Renewable and Sustainable Energy Reviews 152 (2021) 111642

Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

journal homepage: www.elsevier.com/locate/rser

# On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective

Luo Xu [a], Qinglai Guo [a,*], Yujie Sheng [a], S.M. Muyeen [b], Hongbin Sun [a]

[a] Department of Electrical Engineering, State Key Laboratory of Power Systems, Tsinghua University, Beijing, China
[b] Department of Electrical Engineering, Qatar University, Doha, Qatar

ARTICLE INFO

*Keywords:*
Cyber-physical system
Cyberattack
Human-in-the-loop
Natural hazards
Resilience
Smart grid

ABSTRACT

The digital transformation of power systems into cyber-physical systems (CPSs) is the inevitable trend of modern power systems with the integration of large-scale renewable energy. The in-depth interdependence of cyber and physical spaces leads to more complicated external environments for such cyber-physical power systems (CPPSs) and brings great challenges to the resilience of CPPSs. A resilient CPS imposes strict requirements for its ability to cope with high-impact, low-probability cyber-physical disturbances. To better study the vulnerability and resilience of CPPSs, several representative blackouts from the past two decades are reviewed from the cyber-physical perspective. Inspired by general system theory, this study offers a framework with three key features of a CPPS and presents the three-layer interdependences from facilities to functions. The differences between CPPS resilience and conventional power system resilience are also emphasized. Thereafter, the study discusses the influence of cyber-physical disturbances from natural hazards, cyberattacks, and human-in-the-loop on the resilience of CPPSs. Accordingly, a survey of the state-of-the-art resilience-oriented techniques for CPPS in the face of natural hazards is organized based on quantitative metrics as well as planning and operation attributes. Regarding the resilience against cyberattacks, relevant cutting-edge research is reviewed in terms of prevention, detection, and mitigation strategies. Furthermore, from the cyber-physical-social perspective, the exploitation of social behaviors to inform the design of the physical system and the cyber system to ultimately enhance the resilience of CPPSs is also studied. Based on the findings from this research, the remaining challenges and the broad prospects of cyber-physical resilience enhancement techniques are also discussed.

## 1. Introduction

The modern electric power system is the pillar of global industrial development, the lifeblood of the social economy, and will be the key component of future smart grids. With the growing energy demand, increasingly dire environmental considerations, and push for sustainable development, there is an urgent need and an unstoppable tendency of evolution from conventional power systems to the next generation of smart grids [1]. From the perspective of general system theory [2], a power system can be regarded as a set of interrelated and interacting elements in a specific structure. The integration of large amounts of distributed energy sources (DER), such as photovoltaic (PV), wind power (WP), and electric vehicles (EVs), makes the modern power system diversified in its elements, and likewise entails higher requirements for information and communication technologies (ICT).

### 1.1. Motivation of the review

Conventionally, the complex interdependency and coupling of physical and cyber spaces are not always considered. Recent years have witnessed rapid development in the fields of communication, computation, and controlling and sensing technologies. The concept of the cyber-physical system (CPS) has also undergone rapid progress over the last few years and is considered as an emerging field that will be relevant to the next generation of engineered systems [3] and that will drive the in-depth informatization, digitization, and intellectualization reform of the modern power system [4]. To establish a low-carbon power system with renewable energy as the mainstay, digital transformation will be a critical measure to flexibly control and manage large-scale renewable energy generation. Accordingly, the revolutionary advances in electricity networks have caused the concept of the cyber-physical power system (CPPS) to become a focus for both industry [5] and academia [6].

The interdependence of the cyber and physical spaces of a CPPS

* Corresponding author. Department of Electrical Engineering, Tsinghua University, Rm. 3-120, West Main Building, Tsinghua University, 100084, Beijing, China.
*E-mail address:* guoqinglai@tsinghua.edu.cn (Q. Guo).

https://doi.org/10.1016/j.rser.2021.111642
Received 31 December 2020; Received in revised form 26 May 2021; Accepted 27 August 2021
Available online 20 September 2021
1364-0321/

**Abbreviations**

| | |
|---|---|
| ADN | Active distribution network |
| AMI | Advanced metering infrastructure |
| CI&A | Confidentiality, integrity, and availability |
| CLL | Critical load level |
| CNN | Convolutional neural network |
| CPS | Cyber-physical system |
| CPPS | Cyber-physical power system |
| CPSS | Cyber-physical-social system |
| CPTED | Crime prevention through environmental design |
| DER | Distributed energy sources |
| DG | Distributed generators |
| DoS | Denial-of-service |
| EMS | Energy management system |
| EV | Electric vehicle |
| FDIA | False data injection attack |
| ICS | Industrial control system |
| ICT | Information and communication technology |
| ILP | Integer linear programming |
| IoT | Internet of things |
| LFC | Load frequency control |
| LMP | Locational marginal price |
| MDP | Markov decision process |
| MPS | Mobile power resource |
| NTO | Network topology optimization |
| OPGW | Optical fiber composite overhead ground wire |
| OPF | Optimal power flow |
| OTN | Optical transport network |
| PKI | Public key infrastructure |
| PLC | Power line communication |
| PMU | Phasor measurement unit |
| PTP | Precision time protocol |
| PV | Photovoltaic |
| RA | Replay attack |
| RIG | Remote intelligent gateway |
| SCADA | Supervisory control and data acquisition |
| SDH | Synchronous digital hierarchy |
| SDN | Software-defined networking |
| SOP | Soft-open-point |
| TCL | Thermostatically controlled load |
| TEP | Transmission expansion planning |
| VPP | Virtual power plant |
| WAMS | Wide-area measurement system |

promotes the application of advanced information systems in system perception and operation and inversely induces the vulnerability superposition of the two spaces [7]. Likewise, the broader boundary and more complicated environments of a CPPS bring great challenges to its resilience [8]. Over the past few decades, massive electricity outages induced by cyber accidents and disturbances [9] have indicated the destructive power of the cyber system malfunction on power systems. For example, BlackEnergy malware attacked Ukraine's power grid and caused a widespread blackout in December 2015, which can be considered as a milestone in cyberattacks against power systems [10]. In the foreseeable future, with the deployment of smart meters and other intelligent access terminals, an Internet of Things (IoT)-based CPPS is likely to have an open network and multiagent tendency and therefore a higher risk of exposure to various cyber threats (e.g., targeted malware such as Stuxnet) [11].

Moreover, when cyber information system and physical power system malfunctions occur simultaneously due to extreme hazards such as the 2008 Chinese ice storm [12], it may trigger a catastrophic cascading failure to the power system. These potential cyber-physical coupling failures alter the importance of studying the resilience of modern power systems from a cyber-physical perspective.

