learning from past lessons. The system should have the *adaptability* of enhancing its resilience from previous events with improved capabilities.

B. Quantifying Power System Resilience

Conventionally, power systems are evaluated by four main reliability measures, including system average interruption duration index (SAIDI), system average interruption frequency index (SAIFI), customer average interruption duration index (CAIDI), and momentary average interruption frequency index (MAIFI), based on historical data and report. They can generally represent how reliable the system is and provide instructive guidance for investment on strengthening power systems architectures. While reliability is one quantifiable aspect of power system resilience using the above measures, resilience is different from reliability. Reliability is evaluated under low-impact high probability events, which have limited impact on the whole system in a short period. Resilience is investigated with HILF events, which have large and long-term consequences [42]. Quantifying power system resilience necessitates the consideration of power system's cross-domain multilayer architectures surrounding cyber, physical, weather, and human factors. As a spatial–temporal property of the system, it is necessary to evaluate how HILF events could impact the status of power systems and the response or countermeasures that stakeholders take against those events, especially under unexpected events such as cyberattacks and extreme weather. It is of great significance to quantify power system resilience through a cross-domain multilayer perspective with the consideration of compounded impacts from other external influences to system functionality either qualitatively or quantitatively.

The resilience trapezoid is widely used in existing articles to describe, quantify, and demonstrate resilience for power systems [43], [44], [45], [46], [47], [48], [49]. This graphical representation can effectively associate the spatiotemporal development of hazards with power systems' performance against corresponding hazards regardless of the disturbances' sources or causes. Fig. 3 shows a time-variant power system resilience transition when a disruptive event compromises the system. As an inherent property, the initial resilience level (R_{initial}) is assumed to be the optimal resilience level, *which depends on the network structure and operation schemes*. Once the disruptive

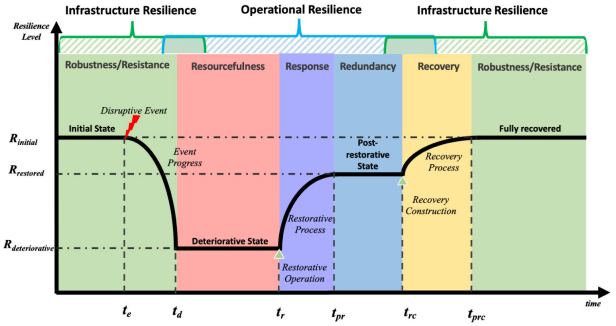


Fig. 3. ***Power system trapezoid resilience curve with a disruptive event.***

event happens at t_e, the infrastructure is compromised. Adaptive actions are taken to maximally maintain the system's integrity. The adverse impact will deteriorate the resilience level to $R_{\text{deteriorative}}$ until the system reaches equilibrium at t_d. As to how much the reduction of the resilience level is, it depends on the system's inherent ability to absorb disturbances and function securely. Such ability comes from the system's structure and adaptive actions. When the system is stable at $R_{\text{deteriorative}}$ and enough information is collected, operators can start restoring the system at t_r. Once the restorative process is done, the system is in a more resilient state (R_{restored}) at t_{pr}. If the infrastructure is not damaged by the event, R_{restored} should be R_{initial}. Otherwise, the network structure will be evaluated and operators need to decide how to reconstruct the infrastructure. Extra time (from t_{rc} to t_{prc}) will be spent on the recovery process to strengthen the system's resilience level to R_{initial} or even a more resilient state.

At different phases of resilience transition depicted in Fig. 3, five characteristics dominate the property of resilience in power systems, which are *robustness/resistance*, *resourcefulness*, *response*, *redundancy*, and *recovery*. *Robustness/resistance* represents power systems' inherent ability to absorb disturbances and function securely without human intervention, referring to the ability of a power system to absorb a shock and continue to operate. It relies on the system's infrastructure and operation schemes on *physical* networks. *Resourcefulness* is the ability of power systems to skillfully manage a crisis as it occurs, showing how fast the information and data of the system can be transferred to operators and stakeholders for decision-making. It relies on the infrastructure and operation on *cyber* networks. How the *cyber* resources are allocated and how the information and data are managed are critical. *Response* is how the operators and/or energy management systems (EMSs) decide the remedial actions to relieve the system's stress in a timely manner. It heavily depends on the information collected and the knowledge of the physical system. *Redundancy* depends on the design of the system. For instance, when contingencies happen, the extra generation reserve can ensure the energy supply and the redundant branches can provide backup pathways for supplying electric energy. With more investment on redundancy, the system can be more resilient. *Recovery* is to completely recover the system from the damage to its initial state. It involves the activities on infrastructure construction and system operation.

From the above discussion, we can say that *power system resilience* consists of *infrastructural resilience* and *operational resilience*, both of which depend on how the infrastructure is designed and how the system is operated [50]. These two aspects overlap in the contexts of *robustness/resistance*, *resourcefulness*, *redundancy*, and *recovery*. Such characteristics determine the level of resilience at each stage as they depend on both the infrastructural architectures and operation schemes. Even though *response* mainly falls within operational resilience as it involves remedial operation, the decisions made by operators are based on the information collected through *cyber* networks and the understanding of *physical* networks. Thus, there is underlying influence of infrastructural resilience on *response*.

Generally speaking, power system resilience is a *spatial–temporal* measure that depends on its infrastructure, operation schemes, and surrounding environment (normal and adversarial). Infrastructural resilience represents the power system's inherent ability of absorbing and tolerating disturbances, while operational resilience represents how human-made decisions can ensure the system's resilience during normal situations and efficiently and effectively defend and restore the system back to the original resilient state during and after adversarial situations. There is a mutual influence between infrastructure resilience and operational resilience.

C. Power System Resilience Enhancements

As presented in Fig. 3, there are different phases of power system resilience that correspond to the progression of an event. Thus, different resilience enhancement techniques can be applied to specific stages, to improve the system's robustness, ensure that the system does not degrade too much or at all when disruptive events happen, or accelerate the response so that the system can more efficiently and securely restore the energy supply. Infrastructure resilience, namely the cyber and physical network design, lays the foundation for normal and contingency operations. Operational resilience can identify weaknesses in infrastructure resilience and provide guidance for enhancement, such as adding redundancy or improving security on components. Fig. 4 presents a guideline for power system resilience enhancements at different phases, from perspectives of *network construction* and *proactive actions* [51], corresponding to *infrastructural resilience* and *operational resilience*.

The proactive actions are *short-term* operations to enhance power systems' reliability and security against events. Meanwhile, network construction refers to *long-term* planning approaches that improve power systems'

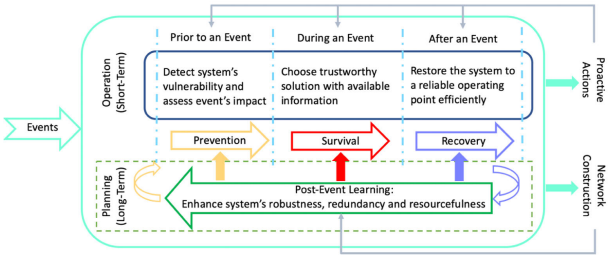


Fig. 4. ***Power system resilience enhancement at different stages, adopted from [51].***

inherent ability to absorb disturbances and maintain functionality securely. Prior to an event, the detection of a system's vulnerability and the assessment of the event's impact can help operators better allocate resources to prevent the system from experiencing unexpected contingencies or minimize their adverse impact. When threats interrupt power systems' normal operations, operators must take countermeasures based on their observability of the system. In this way, operators need to make an optimal decision with available information to ensure the system's overall reliability and security during the event. After an event, restoration should be carried out reliably and efficiently with the given information. Once the system is recovered from the event, system planners, operators, and stakeholders should learn from the experience and harden the system with new construction and operation plans, with the purpose to enhance the systems' robustness, redundancy, and resourcefulness. When similar events happen in the future, the system is able to maintain its secure and reliable operation with improved resilience. Apart from lessons learned from past events, new insights and knowledge of resilience could also provide guidance on resilient network designs.

From a holistic perspective, the resilience enhancement techniques can be further classified into *assessment*, *reinforcement*, and *reaction*, which together comprise the *modern power system resilience enhancement life cycle*, as shown in Fig. 5.

1) *Assessment* refers to techniques that perform ahead-of-time analyses of threats, leveraging their properties and impacts on power systems' security and functionality. The goal of *assessment* is to provide enough situational awareness for operators and stakeholders to better prepare for potential contingencies prior to their occurrence.
2) *Reinforcement* refers to techniques that can strengthen power systems' ability to tolerate disturbances and maintain reliable and secure functionality through resilient network design and operations. The goal of *reinforcement* is to improve the system's capability to anticipate threats and fortify its security against them.
3) *Reaction* refers to techniques of automatic response and human-made control commands against threats using real-time data and information. The goal of *reaction* is to ensure the secure and reliable functionality of power systems during hazards and to maximally and securely maintain a continuous supply of energy.

This *modern power system resilience enhancement life cycle* also relates to *infrastructural resilience* and *operational resilience*. *Infrastructural resilience* depends on how the network is designed and operated during normal and adversarial scenarios, and thus, *reinforcement* falls entirely within it, while *assessment* and *reaction* are partially within it. *Operational resilience* mostly consists of *assessment* and *reaction*, but all of their techniques rely on information and data of the system. Moreover, as a life cycle, these elements mutually influence each other. For example, techniques in *assessment* can identify vulnerable parts that *reinforcement* needs to strengthen with better protection and provide situational awareness that *reaction* can leverage to better prepare countermeasures. Meanwhile, techniques in *reinforcement* can increase the resourcefulness and redundancy in both cyber and physical networks. In this way, *reaction* techniques can leverage more flexibility in the system, and *assessment* techniques can obtain and deliver information more accurately and efficiently. Techniques in *reaction* heavily depend on data and information from *assessment* and resource allocation determined by *reinforcement*. To operate more securely under disturbances with enhanced resilience, the system needs to harden its network and improve its prediction and assessment techniques.

In this article, we have selected and reviewed articles since 2016 that developed resilience enhancement techniques to improve power systems' resilience against unexpected events, including natural disasters, extreme

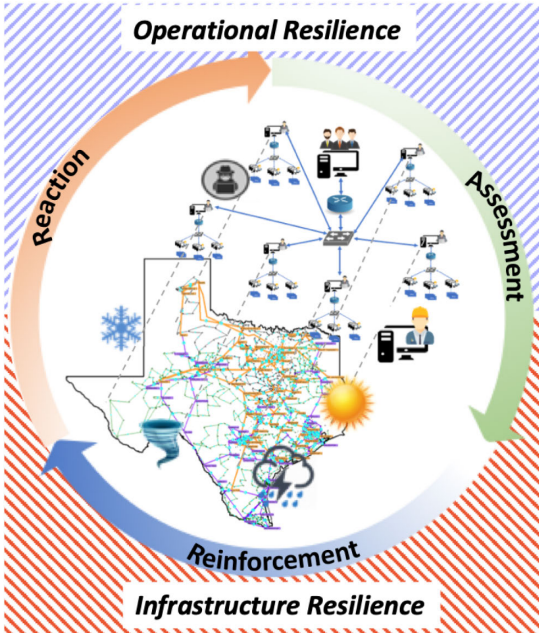


Fig. 5. ***Power system resilience enhancement life cycle.***

Table 1 Summary of Power System Resilience Enhancement Techniques

Refs	Attributes	Resilience Characteristic	Resilience Categorization	Resilience Enhancement Life Cycle
[52]–[61]	Transmission Network Hardening and Design	Robustness/Resistance & Redundancy	Infrastructure Resilience	Reinforcement
[62]–[68]	Distribution Networks with MG and DER	Robustness/Resistance & Redundancy	Infrastructure Resilience	Reinforcement
[69]–[79]	Resilient Communication Networks and Data Delivery Against Adversaries	Resourcefulness & Redundancy	Infrastructure Resilience	Reinforcement
[80]–[93]	Risk Assessment	Robustness/Resistance	Infrastructure Resilience	Assessment
[94]–[98]	Security-Constrained Optimal Power Flow	Robustness/Resistance	Infrastructure Resilience & Operational Resilience	Assessment & Reinforcement
[99]–[106]	Advanced Operational Scheduling and Planning Optimization	Robustness/Resistance	Infrastructure Resilience & Operational Resilience	Assessment & Reinforcement
[107]–[119]	Proactive Operations Against Natural Disasters	Response	Operational Resilience	Assessment & Reaction
[120]–[133]	Defense Mechanisms Against Cyber Attacks	Response	Operational Resilience	Assessment & Reaction
[134]–[139]	Remedial Actions	Response & Recovery	Operational Resilience	Reaction
[140]–[155]	Restoration Operations	Response & Recovery	Operational Resilience	Reaction

weathers, and cyberattacks, from a specific perspective or at a specific phase in the power system resilience trapezoid. Table 1 presents the classification of all reviewed articles from three perspectives of resilience, including *resilience characteristics*: robustness/resistance, resourcefulness, response, redundancy, and recovery; *resilience categorization*: infrastructure resilience and operational resilience; and *resilience enhancement life cycle*: assessment, reinforcement, and reaction. It is important to mention that some techniques belong to more than one element within these categorizations, as all these elements are interdependent and mutually promote the development and enhancement of each other. Sections IV–VI analyze and discuss these techniques.

IV. INFRASTRUCTURAL RESILIENCE ENHANCEMENT

Modern power systems include transmission networks, distribution networks, generation units [traditional generators and distributed energy resources (DERs)], and communication networks. As a cyber–physical system, the communication networks collect and deliver the information of the entire system to operators for decision-making and operations. The resilience of the communication networks is paramount for the whole grid. Thus, the *infrastructural resilience* relies on the design and construction of all of the above networks, as well as their risk assessment and preparation. The following sections present the review of representative works in resilient network design and construction for transmission, distribution, and communication networks, as well as techniques regarding threat assessment and ahead-of-time planning.

A. Resilient Transmission Network Design

Transmission is critical to addressing the climate crisis through the decarbonization of the power sector, increasing transportation electrification, and enabling the clean energy transition. The design and operation of transmission networks always follow $N-1$ reliability [156]. However, with the increasing abruptness of threats from cyber and physical domains, there is a need to expand transmission capacity with stronger and more numerous energy delivery pathways for its reliability and resilience against unexpected multihazard scenarios. Modernizing, hardening, and expanding the grid will enhance the resilience of the entire electric system, while ensuring energy is available to customers where and when it is needed most. A successful transmission network requires deliberate planning and innovative approaches from multiple perspectives.

Nagarajan et al. [52] developed a two-stage mixed-integer stochastic optimization model that aims to upgrade a transmission network's capacity against damages with minimum investment, considering options from building new lines, hardening existing lines, adding flexible alternating current transmission system (FACTS) devices, and allocating DERs. Nezamoddini et al. [53] developed a mixed-integer linear optimization model to determine the optimal investment of protection systems for resilient transmission networks to ensure the load supply against physical attacks. Shao et al. [54] proposed a two-stage optimization model to integrate the planning of the transmission network and natural gas transportation system to improve power grid resilience with less load curtailment in extreme conditions. Lagos et al. [55] proposed a Monte Carlo simulation-based framework considering four phases of power systems under natural hazards to identify the optimal network investments for the highest level of hedge. Panyam et al. [56] proposed a biological food web-based approach to optimize the design of power systems for improved inherent resilience against $N-x$ contingencies. Huang et al. [57] proposed a deep transfer learning approach using bidirectional long short-term memory to identify resilient transmission network structures against short-term voltage stability issues caused by hazards. Garifi et al. [58] formulated a mixed-integer resilience investment optimization problem for transmission network to minimize unserved load over a multitime-period restoration horizon, which determines the enhancement of power grid components considering recovery strategies of unit commitment, transmission line switching, and generator dispatch. Moradi-Sepahvand et al. [59]

built a mixed-integer optimization model for a multistage expansion co-planning model of transmission lines, battery energy storage, and wind farms against extreme weather events for enhanced resilience. This model leverages a fragility curve, a chronological time-period clustering algorithm, and a deep learning approach to consider the adversarial impact of extreme event and the projection of load growth. Huang et al. [60] utilized the long-term resilient food web-based approach again as a benchmark to expand power transmission networks through a mixed-integer optimization model to improve the system's inherent resilience with enhanced capability of anticipating unexpected adversaries with fewer operational violations. Stürmer et al. [61] combined a probabilistic line failure model with a power grid model to simulate the spatiotemporal co-evolution of wind-induced cascading failures on power systems. This approach can serve as an effective tool in identifying and hardening critical lines, thereby improving the grid's resilience against tropical cyclones.

B. Distribution Network With MG Applications

Distribution networks are the last step of supplying electrical energy to consumers. Traditional distribution networks are highly dependent on the main grid to receive energy. Any adverse events, such as cyberattacks, wildfires, and storms, occurring in any sector of power systems could cause outages in distribution system and for customers. However, with the advancement of solar photovoltaics (PVs), battery storage, and MGs, resilient distribution systems can leverage their resourcefulness and flexibility to withstand and rapidly recover from disturbances, thereby enhancing the entire system's resilience.

Yuan et al. [62] proposed a two-stage robust optimization model to design resilient distribution networks with the consideration of hardening the grid and allocating DERs to minimize the system damage against natural disasters for improved resilience. Manshadi and Khodayar [63] proposed a bilevel optimization model to transform the active distribution network with DERs into multiple autonomous MGs to ensure the reliability of energy supply against disruption and thus enhance the system's resilience. He et al. [64] presented a trilevel robust optimization-based network hardening model for integrated electricity and natural gas distribution systems to improve power system resilience with minimum load shedding against natural disasters. Tan et al. [65] formulated a two-stage stochastic optimization model to holistically harden the distribution system and schedule post-disaster repairs, aiming to improve the efficiency of the restoration process against natural disasters with enhanced resilience.

Barnes et al. [66] proposed a two-stage stochastic optimization model to strengthen the resilience of distribution systems by leveraging networked MGs to ensure the energy supply under storms. Nazemi et al. [67] proposed a linear optimization model to determine the capacity and location of the battery energy storage systems for hardening distribution network in order to more reliably supply customers energy with better resilience against earthquakes. Huang et al. [68] proposed a resilience-oriented planning method to determine the optimal configuration of distribution level multienergy systems against HILF events.

C. Resilient Communication Network and Data Delivery Against Adversaries

In modern power systems, communication networks allow the exchange of information, such as measurements and control commands, between field devices and operators. Several industrial communication protocols and standards, such as DNP3, Modbus, IEEE C37.118, and IEC 61850, have been applied to power systems for better observability and controllability. However, cyber networks have uncertainties and vulnerabilities that can be exploited and compromise the system [157], [158], [159]. They have posed threats to power system operation. Thus, ensuring the resilience of cyber networks and the delivery of trustworthy information is even more critical in light of increasing cyberattacks that could exploit vulnerabilities and compromise power system operations.