Against this background, to study the resilience of CPPS in the face of potential cyber threats and cyber-physical coupling failures, it is critical to investigate the coupling mechanism, the interdependence and potential external disturbances between the cyber network and the physical power grid from a cyber-physical perspective. Furthermore, considering these potential disturbances, it is urgent to analyze the current trends and prospects of various cyber-physical techniques to improve the security and resilience of CPPSs.

### 1.2. Related reviews and scope of the review

There is plenty of literature systematically reviewing the resilience of power systems on the physical side. Wang et al. [13] mainly focus on the resilience of power systems under natural disasters, exploring comprehensive methods for the resilience enhancement by forecasting, correction control, and restoration at multiple stages of cascading failures. Mishra et al. [14] present a systematic review on the resilience-oriented planning and operation strategies of active distribution networks (ADNs) against natural disasters and man-made attacks, which mentions that an ADN can be made more resilient by properly incorporating microgrids. Izadi et al. [15] discuss the differences between the resilience of power systems and other related concepts, such as reliability, stability, and vulnerability, and review the metrics for evaluating resilience. Wang et al. [16] comprehensively survey the resilience of microgrids on modeling and operational strategies, and show that microgrids need more resilience enhancement against extreme conditions.

In a CPPS, cyber security is highly related to resilience. Challenges to the cyber security of CPPSs have attracted much attention due to the wide-area application of information systems in power systems. From the cyber side, many scholars have also reviewed the cyber security and the resilience of power systems against cyberattacks. The cyber security issue for wide-area monitoring and control systems is addressed in the work of Ashok et al. [17]. The author also outline an attack-resilient CPS security framework. Deng et al. [18] focus on cyberattacks on state estimation in power systems and related defense strategies, which also outline the future challenges of false data injection attacks (FDIAs). Mo et al. [19] systematically summarize the cyber security requirements of the smart grid infrastructure. Focusing on distributed power systems, in particular, microgrids, Li et al. [9] survey the application of cybersecurity to the operation and control of distributed systems.

Although research on cyber security introduced the concept of CPS, few studies have taken the modern power system as a CPPS and considered the internal interdependences and external environment to study the resilience problem. Investigating the resilience of a CPPS should be established in a systematic framework that fully considers the interdependences between multiple layers of the CPPS and the external disturbances targeting both the cyber and physical sides. Additionally, considering the trend of multi-agent and demand response of new participants such as EVs and DERs, the social environment will have a more significant impact on CPPSs in the future. The cyber-physical-social perspective should be further considered to study the resilience of CPPSs.

Therefore, the scope of this review is four-fold:

1) First, we aim to provide a review on several representative blackouts caused by cyberattacks and hazards from a cyber-physical perspective, such as the 2015 Ukraine cyberattack, the Chinese southern power grid outages caused by the 2008 Chinese ice storm, and the

2016 Xiamen island blackout caused by Typhoon Meranti. This will offer a factual basis for investigating the cyber-physical vulnerability and resilience of CPPS.
2) Second, by analyzing the interdependence between the cyber and physical spaces from the facility level to the function level, we present a framework for identifying the key features of CPPSs, which lays a foundation for exploring the weak points of CPPSs.
3) Third, regarding the cyber and physical spaces as a single entity, the review studies the external environments (e.g., extreme weather, cyber threats) of CPPSs. Going one step beyond focusing on CPPS itself, the human-in-the-loop effect is also taken into account from a cyber-physical-social perspective.
4) Finally, we provide a comprehensive overview of the state-of-the-art resilience-oriented techniques in three categories, namely natural disasters, cyberattacks, and human behaviors. The remaining challenges and future opportunities for resilience enhancement are also discussed.

### 1.3. Structure of the review

The remainder of this review is structured as follows. Section 2 provides a review on recent blackouts from a cyber-physical perspective. In Section 3, the framework of CPPS and its tri-level interdependences from facilities to functions are presented. Accordingly, Section 4 investigates the external disturbances or security threats of CPPS. Section 5 presents a comprehensive review of the current trends and prospects of CPPS resilience and mitigation techniques. Finally, Section 6 concludes this review paper.

## 2. Review on recent blackouts from a cyber-physical perspective

Power systems are robust and resilient by design, especially for N-1 failures. An independent failure by itself generally does not cause a widespread power outage. For instance, a short-circuit fault of a transmission line on the physical side will be dismissed by a fast-response relay protection system on the cyber side. However, due to the superimposed vulnerabilities of the cyber and physical spaces, cyber threats or even cyber-physical coupling failures may lead a CPPS into catastrophic cascading failures. This can also be observed from some widespread blackouts in recent years [12–28], as shown in Table 1.

To better study these historical events from the cyber-physical perspective, we divide the disturbances that caused the blackouts into cyber-side and physical-side disturbances. Furthermore, in this section, several representative events are selected to study the potential weak points in the resilience of CPPSs.

### 2.1. 2015 Ukraine cyberattack

On 23 December 2015, hackers attacked the Ukraine power grid's information systems of three energy distribution companies with a malware named BlackEnergy, resulting in a widespread blackout affecting approximately 225,000 customers for several hours [26]. This is the first known widespread blackout caused by cyberattacks, which can be considered as a "milestone" in cyberattacks against power grids. Although modern power systems are designed to withstand many serious physical disturbances, they are still unprepared to defend against various cyberattacks.

According to the retrospective investigation of this incident, the primary cause was that the BlackEnergy malware was implanted into the corporate networks of the Ukraine power grid using spear-phishing emails, and then it hijacked the Supervisory Control and Data Acquisition (SCADA) system [27]. The hijacked SCADA system was compromised and several generators and substations were remotely shut down. Simultaneously, the denial-of-service attack was executed on a call center to block customers' calls about the real-time outage status. Consequently, the operators had to shut down the SCADA system and activate manual control to restore power.