Lin et al. [69] proposed a self-healing phasor measurement unit (PMU) network that utilizes the software-defined networking (SDN) infrastructure to mitigate the impact of cyberattacks on PMU data. The proposed solution isolates compromised components and reconnects recovered components for enhanced cyber and data resilience. Al-Rubaye et al. [70] proposed an SDN platform using industrial Internet of Things (IIoT) technology to support power systems' resilience. This platform dynamically updates communication networks against adversaries to ensure reliable and flexible operations with real-time system monitoring data. Jin et al. [71] presented an SDN-based communication network architecture for MG operations with multiple functionalities, including self-healing communication network management, real-time and uncertainty-aware communication network verification, and specification-based intrusion detection, against cyberattacks for the whole systems' security and resilience. Sargolzaei et al. [72] proposed a cryptography-free time-delay switch recovery communication protocol enhancement that leverages adaptive channel redundancy techniques and a state estimator to detect and recover from time-delay switch attacks for power systems' stability and resilience. Mylrea and Gourisetti [73] explored the application of blockchain technology and smart contracts to increase the fidelity and security of communications between customer end and system end for enhanced cyber resilience against vulnerabilities. Liang et al. [74] proposed a distributed blockchain-based data protection framework that utilizes the consensus mechanism to enhance the self-defensive capability of power systems against cyberattacks, thus enhancing their inherent cyber resilience. Xu et al. [75] formulated a mixed-integer optimization model to determine the optimal routing policy for cyber–physical

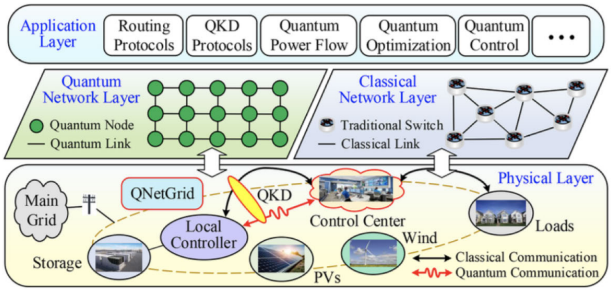


Fig. 6. ***Quantum network-based power grid architecture [78], ©2023 IEEE.***

power systems considering the information and energy flow, as well as the interdependence between cyber and physical components. The optimal routing policy ensured the robustness and resilience of cyber–physical power systems through reliable remedial control actions. Tariq et al. [76] proposed a graphics processing unit (GPU)-enabled adaptive robust state estimation. This approach consists of deep learning, long short-term memory, and a nonlinear extended Kalman filter, taking advantage of advancements in next-generation wireless communication and networking technologies. With a two-level online parametric state estimation, it can enhance the security of data transmission against cyberattacks for load management. Jiang et al. [77] developed a quantum direct communication network for power grids to enhance the cyber resilience for power system operations by providing more secure data transmission against cyberattacks. Tang et al. [78] built a quantum network-based power grid testbed (Fig. 6) to explore the benefits of quantum communication in power systems, with more flexible, secure, and resilient communication and operations. Wang et al. [79] proposed a blockchain-based vehicle-to-vehicle RES trading model. This model features a novel block alliance consensus mechanism with security, decentralization, and infinite scalability to improve the stability and reliability toward a resilient power grid.

D. Threat Prediction and Impact Assessment

The bulk electric power grid is subject to vulnerabilities from natural disasters, cyberattacks, and human-made mistakes, which might lead to cascading outages and large-scale blackout. Thus, identifying vulnerabilities and assessing their impact on cyber–physical power systems are of great importance and can provide useful insights for enhancing security and resilience against extreme and unexpected events.

Vu and Turitsyn [80] constructed a robust assessment toolbox using quadratic Lyapunov functions approaches to provide a real-time transient stability certificate and assessment for power systems under different fault scenarios. Espinoza et al. [81] proposed a time-dependent multiphase resilience assessment framework to evaluate how can systems withstand major disruptions with limited degradation and recover rapidly, considering the stochastic and spatiotemporal properties of events. Kwasinski [82] presented a framework for characterizing resilience using an analogous measure of availability as a quantitative metric to evaluate power system resilience from the customers' perspective, considering the human factors and cyber and physical components. Bajpai et al. [83] proposed an algorithm using a graph-theoretic approach and a Choquet integral to quantify power system resilience and maintain the energy supply to critical loads during extreme contingencies. Ciapessoni et al. [84] presented a probabilistic, risk-based security assessment that ranks risks in both cyber and physical networks in order to help operators improve power system resilience. Zhang et al. [85] proposed a reliability assessment framework using Bayesian attack graph models for wind farm EMSs against coordinated cyberattacks, which operators can use to better prepare defense and remedial strategies for enhanced system resilience. Clark and Zonouz [86] proposed a cyber–physical resilience metric that considered the cyberattacks from the cyber network and its impact on the physical components through a competitive Markov decision process, aiding operators in better defending cyber and physical incidents. Lopez et al. [87] proposed an architecture for smart grids that leverages cloud computing resources, along with collaborative decision algorithms and graph theory, to predict load consumption and safeguard the power grid against communication losses and intrusion attacks, thereby enhancing the safety, security, and resilience of power systems. Dehghanian et al. [88] introduced a weather-driven, probabilistic-based risk metric that uses meteorological information to predict weather hazards, analyze grid vulnerabilities, and quantify financial consequences for corrective operation for enhanced resilience of electric power systems. Specifically, this metric models weather and environmental events in a stochastic process and considers their spatial–temporal correlation on grid components' reliability and functionality. Watson and Etemadi [89] developed a series of models for hurricane exposure, fragility curve-based component damage, and restoration cost using the Monte Carlo simulation to predict power systems' resilience factors, which are the power generation capacity lost and the restoration cost, for electrical transmission grid and power generation system damages. Venkataramanan et al. [90] proposed a compound metric to evaluate the resilience of cyber–physical transmission systems considering the topological properties and functionalities of cyber and physical networks to assist operators with better situational awareness in order to enhance power system resilience against cyber and natural hazards. Overbye et al. [91] presented a number of techniques that can be used to enhance electric grid situational awareness, including the use of geographic data views [160] for operators to make better decisions regarding enhancing system resilience. Zhou and Zhang [92] devised a high expressibility, low-depth quantum circuit to realize quantum-based transient stability assessment

for bulk power systems with a quantum natural gradient algorithm. It enables efficient data-driven transient stability prediction for resilient and secure decision-making in real-world power systems. Kelly-Gorham et al. [93] built a platform that captures the interdependence of various systems with power systems and their impacts on power system resilience. This platform uses stratified sampling from historical data to provide a more accurate description of the risks associated with low-probability events, which is essential for evaluating resilience. The results also suggest that the interaction models between different systems could be more meaningful with more detailed physics models or observations from historical data.

E. Scheduling and Operating Ahead Against Contingencies for Security and Resilience

Avoiding the first few failures near the beginning of a cascade or blackout is supreme for power systems. The security-constrained optimal power flow (SCOPF) is a common approach to ensure power systems' secure operation against planned $N-1$ contingencies. It ensures a secure operating state where demand is met without reliability violations in either the base case or under a set of postulated contingencies. The formulation is given as follows [161]:

$$\min_{\mathbf{u}^0,\mathbf{u}^k} f_0\left(\mathbf{x}_0,\mathbf{u}_0\right) \tag{1}$$

$$\text{subject to: } \mathbf{g}_0\left(\mathbf{x}_0,\mathbf{u}_0\right)=\mathbf{0} \tag{2}$$

$$\mathbf{h}_0\left(\mathbf{x}_0,\mathbf{u}_0\right)\le\mathbf{0} \tag{3}$$

$$\mathbf{g}_k\left(\mathbf{x}_k,\mathbf{u}_k\right)=\mathbf{0} \quad \forall k\in\mathcal{K} \tag{4}$$

$$\mathbf{h}_k\left(\mathbf{x}_k,\mathbf{u}_k\right)\le\mathbf{0} \quad \forall k\in\mathcal{K} \tag{5}$$

$$\left|\mathbf{u}_k-\mathbf{u}_0\right|\le\Delta\mathbf{u}_k \quad \forall k\in\mathcal{K} \tag{6}$$

where subscripts 0 and k denote the pre-contingency state and post-contingency state, respectively; $\mathcal{K}$ is the set of postulated contingencies; $\mathbf{x}_0$ and $\mathbf{x}_k$ are the vectors of state variables; $\mathbf{u}_0$ is the vector of preventive actions; $\mathbf{u}_k$ is the vector of corrective actions; $\Delta\mathbf{u}_k$ is the vector of maximal allowed variation of corrective actions, reflecting the ramping rate of controls; function f_0 is the objective, which usually is modeled as the operation cost; $\mathbf{g}$ is the power flow equations; and $\mathbf{h}$ is the operational limit. The corrective actions, $\mathbf{u}_k$, are constrained under each predefined contingency, which are integrated through discrete variables. Therefore, the SCOPF problem is generally a mixed-integer nonlinear optimization problem considering a set of postulated contingencies [162].

Even though the SCOPF has been proposed over decades and applied in the field, there still remain a lot of development and advancement opportunities to improve its efficiency and effectiveness to ensure power systems' security and resilience. Xiang et al. [94] extended the traditional SCOPF to consider cyberattacks in power systems, thereby enhancing system robustness and ensuring the energy supply under malicious attacks. Madathil et al. [95] developed an optimization model and an algorithm for capacity planning and operations of MGs in a distribution system to include $N-1$ contingency security to improve the resilience in remote communities. Karangelos and Wehenkel [96] extended the SCOPF model with probabilities of contingency events and potential failures in post-contingency corrective controls to achieve probabilistic reliability management. Avramidis et al. [97] included post-contingency behaviors for voltage and frequency control with an SCOPF model using an approximation technique on generator response to improve the potential degradation of solution quality. Weinhold and Mieth [98] proposed an algorithm to identify the minimal set of constraints for SCOPF problems with the exact space of feasible nodal injections for a given network and contingency scenarios, which greatly improves the efficiency of solving this high-dimensional problem.

Apart from SCOPF, other approaches have also been investigated for power systems to ensure their capability to handle scheduled and unexpected contingencies. For example, Yang et al. [99] proposed a centralized MG EMS framework with a flexible time frame DER schedule to improve power systems' resilience and efficiency, leveraging the forecasts of DER and load, as well as economic factors. Shaker et al. [100] proposed a two-stage stochastic model to plan reactive power using networked MGs against extreme events, with reduced load shedding for better resilience. Kamruzzaman et al. [101] partitioned power systems into different regions based on geographic information and proposed a multiagent framework using a deep reinforcement learning algorithm to plan the deployment of shunts, which enhances power system resilience against extreme events and improves voltage stability. Zhao et al. [102] proposed a two-stage distributionally robust optimization problem to enhance the resilience of multienergy systems against cyberattacks in both the day-ahead scheduling and real-time operations. Zakernezhad et al. [103] presented a three-level optimization framework for multienergy systems for improving the operational resilience of multienergy systems. This framework offers operators optimal scheduling and corrective control of distributed energy sources before and after external shocks. Huang et al. [104] utilized a graph and information theory-oriented metric, ecological robustness (R_{ECO}), to formulate an ecological robustness-oriented optimal power flow (R_{ECO} OPF) to improve power systems' survivability agnostic against the source of disturbances. Tobajas et al. [105] proposed a resilience-oriented optimization problem for MGs' day-ahead scheduling with the consideration of hybrid energy storage systems. It aims to maximize the energy support during main grid blackouts and ensure a continuous energy supply for critical loads, thereby enhancing the system's resilience. Lv et al. [106] proposed resilience-oriented scheduling for integrated power distribution networks and natural gas systems with multilevel decentralized reserves, including electricity and natural

gas systems, thermal storage devices, and building air thermal storage, to mitigate the operational risks.

It is important to point out that all techniques within this section lie at the intersection of infrastructural and operational resilience enhancements as classified in Table 1. They rely on infrastructure design and risk assessment and can be controlled and operated to enhance a system's inherent resilience in advance.

V. OPERATIONAL RESILIENCE ENHANCEMENT

In addition to the inherent resilience residing in networks, researchers have studied various techniques and algorithms to defend against threats, including emergency power supply, network reconfiguration, failed component replacement, self-healing mechanisms, and mitigation strategies. The following sections review preventative measures against natural disasters, defense mechanisms against cyberattacks, and remedial actions and restoration strategies after contingencies have occurred.

A. Resilience-Oriented Preventative Operations Against Natural Hazards

Natural disasters have caused the most disturbances in power systems due to their abruptness and intensity, resulting in tremendous societal and economic losses. To maintain the system's resilience, it is necessary to take preemptive actions to counteract the adverse impact of different extreme natural events *just ahead time*.

Wang et al. [107] leveraged the Markov process to model the uncertain sequential transition of system states under extreme weather and formulated a recursive value function at each state to determine the optimal proactive operation strategy for enhancing system resilience. Gholami et al. [108] presented a two-stage stochastic programming approach for the optimal scheduling of MG, considering uncertainties from renewable energy resources, electrical vehicles (EVs), and market price, against natural disasters to improve the system resilience. Trakas and Hatziargyriou [109] proposed a stochastic programming approach that leveraged a model of dynamic line ratings and the uncertainty of solar and wind, as well as their impact on DER output during wildfire progression, to improve the resilience of a distribution system. Trakas and Hatziargyriou [110] also formulated a trilevel optimization problem for resilient constrained day-ahead unit commitment. The goal was to minimize unit commitment and operational cost while accounting for the worst outcome from extreme weather. Wang et al. [111] proposed a resilience-oriented hourly unit commitment problem through a sequential and Monte Carlo-based framework to seek a tradeoff among operation cost, the homogeneity of flow distributions in power networks, and the loading rates of local lines affected by extreme weather. Ciapessoni et al. [112] proposed a security-constrained redispatching approach to predict potential critical scenarios, satisfy additional $N-1$ security criteria, and increase the system resilience against wet snowstorms. Wang et al. [113] proposed a resilience index to capture systems' reliability and risk impact using the Monte Carlo simulation. Based on that, they formulated a resilience-constrained economic dispatch against extreme weather events to improve power system resilience. Yan et al. [114] proposed a two-stage robust optimization model for the optimal coordination of power system schedule with the prepositioning and routing of mobile dc deicing devices against ice storms for power transmission system resilience enhancement. Zhao et al. [115] proposed a resilient unit commitment problem using a two-stage distributionally robust and robust optimization model. Their aim was to mitigate the adverse impact of the worst load forecasting and line failure scenario from hurricanes for day-ahead market. Pandey et al. [116] proposed a resilience-driven pre-event distribution reconfiguration approach with intentional islanding. They leveraged a maximum likelihood estimation ensemble model with distribution synchrophasor data to identify the load at risk and then reconfigure the topology between load and distribution system to minimize the impact of unexpected natural events on critical loads. Gutierrez-Rojas et al. [117] introduced a predictive weather-based control policy for battery energy storage systems to manage MGs under interruptions for better resilience. It is a multiobjective optimization problem integrated with a decision-tree-based learning algorithm in order to better predict the load demand, solar production, and upstream interruptions. Zhang et al. [118] utilized the Poisson process theory to estimate the time interval between successive failures and then proposed a systematic preventive control framework against successive failures to enhance security, stability, and resilience. Kadir et al. [119] modeled the proactive control problem against wildfire events as a Markov decision process to minimize load outages and solved the problem using a deep reinforcement learning-based power generation coordination approach, which provides decision support for grid operators.

B. Resilience-Oriented Defense Mechanism Against Cyberattacks

Delicate cyberattacks, such as denial of service (DoS) attacks and FDI, can directly compromise information delivery and decision-making for power systems, leading to reduced resilience level. Therefore, it is essential to take timely and effective control actions to ensure power systems remain resilient in the face of those attacks.

Liu et al. [120] proposed an attack-resilient cooperative control strategy for distributed generators, incorporating properly designed observation networks to ensure the functionality and resilience of the entire distribution network against communication failure and cyberattacks (e.g., DoS attack and deceptive attack). Farraj et al. [121] proposed a parametric feedback linearization-based framework for delay-resilient cyber–physical control of smart

grid systems, enhancing their time-delay tolerance for transient stability against DoS attack and communication latency. Ashok et al. [122] proposed an end-to-end attack-resilient cyber–physical security framework with defense-in-depth architecture for wide-area monitoring, protection, and control applications to achieve attack resilience at both the infrastructure layer and the application layer for power systems. Musleh et al. [123] proposed a multisensor temporal prediction-based wide-area control scheme to accurately address FDI attacks and control the smart grid's voltage profile for system's stability and resilience. Habib et al. [124] proposed an adaptive protection scheme with an autonomous control algorithm for the supercapacitor's ac/dc converter, leveraging its capacitive energy storage to enhance system resilience against communication outages caused by communication link failures and DoS attacks. Huang et al. [125] proposed an online framework using dynamic watermarking techniques to detect cyberattacks (e.g., replay attack, noise injection attack, and destablization attack) on automatic generation control (AGC) to ensure their validity and the systems' resilience. Davarikia and Barati [126] proposed a trilevel interdiction optimization model considering the actions from defender, attacker, and operator to improve power grid resilience with hardening strategies for vulnerable components against hazards. Lai et al. [127] proposed both deterministic and stochastic coupling strategies for asymmetric cyber–physical power systems to improve its robustness against both random and intentional cyberattacks. Chen et al. [128] presented a distributed dynamic filtering (state estimation) scheme taking advantage of two Riccati-like difference equations and a recursive algorithm to minimize the error against DoS attacks and gain perturbations to ensure the observability and controllability of power systems. Lai et al. [129] proposed a robustness-oriented economic dispatch model with a battery storage sizing algorithm for MGs to improve energy supply against attacks. Abbaspour et al. [130] proposed a resilient control design for load frequency control system leveraging the Luenberger observer, Kalman filter, and artificial neural networks (ANNs) for online detection of FDI attacks and compensate their adverse effects for system stability and resilience. Lai et al. [131] proposed a trilevel optimization model considering a coordinated attack scenario with short-circuiting transmission line and cyber-induced disabled protective relay to identify the optimal defending resource allocation to hedge against coordinated attacks, enhance the system's security and energy supply, and save the system from cascading failures. Wang and Govindarasu [132] presented a multiagent-based attack-resilient system integrity protection design to enhance the cyber resilience with a support vector machine embedded layered decision tree algorithm to detect multiclass anomalies and an adaptive load rejection strategy to mitigate the load shedding against DoS attacks. Elimam et al. [133] presented two deep learning-based models to detect PMU data manipulation attacks and to recover the corrupted measurements for power systems steady- and transient-state operations with improved security and resilience.

C. Resilience-Oriented Remedial Actions and Restoration Strategies

Once a contingency has caused the power system to operate under stress, it is paramount to take remedial actions to relieve the system stress and ensure maximum energy supply for customers. While blackouts are rare, it is still important to study and prepare the restoration schemes that prioritize speed and effectiveness while taking economic factors into consideration.

Huang et al. [134] presented an integrated resilience response framework with a two-stage robust mixed-integer optimization model that linked the situation awareness with resilience enhancement for effective and efficient responses against natural disasters in preventive and emergency states. Amraee and Saberi [135] proposed a controlled splitting strategy with a mixed-integer optimization model considering the slow coherency of synchronous generators and system stability to determine the splitting points of an interconnected power system to maintain its security and resilience against contingencies. Teymouri et al. [136] developed a controlled network partitioning model through a mixed-integer linear programming formulation to improve power grid resilience considering frequency stability and minimizing load shedding against catastrophic events. Hossain-McKenzie et al. [137] proposed online remedial action schemes utilizing clustering and factorization mechanisms to find the most effective control against cyberattacks and extreme events that could effectively relieve system stress for better resilience. Yan et al. [138] proposed a trilevel two-stage robust model for an integrated energy system, leveraging the energy hub architecture with power and gas network constraints (regional model), and the energy hub architecture for multiple districts (district model) to determine preventive and corrective responses against natural disasters for enhancing the integrated system's inherent resilience. Hussain et al. [139] proposed a fast and efficient linear sensitivity-based transmission switch algorithm, leveraging line outage distribution factors to reduce the loss of load under extreme events for boosting power system resilience.

Gao et al. [140] formulated a two-objective chance-constrained optimization model considering the uncertainties in renewable energy resources and load demand in the distribution system to leverage MGs for assisting critical load restoration with maximum energy supply and minimum load voltage variations after extreme events. Sedzro et al. [141] developed a mixed-integer optimization model of the post-disaster MG formation to maximize critical load pickup while satisfying the operational constraints for power system restoration considering fixed and mobile distributed generator units and DERs. Qiu and Li [142] presented a mixed-integer optimization model to integrate the sectionalization and the generator start-up

sequencing into a unified model for an effective and executable restoration plan satisfying operational constraints. Chen et al. [143] presented a distribution system restoration decision support tool leveraging the techniques of distribution automation and advanced metering infrastructure to maintain grid resilience with improved situational awareness of system damage status and customer survivability against extreme weather events. Poudel and Dubey [144] formulated a mixed-integer linear model for distribution systems to obtain a robust restoration plan leveraging DERs after natural disaster that maximizes the amount of restored critical load and optimizes the restoration time considering the potential failures during the restoration process. Dehghanian et al. [145] proposed a resilience-based corrective topology control optimization with *direct current optimal power flow* to provide an agile restoration strategy with both generator dispatch and transmission line switch against the anticipated HILF events for improving the system's resilience.

Li et al. [146] proposed an integrated restoration strategy using linearized optimal power flow dispatch and reinforcement learning-based optimal link restoration to maximally supply energy after events. Bedoya et al. [147] proposed a deep learning model with Monte Carlo tree search to efficiently restore a distribution system for enhanced resilience, considering asynchronous and partial information scenarios. Zhao et al. [148] proposed a fast robust load restoration strategy for bulk system with high penetration of wind power. They leveraged deep neural network and deep convolutional neural network to obtain the optimal load pickup decision and ensure the system security considering the uncertainties during the process. Hosseini and Parvania [149] developed an intelligent resilience controller using deep reinforcement learning to achieve fast real-time operation decision after outages in order to restore energy supply. Birchfield [150] proposed a computationally efficient blackstart restoration algorithm that leverages directed graph decomposition to sectionalize a large-scale system into multiple islands and correctly prioritizes restoring loads and cranking generators in each island, with the objective of minimizing the total cost of load outages while maintaining system's stability. Li et al. [151] introduced a load restoration strategy after extreme natural events based on an optimal multienergy flow model to improve multienergy systems' resilience, accounting for the integrated power, heat, and gas networks. Edib et al. [152] proposed a concept of *cyber restoration* for cyber–physical power systems considering their observability and information recovery in communication networks after blackouts and formulated a mixed-integer linear programming to determine an optimal cyber restoration scheme to efficiently recover power systems' observability for physical networks' operations. Zhang et al. [153] proposed a Bayesian deep reinforcement learning-based real-time control for multienergy MGs. This approach captures uncertainties associated with RES output to provide energy management and control to improve the system's resilience after extreme events. Wang et al. [154] introduced a decentralized operating paradigm to coordinate local multienergy MGs for system-wise bulk power system load restoration with a topology-aware multitask reinforcement learning. Fu et al. [155] proposed a hybrid quantum–classical approach to coordinate multiple energy resources for post-disaster restoration in distribution systems. This approach decomposes the original mixed-integer linear programming for coordinated post-disaster restoration problems into subproblems, and the mixed binary problem can be solved using a quantum approach.

VI. DISCUSSION OF RESILIENCE ENHANCEMENT TECHNIQUES

In this section, we present a more in-depth discussion of the reviewed articles, focusing on their modeling and problem formulations, and their quantification of resilience with various considerations. In addition, we explore the gaps between these studies and their applications in the field while also highlighting the importance of stakeholders' participation.

A. Modeling and Problem Formulation

The modeling and problem formulation of resilience enhancement techniques can be categorized into *optimization modeling*, *statistical methods*, *machine learning techniques*, and *advanced technologies* for enhancing infrastructural and operational resilience. Based on the reviewed articles and their main contributions to enhancing power system resilience, we select three primary approaches under each category and match them with specific applications in power systems, as illustrated in Fig. 7. It is important to note that some approaches overlap as they work collectively.

1) Optimization Modeling: Among all approaches, *optimization modeling* has been used the most at different stages to enhance power system resilience. As presented in Sections IV and V, various optimization models have been proposed with a particular objective to harden power grids with more resilient network design and/or system operation schemes in the face of HILF events, especially the mixed-integer optimization model and the stochastic optimization model. The mixed-integer optimization model is capable to explicitly include power system constraints and conditions with specific scenario or application that needs discrete variables to represent ON/OFF status of particular elements. In [52], [53], [58], [59], and [60], the mixed-integer optimization model is used to model options of hardening the network design. In [94], [95], [96], [97], and [98], the SCOPF problem is formulated as a mixed-integer optimization problem to explicitly consider the postulated set of contingencies so that the optimized operation scheme is both economic and secure in anticipation of those contingencies. In [75], the mixed-integer optimization model is to link different domains, namely

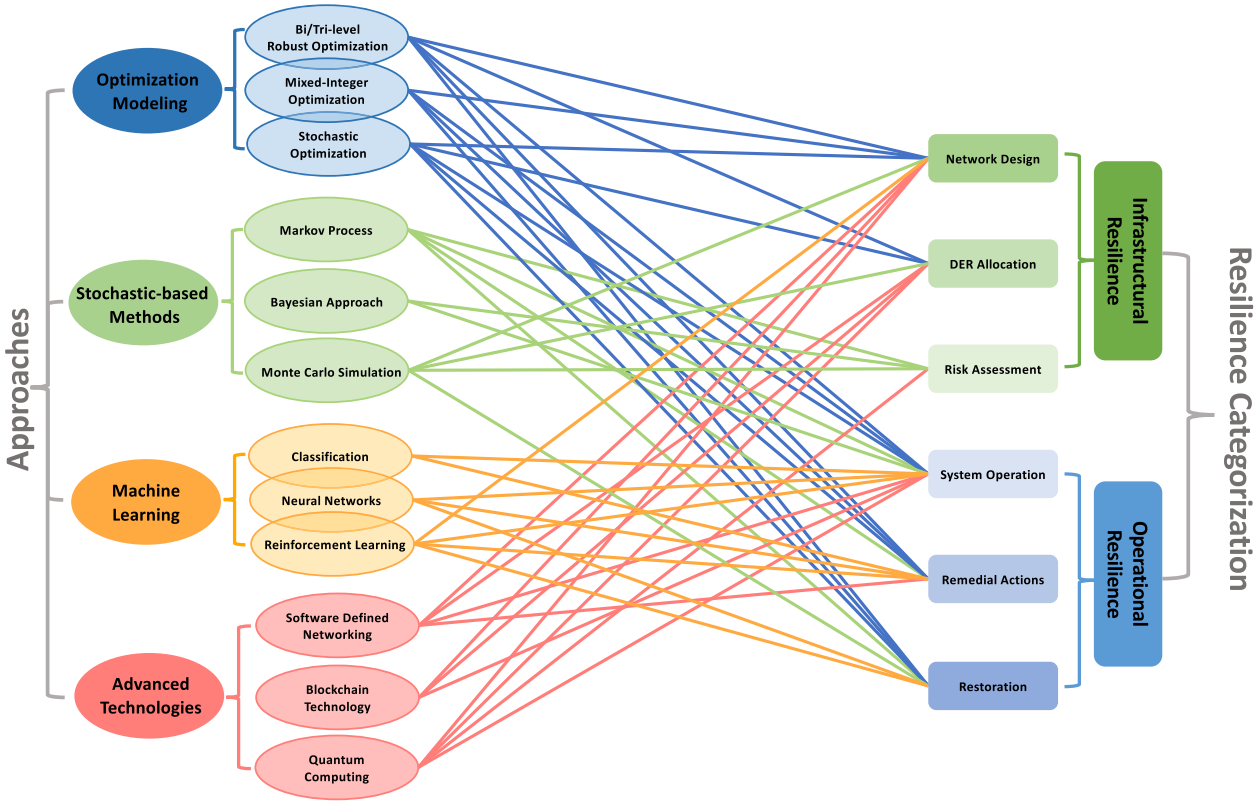


Fig. 7. ***Categorization of power system resilience enhancement approaches together with their applications.***

energy and information flows, to optimize the network routing policy against adversaries. In [134], [135], and [136], the impact of different adversaries in power systems is integrated to obtain the optimal remedial actions. In [141], [142], and [144], the operation of MGs and DERs is integrated through the mixed-integer optimization model to determine the optimal restoration schemes. With the integration of other energy infrastructures, mixed-integer optimization has also been used for multienergy systems to link constraints and objectives in different systems for their resilience-oriented load restoration [151], [155]. In [152], the mixed-integer optimization model aggregates each physical component's observability through discrete variables to determine the optimal cyber restoration scheme for the entire system's observability. The stochastic optimization model is used to optimize the expected aggregated benefits considering the stochastic nature of adversarial events and DERs. In [52], [65], [66], and [68], the stochastic optimization model is used to strengthen distribution systems' design, accounting for the impact of extreme natural events. In [108], [109], and [100], the optimal operational schemes are obtained considering the uncertainties from DERs against unexpected events by solving a stochastic optimization problem. In [127], the stochastic nature of cyberattacks is considered for coupling strategies in cyber–physical power systems. Besides the problems mentioned above, two-stage or trilevel robust optimization models have been used to incorporate more properties of modern power systems, including the interdependence and uncertainties raised from cyber and physical infrastructures and operations. In [52], a two-stage mixed-integer stochastic optimization is employed to strengthen the inherent resilience of power networks by considering various hardening strategies. Bilevel and trilevel optimization models have also been used in interdependent power and gas network optimization for transmission [54] and distribution systems [64], respectively. When considering DERs, Yuan et al. [62], Manshadi and Khodayar [63], Tan et al. [65], and Barnes et al. [66] have formulated different bilevel optimization models to design distribution networks with improved resilience. In addition, Shaker et al. [100], Gholami et al. [108], and Trakas and Hatziargyriou [110] have formulated bilevel and trilevel optimization models to operate DERs and MGs to ensure energy supply under contingencies. Considering the impacts of natural disasters, Yan et al. [114] and Zhao et al. [115] used two-stage optimization models to determine preventative actions. In the case of defending cyberattacks, Davarikia and Barati [126] and Lai et al. [131] utilized trilevel optimization models to determine defense operations considering multiple roles in power system operations, including operators, attackers, and defenders. For multienergy systems, Zhao et al. [102], Lv et al. [106], and Yan et al. [138] presented multistage optimization models to incorporate different resources and enhance the resilience of power systems under various contingencies.

It is worth noting that there is some overlap among mixed-integer optimization, stochastic optimization, and bilevel/trilevel optimization. Integer variables are used to connect external constraints, scenarios, and objectives for some stochastic and bilevel/trilevel optimization problems. In this discussion, we only consider each article and its methodology based on its primary contributions.

Undoubtedly, optimization models have great capability to formulate design and operation problems from various perspectives for enhancing power system resilience. However, it is necessary to mention that different levels of relaxations and approximations have been applied to solve those complicated nonlinear optimization problems under the context of power system constraints. Although optimization models can be used almost at each phase of power system resilience, it is hard to ensure *real-time* or *online* agile response against threats solely based on state-of-the-art optimization solvers, not to mention processing the large amount of heterogeneous data across different domains and the increasing number of variables and complexities in optimization problems.

2) Stochastic-Based Approaches: Stochastic-based approaches are becoming more prevalent in modern power systems, given the increasing uncertainties raised by the integration of RESs and communication networks. *Monte Carlo simulation* has been widely used to quantify power systems' reliability by leveraging random sampling to obtain numerical results [163]. For resilience enhancement, Monte Carlo simulation can provide numerical analyses of adversarial events to guide the network design and system operation by considering the probabilistic characteristics of investigated hazards [55], [89], [111], [113]. Different probability and vulnerability models have been implemented based on historical data and observations. *Markov Process*, a stochastic model describing a sequence of possible events, has been used to account for power systems' state transition during an unfolding natural or cyber event and thus provide assessment of events' impact, where the transition probability is calculated with vulnerability and/or frangibility models of investigated contingencies or simulated data of investigated cases [86], [107], [119]. *Bayesian attack graph* has also been used to represent the procedures of cyberattacks in power systems for reliability assessment [85]. *Poisson process theory* has been utilized to model the successive failure propagation of power system components under extreme weather [118]. Other probability-based frameworks leveraging components' fragility curve, failure rate, and vulnerability with historical observations and data assess the risk and impact of adversarial events on power systems [61], [84], [88], [89], [96], [164].

Stochastic-based methods certainly provide more situational awareness regarding threats from extreme weather events and cyberattacks, which enable operators and stakeholders to better prepare the system with better resilience. However, the gap between risk assessment or situational awareness and the design and operation of modern power systems lies in how to *seamlessly* integrate cross-domain information associated with power systems, including data of system status, cyber, weather, and customer. This could be even more complicated than the optimization modeling.

3) Machine Learning: Machine learning techniques and data analytic have been used in various domains leveraging their high efficiency and accuracy in dealing with large amount of data for different problems. In power systems, these techniques have been widely used in different areas [165]. In this article, we narrow down their applications that particularly enhance power system resilience. ANNs [130] and deep learning [76] have been used with Kalman filter to perform online false data detection and estimation. The decision tree algorithm has been used for prediction of load and solar [117] and to detect and classify cyber and physical anomalies in smart grid [132]. The clustering and factorization mechanisms have been used together to reduce the searching space for determining online remedial actions against cyberattacks and extreme events [137]. Deep learning algorithms have been used at different phases to enhance resilience, including network design [57], [59], preventative operations [101], proactive operations [119], [133], and restoration [146], [147], [148], [153], [154]. These problems leverage deep learning algorithms to improve the efficiency of the solving process with heterogeneous data and models.

Machine learning techniques provide additional approaches to enhance power system resilience with better efficiency through delicate modeling or mapping between machine learning algorithms and modern power systems. Their great capability to deal with large amount of heterogeneous data is leveraged for online decision-making, which prompts the efficiency of solving complex system problems. However, the aleatory and epistemic uncertainties that reside in data, models, and machine learning algorithms could compromise the accuracy or confidence of the output, which limits the application of machine learning for critical infrastructures. Therefore, it is of great interest to develop machine learning algorithms leveraging power system properties for improving resilience with guaranteed confidence and interoperability.

4) Advanced Technologies: Merging technologies are being explored and applied to improve the cyber resilience of modern power systems. SDN has been used in communication networks to enhance the resilience of power systems by providing more reliable and trustworthy data for monitoring and control [69], [70], [71]. Blockchain technology enhances the security of information transactions between customers and system operators with efficient secure decentralized paradigms. This protects data against cyber threats [73], boosts power systems' self-defensive capability [74], and facilitates peer-to-peer communication among EVs for system's stability and reliability [79].

Quantum communication has demonstrated its ability to enhance both cyber and physical resilience with more secure and robust data exchange and fast computation for system operations in adversarial scenarios [77], [78]. Furthermore, quantum computing can be applied to solve power system problems more efficiently, including transient stability analyses [92] and the optimal decision-making process [155].

The demand for secure and resilient modern power systems drives the development of innovative technologies, and these advanced technologies have demonstrated their advantages and benefits in securing modern power systems. However, revolutionizing a wide-area complex system with new technologies is a costly and time-consuming process. Justifying the investment and benefits of new technologies in the field as well as reducing costs through commercialization are important considerations.

B. Quantifiable Resilience Metrics

Regardless of the approach used to enhance power system resilience, it is essential to determine the objective of that approach, with the aim of guiding network design or system operation. As there is no standardized measure of power system resilience capturing its *spatial–temporal* characteristic, most existing works use functional objectives, such as investment, operational cost, and expected energy supply, to design and operate system with preferred resilience.

However, power system resilience can be conceptually quantified as a time-dependent metric of the difference between ideal and real system performance from the beginning of the adverse event until the end of system restoration, referred to the resilience trapezoid as follows [45]:

$$R = \int_{t_0}^{T} (P_i - P_r)\,\mathrm{d}t \tag{7}$$

where R is the system resilience, P_i is the ideal performance level of the system, P_r is the real performance level of the system, and $[t_0, T]$ is period of power system anticipating the event till resuming to normal. The system performance is conventionally measured as how many households can get electricity supply under contingencies and how fast the restoration can be after the contingencies [166]. In order to enhance power system resilience, it is either making P_r as close as P_i or reducing the period of event.

P_i can be a constant value to represent the ideal situation of power systems. However, mathematically formulating P_r for the entire period can be cumbersome due to the time-dependent function that is influenced by system infrastructure, operators' decision-making, and valid information of systems and events. Instead of integrating the comprehensive resilience measure in (7), most of the existing measures focus on particular stage or phase in the resilience trapezoid (Fig. 3) to enhance modern power systems' resilience by leveraging power systems' functional, infrastructural, and/or operational properties. Various metrics have been proposed from different perspectives, such as *energy supply*, *economic benefits*, and *structural properties*. Here are some examples.

In [140], an energy-based operational resilience metric is developed as follows:

$$R = \int_{t_r}^{t_r+T_0} \sum_{c\in C} W_c \cdot P_c\,(t)\ \mathrm{d}t \tag{8}$$

where C is the set of critical loads restored by MGs, W_c is the weight of a critical load c, $P_c(t)$ is the active power of load c at time t, and $[t_r, t_r + T_0]$ is the period of restoration process. This resilience metric represents the total energy supplied to the critical loads weighted by their priority. Thus, it can guide the restoration of distribution system to achieve the maximum energy supply to critical loads for the system's resilience.

In [54], a deterministic resilience metric is proposed considering the minimal cost of load curtailment after the occurrence of the most severe event

$$R = \min_{\mathbf{z}} \max_{\mathbf{p,g}} \sum_{i,b,t} f_i\,(pd_{i,b,t}) \tag{9}$$

where **z** is the set of uncertain events, **p,g** is the vector of system operation variables, $f_i()$ is the load loss cost function, $pd_{i,b,t}$ is the load curtailment, and (i, b, t) is the index of bus, load block, and expansion period, respectively. This resilience metric considers the economic factors of load curtailment under a series of adverse events. It is used as an upper bound constraint for system planning to ensure system's resilience with minimum investment.

In [116], a topology-based resilience metric is formulated to guide the reconfiguration of distribution network

$$R = \frac{w_1 \cdot \mathrm{bc}_n}{w_2 \cdot \frac{l_{g,n}}{l_{\max}}} \times \frac{P_c}{P_n} \tag{10}$$

where w_1 and w_2 are system-specific weights determined through analytical hierarchical processes; bc_n is the betweenness centrality of the node being assessed for its resilience; $l_{g,n}$ represents the geodesic path of between a node and a generator, $l_{\max}$ is the maximum of all path lengths in a given network; and P_c and P_n are the real power demands of the critical and all loads, respectively, at and downstream of the assessed node. This resilience metric leverages the functional importance of critical loads and topological importance of each node with respect to their downstream nodes. Thus, it is used to guide the restoration of critical loads considering the network topology.

In [56] and [60], an ecosystem-inspired fitness metric, R_{ECO} [see (11)–(15)], is used to guide the design

of physical power networks for resilience, improving the ability of the grid to tolerate disturbances and maintain functionality securely. Through an analogy between biological food webs and power systems, this metric considers the network topology and power flow magnitudes to quantify the balance between functional redundancy and efficiency in power systems. The unique balance of functional redundancy and efficiency in food webs, known as the ecological "window of vitality," serves as the inspiration due to its association with the resilience of long established ecological food webs [167]

$$R_{\text{ECO}} = -\left(\frac{\text{ASC}}{\text{DC}}\right)\ln\left(\frac{\text{ASC}}{\text{DC}}\right) \tag{11}$$

$$[\mathbf{T}] = f\left(P_{ij}, P_{\text{gen}_i}, P_{\text{load}_i}, P_{\text{loss}_i}\right) = \begin{bmatrix} 0, & P_{\text{gen}_i}, & 0, & \dots & \dots & 0 \\ 0, & \dots & P_{\text{gen}_i}, & 0, & \dots & 0 \\ 0, & \dots & \dots & \dots & \dots & P_{\text{loss}_j} \\ 0, & \dots & P_{ij}, & \dots & P_{\text{load}_i}, & \dots \\ 0, & \dots & \dots & \dots & \dots & \dots \\ 0, & \dots & \dots & \dots & \dots & 0 \end{bmatrix} \tag{12}$$

$$TSTp = \sum_{i=1}^{N+3}\sum_{j=1}^{N+3} T_{ij} \tag{13}$$

$$\text{ASC} = -TSTp \sum_{i=1}^{N+3}\sum_{j=1}^{N+3}\left(\frac{T_{ij}}{TSTp}\log_2\left(\frac{T_{ij}TSTp}{T_iT_j}\right)\right) \tag{14}$$

$$\text{DC} = -TSTp \sum_{i=1}^{N+3}\sum_{j=1}^{N+3}\left(\frac{T_{ij}}{TSTp}\log_2\left(\frac{T_{ij}}{TSTp}\right)\right) \tag{15}$$

where $[\mathbf{T}]$ is a square matrix containing power flow magnitudes transferred among generators and buses, *TSTp* is the sum of all flows, ASC is a dimensional evaluation of system uncertainty, and DC is the dimensional aggregated impacts (uncertainty) from all events (surprisals). Thus, R_{ECO} has the ability to account for the presence of unknown events, or interruptions, that can happen in the system and maintain system's safety. Optimization over R_{ECO}, which results in an ecologically similar performance captured by a range of ASC/DC values known as the ecological "window of vitality" [167], [168], can enhance the system's ability to tolerate disturbances and maintain its functionality securely. This ecological range has been found to be beneficial for the resilience of not only physical power grids but also water distribution networks [169] and more generic systems of systems [170], [171].