**Table 1**
Several blackouts related to cyber-physical disturbances and their impacts.

| Blackout event | Disturbances | | Impact |
|---|---|---|---|
| | Cyber side | Physical side | |
| 2003 US-Canada [20,21] | State estimation malfunction due to software bug | Cascading line tripped in Ohio | Cumulative loss load of 61,800 MW; more than 50 million customers were impacted |
| 2003 Italy [22,23] | Partial failure of the SCADA system | A 400 kV line tripped, causing overload and low frequency | Almost the whole of Italy and its population of 57 million were affected |
| 2008 Florida [24] | Relay protection disabled in an automated substation | Voltage control equipment caught fire | About 1 million customers lost 3650 MW load |
| 2008 Southern China [12,25] | Cyber-physical coupling failures<br>Transmission towers collapsed due to severe ice storm and accretion | | Maximum 14.82 GW load; about 53,982 industrial customer and 6.42 million resident customers were affected |
| 2015 Ukraine [26,27] | SCADA/EMS system was hijacked and compromised | Substations were switched off by the hijacked SCADA system | Approximately 225,000 customers were affected |
| 2016 Xiamen [28] | Failures of optical fibers and transmission lines due to violent Typhoon Meranti | | Affected about 3 million customers; five 500 kV towers, ten 220 kV towers, and one 110 kV transmission tower collapsed |

Notably, the BlackEnergy malware in this event was not precisely customized to a certain grid. The hackers used a large-area and indiscriminate attack on the relevant equipment in the SCADA system to force it to shut down, thereby affecting the security of the power system. What is worrying is whether future cyberattacks will take a more concealed method to target the weak points of power systems and result in more severe damage. Existing studies have shown that the precise construction of an FDIA for state estimation can perfectly avoid bad data detection and even affect the power market [29]. This incident also reminds us that how to improve the resilience of CPPS against cyberattacks will be a key challenge under a more open network environment with access to multiple participants in future smart grids.

### 2.2. 2008 Chinese ice storm

In early 2008, the southern power grid region of China suffered a historically severe ice storm. As shown in Fig. 1, the disaster severely ravaged seven provinces in southern China, with a maximum load loss of 14.82 GW, and about 53,982 industrial customers and 6.42 million resident customers were affected [12,25]. The primary cause of this accident was the heavy ice covering the transmission lines, which induced widespread line outages and transmission tower collapses. It was reported that 678 towers with 500 kV lines and 1432 towers with 220 kV lines collapsed [30].

Although there have been studies on the large-scale disturbances on the physical side, we can still find some important results and experiences from the cyber-physical perspective. As the backbone communication network of China's transmission power grid is based on optical fiber composite overhead ground wire (OPGW), the fibers carry various services of power system such as relay protection and control services. When the transmission towers collapsed due to the severe ice storms, the high-voltage transmission lines and communication links were interrupted simultaneously, that is, cyber-physical coupling failure occurred. Due to the fragile structure of the communication network in the ice storm region, the area was unobservable and uncontrollable. Consequently, the system failure continued to expand, leading to this

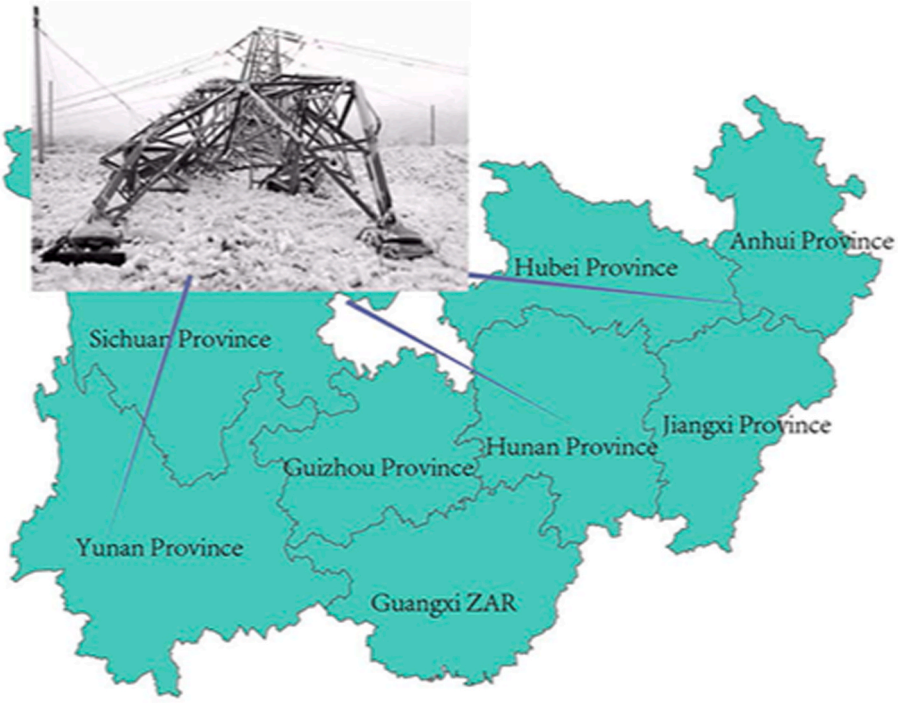


**Fig. 1.** High-voltage transmission towers in seven provinces in southern China collapsed in the 2008 Chinese ice storm.

catastrophic cascading failure. It can be learned from this event that a robust communication network is critical to the resilience of a power system.

### 2.3. 2016 Xiamen blackout by Typhoon Meranti

On September 15, 2016, Typhoon Meranti stroke Xiamen Island, China (one of the most developed cities in Fujian Province). Meranti, with a 48 m/s central wind speed and 70 m/s maximum gust speed, caused a widespread blackout on Xiamen Island and its surrounding areas, affecting about 3 million customers. Compared with the typhoon that had hit Xiamen previously, the collapse of transmission towers was the main reason for the tremendous impact of Meranti, as shown in Fig. 2. According to an undisclosed report, there were collapses of five 500 kV, ten 220 kV, and one 110 kV transmission towers.

The two main 500 kV transmission lines (H-X Line I and H-X Line II) and other 220 kV lines supporting the electricity of Xiamen Island were interrupted due to the collapse of their corresponding transmission towers. It is noteworthy that the optic fibers in the OPGW of this section of the transmission line were also broken at the same time. The real-time


**Fig. 2.** Collapses of high-voltage transmission towers in Xiamen due to 2016 Typhoon Meranti.

control and partial relay protection services in the optical transport network (OTN) of the Xiamen power grid adopts the "1 + 1" or even "1 + 2" main-alternate routing mechanism based on circuiting switching, which is carried in the optic fibers in OPGWs. The automatic switching of the alternate routing guarantees the reliability of communication links in any N-1 situation. However, due to the influence of Typhoon Meranti, the communication network of the northwest part of the Xiamen Island power grid was severely damaged, resulting in the unreachable critical services of Xiamen communication network for power systems remedial control. This event also reminds us that the improvement of the resilience of the CPPS cannot ignore the impact of such cyber-physical coupling failures.

### 2.4. Discussion

Traditional power system blackout and resilience research focuses on passive disturbances (passive attacks) caused by external natural hazards. With the superposition of information systems, from the CPS perspective, the threat of cyberattacks and the impact of human behaviors on physical power grids are increasing, which reconstructs the external environment of a CPPS with a higher risk of active attacks.

It is noteworthy that such active attacks are significantly different from passive attacks in terms of their impact on the vulnerability, reliability, and resilience of CPPSs. It can be observed from the real-world blackout events in Table 1 that active attacks are more targeted and affect the CPPS by manipulating the information system on the cyber side. Such active attacks may be crafted carefully and stealthily. While passive attacks are more random, they tend to be more regional and attack CPPSs by destroying the infrastructure.