The examples above demonstrate various power system resilience measures that consider different aspects of power system properties, such as network topologies, power flow distribution, energy supply, or load importance. However, it is worth noting that there are also various resilience measures focusing on the assessment or prediction of risk with external information. Through risk assessment and evaluation of countermeasures, operators can better prepare hardening strategies, and preventative and remedial actions against HILF events, thereby enhancing power systems' resilience. Umunnakwe et al. [46] and Stanković et al. [47] have summarized those resilience-related metrics in detail and systematically analyzed their features and application scenarios within the context of the resilience trapezoid.

Regardless of the inputs and methodologies used for power system resilience quantification, these measures have to be integrated with power system constraints, thereby guiding the design and operation of modern power systems as well as the development and application of advanced technologies for inherently resilient power grids. As *Kirchhoff's law*-dominated power systems become increasingly dependent on weather and human factors (e.g., system operators situational awareness and customer-based demand response), it is paramount to leverage features across different domains, including cyber, weather, and societal systems, to study their interactions and interdependencies that can impact the system performance. Accounting for modern power system resilience cannot be done otherwise.

C. Gaps Between Research and Realization

Research is conventionally ahead of field applications with a new technology or a new perspective. It could prompt actions such as the adoption of EVs, the construction of transmission lines, and the deployment of advanced technologies. Their outcomes may challenge existing norms and potentially necessitate substantial investments to renovate the system. For a widespread critical infrastructure, whether or how stakeholders adopt *unconventional* recommendations or methodologies depends on various factors.

As discussed earlier, new technologies, such as blockchain technologies and quantum computing, have the potential to enhance power systems' resilience and security. Blockchain technologies can facilitate more secure and efficient communication among different sectors within power systems. The decentralized paradigm of blockchain technology can contribute more redundancy and resilience for power systems against system failures and cyberattacks, in contrast to the centralized paradigm. Many existing applications and investigations of blockchain technology in power systems focus on realizing peer-to-peer trading, securing energy management of EV and DERs, and implementing demand response [172]. Moving beyond these applications, Mylrea and Gourisetti [73], Liang et al. [74], and Wang et al. [79] have demonstrated the benefits of enhancing resilience in power systems using blockchain technology, considering various adversaries scenarios. Quantum computing introduces a new mechanism for modeling and solving entangled states and intractable problems with improved efficiency and scalability, which can enhance the resilience of power systems through power system analytic, decision-making, and device control. Several companies now offer quantum

computing services with noisy-intermediate-scale quantum computers [173], bringing quantum technology closer to practical applications. Jiang et al. [77], Tang et al. [78], Zhou and Zhang [92], and Fu et al. [155] have utilized quantum computing services to devise their quantum circuits, testbeds, and algorithms, showcasing the effectiveness of quantum computing to enhance power systems' resilience with faster and more efficient computation and analytic capabilities. However, it is important to note that the existing applications and demonstration are limited in small-scale virtual or laboratory environments due to the cost and the complexity of modeling power systems under the new mechanism. When deployed in a real system with customers, operators, and potential cyber and physical attacks, the complexity of the system, the volume of data, and the *noise* in the system could discount their benefits. Stakeholders may raise concerns about the effectiveness or cost-effectiveness of implementing these new technologies, as it would require significant financial investments from both customers and utility owners. Mollah et al. [172], Zhou et al. [173], Ajagekar and You [174], Ullah et al. [175], Di Silvestre et al. [176], and Mohammadi and Saif [177] have summarized the applications, development, limitations, and directions of quantum computing and blockchain technologies in power systems. It should be recognized that further development and advancement of quantum computing and blockchain technologies are still needed for their everyday applications. We are optimistic that these advanced technologies will soon be extensively applied to power systems, leveraging their significant *computing and security capabilities* to enhance the resilience of modern power systems.

The modeling of power systems relies on existing benchmark models [178], [179] or synthetic models based on geographic and demographic information [180], [181], [182], [183] that capture the physics and topological characteristics of real power grid. However, these models do not include the realistic consideration of customer-side resources. In theory, customers now have the ability to take proactive actions to ensure and enhance power systems' resilience with their own EVs and DERs [62], [63], [79], [108], [141], [144]. These resources and customers' responses are simplified as additional inputs to existing models. However, there is a gap between this hypothetical model and real situation during hazards or disruptions. There is a need to investigate and validate the penetration of EVs and DERs in households, the controllability of individual assets during hazards, and the customers' *wiliness* and benefits to participate in power system operation and regulation. The increasing penetration of RES has made modern power systems increasingly reliant on weather information for predicting both RES output, end users' consumption, and network status. It is essential to include weather, geographic, and demographic information into power system models to better account for external influences on power systems operation. The impacts of temperature on power networks can be captured through heat balance equation [184], which can be integrated with power flow equations [185], [186], [187] to analyze the power flow distribution under extreme and unexpected environment. Ahmed et al. [188] and Overbye et al. [189] presented methodologies for including more weather information, such as ambient temperature, wind speed, wind angle, and solar radiance. Zheng et al. [190] presented an open-access data hub that integrates external data of weather, human, health with electricity load data with mobile device location, and satellite imaging data for a comprehensive analysis. Last but not least, cyber networks are the carrier of information and data for operators to monitor and control power systems. As introduced in [157], [158] and [159], a successful high-impact cyberattack involves several steps, from planning to execution, which requires knowledge from both cyber and physical domains. Traditional cybersecurity studies on power systems only consider *execution*, such as FDI and false command injection, on physical networks. Nevertheless, there are some signatures in the cyber data that can help operators identify the threat in an early stage and thus ensure the system's security and resilience. It is crucial to create a granular model of the cyber network, considering its functionality and topology, to fully comprehend cyberattack's impact on power systems. By emulating the entire multistage cyberattacks, we can obtain realistic cyber–physical datasets for different studies. The functionality of communication systems can be emulated with various software [191], [192], [193]. However, their topological characteristics are often simplified by equating them to the connected physical network or using models of scale-free, random, or small-world networks, which overlook cyber networks' distinct features. Sahu et al. [194] have presented a hierarchical model of communication network that captures all detailed interactions among different stakeholders and participators in power grids considering various communication and intelligent electronic devices. A detailed and realistic cyber model allows the investigation of cybersecurity at different phases of cyber intrusion [195], [196]. This level of granularity should be incorporated into future cyber–physical power systems' modeling and studies to enhance modern power systems' inherent resilience against cyber disturbances.

Existing operational and design standards are not easily modified. For example, power system operation utilizes OPF or SCOPF to ensure their security and resilience with minimum operational cost. These concepts and models are well established and implemented, *guaranteeing* the most economic operations. An innovative R_{ECO} OPF is proposed in [104] and exhibits its superiority over OPF and SCOPF regarding the systems' survivability under $N-x$ contingencies. Nonetheless, the operational cost of the more resilient R_{ECO} OPF is higher than OPF and SCOPF. Other reviewed resilience metrics and methodologies [60], [100], [101], [111], [116], [140] also take noneconomic factors into consideration. Although the analyses demonstrate economic benefits in long term, there are still uncertainties

regarding whether or when the investigated contingency scenarios will happen. This raises a question for stakeholders: whether they are willing to bear the increased cost of designing and operating power systems for enhanced resilience or choose to take the risk of operating the system at its economic margin and implement actions only after contingencies occur to restore the system back.

Balancing the tradeoffs among resilience, cost, and efficiency is a critical task when considering various strategies to enhance the resilience of modern power systems. Moreover, the integration of RES and EVs underscores the necessity of including and validating the environmental benefits when researchers advocate their work in the context of enhancing the resilience of modern power systems. Deriving a series quantifiable metrics of resilience regarding modern power systems' infrastructure and functionalities will enable the analysis to trade off resilience enhancements, economic benefits, and environmental benefits. Nevertheless, determining these tradeoffs among resilience, cost, and efficiency for different resilience enhancement strategies in modern power systems is complex. Considering modern power systems' cross-domain multilayered architecture, the design and operation of modern power systems depend on various factors. Consequently, one resilience enhancement strategy may entail compounded benefits, require additional investment, or face constraints from other domains. Furthermore, as critical infrastructure, the development of modern power systems is influenced by policymakers' prioritization of objectives across various issues. Overall, identifying the right balance among resilience, cost, and efficiency of different resilience enhancement strategies is decided by the stakeholders, including grid operators, market participators, customers, and policymakers, and based on subject-matter expertise.

There needs to be a transition period during which utilities, operators, and customers should participate in the field testing of new technologies, models, and standards under normal and adversarial conditions. It is also essential to assess how stakeholders in different domains react to new schemes, technologies, and environments toward more resilient modern power systems. Holistically modeling and analyzing modern power systems with cross-domain information, along with evaluation of resilience, cost, efficiency, and other benefits, can assist all stakeholders in understanding how to prioritize different resilience enhancement strategies.

VII. NEW OPPORTUNITIES IN MODERN POWER SYSTEM RESILIENCE ENHANCEMENTS

Based on all reviewed articles, we believe that *infrastructural resilience* lays the foundation for the entire system's inherent resilience against all potential hazards, and *operational resilience* determines how resilient the system can be during and after hazards with available resources. However, modern power systems consist of heterogeneous networks and data, forming a complex system of systems. Physical networks are the backbone structure of entire systems for energy deliver, cyber networks are collecting and delivering data, and human networks are making decisions. Data from the weather, physical, cyber, and human domains together determine the resilience of modern power systems. The modeling, data analytic, and resilience metrics are interrelated for ensuring and enhancing the resilience of energy infrastructure and services [197]. There are some inconsistencies and disconnects on modeling modern power systems considering their heterogeneous network and data across different domains [198]. However, it is significant to characterize interdependencies across different domains as well as explicitly incorporate them for holistically enhancing modern power systems' resilience [199].

As suggested in [93], it is essential to include more detailed physical interaction models to capture the impact of other domains on power systems' resilience. An example of this focused on the direct inclusion of weather information in the power flow is presented in [189]. It improves the accuracy of power flow studies considering the integration of RES through the direct inclusion of weather data. The fusion of cyber and physical data also benefits the detection and defense against cyber and physical attacks for the security of modern power systems. Sahu et al. [200] utilized several machine learning techniques to fuse the cross-domain cyber and physical data to prevent cyberattacks with more accurate identification of cyberattacks. Huang et al. [201] proposed a series of programmable logic controllers logic to detect and defend cyberattacks using the IEC 61131-3 engine with the cyber information and physical measurements in industrial controllers. With the cross-domain cyber and physical information, the proposed cyber–physical alert and control logic can more accurately detect and determine the source of contingencies whether they are from the cyber or physical domain. These examples demonstrate the necessity to leverage modern power systems' heterogeneous networks and data from different domains to holistically enhance their inherent resilience. It is essential to develop a granular model of modern power systems that considers the interconnected cross-domain networks and encapsulates heterogeneous information and external factors. Such a model can facilitate comprehensive studies on resilience enhancements against various threats.

Toward resilient modern power systems, there is a need to *holistically* enhance or optimize both *infrastructural resilience* and *operational resilience* considering their *cross-domain multilayer* data and infrastructures. Therefore, two challenges must be overcome to achieve the goal: 1) derive a benchmark to determine the level of resilience and guide the design of modern power systems' architecture considering the interdependence among heterogeneous networks across different domains and 2) develop an intelligent agent to inform and control the system for its optimal

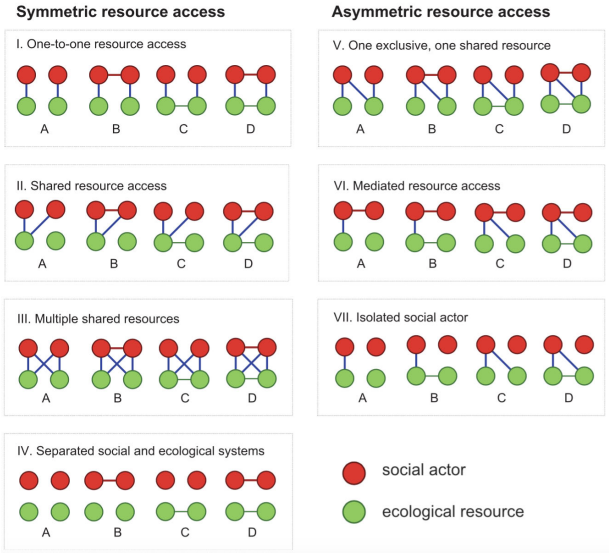


Fig. 8. ***Seven different social–ecological systems motif families [202].***

resilience considering heterogeneous data across different domains.

The following sections present potential directions to address the above challenges using *higher order subgraph analyses* and SciML). As new perspectives on analyzing modern power systems, we also discuss the requirements necessary to implement them for future research and applications.

A. Higher Order Subgraph Analyses to Determine the Benchmark of Infrastructural Resilience

Topological analyses of power networks play an important role in understanding their infrastructural resilience and can provide guidance for operational resilience. Metrics, such as node degree, betweenness centrality, and shortest path, have been integrated with power systems' properties to assess node and edge importance for resilience-oriented design and operation [204]. One of the most important developments in this field has been in the creation of high quality, geographically based synthetic electric grids [181], [205], [206], with validation of these grids presented in [182]. However, there is an urgent need to understand the interdependence among heterogeneous networks, including cyber, physical, and human networks, for modern power systems. Node- or edge-based studies cannot capture the underlying relationship, while the higher order subgraphs associated with intranode or internode and edges may reveal more information regarding the interdependence and interactions among heterogeneous networks [207]. For example, Bodin and Tengö [202] utilized the four-node motifs (as shown in Fig. 8) where two nodes are from social systems (social actors) and two nodes are from ecological systems (ecological resources) to understand the social–ecological interdependencies for interconnected social and ecological networks. Both social–ecological systems and cyber–physical systems are multilayered networks. Intuitively, the patterns of interdependence between social and ecological systems could also be employed to understand the interdependence between cyber and physical networks at their boundaries.

Higher order subgraph analyses are emerging tools for understanding the properties of complex networks. *Network motifs* are defined as patterns of interconnections or subgraphs occurring in complex networks at numbers that are significantly higher than those in randomized networks [208]. They have been used to analyze the structural properties of ecological food webs and neuron networks, which have turned out, can be useful for complex networks. Benson et al. [209] used a network motifs-based framework for network partitioning and revealed new organizational patterns and modules in complex systems. Stone et al. [210] demonstrated that identifying network motifs embedded in a larger network could indicate the presence of evolutionary design principles or an overly influential role in system-wide dynamics. In power networks, network motifs have been used to assess power grids' reliability and risks [211], [212].

1) Higher Order Motifs With Ecological Robustness: As mentioned earlier, *resilience* originated from ecosystems and various metrics have been derived to quantify the features of long-term resilient ecosystems. R_{ECO} [see (11)–(15)] is one of metrics that has been related to features in ecosystems that support their resilience and has been used to translate the resilient properties of food webs to power systems through redistributing power flows [104] and redesigning power networks [56], [60]. An extended model has been proposed to analyze power systems' resilience with reactive and apparent power flows considering structural impacts from generators and shunt capacitors [213], [214]. This metric has been applied to other human networks, such as water distribution networks [169], supply chains [215], and more generic systems of systems [171], and shown great enhancements on system's resilience. Since both R_{ECO} (resilience property) and network motifs (higher order subgraph analyses) are originated from ecosystems, the motif analyses of the R_{ECO}-oriented power networks may reveal new suggestions on resilient power network design. Here is a preliminary study.

Fig. 9 shows all connected undirected four-node motifs, which are six types of induced subgraphs. Dey et al. [211] demonstrated that the four-node motifs' motif characteristics, motif concentration (C_i), can be used as an indispensable tool for understanding local network structure that contributes to power grid resilience. C_i is the ratio of the number of occurrences of the type i motif (N_i) to the total number of all n-node motifs in the network

$$C_i = \frac{N_i}{\sum_i N_i} \tag{16}$$

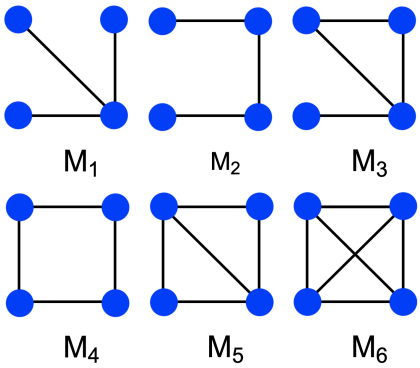


Fig. 9. *All connected four-node motifs.*

where $\sum_i N_i$ is the total occurrence of all n-node motifs in the network.

Fig. 10 shows four R_{ECO}-oriented ACTIVSg200 networks [60], and Fig. 11 shows the analyses of R_{ECO}, N_i, C_i, and survivability for each case. The survivability is evaluated under $N - x$ contingencies, where a different number of power system components (branches, generators, and buses) are removed from the system, and it is quantified as the number of violations and unsolved contingencies.

With more branches added to the original network, the system's inherent ability to tolerate disturbances (corresponding to the reduction on the violations and unsolved contingencies) is improved and shows an increase in R_{ECO}. Through a comparison of different R_{ECO}-oriented power networks, M_3 and M_5 may be favored by ecosystems' resilient traits. From Fig. 11, M_1 and M_2 dominate the power networks with the most occurrences in the graph and highest motif concentration. However, the trend of C_i shows that the increments of M_3 and M_5 are more noticeable. Since R_{ECO} favors redundancy over efficiency for food webs [168], we can deduce that both M_3 and M_5 highlight this feature. Thus, it could be beneficial to intentionally increase M_3 and M_5 when we design power networks for better inherent infrastructural resilience. It is important to further validate this claim under dynamic adversarial events and analyze motif patterns, which will be a future work.

2) Higher Order Motifs in Cyber–Physical Power Grid: As we mentioned earlier, higher order motifs have been used to disentangle the interdependence between ecosystems and social systems, which are essentially heterogeneous networks regarding their topology and functionality. There is great potential to apply higher order motifs-based analyses into cross-domain multilayered power systems with a granular graphic representation to identify the critical local structure connecting cyber and physical networks that are essential for systems' inherent resilience and security.

Huang et al. [216] utilized the *four-node all-connected motifs* to characterize the interdependence between cyber and physical networks considering three cyberattack scenarios on an augmented cyber–physical WSCC 9-bus system [217]. Unlike previous work, this augmented cyber–physical WSCC 9-bus system considered a more realistic and detailed cyber topology with various components, including protective relay, network switch, router, and control center computers, as shown in Fig. 12. Protective relays connect cyber and physical networks with capabilities of control and monitoring the physical network and transferring data and information over the cyber network.