Although the failure of a physical power grid can directly affect the power supply, modern power systems are embedded with many advanced information systems to prevent physical cascading failures and thus alleviate the impacts of physical power grid failures. However, cyber network malfunction may cause wide-spread blackouts due to the loss of controllability and observability. Additionally, malicious attackers can perform a more stealthy, large-scale attack on the resilience of CPPSs. Considering the cyber-physical coupling characteristic of modern power systems, cyber-physical coupling failures bring more challenges to the resilience of CPPSs.

## 3. Cyber-physical power system framework and its interdependence analysis

In this section, we aim to present the general framework of a CPPS and its key features. Subsequently, we analyze the interdependence characteristics of the CPPS on facilities, topologies, and functions from the bottom up. Through this analysis, we hope to explore the weak points and vulnerability of the CPPS and thus provide a basis for improving its resilience.

### 3.1. Framework and key features

A CPPS can be regarded as an in-depth coupled system of the cyber and the physical spaces. Its cyber space is composed of communication networks and advanced information systems, including ubiquitous measurement, information transmission and processing, and decision-making activities. The physical space consists of the basic components of a power system and its energy flow. The cross-space interaction of information flow and energy flow makes the cyber and physical spaces tightly coupled.

Thinking of a CPPS from Bertalanffy's general system theory [2], the CPPS can be defined as a set of elements, interconnections, and functions. Specifically, these objects in the set are described as follows:

- **Elements:** The elements in a CPPS refer to its components and facilities on both the cyber side and the physical side, such as power plants, substations, sensors, actuators, and optical cables. For modern power systems, some new participants, e.g., DERs, EVs, and humans, can also be regarded as elements in a CPPS.
- **Interconnections:** The interconnections construct power facilities and communication equipment into the power grid and the communication network, respectively, and achieve interaction between elements through energy flow and information flow. The integration of multi-agent renewable energy and EVs introduces the interconnections of social network and transportation network in a CPPS.
- **Functions:** The functions of a CPPS are related to many advanced information systems, such as the energy management system (EMS), to meet the electricity demand and the security of the power system. The functions are the driving forces to achieving deep integration between the cyber and physical spaces. In a modern power system with various participants, the functions of the electricity market and demand response further deepen the effects on the elements of CPPSs.

To clarify how elements, interconnections and functions constitute an operational CPPS with integrality, as shown in Fig. 3, the relationships between these components of a CPPS are further explained as follows: 1) From elements to interconnections: Isolated, unconnected elements cannot form a system with integrality. The interconnections between the elements of a CPPS constitute the basic cyber-physical network structure, laying the foundation of carrying information and energy flow. 2) From interconnections to functions: The cyber-physical network with interconnections of elements needs to perform specific functions to form an operational system. For a CPPS, the functions can be regarded as the energy flow and information flow over physical power grids and information systems. 3) From functions to elements: The functions, like the brain of a CPPS, perceive and control the state of the elements through the interconnections of information flow and energy flow, which is a critical relationship for a CPPS to maintain stability and the functional operation of the elements.

Before analyzing the interdependence of a CPPS, inspired by Meadows [31], and based on the above framework of CPPS, we describe

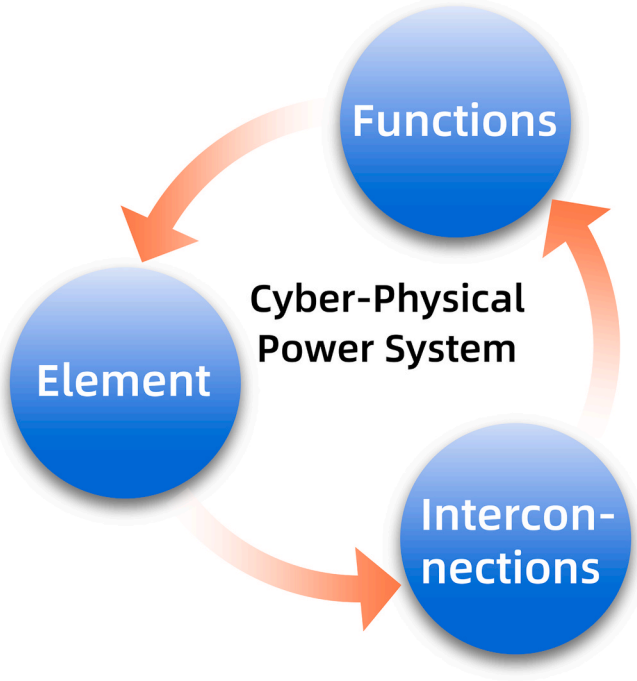


**Fig. 3.** The framework of a cyber-physical power system (CPPS) from a system-theory perspective.

the following key features of a CPPS:

1) Hierarchy

Hierarchy is an important feature of a CPPS that allows the CPPS to be clearly divided into several subsets. There are stronger interconnections between elements within each subset than across subsets. A hierarchical structure can be found in both the cyber and physical spaces of a CPPS. In the physical space, the power grid can be divided into transmission systems, distribution systems, and even microgrids. Correspondingly, the backbone network on the cyber side is tightly coupled with the transmission system, and the access network achieves the situational awareness and control of the distribution system. Apparently, the hierarchical structure improves the operational efficiency and performance of stability of the CPPS [32]. In general, from conventional centralized to decomposition and coordination or further to the distributed mode, a control architecture that adapts to a hierarchical CPPS shows better performance in resilience [33]. The hierarchical characteristic also reminds us that the resilience of CPPSs can be studied from different system levels and architectures.

2) Self-organization

Self-organization is one of the fascinating characteristics existing in many natural systems. It describes the property of an open system that can spontaneously tend to an equilibrium point or a stable state when there is no interaction with its outside environments, which is a general paradigm for many industrial control systems [34]. As a closed-loop feedback control system, a CPPS deeply relies on advanced information systems. Many important functions (e.g., automatic generation control) can automatically achieve decision-making and execution. These functions make the CPPS tend to an economical and stable operation point spontaneously, such as maintaining the equal incremental rate criterion [35] and 50/60 Hz frequency stability [36].

3) Resilience and vulnerability

Resilient CPPSs in adversarial environments require 1) toughness to maintain the core functions and 2) elasticity to recover to the normal system state in a timely manner [37]. The primary purpose of integrating advanced information systems into power systems is to satisfy the requirement of power system resilience against disturbances. The stable and secure operation of a modern power system highly depends on its information systems such as EMS, which illustrates that a CPPS is also designed by resilience. However, although resilience and vulnerability are contradictory, they also coexist and are inseparable for a CPPS [8]. The usage of these information systems is essential to improve the controllability and observability of the physical power grid, but it also makes the vulnerability of the entire system superimposed. The power system will face a higher risk of cyber-side disturbance being transmitted to the physical side [38].

Resilience is a necessary but not sufficient condition for the reliable operation of a CPPS. Due to disturbances and vulnerability, a CPPS with a certain degree of resilience may still collapse, just as the human body has an immune system and may still get sick. Therefore, how to quantify and improve the resilience of a CPPS should be the key issue in the system design. In the follow-up of this review, we will focus on this feature.

It is noteworthy that the concepts of CPPS resilience and power system resilience should be distinguished, which helps to better understand the resilience of CPPSs so as to study the resilience-enhancement techniques for CPPSs. Although the concept of CPPS resilience is defined in state-of-the-art research (e.g., in Ref. [8], cyber-physical resilience is defined as *the system's ability to maintain continuous electricity flow to customers given a certain load prioritization scheme*), the differences between the CPPS resilience and the traditional power system resilience have not been emphasized. Exploring the differences in the resilience of different systems can clarify the objects of their applications, the environments or disturbances they face, and the emphasis of resilience-enhancement techniques.

**Remark 1:** Different from the traditional perspective of power system resilience, the object of CPPS resilience targets the integrated cyber-physical system as a single entity, as shown in Table 2. Due to the more complicated external environments of CPPSs, CPPS resilience faces great challenges from multiple, heterogeneous disturbances (e.g., natural hazards, cyber threats, human behaviors, and even cyber-physical coupling failures). The coupling of cyber and physical spaces also results in the superposition of vulnerability. Because the operation of a CPPS highly depends on situational awareness based on information systems, the restoration of a resilient CPPS should give priority to its information systems to ensure the controllability and observability of the physical system such as an inverter-based microgrid. Compared with the optimization and scheduling of physical facilities for power system resilience, the resilience-oriented enhancement strategies of a CPPS emphasize the combination of advanced ICT and the application of cyber-physical collaborative techniques.

To explore the potential weaknesses of a hierarchical CPPS, combined with the above-mentioned framework and key features, we divide its interdependences into three layers, as shown in Fig. 4. More specifically, we discuss them separately in the follow-up.

### 3.2. Interdependence on facilities

Facilities are the key component of the elements in the above CPPS framework. Under the background of the application of IoT enabling technologies, many advanced devices in CPPSs are embedded with advanced sensing and control units, such as power inverters of distributed generators (DGs) [39], smart meters [40], and electronic-based solid-state transformers [41]. These facilities build a bridge for the interaction of information flow and energy flow so that the cyber and physical spaces are highly interdependent at the level of facilities.

Taking the inverters as an example, the inverter of DGs measures the state of the physical system, such as frequency through the phase-locked loop, and then controls the active and reactive output of DGs. This closed-loop feedback system at the facility level embodies the cyber-physical integration. Furthermore, Ilić et al. [42] propose a cyber-physical module of power plants and loads, which also reflects the interdependence on facilities. Furthermore, the increasing integration of inverter-based DGs leads the hierarchical CPPS to be distributed and deepens this facility-level interdependence, which induces the risk of third-party cyber threats against these smart inverters [43]. Recent research by He et al. [44] shows that a proposed double modulation strategy applied in dc-dc power converters can achieve "talkative power" for both power and data by a frequency hopping-differential phase shift keying method, which provides deeper integration of power and communication systems in future inverter-based CPPSs.

**Table 2**
Comparison of traditional power system resilience and CPPS resilience.

| | Power system resilience | CPPS resilience |
|---|---|---|
| **Object** | Traditional power systems | Cyber-physical power systems |
| **Disturbances** | Natural hazards | Natural hazards/cyber threats/ cyber contingency/human behaviors |
| **Vulnerability** | Only physical space | Cyber and physical space superposition |
| **Recovery priority** | – | Cyber side prior to physical side |
| **Enhancement** | Optimization and scheduling of physical facilities | Advanced ICT and cyber-physical collaborative techniques |

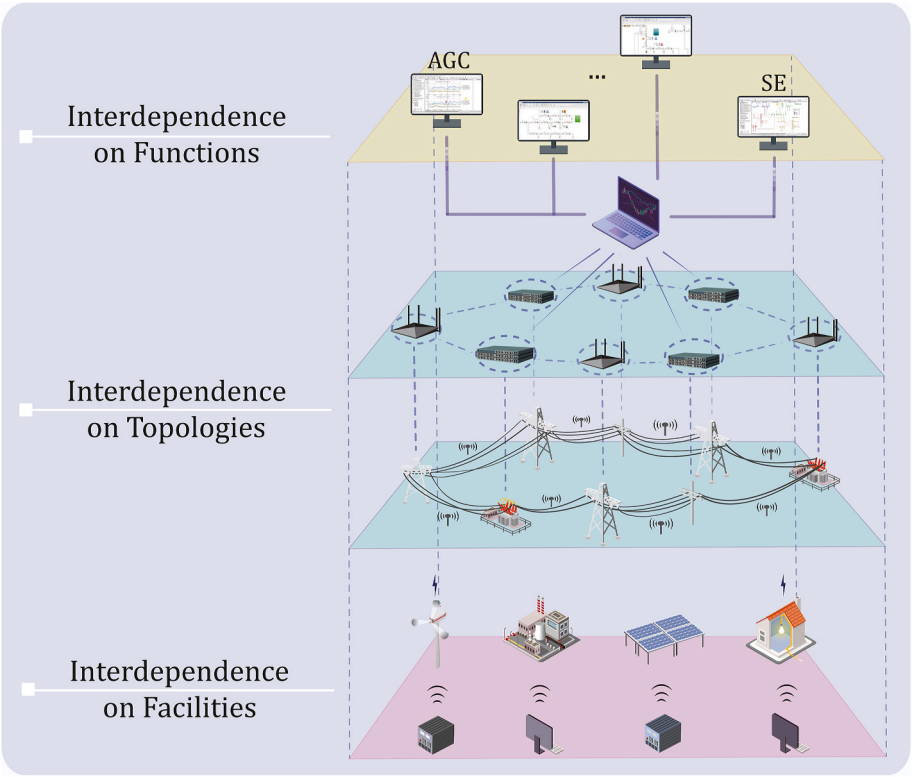


**Fig. 4.** Three-layer interdependences of a CPPS.

### 3.3. *Interdependence on topologies*

On the physical side, the transmission of electricity is inseparable from the grid formed by power transmission lines. Similarly, the accessible communication between the control center and the substation also relies on the communication network established by communication links. To guarantee the reliability of real-time control services, the synchronous digital hierarchy (SDH)-based optical network (SONET) has been widely used in power system communications [45,46]. Ubiquitous sensor units and advanced ICT have resulted in a data explosion for CPPSs. To meet the real-time communication requirements of smart grids, an optical transport network (OTN) combined with wavelength division multiplexing (WDM) and SDH has become a considerable option for the next generation of backbone communication networks for power systems [47].