Fig. 13 shows the preliminary study on the motif patterns at the cyber–physical connection under different attack scenarios. The investigated cyberattack scenarios consider cascading failures from communication networks to physical networks, which is connected through protective relays. Based on the topological importance of cyber nodes, the adversary targets the most important cyber node and removes it along with all connected edges. The importance of cyber nodes is measured by their topological properties, including node degree, closeness centrality, and betweenness centrality. Once the cyberattack reaches protective relays, which controls and monitors physical networks, the connected physical component is removed from the physical network. This action can result in a physical disturbance affecting the operation of the power system. With the simulation, there is a remark of "physical network breakdown," specified by the black dashed lines in Fig. 13, showing the period from the initial physical disturbance triggered by cyberattacks until all loads are not supplied by the system or the system is blackout (whichever comes first).

Under all attack scenarios, we can observe that the *physical network breakdown* is triggered by the decrease of M_2–M_4. M_2 is *I.C* in Fig. 8, wherein two cyber nodes are connected and each one controls a physical device. Since protective relays bridge the cyber and physical network, the reduction of above motifs can indicate the potential risk of cascading failures and disturbances on power systems' functionalities. Based on the results, we observe that the four-node motifs, particularly M_2–M_4, can represent the resilience and reliability of the cyber–physical power grid against cyberattacks at cyber–physical connections. A higher percentage of M_2 and M_3 in the system indicates that the cyber–physical network possesses greater resistance to prevent cyberattacks from disrupting physical network and thus maintain the functionality of power systems. Inspecting M_2–M_4 at the boundary of the cyber and physical networks can provide valuable information about potential risks within the system.

From the above preliminary study, it can be observed that higher order subgraph analyses can provide new insights into resilient network design and system risk analyses, especially for small networks with nodes from different domains. Further investigation and development of high-order subgraph analyses on modern power systems could enhance situational awareness of cascading failures across different networks by examining variations of motifs. In addition, Binqadhi et al. [218] investigated the resilience of cyber–physical power systems, leveraging

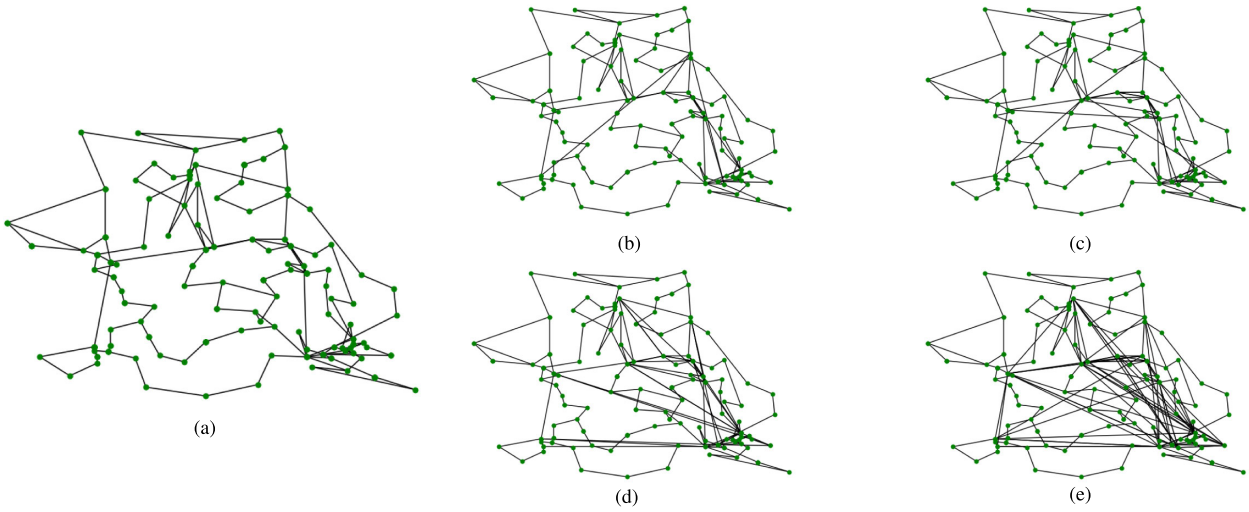


Fig. 10. *R_{ECO}-oriented ACTIVSg200 network structures, the case information is available in [203]. (a) Original network topology. (b) R_{ECO}-oriented network topology 1 (added five branches). (c) R_{ECO}-oriented network topology 2 (added 15 branches). (d) R_{ECO}-oriented network topology 3 (added 26 branches). (e) R_{ECO}-oriented network topology 4 (added 31 branches).*

higher order motifs to account for the impact of cyber networks on power delivery against various hazards. For modern power systems, it is paramount to consider heterogeneous networks of cyber, physical, and social domains. Even though the topologies of these networks are geographically overlapped, there are many distinctions within local networks, where the higher order subgraph analyses at the level of small network patterns will be more useful. The interactions and interdependence among different networks also involve with different patterns of subgraphs. The risks and uncertainties associated with nodes may impact the higher order subgraph patterns by taking out suspected nodes from the network. Higher order subgraph analyses can be a useful tool to dissect the underlying relationships for more stringent design with better resilience against propagated adversarial events.

Through a granular graphical representation of multilayered power systems, higher order subgraph analyses can disclose the key local structure within the network as well as identify critical connections across different networks, especially for the interconnected cyber and physical networks. The cyber network serves as the carrier of information and data that are critical for the physical network to reliably deliver energy. Existing standards and requirements for network design and system operation emphasize reliability and resilience within each network or domain but often overlook the compounded effects stemming from interactions with other systems [156]. In addition, there is an increasing integration of RES at both large-scale power plants and residential-level DERs. This rising penetration of RES has introduced more uncertainties into operating power systems, considering the stochastic nature of weather information and human decision-making. Given the reliance on communication networks for monitoring and controlling RES, cybersecurity becomes crucial for the security and safety of both RES and the entire power grid. Higher order subgraph analyses can contribute valuable insights to the network design of interconnected cyber–physical systems, bridging the information technology (IT) and operational technology (OT) to ensure and enhance the resiliency and security of modern power systems. The interconnected human/social networks with power grid can also be analyzed through network motifs to dissect their interdependence, especially considering the impact of RES, for a resilient multilayered network design. New benchmarks could be developed for designing resilient modern power networks, considering their heterogeneous architecture using network motifs.

B. SciML for the Optimal Operational Resilience

Machine learning and data analytic are important tools for modern power systems considering the need to process large amount of data across different domains. Various machine learning algorithms have been applied to power systems for secure and resilient operations. They can provide suggestions or recommendations to operators to ride through contingencies if similar patterns have been included in historical or they are predictable. However, increasing *unexpected* hazards, whose patterns are not included or predictable, could compromise the trustworthiness of machine learning algorithms. It is important to consider distinct governing mechanisms in different systems across different domains and devices to make optimal decisions, but this can lead to intractable problems. With the introduction of more external influences, particularly the highly stochastic human and weather factors, into power system design and operation, numerous intractable tasks need to be addressed in power system operations. Unlike the optimization models, where all power system

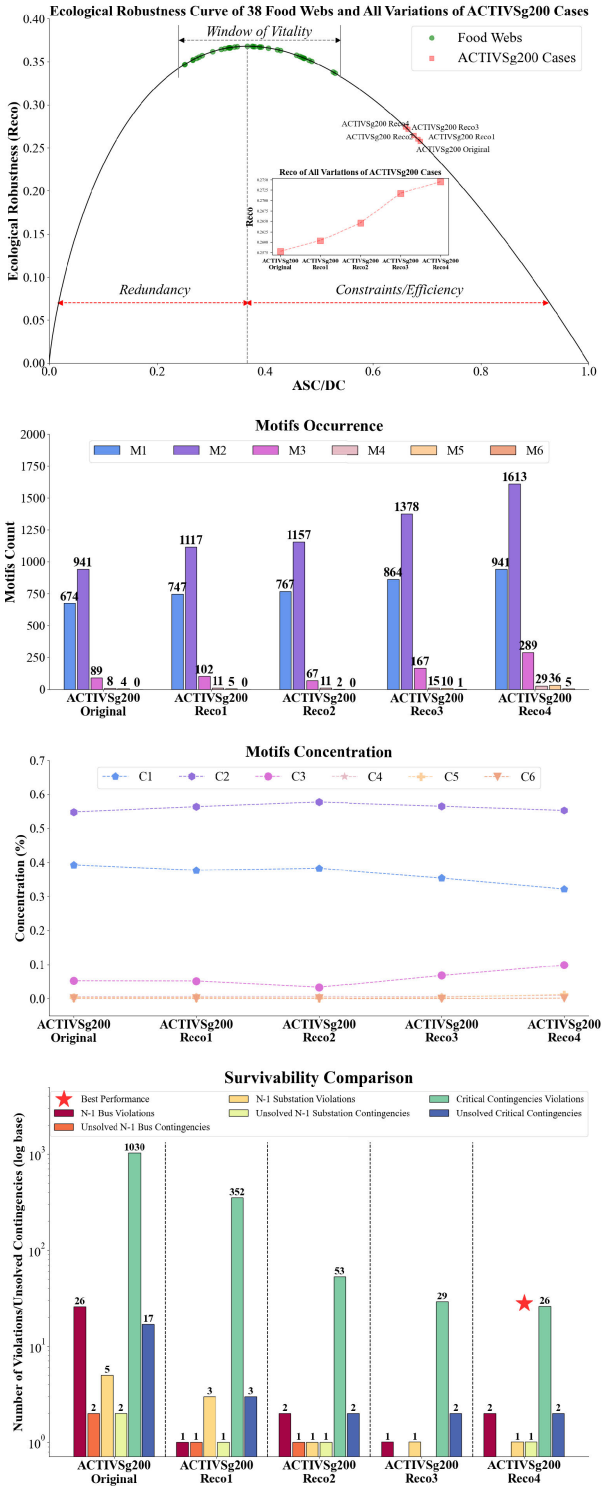


Fig. 11. ***Motif-based structural, R_{ECO}, and resilience analyses for all variations of ACTIVSg200 cases.***

constraints are explicitly listed, machine learning techniques are limited for their applications in power systems, considering the need of high quality and quantity of training data, their infeasible or inconsistent solutions for practical implementation, and their low generalizability and interpretability. In order to prompt the development and application of artificial intelligence (AI) in critical infrastructures with direct control and operation, it is of great importance to validate and verify aleatory uncertainties from heterogeneous data and epistemic uncertainties from machine learning algorithms.

SciML is an emerging field that combines machine learning and scientific computation to provide interpretable models with improved verification and validation in applications [219]. It becomes crucial for efficient, explainable, and trustworthy decision-making and problem-solving leveraging machine learning and scientific computation to ensure system reliability, security, and resilience. Physics-informed neural network (PINN) is one type of SciML, which has encoded model equations, such as partial differential equations and physics constraints, as components of deep neural networks. These features allow PINNs to address problems that are described by few data or noisy experiment observations. PINNs can be viewed as unsupervised learning when they are trained solely using physical equations and boundary conditions for forward problems. For inverse problems or dealing with noisy data, PINNs are considered as supervised learning with labeled datasets [220]. For power systems, the core paradigm of PINNs, including physics-informed *loss function*, *initialization*, *design of architecture*, and *hybrid physics–deep learning*, has been used for various applications, such as state estimation, dynamic analysis, power flow calculation, optimal power flow, anomaly detection and location, and model and data synthesis. The improved accuracy, efficiency, and generalizability have demonstrated the benefits of PINNs in power system problems [221]. However, existing applications focus on the physical networks, while modern power systems are cyber–physical systems with

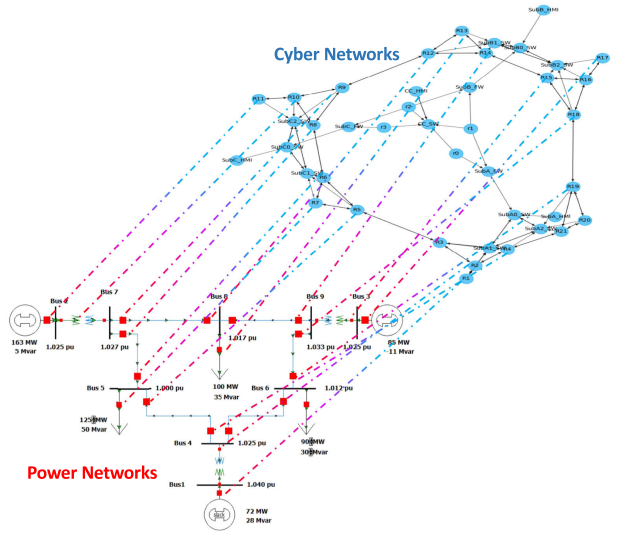


Fig. 12. ***Augmented cyber–physical representation for WSCC system [217].***

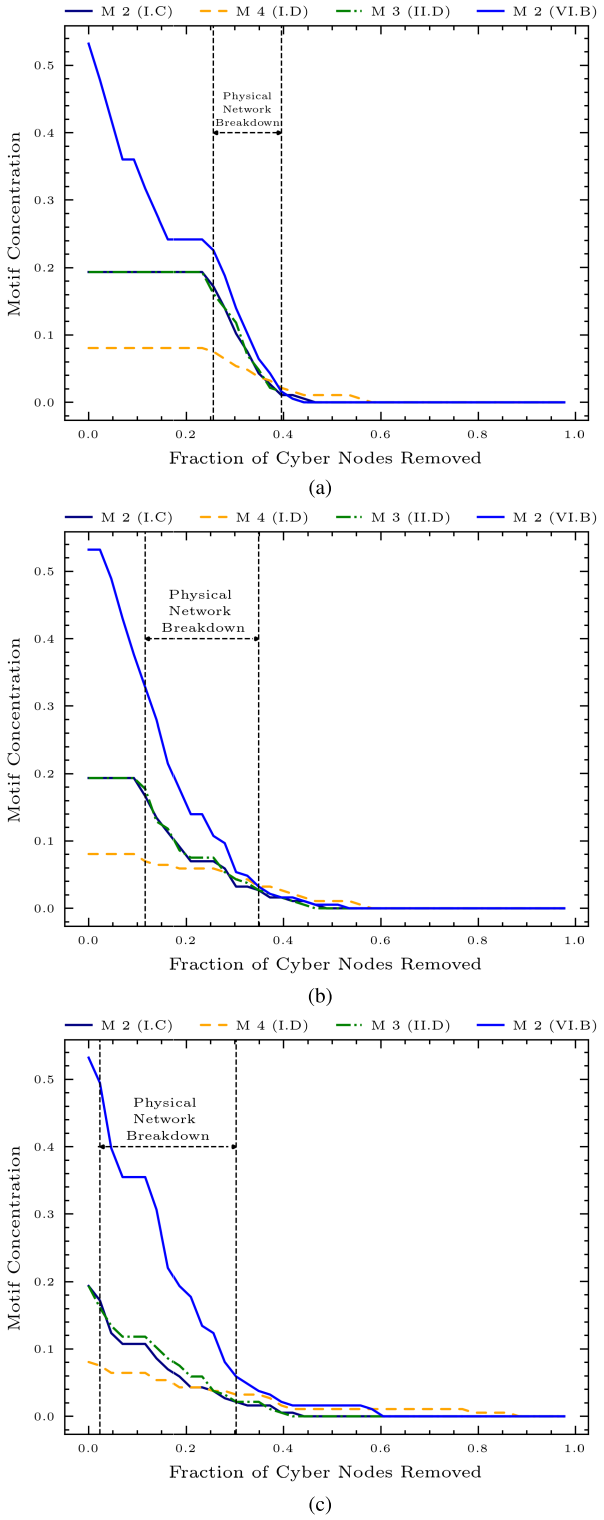


Fig. 13. ***Motif concentration on the WSCC 9-bus cyber–physical connections under different cyberattacks [216]. (a) Node degree-based attack. (b) Closeness centrality-based attack. (c) Betweenness centrality-based attack.***

RES, associated with more uncertainties. It is essential to consider heterogeneous architectures and data from different domains to account for external influences on power system problems. Meanwhile, the spatial–temporal property of resilience should be considered during the development of SciML for its application in power systems problems, leveraging its scientific computing capabilities to provide feasible and trustworthy solutions for resilience enhancement.

Modern power systems are generally graphs with different attributes across different domains. The associated data and features can be represented using the graph-structured data as $\boldsymbol{G} = \boldsymbol{(V, E)}$, where $\boldsymbol{V}$ is the set of nodes and $\boldsymbol{E}$ is the set of edges. There are generally a nodal feature matrix $\mathbf{X}^{\text{node}}$ and an edge feature matrix $\mathbf{X}^{\text{edge}}$ associating with $\boldsymbol{V}$ and $\boldsymbol{E}$, respectively [222]. For the spatial–temporal graph, the data can be represented as $\mathbf{G}^{(t)} = (\mathbf{V}^{(t)}, \mathbf{E}^{(t)}, \mathbf{X}^{(t)})$ considering the variation of topology and attributes along with time t [223]. As modern power systems are increasingly dependent on weather and end-user behaviors, which depend on the geographic and demographic information, such information may play an important role in influencing power system operations. The geometric correlation of data across power systems, weather, and human factors is necessary for inferring modern power systems' status. In addition, cyber networks carry all information for operators and stakeholders. The topological attributes and data of cyber networks are essential for cyber resilience. Graph data of cyber networks should consider cyber features, such as re-transmissions, round trip time, number of packets, and frame length. These factors can determine the security of cyber networks, as well as the physical data carried by cyber network, which can determine the status of power systems. The information on external factors, such as weather conditions and human behaviors, can also be transmitted to improve the assessment of the operation of weather- and human-dependent RES.

Graph neural networks (GNNs) are a popular machine learning and data mining approach for graph data. GNNs have demonstrated great capability in handling graph data in different fields such as computer vision, forecasting, recommendation systems, and event detection, leveraging topological attributes [224]. GNNs have also been integrated with different power system problems, including load forecasting, anomaly detection, and contingency prediction, through encoding power system data in graphs [225], [226], [227]. Considering the interaction and interdependence across different domains, particularly their heterogeneous networks and data, there is a great interest in further developing GNNs to process graph data from various domains in modern power systems. Simplicial neural networks (SNNs) have recently emerged as a way to deal with *multidimensional graphs* with *higher order interactions* between vertices [228]. Chen et al. [229] proposed a block simplicial complex neural networks (BScNets) to integrate knowledge on interactions among multiple higher order graph structures for link prediction. Chen et al. [230] utilized persistent homology and SNNs to

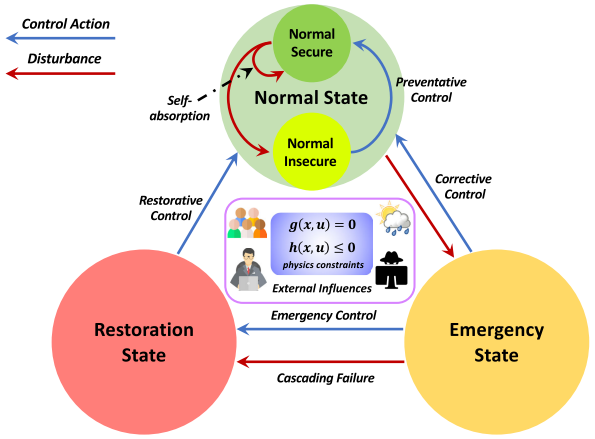


Fig. 14. ***Power system state transitions considering disturbances and control actions.***

construct higher order topological neural networks to efficiently learn outages in distribution networks. SNNs could potentially be applied to interpolate data and their interactions across heterogeneous networks in modern power systems, leveraging the topological features (both geographic and geometric information) and attributes across different domains.

Fig. 14 categorizes the states of modern power system into *normal secure*, *normal insecure*, *emergency*, and *restoration* based on operational conditions, as well as demonstrates the transition among these states to capture the temporal property of resilience under adversarial events.