To build a more robust backbone communication network, optical fiber composite overhead ground wire (OPGW) on the top of transmission towers has a popular structure in modern power systems [48]. In

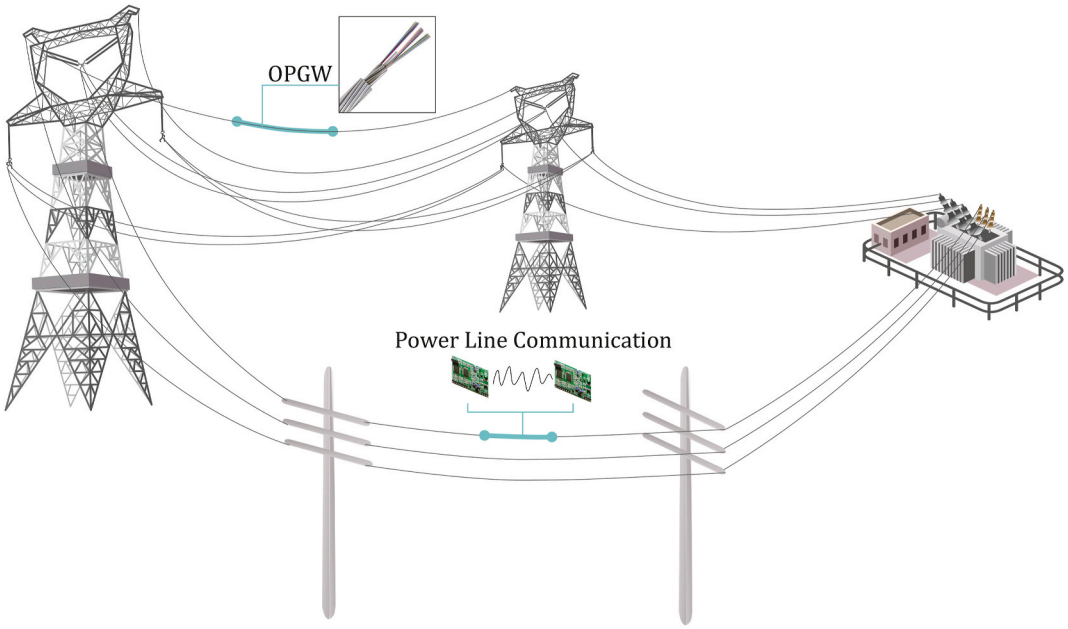


**Fig. 5.** Schematic of optical fiber composite overhead ground wire (OPGW) and power line communication (PLC) solutions.

low-voltage transmission networks or distribution networks, power line communication (PLC) has been widely used to construct access communication networks [49]. It is worth noting that these OPGW-based and PLC-based communication networks for power systems make the topology of the communication network and the topology of the power grid have a high degree of spatial consistency, as shown in Fig. 5. Naturally, two spatially strong interdependent networks also face a higher risk of catastrophic cyber-physical coupling cascading failures [50].

### 3.4. Interdependence on functions

As shown in Fig. 4, as the top-level structure of a hierarchical CPPS, functions affect the facilities from top to bottom through interconnections so as to maintain the steady-state equilibrium (self-organization feature) and the stability of the CPPS under disturbance (resilience feature). The EMS, as an important advanced information system for CPPSs, can measure the state of the physical power grid through SCADA for decision making and control the power system by issuing corresponding control commands. According to Ref. [51], the function of the EMS in a CPPS is modeled by an information-energy flow that involves four activities: 1) energy flow, which reflects the energy distribution state of the power grid; 2) energy to information, which corresponds to the measurement activity; 3) information flow, which includes information transmission, processing, and decision making in the closed-loop control system; and 4) information to energy, which corresponds to the control execution activity. In addition, the massive energy consumers can also be regarded as a kind of function, which involves two activities: 1) situational awareness in the physical system and receiving incentive information from the cyber system; and 2) utility assessment and behavior decision making in energy consumption.

Such an information-energy flow structure reflects the interdependence of functions of a CPPS. When cyber contingencies occur in the information flow, due to such interdependence, disturbances may propagate from the information flow to the energy flow through functions, thereby affecting the security of the CPPS.

### 3.5. Multi-layer interdependences

A CPPS consists of elements, interconnections, and functions corresponding to the interdependences on facilities, topologies, and functions, respectively. Furthermore, as shown in Fig. 3, an operational CPPS with integrality includes interdependences from facilities to topologies and then to functions, that is, multi-layer interdependences.

It is noteworthy that under steady-state operation, such multi-layer interdependences are the necessary condition to guarantee the efficient, safe, and economical operation of a CPPS. However, the multi-layer interdependences of the CPPS also provide a basis for cross-layer and cross-space failure spreading, leading to cascading failures. The failure of interdependent facilities will affect the operation of physical infrastructure and the perception of cyber units due to the interdependences on facilities. Then, since the facilities are important components of topologies, the failures can impair the reliability and resilience of both the communication networks and power grids from equipment to topology. At the function level, considering the dependence of the functions on the topologies, the availability of the information flow of a CPPS will be affected by the network malfunction. Similarly, the disturbances of the power flow may further lead to the instability of the CPPS. Therefore, the influence of multi-layer interdependences on the resilience of CPPSs should be further emphasized.

## 4. Disturbances and security threats of cyber-physical power systems

As an open system, the CPPS needs to maintain equilibrium not only between internal elements but also between itself and the external environment through input, output, and feedback. Compared with conventional power systems, the CPPS broadens its boundary with the combination of advanced information systems on the cyber side. It faces a more complicated environment and the corresponding disturbances.

Combining the recent blackout review in Section 2, and the framework of CPPS and its interdependences in Section 3, this section focuses on the external disturbances and potential cyber threats against the resilience of CPPSs.

### 4.1. Natural hazards

As discussed in the blackouts review in Section 2, recent years have witnessed the impact of natural hazards on the resilience of CPPSs, especially when cyber-physical coupling failures occur. According to Climate Central's analysis of data from North American Electric Reliability Corporation, nearly 80% of all power outages from 2003 to 2012 were weather-related, including hurricanes, tornadoes, cold weather with ice storms, and a combination of extreme heat events and wildfires [52]. In late 2019, residents in California suffered from the longest power outage in history due to wildfires [53]. It has also been reported that some large blackouts fall into multiple initiating-event categories, such as extreme weather combined with supply shortage or even renewable generation fluctuation [54]. For a power grid, these natural disasters strike the physical infrastructure of the power system. Overhead transmission and distribution lines may trip due to hurricanes and windstorms [55]. Towers may collapse due to severe ice accretion that exceeds the designed carrying capacity, as in the 2008 Chinese ice storm.

However, unlike the traditional perspective of the impact of hazards on power systems, our review aims to analyze the challenges brought by hazards to the resilience of CPPSs on both the cyber and the physical spaces. Learning from previous blackouts, extreme weather may simultaneously affect a CPPS based on the interdependence on topologies presented in Section 2. For example, typhoons, ice storms, etc. induce the collapse of transmission towers, and the corresponding power lines and OPGW-based communication links are interrupted at the same time. OPGW combines ground wire for lighting conductor and optic fiber for communication. A field test by Cardiff University's Lightning Laboratory [56] shows that lightning strikes significantly affect the rate of the state of polarization of light in the fiber and can even cause communication interruption.

At present, the introduction of new technologies such as renewable energy power generation and EVs has effectively dealt with the crisis of energy and environment, but it also makes CPPS face more challenges under natural hazards.

Different from a geographically fixed load, the possible redistribution of mobile EV charging demand in the case of extreme events (e.g., typhoon, hurricane, wildfire) poses a greater threat to CPPS resilience. The impact of EV evacuations during wildfire events on grid resiliency is analyzed by Donaldson et al. [57]. Their work shows that increasing EV penetration might cause an exponential increase in the resiliency indices. This potential risk has been demonstrated in accidents in recent years. On Sept. 15, 2018, numerous charging stations in Shenzhen, China were closed due to Typhoon Mangkhut, which caused many taxis to be out-of-service [58]. Apart from the paralysis of the transportation system, the large-scale transfer of EV taxi charging loads may also bring local overloading risks to the already fragile power system.

Different from conventional generators, DERs such as PVs are subject to the intermittency and uncertainty of the natural environment, which brings challenges to CPPS resilience in various aspects [59]. For instance, the low-inertia problem induced by power electronic converters makes a CPPS more vulnerable to uncertain disturbances, which can further lead to frequency oscillations of the CPPS and even make the system unstable. It is foreseeable that natural hazards will have a more significant impact on the resilience of CPPSs with high penetration of

renewable energy.

Because many critical measurement and emergency control services related to interrupted power lines are carried in OPGW above the transmission line, such as relay protection, these critical services may be interrupted due to a cyber-physical coupling failure. Disturbances of these interdependent facilities and topologies may in turn cause more catastrophic cascading failures due to functional interdependence.

### 4.2. Cyberattacks

The concept of industry 4.0 with IoT, industrial Ethernet, TCP/IP, and other open communication protocols has become widely accepted for use in industrial control systems (ICSs) [60,61]. A CPPS is based on an ICS with extremely high security requirements. It is noteworthy that under the trend of large-scale DERs being integrated with the CPPS, the CPPS has become a multi-agent system with various participants [62,63]. Since the interaction between third-party entities such as active users and power systems will significantly increase, the ICS of a future CPPS will most likely be in an open environment [64]. A multi-agent system will play a more important role in a CPPS under an open network environment. This increases the risk of attacking the traditional isolated ICS of the power system through a path of an open network environment, exposing the CPPS to various cyber threats [65].

As the major concern of this review is the impact of cyberattacks on the resilience of CPPSs, according to the "CI&A" cyber security objectives (confidentiality, integrity, and availability) defined by the US National Institute of Standards and Technology [66,67], cyber threats that impair the resilience of CPPSs can be divided into two direct types (targeting integrity and availability) and one oblique type (targeting confidentiality).

1) Cyber threats targeting integrity

FDIA is a typical cyber threat to the data integrity of CPPSs and has been widely studied [68]. FDIA targets the state estimation function of EMS by injecting a stealthy attack data vector that can evade the widely used residue test for bad data detection. Because many critical functions of the CPPS rely on advanced information systems, such as economic dispatch and locational marginal prices (LMPs) for electricity markets, the economy and security of CPPS may be severely damaged by FDIA. Tajer [69] presents an FDIA that can affect the LMPs in an electricity market by adversaries with limited information of the power system. Moreover, an FDIA can also be used on a multi-agent distributed energy system. Duan and Chow [70] provide a novel data integrity attack on a consensus-based energy management system of microgrids, which uses only local information to complete the attack without additional information. In addition, the Address Resolution Protocol (ARP) spoofing and a stealthy adversary data-based misleading of the control center with an incorrect network topology based on man-in-the-middle attack (MITM) is also a form of attack against integrity [71,72].

Targeting system integrity, malware can manipulate advanced information systems and switch off the critical infrastructure of power grids, resulting in the abnormal operation of a CPPS and even inducing widespread blackouts (e.g., Stuxnet in 2015 Ukraine Blackout [27]).

2) Cyber threats targeting availability

Attacks against the availability of a CPPS's information system mainly affect the accessibility of information flow by obstructing and delaying communication. Denial-of-service (DoS) attacks make use of deficiencies in network protocol by continuously sending a large number of useless requests, thereby occupying the network bandwidth, resulting in communication inefficiency and culminating in the unavailability of components in the communication network [73]. DoS attacks on the load frequency control (LFC) of a smart grid are tested, which shows how the attacks affect the dynamic performance of a CPPS [74]. Notably, DoS attacks can be performed in a distributed way, that is, distributed denial-of-service to disrupt normal traffic of information systems of CPPSs [75]. As the stability of a power system highly depends on the time delay of real-time control services, an adversary may introduce delays into a control cycle in a stealthy way, that is, a time delay attack [76].

3) Cyber threats targeting confidentiality

Intuitively, the main purpose of cyberattacks targeting confidentiality is to steal private data for profit, and they do not directly affect the resilience of a CPPS. However, when an attacker has the ability to perceive the global information of the power grid, a refined cyberattack that is more likely to evade detection can be designed. Cyberattacks have proven to be imperfect under the cases of adversaries with incomplete network information [77]. This illustrates that cyber threats targeting confidentiality can obliquely affect the resilience of a CPPS by superimposing cyberattacks on integrity and availability.

To perform an FIDA that is difficult to detect, an attacker without the full topology and parameter information of a power grid needs to estimate the required parameters [69]. Conversely, if an attacker can target both confidentiality and integrity/availability, a more precise cyberattack can be performed. Therefore, if the integrity-oriented or availability-oriented attacks are simultaneously supplemented by the attack targeting confidentiality, it will pose a more harmful threat to the resilience of a CPPS. This illustrates the relationship between integrity/availability and confidentiality.