1) *Normal Secure:* All equipment is operating within limits and no critical contingency will cause real-time operational limit violations.
2) *Normal Insecure:* All equipment is operating within real-time operating limits, but one or more contingencies will cause operational limit violations.
3) *Emergency:* Some equipment is operating outside of real-time operational limits.
4) *Restoration:* There has been a major outage.

Disturbances from natural disasters, device failures, cyberattacks, or human mis-operations can cause a modern power system to transition from *normal secure* to other states, depending on the severity of the disturbance and the system's level of its inherent resilience. Different control actions are taken to return the system back to *normal secure*. It is worth noting that some *emergency state* situations have to shed loads for system-wide resilience and security. Thus, the *emergency control* first brings the system into *restoration state* with regional outage and then moves to *normal state* for the entire system through *restorative control*. This state transition can be explicitly expressed through physical models and constraints of power systems, and disturbances from other domains (e.g., extreme weather, cyber threats, and human factors) could be estimated through machine learning techniques. In addition, this state classification with the consideration of external influences can assist human operators and machine learning techniques more *efficiently* identify the *optimal* solution for modern power systems' resilience by eliminating inappropriate actions and state transitions.

By leveraging PINNs' capability to interpolate physical models with encoded equations, GNNs' capability to handle graph data, deep learning's capability to process heterogeneous data, and the physics-guided state transition, we propose a generalized SciML-based framework for modern power systems, as shown in Fig. 15. The proposed SciML-based framework aims to provide trustworthy analyses, recommendation, and control for modern power systems considering their heterogeneous networks and data across different domains.

From our perspective, in modern power systems, heterogeneous networks, including operator networks, communication networks, and physical networks, can be abstracted from the entire system, along with their interconnections. These networks can be represented with different graphs and graph-structured data as multiattribute nodes and edges. These interconnected graphs capture the system's status, incorporating physical measurements and cyber features, geographic information along with associated weather data, and demographic information for inferring energy consumption and local flexibility with households' DERs and EVs. With the physical models and constraints of power systems, SciML has the potential to harness these data for efficient and trustworthy decision-making processes, thereby enhancing modern power systems' operational resilience against unexpected contingencies. The proposed generalized SciML framework will take in this graph-structured data as input and handle the intergraph and intragraph, heterogeneous data, and mathematical models that describe the state of modern power systems, guiding operations for optimal resilience. In particular, the integration of RES and EVs into power grids has increased the complexity of control problems, affecting the system's stability and security. Stochastic influences from weather condition, human decision, and cybersecurity need to be estimated for their compounded impacts on system operations. The goal of this generalized SciML-based framework is to holistically analyze modern power systems, considering the heterogeneous networks and data for theoretically explainable situational awareness of foreseeing disturbances. This framework aims to offer trustworthy recommendations for operators to defend against contingencies and directly control the system or devices to prevent or ride through cascading failures, utilizing all available resources connected to modern power systems.

C. Implications and Implementations

As we emphasized earlier, constructing a granular model of modern power systems that considers interconnected cross-domain networks and encapsulates heterogeneous information and external factors is crucial. Based on the

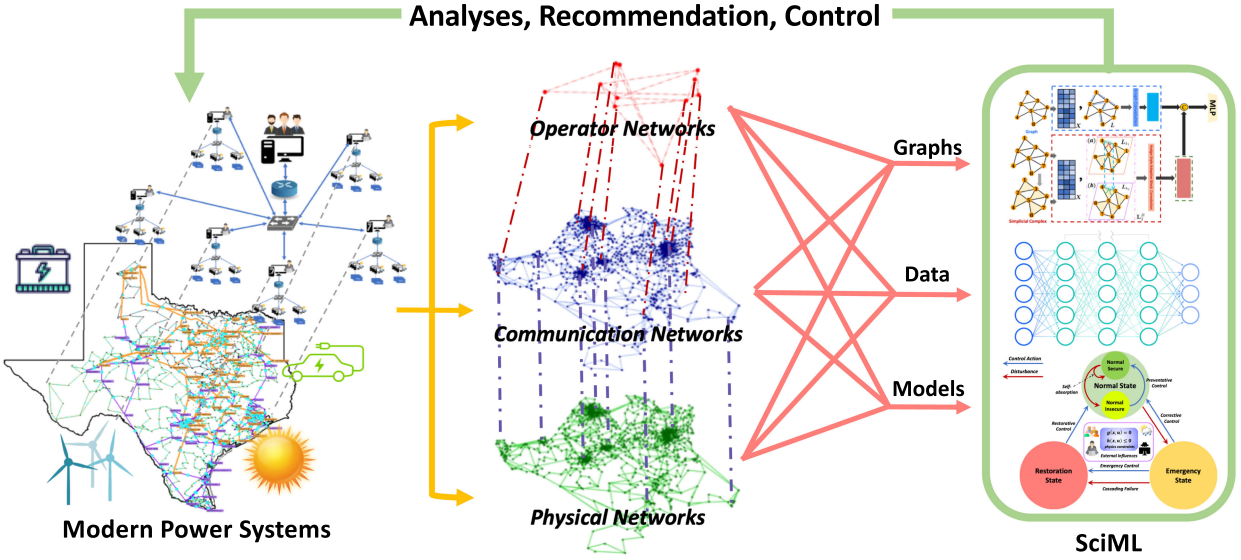


Fig. 15. *Generalized SciML-based framework to handle heterogeneous networks and data of modern power systems for verifiable and trustworthy analyses, recommendation, and control with the enhanced entire system's resilience.*

above discussion, we believe that higher order subgraph analyses and SciML have the potential to generate new knowledge and advance techniques for enhancing the inherent resilience of modern power systems, considering their interconnected heterogeneous networks and data. While both techniques exhibit great potential for improving the resilience of modern power systems, given their cross-domain multilayer architectures, there remains a need for additional research and development to facilitate their integration into real power systems.

1) Implications: Higher order subgraph analyses enable a comprehensive view and analyses of multilayered heterogeneous networks in power systems. The preliminary studies in this article show that specific motif patterns are essential local structures for the security and inherent resilience of modern power systems regarding their physical networks as well as interconnections between cyber and physical networks. As modern power systems closely interconnect with other critical infrastructures, such as transportation networks, gas networks, and thermal networks, higher order subgraph analyses can also be applied to discover the key connections among those networks for overall resilience enhancement. Higher order subgraph analyses offer a pathway to contribute new knowledge and set standards for the resilient system design in both single- and cross-domain networks, enhancing the inherent resilience and security of modern power systems and other interconnected infrastructures.

SciML will be an indispensable tool for future power systems and other critical infrastructures to provide trustworthy solutions for various complicated and intractable tasks. As shown in Fig. 15, the proposed generalized SciML-based framework has the capability of processing large amounts of heterogeneous data across different domains and networks and to provide explainable and trustworthy decision-making for system operations with guaranteed resilience, leveraging features from PINNs, GNNs, reinforcement learning, and deep learning. Integrating SciML with industrial control and monitoring devices and EMSs can enable agile and trustworthy operations in power systems against unexpected events raised from different domains and thus enhance the system's operational resilience. It is important to note here that the proposed framework is a *general* direction for developing SciML algorithms for their applications in modern power systems. This generalized SciML-based framework aims to bridge recent advancements of SciML and broader AI with their applications to modern power systems considering their cross-domain multilayered architectures. With specified *tasks*, *constraints*, *features*, and *data*, the developed SciML-based applications should be compatible with any power grid in different regions for various situations.

With the electrification of other critical infrastructures, such as transportation systems, water systems, and manufacturing systems, it is essential to consider the interdependence and interactions of interconnected heterogeneous networks in their design and operation. Further investigation and development of higher order subgraph analyses and SciML can advance their applications to other critical infrastructures, enhancing their resilience and security.

2) Implementations: First, synthetic cyber–physical power system models are essential for studying modern power systems, considering their cross-domain multilayer architectures. These models can enable comprehensive analyses of how disturbances from different domains, such as cyber, weather, and human factors, can impact

system performance. This is necessary for the investigation and development of higher order subgraph analyses and SciML on modern power systems. As mentioned earlier, synthetic power grids of physical networks [180], [181], [182], [183] have been created based on geographic and demographic information, providing significant values for power system studies. However, these models lack a corresponding cyber model that captures the interactions and data transactions among utilities, operators, and customers. The core structure of cyber network is characterized in [194], which can be utilized to create synthetic cyber models. By mapping cyber and physical networks, it becomes possible to establish connections between power system simulation and communication emulation through communication protocols, which can provide a more comprehensive power system model. This approach offers a comprehensive view of modern power systems and allows researchers to replicate various hazard scenarios with more detailed data across different domains.

Second, *real* or *realistic data* of modern power systems is crucial for the development and application of SciML. The increasing integration of EVs and RES on the customer side has highlighted the importance in human factors to the system's operation, which are highly stochastic. Human factors and customer-side decisions are influenced by various factors, including weather and economic considerations (e.g., electricity prices and incentive mechanisms). It is essential to recognize that the data for modern power systems should encompass measurements of physical networks, such as energy consumption, power flows, voltage, and currents, as well as external influences, such as weather information, cybersecurity data, and economic information. Furthermore, these data should be linked with the power system model, both topologically or geographically, to better capture their underlying correlations. A systematic dataset can facilitate the development and validation of SciML-based data-driven approaches.

Last but not least, computing power is needed for both higher order subgraph analyses and SciML for their applications in large-scale power systems. The number of motifs increases exponentially with the increase of nodes in the system, which can take a long time to finish the subgraph analyses for cross-domain multilayer power systems. In particular, the real cyber network has more components than physical networks to facilitate a comprehensive analysis, and the social network involving DERs and EVs requires different levels of abstraction to effectively aggregate and estimate their impacts on power grids. As for SciML, there are millions of variables and data in the system. Training a model with such a large dataset also takes a significant amount of time. Leveraging GPU or cloud computing to perform these tasks is necessary. It is also possible to utilize quantum computing to address the intractable problems associated with SciML, given the promise of its large-scale commercial utilization. In addition, the transmission of a large amount of data over a wide area also warrants the development of communication networks. However, the investment and allocation of computing resources to support various analyses and applications that enhance the resilience and security of critical infrastructures depends on stakeholders' decisions.

Overall, the adoption of higher order subgraph analyses and SciML in modern power systems should consider the following three key aspects.

1) It is necessary to create or obtain comprehensive realistic cyber–physical power system models that respect the heterogeneity in cyber and physical networks regarding their topology as well as their interconnected and interdependent functionalities.
2) It is essential to obtain real or realistic power system data across different domains, including physical measurement, cyber features, weather data, and geographic and demographic information.
3) More computational capability is needed for the implementation of higher order subgraph analyses and SciML in large-scale power systems considering their networks' complexity and large amounts of variables in different domains.

VIII. CONCLUSION

Modern power systems are cross-domain multilayer complex systems of systems with the integration of cyber and physical networks, and an increasing penetration of RES at both transmission and distribution levels. As the frequency of unexpected disturbances increases, resilience becomes an essential and desirable property for modern power systems to maintain their functionality under any circumstance. In this article, we have provided a comprehensive review and discussion of power system resilience and its enhancement techniques from different perspectives. Considering the complexity of modern power systems, existing power system resilience enhancement techniques have focused on certain domains: cyber or physical; specific levels: generation, transmission, or distribution; or particular stages: construction or operation. However, it is important to recognize that there are mutual influences among different resilience enhancement techniques. Enhancing cyber resilience ensures data integrity for monitoring and control power systems, thereby improving operational resilience. Enhancing infrastructural resilience provides additional flexibility and resources to enhance operational resilience. Enhancing operational resilience necessitates strengthening and investing in both cyber and physical infrastructures. These techniques from different categories could prompt the development of each other for the entire system's resilience. The interdependence and interactions across different networks play a critical role to determine and enhance the resilience of modern power systems against unexpected events.

As a cross-domain multilayer complex system of systems, it is paramount to holistically design and operate

modern power systems considering heterogeneous networks and data for optimal resilience. This requires an understanding of the interdependence among different networks structurally and functionally, as well as the ability to deal with mixed data from different domains in modern power systems. As a critical infrastructure for modern society, it is necessary to provide explainable, interpretable, and verifiable models and tools for trustworthy decisions on constructions and operations. Leveraging the rapid development and application of AI, we propose two directions for future studies of resilient modern power systems: higher order subgraph analyses and SciML. Higher order subgraph analyses can disclose more underlying relationships of network resilience for intradomain and interdomain network design. SciML can be developed to deal with heterogeneous data and network structures for agile system operations with ensured resilience against unexpected hazards raised from different domains. With a comprehensive cross-domain multilayer modern power system model and its data from different domains, the new knowledge and techniques from higher order subgraph analyses and SciML can contribute to new standards and requirements for resilient modern power system design, operation, and management. ■

REFERENCES

[1] O. Ellabban, H. Abu-Rub, and F. Blaabjerg, "Renewable energy resources: Current status, future prospects and their enabling technology," *Renew. Sustain. Energy Rev.*, vol. 39, pp. 748–764, Nov. 2014.

[2] D. Gielen, F. Boshell, D. Saygin, M. D. Bazilian, N. Wagner, and R. Gorini, "The role of renewable energy in the global energy transformation," *Energy Strategy Rev.*, vol. 24, pp. 38–50, Apr. 2019.

[3] E. Guelpa, A. Bischi, V. Verda, M. Chertkov, and H. Lund, "Towards future infrastructures for sustainable multi-energy systems: A review," *Energy*, vol. 184, pp. 2–21, Oct. 2019.

[4] S. A. Shield, S. M. Quiring, J. V. Pino, and K. Buckstaff, "Major impacts of weather events on the electrical power delivery system in the United States," *Energy*, vol. 218, Mar. 2021, Art. no. 119434.

[5] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[6] G. Andersson et al., "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[7] T. J. Overbye, "Engineering resilient cyber-physical systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2012, p. 1.

[8] T. R. Hutchins and T. J. Overbye, "Power system dynamic performance during the late-time (E3) high-altitude electromagnetic pulse," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Jun. 2016, pp. 1–6.

[9] T. J. Overbye, J. Snodgrass, A. Birchfield, and M. Stevens, "Towards developing implementable high altitude electromagnetic pulse E3 mitigation strategies for large-scale electric grids," in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, Feb. 2022, pp. 1–6.

[10] U.S. National Oceanic and Atmospheric Administration (NOAA). (2018). *Billion Dollar Weather and Climate Disasters: Table of Events*. [Online]. Available: https://www.ncdc.noaa.gov/billions/events/U.S./1980-2018

[11] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters—A review," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1604–1613, Mar. 2016.

[12] X. Liang, "Emerging power quality challenges due to integration of renewable energy sources," *IEEE Trans. Ind. Appl.*, vol. 53, no. 2, pp. 855–866, Mar. 2017.

[13] Z. Hu, Y. Xu, M. Korkali, X. Chen, L. Mili, and J. Valinejad, "A Bayesian approach for estimating uncertainty in stochastic economic dispatch considering wind power penetration," *IEEE Trans. Sustain. Energy*, vol. 12, no. 1, pp. 671–681, Jan. 2021.

[14] J. L. Wert, T. Chen, F. Safdarian, J. Snodgrass, and T. J. Overbye, "Calculation and validation of weather-informed renewable generator capacities in the identification of renewable resource droughts," in *Proc. IEEE Belgrade PowerTech*, Jun. 2023, pp. 1–6.

[15] *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Electricity Information Sharing and Analysis Center (EISAC), Defense Use Case, Intelligence Washington, DC, USA, 2016.

[16] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[17] E. Targett. (Mar. 2020). *High Voltage Attack: EU's Power Grid Organisation Hit By Hackers*. [Online]. Available: https://www.cbronline.com/news/eu-power-grid-organisation-hacked

[18] S. I. Gerasopoulos, N. M. Manousakis, and C. S. Psomopoulos, "Smart metering in EU and the energy theft problem," *Energy Efficiency*, vol. 15, no. 1, pp. 1–18, Jan. 2022.

[19] (2022). *Electric Disturbance Events (OE-417) Annual Summaries*. [Online]. Available: https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

[20] A. Smith, *2010–2019: A Landmark Decade of U.S. Billion-Dollar Weather and Climate Disasters*. Washington, DC, USA: National Oceanic and Atmospheric Administration, 2020.

[21] A. Thompson. (Dec. 2020). *A Running List of Record-breaking Natural Disasters in 2020*. [Online]. Available: https://www.scientificamerican.com/article/a-running-list-of-record-breaking-natural-disasters-in-2020/

[22] *The Future Electric Power United States*, National Academies of Sciences, Engineering, and Medicine, Washington, DC, USA, 2021.

[23] K. M. J. Rahman, M. M. Munnee, and S. Khan, "Largest blackouts around the world: Trends and data analyses," in *Proc. IEEE Int. WIE Conf. Electr. Comput. Eng. (WIECON-ECE)*, Dec. 2016, pp. 155–159.

[24] 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.

[25] C. J. Wallnerström, M. Dalheim, M. Seratelius, and T. Johansson, "Power outage related statistics in Sweden since the early 2000s and evaluation of reliability trends," in *Proc. Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Aug. 2020, pp. 1–6.

[26] V. S. Rajkumar, A. Stefanov, A. Presekal, P. Palensky, and J. L. R. Torres, "Cyber attacks on power grids: Causes and propagation of cascading failures," *IEEE Access*, vol. 11, pp. 103154–103176, 2023.

[27] *Enhancing the Resilience of the Nation's Electricity System*. : National Academies, National Academies of Sciences, Engineering, and Medicine, Washington, DC, USA, 2017. [Online]. Available: https://www.nap.edu/catalog/24836/enhancing-the-resilience-of-the-nations-electricity-system

[28] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Rel. Eng. Syst. Saf.*, vol. 145, pp. 47–61, Jan. 2016.

[29] W. F. Watson, "NERC mandatory reliability standards: A 10-year assessment," *Electr. J.*, vol. 30, no. 2, pp. 9–14, Mar. 2017.

[30] S. Pahwa, C. Scoglio, and A. Scala, "Abruptness of cascade failures in power grids," *Sci. Rep.*, vol. 4, no. 1, p. 3694, Jan. 2014.

[31] L. Xu et al., "Resilience of renewable power systems under climate risks," *Nature Rev. Electr. Eng.*, vol. 1, no. 1, pp. 53–66, Jan. 2024.

[32] Y. Zhao, A. Goldsmith, and H. Vincent Poor, "Minimum sparsity of unobservable power network attacks," *IEEE Trans. Autom. Control*, vol. 62, no. 7, pp. 3354–3368, Jul. 2017.

[33] C. S. Holling, "Resilience and stability of ecological systems," *Annu. Rev. Ecol. Systematics*, vol. 4, no. 1, pp. 1–23, Nov. 1973.

[34] Y. Y. Haimes, "On the definition of resilience in systems," *Risk Anal.*, vol. 29, no. 4, pp. 498–501, Apr. 2009.

[35] *Critical Infrastructure Resilience: Final Report and Recommendations*, National Infrastructure Advisory Council, National Infrastructure Advisory Council (U.S.), Washington, DC, USA, 2009.

[36] *Severe Impact Resilience: Considerations and Recommendations*, North American Electric Reliability Corporation, Severe Impact Resilience Task Force, Atlanta, GA, USA, 2012.

[37] M. Chaudry et al., *Building a Resilient U.K. Energy System*. London, U.K.: U.K. Energy Research Centre, 2011.

[38] M. Kezunovic and T. J. Overbye, "Off the beaten path: Resiliency and associated risk," *IEEE Power Energy Mag.*, vol. 16, no. 2, pp. 26–35, Mar. 2018.

[39] M. McGranaghan, M. Olearczyk, and C. Gellings, "Enhancing distribution resiliency: Opportunities for applying innovative technologies," *Electr. Today*, vol. 28, no. 1, pp. 46–48, 2013.

[40] *Presidential Policy Directive/PPD 21—Critical Infrastructure Security and Resilience*, White House, Washington, DC, USA, 2013.

[41] J. Taft, *Electric Grid Resilience and Reliability for Grid Architecture*. Richland, WA, USA: Pacific Northwest National Laboratory (PNNL), 2017.

[42] B. Yang, S. Ge, H. Liu, J. Li, and S. Zhang, "Resilience assessment methodologies and enhancement strategies of multi-energy cyber-physical systems of the distribution network," *IET Energy Syst. Integr.*, vol. 4, no. 2, pp. 171–191, Jun. 2022.

[43] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renew. Sustain. Energy Rev.*, vol. 58, pp. 1060–1069, May 2016.

[44] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and quantification of operational and infrastructure resilience in power systems," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4732–4742, Nov. 2017.

[45] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the extreme: A study on the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1253–1266,

Jul. 2017.
[46] A. Umunnakwe, H. Huang, K. Oikonomou, and K. R. Davis, "Quantitative analysis of power systems resilience: Standardization, categorizations, and challenges," *Renew. Sustain. Energy Rev.*, vol. 149, Oct. 2021, Art. no. 111252.
[47] A. M. Stanković et al., "Methods for analysis and quantification of power system resilience," *IEEE Trans. Power Syst.*, vol. 38, no. 5, pp. 4774–4787, Oct. 2022.
[48] A. Younesi, H. Shayeghi, Z. Wang, P. Siano, A. Mehrizi-Sani, and A. Safari, "Trends in modern power systems resilience: State-of-the-art review," *Renew. Sustain. Energy Rev.*, vol. 162, Jul. 2022, Art. no. 112397.
[49] R. Rocchetta, "Enhancing the resilience of critical infrastructures: Statistical analysis of power grid spectral clustering and post-contingency vulnerability metrics," *Renew. Sustain. Energy Rev.*, vol. 159, May 2022, Art. no. 112185.
[50] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter: Presenting a conceptual framework of power system resilience," *IEEE Power Energy Mag.*, vol. 13, no. 3, pp. 58–66, May 2015.
[51] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32035–32053, 2018.
[52] H. Nagarajan, E. Yamangil, R. Bent, P. Van Hentenryck, and S. Backhaus, "Optimal resilient transmission grid design," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Jun. 2016, pp. 1–7.
[53] N. Nezamoddini, S. Mousavian, and M. Erol-Kantarci, "A risk optimization model for enhanced power grid resilience against physical attacks," *Electr. Power Syst. Res.*, vol. 143, pp. 329–338, Feb. 2017.
[54] C. Shao, M. Shahidehpour, X. Wang, X. Wang, and B. Wang, "Integrated planning of electricity and natural gas transportation systems for enhancing the power grid resilience," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4418–4429, Nov. 2017.
[55] T. Lagos et al., "Identifying optimal portfolios of resilient network investments against natural hazards, with applications to earthquakes," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1411–1421, Mar. 2020.
[56] V. Panyam, H. Huang, K. Davis, and A. Layton, "Bio-inspired design for robust power grid networks," *Appl. Energy*, vol. 251, Oct. 2019, Art. no. 113349.
[57] W. Huang, X. Zhang, and W. Zheng, "Resilient power network structure for stable operation of energy systems: A transfer learning approach," *Appl. Energy*, vol. 296, Aug. 2021, Art. no. 117065.
[58] K. Garifi, E. S. Johnson, B. Arguello, and B. J. Pierre, "Transmission grid resiliency investment optimization model with SOCP recovery planning," *IEEE Trans. Power Syst.*, vol. 37, no. 1, pp. 26–37, Jan. 2022.
[59] M. Moradi-Sepahvand, T. Amraee, and S. S. Gougheri, "Deep learning based hurricane resilient coplanning of transmission lines, battery energy storages, and wind farms," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 2120–2131, 2021.
[60] H. Huang, Z. Mao, V. Panyam, A. Layton, and K. R. Davis, "Ecological robustness-oriented grid network design for resilience against multiple hazard," *IEEE Trans. Power Syst.*, *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 416–428, Jan. 2024.
[61] J. Stürmer et al., "Increasing the resilience of the Texas power grid against extreme storms by hardening critical lines," *Nature Energy*, vol. 9, no. 5, pp. 526–535, May 2024.
[62] W. Yuan, J. Wang, F. Qiu, C. Chen, C. Kang, and B. Zeng, "Robust optimization-based resilient distribution network planning against natural disasters," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2817–2826, Nov. 2016.
[63] S. D. Manshadi and M. E. Khodayar, "Expansion of autonomous microgrids in active distribution networks," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1878–1888, May 2018.
[64] C. He, C. Dai, L. Wu, and T. Liu, "Robust network hardening strategy for enhancing resilience of integrated electricity and natural gas distribution systems against natural disasters," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 5787–5798, Sep. 2018.
[65] Y. Tan, A. K. Das, P. Arabshahi, and D. S. Kirschen, "Distribution systems hardening against natural disasters," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6849–6860, Nov. 2018.
[66] A. Barnes, H. Nagarajan, E. Yamangil, R. Bent, and S. Backhaus, "Resilient design of large-scale distribution feeders with networked microgrids," *Electr. Power Syst. Res.*, vol. 171, pp. 150–157, Jun. 2019.
[67] M. Nazemi, M. Moeini-Aghtaie, M. Fotuhi-Firuzabad, and P. Dehghanian, "Energy storage planning for enhanced resilience of power distribution networks against earthquakes," *IEEE Trans. Sustain. Energy*, vol. 11, no. 2, pp. 795–806, Apr. 2020.
[68] W. Huang, X. Zhang, K. Li, N. Zhang, G. Strbac, and C. Kang, "Resilience oriented planning of urban multi-energy systems with generalized energy storage sources," *IEEE Trans. Power Syst.*, vol. 37, no. 4, pp. 2906–2918, Jul. 2022.
[69] H. Lin et al., "Self-healing attack-resilient PMU network for power system operation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1551–1565, May 2018.
[70] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial Internet of Things driven by SDN platform for smart grid resiliency," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 267–277, Feb. 2019.
[71] D. Jin et al., "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.
[72] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar, "Resilient design of networked control systems under time delay switch attacks, application in smart grid," *IEEE Access*, vol. 5, pp. 15901–15912, 2017.
[73] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Proc. Resilience Week (RWS)*, Sep. 2017, pp. 18–23.
[74] 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 Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.
[75] L. Xu, Q. Guo, T. Yang, and H. Sun, "Robust routing optimization for smart grids considering cyber-physical interdependence," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5620–5629, Sep. 2019.
[76] M. Tariq, M. Ali, F. Naeem, and H. V. Poor, "Vulnerability assessment of 6G-enabled smart grid cyber–physical systems," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5468–5475, Apr. 2021.
[77] Z. Jiang, Z. Tang, Y. Qin, C. Kang, and P. Zhang, "Quantum internet for resilient electric grids," *Int. Trans. Electr. Energy Syst.*, vol. 31, no. 6, Jun. 2021, Art. no. e12911.
[78] Z. Tang, P. Zhang, W. O. Krawec, and L. Wang, "Quantum networks for resilient power grids: Theory and simulated evaluation," *IEEE Trans. Power Syst.*, vol. 38, no. 2, pp. 1189–1204, Mar. 2023.
[79] Y. Wang et al., "Enhancing power grid resilience with blockchain-enabled vehicle-to-vehicle energy trading in renewable energy integration," *IEEE Trans. Ind. Appl.*, vol. 60, no. 2, pp. 2037–2052, Mar. 2024.
[80] T. L. Vu and K. Turitsyn, "A framework for robust assessment of power grid stability and resiliency," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1165–1177, Mar. 2017.
[81] S. Espinoza, M. Panteli, P. Mancarella, and H. Rudnick, "Multi-phase assessment and adaptation of power systems resilience to natural hazards," *Electr. Power Syst. Res.*, vol. 136, pp. 352–361, Jul. 2016.
[82] A. Kwasinski, "Quantitative model and metrics of electrical grids' resilience evaluated at a power distribution level," *Energies*, vol. 9, no. 2, p. 93, Feb. 2016.
[83] P. Bajpai, S. Chanda, and A. K. Srivastava, "A novel metric to quantify and enable resilient distribution system using graph theory and choquet integral," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2918–2929, Jul. 2018.
[84] E. Ciapessoni, D. Cirio, G. Kjølle, S. Massucco, A. Pitto, and M. Sforna, "Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2890–2903, Nov. 2016.
[85] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2343–2357, Sep. 2017.
[86] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019.
[87] J. Lopez, J. E. Rubio, and C. Alcaraz, "A resilient architecture for the smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3745–3753, Aug. 2018.
[88] P. Dehghanian, B. Zhang, T. Dokic, and M. Kezunovic, "Predictive risk analytics for weather-resilient operation of electric power systems," *IEEE Trans. Sustain. Energy*, vol. 10, no. 1, pp. 3–15, Jan. 2019.
[89] E. B. Watson and A. H. Etemadi, "Modeling electrical grid resilience under hurricane wind conditions with increased solar and wind power generation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 929–937, Mar. 2020.
[90] V. Venkataramanan, A. Srivastava, and A. Hahn, "CP-TRAM: Cyber-physical transmission resiliency assessment metric," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5114–5123, Nov. 2020.
[91] T. J. Overbye et al., "Techniques for maintaining situational awareness during large-scale electric grid simulations," in *Proc. IEEE Power Energy Conf. Illinois (PECI)*, Apr. 2021, pp. 1–8.
[92] Y. Zhou and P. Zhang, "Noise-resilient quantum machine learning for stability assessment of power systems," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 475–487, Jan. 2023.
[93] M. R. Kelly-Gorham, P. D. H. Hines, and I. Dobson, "Ranking the impact of interdependencies on power system resilience using stratified sampling of utility data," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 1251–1262, Jan. 2024.
[94] Y. Xiang, L. Wang, and N. Liu, "A robustness-oriented power grid operation strategy considering attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4248–4261, Sep. 2018.
[95] S. C. Madathil et al., "Resilient off-grid microgrids: Capacity planning and N-1 security," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6511–6521, Nov. 2018.
[96] E. Karangelos and L. Wehenkel, "An iterative AC-SCOPF approach managing the contingency and corrective control failure uncertainties with a probabilistic guarantee," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3780–3790, Sep. 2019.
[97] I.-I. Avramidis, F. Capitanescu, S. Karagiannopoulos, and E. Vrettos, "A novel approximation of security-constrained optimal power flow with incorporation of generator frequency and voltage control response," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 2438–2447, May 2021.
[98] R. Weinhold and R. Mieth, "Fast security-constrained optimal power flow through low-impact and redundancy screening," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4574–4584, Nov. 2020.
[99] F. Yang, X. Feng, and Z. Li, "Advanced microgrid energy management system for future sustainable and resilient power grid," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7251–7260, Nov. 2019.

[100] A. Shaker, A. Safari, and M. Shahidehpour, "Reactive power management for networked microgrid resilience in extreme conditions," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 3940–3953, Sep. 2021.

[101] Md. Kamruzzaman, J. Duan, D. Shi, and M. Benidris, "A deep reinforcement learning-based multi-agent framework to enhance power system resilience using shunt resources," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5525–5536, Nov. 2021.

[102] P. Zhao et al., "Cyber-resilient multi-energy management for complex systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 2144–2159, Mar. 2022.

[103] H. Zakernezhad, M. S. Nazar, M. Shafie-Khah, and J. P. S. Catalão, "Optimal resilient operation of multi-carrier energy systems in electricity markets considering distributed energy resource aggregators," *Appl. Energy*, vol. 299, Oct. 2021, Art. no. 117271.

[104] H. Huang, Z. Mao, A. Layton, and K. R. Davis, "An ecological robustness oriented optimal power flow for power systems' survivability," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 447–462, Jan. 2023.

[105] J. Tobajas, F. Garcia-Torres, P. Roncero-Sánchez, J. Vázquez, L. Bellatreche, and E. Nieto, "Resilience-oriented schedule of microgrids with hybrid energy storage system using model predictive control," *Appl. Energy*, vol. 306, Jan. 2022, Art. no. 118092.

[106] C. Lv, R. Liang, W. Jin, Y. Chai, and T. Yang, "Multi-stage resilience scheduling of electricity-gas integrated energy system with multi-level decentralized reserve," *Appl. Energy*, vol. 317, Jul. 2022, Art. no. 119165.

[107] C. Wang, Y. Hou, F. Qiu, S. Lei, and K. Liu, "Resilience enhancement with sequentially proactive operation strategies," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2847–2857, Jul. 2017.

[108] A. Gholami, T. Shekari, F. Aminifar, and M. Shahidehpour, "Microgrid scheduling with uncertainty: The quest for resilience," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2849–2858, Nov. 2016.

[109] D. N. Trakas and N. D. Hatziargyriou, "Optimal distribution system operation for enhancing resilience against wildfires," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 2260–2271, Mar. 2018.

[110] D. N. Trakas and N. D. Hatziargyriou, "Resilience constrained day-ahead unit commitment under extreme weather events," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1242–1253, Mar. 2020.

[111] Y. Wang, L. Huang, M. Shahidehpour, L. L. Lai, H. Yuan, and F. Y. Xu, "Resilience-constrained hourly unit commitment in electricity grids," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 5604–5614, Sep. 2018.

[112] E. Ciapessoni, D. Cirio, A. Pitto, P. Marcacci, and M. Sforna, "Security-constrained redispatching to enhance power system resilience in case of wet snow events," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Jun. 2018, pp. 1–7.

[113] 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 Trans. Smart Grid*, vol. 11, no. 1, pp. 590–601, Jan. 2020.

[114] M. Yan et al., "Enhancing the transmission grid resilience in ice storms by optimal coordination of power system schedule with pre-positioning and routing of mobile DC de-icing devices," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2663–2674, Jul. 2019.

[115] T. Zhao, H. Zhang, X. Liu, S. Yao, and P. Wang, "Resilient unit commitment for day-ahead market considering probabilistic impacts of hurricanes," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1082–1094, Mar. 2021.

[116] S. Pandey, S. Chanda, A. K. Srivastava, and R. O. Hovsapian, "Resiliency-driven proactive distribution system reconfiguration with synchrophasor data," *IEEE Trans. Power Syst.*, vol. 35, no. 4, pp. 2748–2758, Jul. 2020.

[117] D. Gutierrez-Rojas et al., "Weather-driven predictive control of a battery storage for improved microgrid resilience," *IEEE Access*, vol. 9, pp. 163108–163121, 2021.

[118] Z. Zhang et al., "Preventive control of successive failures in extreme weather for power system resilience enhancement," *IET Gener., Transmiss. Distrib.*, vol. 16, no. 16, pp. 3245–3255, Aug. 2022.

[119] S. U. Kadir et al., "Reinforcement learning based proactive control for enabling power grid resilience to wildfire," *IEEE Trans. Ind. Informat.*, vol. 20, no. 1, pp. 795–805, Jan. 2024.

[120] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2923–2932, Nov. 2016.

[121] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215, Mar. 2018.

[122] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.

[123] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, Mar. 2019.

[124] H. F. Habib, A. A. S. Mohamed, M. El Hariri, and O. A. Mohammed, "Utilizing supercapacitors for resiliency enhancements and adaptive microgrid protection against communication failures," *Electric Power Syst. Res.*, vol. 145, pp. 223–233, Apr. 2017.

[125] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, Nov. 2018.

[126] H. Davarikia and M. Barati, "A tri-level programming model for attack-resilient control of power grids," *J. Modern Power Syst. Clean Energy*, vol. 6, no. 5, pp. 918–929, Sep. 2018.

[127] R. Lai, X. Qiu, and J. Wu, "Robustness of asymmetric cyber-physical power systems against cyber attacks," *IEEE Access*, vol. 7, pp. 61342–61352, 2019.

[128] W. Chen, D. Ding, H. Dong, and G. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1688–1697, Aug. 2019.

[129] K. Lai, Y. Wang, D. Shi, M. S. Illindala, Y. Jin, and Z. Wang, "Sizing battery storage for islanded microgrid systems to enhance robustness against attacks on energy sources," *J. Modern Power Syst. Clean Energy*, vol. 7, no. 5, pp. 1177–1188, Sep. 2019.

[130] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 9, pp. 7951–7962, Sep. 2020.

[131] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Appl. Energy*, vol. 235, pp. 204–218, Feb. 2019.

[132] P. Wang and M. Govindarasu, "Multi-agent based attack-resilient system integrity protection for smart grid," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3447–3456, Jul. 2020.

[133] M. Elimam, Y. J. Isbeih, S. K. Azman, M. S. E. Moursi, and K. A. Hosani, "Deep learning-based PMU cyber security scheme against data manipulation attacks with WADC application," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2148–2161, May 2023.

[134] G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo, "Integration of preventive and emergency responses for power grid resilience enhancement," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4451–4463, Nov. 2017.

[135] T. Amraee and H. Saberi, "Controlled islanding using transmission switching and load shedding for enhancing power grid resilience," *Int. J. Electr. Power Energy Syst.*, vol. 91, pp. 135–143, Oct. 2017.

[136] F. Teymouri, T. Amraee, H. Saberi, and F. Capitanescu, "Toward controlled islanding for enhancing power grid resilience considering frequency stability constraints," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1735–1746, Mar. 2019.

[137] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz, "Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 188–197, Dec. 2017.

[138] M. Yan, Y. He, M. Shahidehpour, X. Ai, Z. Li, and J. Wen, "Coordinated regional-district operation of integrated energy systems for resilience enhancement in natural disasters," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4881–4892, Sep. 2019.

[139] T. Hussain, S. Suryanarayanan, T. M. Hansen, and S. M. S. Alam, "A fast and scalable transmission switching algorithm for boosting resilience of electric grids impacted by extreme weather events," *IEEE Access*, vol. 10, pp. 57893–57901, 2022.

[140] H. Gao, Y. Chen, Y. Xu, and C.-C. Liu, "Resilience-oriented critical load restoration using microgrids in distribution systems," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2837–2848, Nov. 2016.

[141] K. S. A. Sedzro, A. J. Lamadrid, and L. F. Zuluaga, "Allocation of resources using a microgrid formation approach for resilient electric grids," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2633–2643, May 2018.

[142] F. Qiu and P. Li, "An integrated approach for power system restoration planning," *Proc. IEEE*, vol. 105, no. 7, pp. 1234–1252, Jul. 2017.

[143] C. Chen, J. Wang, and D. Ton, "Modernizing distribution system restoration to achieve grid resiliency against extreme weather events: An integrated solution," *Proc. IEEE*, vol. 105, no. 7, pp. 1267–1288, Jul. 2017.

[144] S. Poudel and A. Dubey, "Critical load restoration using distributed energy resources for resilient power distribution system," *IEEE Trans. Power Syst.*, vol. 34, no. 1, pp. 52–63, Jan. 2019.

[145] P. Dehghanian, S. Aslan, and P. Dehghanian, "Maintaining electric system safety through an enhanced network resilience," *IEEE Trans. Ind. Appl.*, vol. 54, no. 5, pp. 4927–4937, Sep. 2018.

[146] Q. Li et al., "Integrating reinforcement learning and optimal power dispatch to enhance power grid resilience," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 3, pp. 1402–1406, Mar. 2022.

[147] J. C. Bedoya, Y. Wang, and C.-C. Liu, "Distribution system resilience under asynchronous information using deep reinforcement learning," *IEEE Trans. Power Syst.*, vol. 36, no. 5, pp. 4235–4245, Sep. 2021.

[148] J. Zhao, F. Li, X. Chen, and Q. Wu, "Deep learning based model-free robust load restoration to enhance bulk system resilience with wind power penetration," *IEEE Trans. Power Syst.*, vol. 37, no. 3, pp. 1969–1978, May 2022.

[149] M. M. Hosseini and M. Parvania, "Resilient operation of distribution grids using deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 2100–2109, Mar. 2022.

[150] A. B. Birchfield, "Graph decomposition for constructing blackstart restoration strategies in benchmark cases," *Electric Power Syst. Res.*, vol. 212, Nov. 2022, Art. no. 108402.

[151] X. Li, X. Du, T. Jiang, R. Zhang, and H. Chen, "Coordinating multi-energy to improve urban integrated energy system resilience against extreme weather events," *Appl. Energy*, vol. 309,

Mar. 2022, Art. no. 118455.
[152] S. N. Edib, Y. Lin, V. M. Vokkarane, F. Qiu, R. Yao, and B. Chen, "Cyber restoration of power systems: Concept and methodology for resilient observability," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 53, no. 8, pp. 5185–5198, Aug. 2023.
[153] T. Zhang, M. Sun, D. Qiu, X. Zhang, G. Strbac, and C. Kang, "A Bayesian deep reinforcement learning-based resilient control for multi-energy micro-gird," *IEEE Trans. Power Syst.*, vol. 38, no. 6, pp. 5057–5072, Nov. 2023.
[154] Y. Wang, D. Qiu, X. Sun, Z. Bie, and G. Strbac, "Coordinating multi-energy microgrids for integrated energy system resilience: A multi-task learning approach," *IEEE Trans. Sustain. Energy*, vol. 15, no. 2, pp. 920–937, Apr. 2024.
[155] W. Fu et al., "Coordinated post-disaster restoration for resilient urban distribution systems: A hybrid quantum-classical approach," *Energy*, vol. 284, Dec. 2023, Art. no. 129314.
[156] (2014). *The North American Electric Reliability Corporation (NERC)*. [Online]. Available: https://www.nerc.com/Pages/default.aspx
[157] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," *SANS Inst. InfoSec Reading Room*, vol. 1, no. 1, p. 2, 2015.
[158] O. Alexander, M. Belisle, and J. Steele, *MITRE ATT&CK for Industrial Control Systems: Design and Philosophy*. Bedford, MA, USA: MITRE Corporation, 2020, p. 29.
[159] L. Martin. (2014). *Cyber Kill Chain*. Accessed: Nov. 2, 2023. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-Martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
[160] T. J. Overbye, J. L. Wert, K. S. Shetye, F. Safdarian, and A. B. Birchfield, "The use of geographic data views to help with wide-area electric grid situational awareness," in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, Feb. 2021, pp. 1–6.
[161] F. Capitanescu, "Approaches to obtain usable solutions for infeasible security-constrained optimal power flow problems due to conflicting contingencies," in *Proc. IEEE Milan PowerTech*, Jun. 2019, pp. 1–6.
[162] A. Marano-Marcolini, F. Capitanescu, J. L. Martinez-Ramos, and L. Wehenkel, "Exploiting the use of DC SCOPF approximation to improve iterative AC SCOPF algorithms," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1459–1466, Aug. 2012.
[163] W. Li et al., *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. Cham, Switzerland: Springer, 2013.
[164] F. Dehghani, M. Mohammadi, and M. Karimi, "Age-dependent resilience assessment and quantification of distribution systems under extreme weather events," *Int. J. Electr. Power Energy Syst.*, vol. 150, Aug. 2023, Art. no. 109089.
[165] A. Tajer, S. M. Perlaza, and H. V. Poor, *Advanced Data Analytics for Power Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2021.
[166] M. Shinozuka et al., *Resilience of Integrated Power and Water Systems*. Princeton, NJ, USA: Citeseer, 2004.
[167] B. D. Fath, "Quantifying economic and ecological sustainability," *Ocean Coastal Manage.*, vol. 108, pp. 13–19, May 2015.
[168] R. E. Ulanowicz, S. J. Goerner, B. Lietaer, and R. Gomez, "Quantifying sustainability: Resilience, efficiency and the return of information theory," *Ecolog. Complex.*, vol. 6, no. 1, pp. 27–36, Mar. 2009.
[169] T. Dave and A. Layton, "Designing ecologically-inspired robustness into a water distribution network," *J. Cleaner Prod.*, vol. 254, May 2020, Art. no. 120057.
[170] A. Chatterjee, R. Malak, and A. Layton, "Ecology-inspired resilient and affordable system of systems using degree of system order," *Syst. Eng.*, vol. 25, no. 1, pp. 3–18, Jan. 2022.
[171] A. Chatterjee, R. Malak, and A. Layton, "Exploring system of systems resilience versus affordability trade-space using a bio-inspired metric," *J. Comput. Inf. Sci. Eng.*, vol. 21, no. 5, pp. 050905-1–050905-10, Oct. 2021.
[172] M. B. Mollah et al., "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021.
[173] Y. Zhou et al., "Quantum computing in power systems," *iEnergy*, vol. 1, no. 2, pp. 170–187, Jun. 2022.
[174] A. Ajagekar and F. You, "Quantum computing for energy systems optimization: Challenges and opportunities," *Energy*, vol. 179, pp. 76–89, Jul. 2019.
[175] M. H. Ullah, R. Eskandarpour, H. Zheng, and A. Khodaei, "Quantum computing for smart grid applications," *IET Gener., Transmiss. Distrib.*, vol. 16, no. 21, pp. 4239–4257, Nov. 2022.
[176] M. L. Di Silvestre et al., "Blockchain for power systems: Current trends and future applications," *Renew. Sustain. Energy Rev.*, vol. 119, Mar. 2020, Art. no. 109585.
[177] F. Mohammadi and M. Saif, "Blockchain technology in modern power systems: A systematic review," *IEEE Syst., Man, Cybern. Mag.*, vol. 9, no. 1, pp. 37–47, Jan. 2023.
[178] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[179] K. P. Schneider et al., "Analytic considerations and design basis for the IEEE distribution test feeders," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 3181–3188, May 2018.
[180] W. Bukhsh and K. McKinnon. (2013). *Network Data of Real Transmission Networks*. [Online]. Available: http://www.maths.ed.ac.uk/optenergy/NetworkData
[181] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3258–3265, Jul. 2017.
[182] A. Birchfield et al., "A metric-based validation process to assess the realism of synthetic power grids," *Energies*, vol. 10, no. 8, p. 1233, Aug. 2017.
[183] R. Meyur et al., "Ensembles of realistic power distribution networks," *Proc. Nat. Acad. Sci. USA*, vol. 119, no. 42, Oct. 2022, Art. no. e2205772119.
[184] *IEEE Standard for Calculating the Current-Temperature Relationship of Bare Overhead Conductors*, Standard 738-2012 (Revision IEEE Std 738-2006 Incorporates IEEE Std 738-2012 Cor 1-2013), 2013, pp. 1–72.
[185] V. Cecchi, M. Knudson, and K. Miu, "System impacts of temperature-dependent transmission line models," *IEEE Trans. Power Del.*, vol. 28, no. 4, pp. 2300–2308, Oct. 2013.
[186] S. Frank, J. Sexauer, and S. Mohagheghi, "Temperature-dependent power flow," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4007–4018, Nov. 2013.
[187] M. Rahman, V. Cecchi, and K. Miu, "Power handling capabilities of transmission systems using a temperature-dependent power flow," *Electr. Power Syst. Res.*, vol. 169, pp. 241–249, Apr. 2019.
[188] A. Ahmed, F. J. S. McFadden, and R. Rayudu, "Weather-dependent power flow algorithm for accurate power system analysis under variable weather conditions," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2719–2729, Jul. 2019.
[189] T. Overbye, F. Safdarian, W. Trinh, Z. Mao, J. Snodgrass, and J. Yeo, "An approach for the direct inclusion of weather information in the power flow," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2023, pp. 2681–2690.
[190] X. Zheng, D. Wu, L. Watts, E. N. Pistikopoulos, and L. Xie, "Analyzing extreme events in power systems: An open, cross-domain data-driven approach," *IEEE Power Energy Mag.*, vol. 20, no. 6, pp. 47–55, Nov. 2022.
[191] J. Ahrenholz, C. Danilov, T. R. Henderson, and J. H. Kim, "CORE: A real-time network emulator," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2008, pp. 1–7.
[192] Minimega Developers. (2019). *Minimega: A Distributed Vm Management Tool*. Accessed: Nov. 2, 2023. [Online]. Available: https://minimega.org/
[193] A. Afanasyev et al. *NS-3: Network Simulator-3*. Accessed: Nov. 2, 2023. [Online]. Available: https://github.com/nsnam
[194] A. Sahu, K. Davis, H. Huang, A. Umunnakwe, S. Zonouz, and A. Goulart, "Design of next-generation cyber-physical energy management systems: Monitoring to mitigation," *IEEE Open Access J. Power Energy*, vol. 10, pp. 151–163, 2023.
[195] P. Wlazlo et al., "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 6, no. 3, pp. 164–177, Sep. 2021.
[196] H. Huang et al., "Validating an emulation-based cybersecurity model with a physical testbed," *IEEE Trans. Dependable Secure Comput.*, early access, pp. 1–15, Oct. 2023.
[197] C. Ji, Y. Wei, and H. V. Poor, "Resilience of energy infrastructure and services: Modeling, data analytics, and metrics," *Proc. IEEE*, vol. 105, no. 7, pp. 1354–1366, Jul. 2017.
[198] B. Singer et al., "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2023, pp. 554–571.
[199] L. Xu, Q. Guo, Y. Sheng, S. M. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renew. Sustain. Energy Rev.*, vol. 152, Dec. 2021, Art. no. 111642.
[200] A. Sahu et al., "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119118–119138, 2021.
[201] H. Huang et al., "Cyberattack defense with cyber-physical alert and control logic in industrial controllers," *IEEE Trans. Ind. Appl.*, vol. 58, no. 5, pp. 5921–5934, Sep. 2022.
[202] Ö. Bodin and M. Tengö, "Disentangling intangible social–ecological systems," *Global Environ. Change*, vol. 22, no. 2, pp. 430–439, May 2012.
[203] (2021). *Katherine Davis Project Lists*. [Online]. Available: https://katedavis.engr.tamu.edu/projects/bio-inspired-design-of-complex-energy-systems/
[204] A. M. Amani and M. Jalili, "Power grids as complex networks: Resilience and reliability analysis," *IEEE Access*, vol. 9, pp. 119010–119031, 2021.
[205] T. Xu, A. B. Birchfield, and T. J. Overbye, "Modeling, tuning, and validating system dynamics in synthetic electric grids," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6501–6509, Nov. 2018.
[206] F. Safdarian, A. B. Birchfield, K. S. Shetye, and T. J. Overbye, "Additional insights in creating large-scale, high quality synthetic grids: A case study," in *Proc. IEEE Kansas Power Energy Conf. (KPEC)*, Apr. 2021, pp. 1–6.
[207] D. Ofori-Boateng, A. K. Dey, Y. R. Gel, B. Li, J. Zhang, and H. V. Poor, "Assessing the resilience of the Texas power grid network," in *Proc. IEEE Data Sci. Workshop (DSW)*, Jun. 2019, pp. 280–284.
[208] R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, and U. Alon, "Network motifs: Simple building blocks of complex networks," *Science*, vol. 298, no. 5594, pp. 824–827, Oct. 2002.
[209] A. R. Benson, D. F. Gleich, and J. Leskovec, "Higher-order organization of complex networks," *Science*, vol. 353, no. 6295, pp. 163–166, Jul. 2016.
[210] L. Stone, D. Simberloff, and Y. Artzy-Randrup, "Network motifs and their origins," *PLOS Comput. Biol.*, vol. 15, no. 4, Apr. 2019, Art. no. e1006749.
[211] A. K. Dey, Y. R. Gel, and H. V. Poor, "What network motifs tell us about resilience and reliability of complex networks," *Proc. Nat. Acad. Sci. USA*, vol. 116, no. 39, pp. 19368–19373, Sep. 2019.
[212] K. Zhou, I. Dobson, and Z. Wang, "The most frequent N-K line outages occur in motifs that can

improve contingency selection," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 1785–1796, Mar. 2024.
[213] H. Huang, K. R. Davis, and H. V. Poor, "An extended model for ecological robustness to capture power system resilience," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2023, pp. 1–5.
[214] H. Huang, H. V. Poor, and K. Davis, "Inclusion of reactive power into ecological robustness-oriented optimal power flow for enhancing power system resilience," in *Proc. 57th Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2024, pp. 3103–3112.
[215] A. Chatterjee and A. Layton, "Mimicking nature for resilient resource and infrastructure network design," *Rel. Eng. Syst. Saf.*, vol. 204, Dec. 2020, Art. no. 107142.
[216] H. Huang, H. V. Poor, D. Flynn, and M. Al-Muhaini, "Understanding a power grid's cyber-physical interdependence through higher-order motifs," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2024.
[217] S. Hossain-McKenzie et al., "Towards the characterization of cyber-physical system interdependencies in the electric grid," in *Proc. IEEE Power Energy Conf. Illinois (PECI)*, Mar. 2023, pp. 1–8.
[218] H. Binqadhi, M. AlMuhaini, H. V. Poor, and H. Huang, "Motif-based reliability analysis for cyber-physical power systems," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT EUROPE)*, Oct. 2023, pp. 1–5.
[219] N. Baker et al., *Workshop Report on Basic Research Needs for Scientific Machine Learning: Core Technologies for Artificial Intelligence*. Washington, DC, USA: U.S. DOE Office of Science (SC), 2019.
[220] S. Cuomo, V. S. Di Cola, F. Giampaolo, G. Rozza, M. Raissi, and F. Piccialli, "Scientific machine learning through physics–informed neural networks: Where we are and what's next," *J. Sci. Comput.*, vol. 92, no. 3, p. 88, Sep. 2022.
[221] B. Huang and J. Wang, "Applications of physics-informed neural networks in power systems—A review," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 572–588, Jan. 2023.
[222] V. N. Ekambaram, G. C. Fanti, B. Ayazifar, and K. Ramchandran, "Spline-like wavelet filterbanks for multiresolution analysis of graph-structured data," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 1, no. 4, pp. 268–278, Dec. 2015.
[223] C. Tang, J. Sun, Y. Sun, M. Peng, and N. Gan, "A general traffic flow prediction approach based on spatial-temporal graph attention," *IEEE Access*, vol. 8, pp. 153731–153741, 2020.
[224] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 1, pp. 4–24, Jan. 2021.
[225] W. Liao, B. Bak-Jensen, J. R. Pillai, Y. Wang, and Y. Wang, "A review of graph neural networks and their applications in power systems," *J. Modern Power Syst. Clean Energy*, vol. 10, no. 2, pp. 345–360, Mar. 2022.
[226] B. Bush, Y. Chen, D. Ofori-Boateng, and Y. R. Gel, "Topological machine learning methods for power system responses to contingencies," in *Proc. AAAI Conf. Artif. Intell.*, 2021, vol. 35, no. 17, pp. 15262–15269.
[227] O. Boyaci, M. R. Narimani, K. R. Davis, M. Ismail, T. J. Overbye, and E. Serpedin, "Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 807–819, Jan. 2022.
[228] S. Ebli, M. Defferrard, and G. Spreemann, "Simplicial neural networks," in *Proc. Topological Data Anal. Beyond Workshop Conf. Neural Inf. Process. Syst. (NeurIP)*, 2020, pp. 1–7.
[229] Y. Chen, Y. R. Gel, and H. V. Poor, "BScNets: Block simplicial complex neural networks," in *Proc. AAAI Conf. Artif. Intell.*, 2022, vol. 36, no. 6, pp. 6333–6341.
[230] Y. Chen, R. A. Jacob, Y. R. Gel, J. Zhang, and H. V. Poor, "Learning power grid outages with higher-order topological neural networks," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 720–732, Feb. 2024.

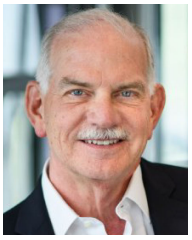
ABOUT THE AUTHORS

Hao Huang (Member, IEEE) received the B.S. degree in electrical engineering (power system and its automation) from Harbin Institute of Technology, Harbin, Heilongjiang, China, in 2014, the M.S. degree in electrical engineering (electric Power) from the University of Southern California, Los Angeles, CA, USA, in 2016, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2022.

He is currently a Postdoctoral Research Associate at Princeton University, Princeton, NJ, USA. His research focuses on power system resilience, data-driven approaches for power systems, and cyber–physical security.

Katherine R. Davis (Senior Member, IEEE) received the B.S. degree from The University of Texas at Austin, Austin, TX, USA, in 2007, and the M.S. and Ph.D. degrees from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 2009 and 2011, respectively, in electrical engineering.

She is currently an Associate Professor of electrical and computer engineering with Texas A&M University, College Station, TX, USA. Her research interests include operation and control of power systems, interactions between computer networks and power networks, security-oriented cyber–physical analysis techniques, and data-driven and model-based coupled infrastructure analysis and simulation.



H. Vincent Poor (Life Fellow, IEEE) received the Ph.D. degree in electrical engineering and computer science (EECS) from Princeton University, Princeton, NJ, USA, in 1977.

From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana–Champaign, Champaign, IL, USA. Since 1990, he has been on the faculty at Princeton University, where he is currently the Michael Henry Strater University Professor. From 2006 to 2016, he was the Dean of the School of Engineering and Applied Science, Princeton University. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory; machine learning and network science; and their applications in wireless networks, energy systems, and related fields. Among his publications in these areas is the book *Advanced Data Analytics for Power Systems* (Cambridge University Press, 2021).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences and a Foreign Member of the Royal Society and other national and international academies. He received the IEEE Alexander Graham Bell Medal in 2017.

Thomas J. Overbye (Fellow, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the University of Wisconsin–Madison, Madison, WI, USA, in 1983, 1988, and 1991, respectively.

He is currently with Texas A&M University, College Station, TX, USA, where he is also a Professor and holds the O'Donnell Foundation Chair III. He has extensive experience in many aspects of electric power systems and leads numerous large-scale electric grid studies.

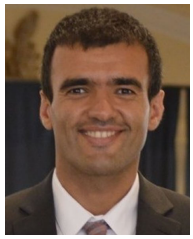
Dr. Overbye is a member of the U.S. National Academy of Engineering.

Astrid Layton (Member, IEEE) received the B.S. degree in mechanical engineering from the University of Pittsburgh, Pittsburgh, PA, USA, in 2009, and the Ph.D. degree in mechanical engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2014.

She is currently an Assistant Professor at the Department of Mechanical Engineering, Texas A&M University, College Station, TX, USA. Her research looks at bioinspired network design problems, focusing on the use of biological ecosystems as inspiration for the design of sustainable and resilient complex human networks and systems.

Ana E. Goulart (Member, IEEE) received the B.S. degree in electrical engineering from the Federal School of Engineering of Itajubâ (EFEI), Itajubâ, Brazil, in 1991, the M.S. degree in information systems management from the Pontifical University Catholic of Campinas, Campinas, Brazil, in 1997, the M.Sc. degree in computer engineering from North Carolina State University, Raleigh, NC, USA, in 1998, and the Ph.D. degree in electrical and computer engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2005.

She is currently a Professor with the Electronics Systems Engineering Technology Program, Texas A&M University, College Station, TX, USA. Her research interests include protocols for real-time voice and video communications and their performance, internet protocol (IP)-based emergency communications, last-mile communication links and cybersecurity for the smart grid, wireless network systems, and rural telecommunications.



Saman Zonouz (Member, IEEE) received the Ph.D. degree in computer science from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 2011.

He is currently an Associate Professor with the School of Cybersecurity and Privacy (SCP) and the School of Electrical and Computer Engineering (ECE), Georgia Institute of Technology, Atlanta, GA, USA. His research interests include cyber–physical security and survivable systems, and resilient control systems.

Dr. Zonouz received the Presidential Early Career Award for Scientists and Engineers (PECASE) from the U.S. President in 2019.