### 4.3. Human-in-the-loop

With the increasing importance of social behaviors such as investment, transaction, management, and user selection in power system research, humans are expected to use and be impacted by a CPS. It is necessary to consider the human-in-the-loop factors of the current CPS framework and extend it to a human-centric CPS called a cyber-physical-social system (CPSS). Based on the concept of CPS, the CPSS further considers the influence of the perception, analysis, decision-making, and behavior of the social system on the physical system and information system in the CPS, as is shown in Fig. 6. Xue et al. [78] introduce the concept into the energy system and put forward the concept of a CPSS in the field of energy.

In resilience studies, the social aspect can no longer be ignored, and adopting the CPSS perspective becomes necessary, which further extends the concept of resilience into community resilience. According to the definition stated by the National Institute for Standards and Technology [79], community resilience is "the ability of a community to

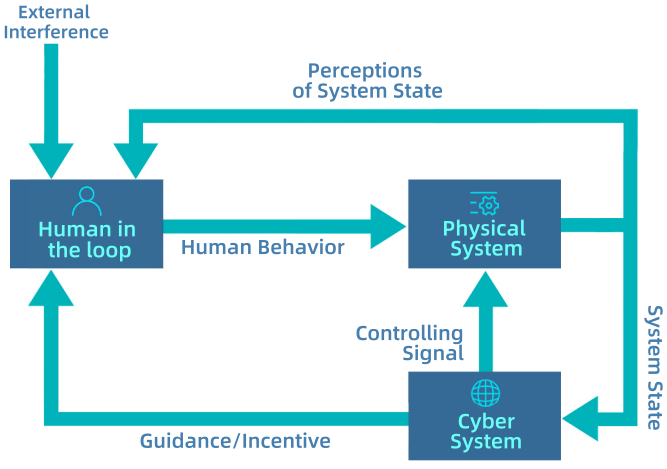


**Fig. 6.** CPSS: Human-in-the-loop CPS.

prepare for anticipated hazards, adapt to changing conditions, and withstand and recover rapidly from disruptions." From the perspective of modeling, human cognition and decision-making behaviors need to be integrated into the comprehensive planning of restoration processes after disruptions. From the perspective of optimization, as the end-users of a CPPS determine the utility of the whole system, any advancement should aim to improve the quality of life of the end-users. The social expectations from various perspectives need to be integrated with the restoration scheduling of CPPSs [80].

Furthermore, the human-in-the-loop factors might pose direct threats to the operation of CPPS and even cause cascading failures. The wrong operation or decision of a few key operators, such as wrong scheduling instructions or negligence in maintenance, will lead to the deviation of CPPS from the secure state. Such mistakes happen almost every day, and are related to the experience, knowledge, and psychological state of the operators. Due to the robustness of the power system, most faults have little impact. However, mis-operation in critical situations may lead to large-scale accidents. For example, the 2012 India blackout and the 2017 Taiwan Island blackout were both caused by human errors.

In addition, the aggregated effect of numerous end-users' active behavior might impact power system operations. The end-users' decisions depend on multiple different criteria, such as cost savings, comfort, ease of use, and privacy. Considering the unpredictable and irrational features of consumer behavior, humans have proven to be one of the weakest links in the power grid.

To influence the end-users' demand response at fixed places, the spread of false messages (e.g., pricing information) might manipulate the individual energy consumers' behavior to shift their power demand into the peak-demand period, which might cause system reserves reduction, peak demand increase, distribution lines overloading, voltage constraints violation, and potential system blackouts [81]. The fake pricing information might be spread through smart meters [82], the internet [83–85], or social networks [86–88]. Therefore, system vulnerabilities come not only from the physical hardware and cyber software but also from the behavior of human consumers.

Regarding EVs with spatial flexibility, an unbalanced redistribution of fast-charging demand after infrastructure faults (e.g., charging station fault [89], roadblock [90], road capacity loss [91], and wildfires [1]) might cause local overloading in the power distribution network and congestion in the traffic network. On May 19, 2018, several fast-charging stations in Shenzhen were in an outage due to load management. Approximately 2700 EV taxis could not be charged, which resulted in long waiting queues at other charging stations. Apart from the reported phenomena, the large-scale redistribution of charging loads to adjacent areas will result in the redistribution of power flow in the power distribution network, which might cause congestion and overloading in the power network of adjacent areas, especially when the adjacent networks have been under heavy loads. As the load redistribution is the aggregated effect of the routing and charging choice of numerous individual drivers, such vulnerabilities essentially arise from human consumers.

## 5. CPPS resilience-enhancement techniques

### 5.1. Resilience-oriented techniques against natural hazards

As mentioned in Section 4.2, although natural disasters are often low-probability events such as windstorms and earthquakes, due to the significant impact of natural hazards on CPPSs, developing resilience-oriented techniques for these high-impact and low-probability events is one of the most critical issues for guaranteeing the reliable operation of CPPSs. Before understanding the resilience of a CPPS, the vulnerability reflecting the effects of natural hazards on the CPPS should be analyzed [8]. Then, the quantification of resilience lays the foundation for resilience enhancement techniques. Therefore, the resilience-oriented techniques of CPPSs against natural hazards consist of the following three parts: 1) vulnerability and resilience assessment metrics; 2) resilience-oriented planning methods; and 3) resilience-oriented operation and restoration approaches. The framework of resilience-oriented techniques of CPPSs against natural hazards is shown in Fig. 7.

#### 5.1.1. Vulnerability and resilience assessment metrics

Vulnerability is highly correlated with the possibility of a disaster and its potential negative impact [92], describing the ability of failures to affect the system. Resilience denotes the ability of the system to recover from low-probability and high-impact events. A power system with high-level vulnerability against low-probability and high-impact events has a low-level resilience [15]. As stated in Section 3, the vulnerability and resilience of a CPPS are highly related. A CPPS relies on the real-time control services of advanced information systems to improve its security and resilience, but this also exposes the CPPS to more loopholes due to the superposition of the vulnerability of the cyber and physical spaces. Before studying the resilience enhancement techniques of a CPPS, quantifying the vulnerability and resilience of a CPPS is a key precursor. As mentioned before, natural hazards may lead to catastrophic cascading failures of a CPPS. Different from the cyberattack-resilience techniques to be discussed in Section 5.2, this section focuses on the vulnerability and resilience of CPPSs when facing hazards and information system malfunctions without cyberattacks.

1) Vulnerability of CPPSs

Following the cascading failures of interdependent networks based on percolation theory proposed by Buldyrev et al. [7], Vespignani [93] studies the vulnerability of the tightly coupled cyber-physical infrastructures under cascading failures based on the percolation analysis of two mutually dependent networks, which shows that the interdependent characteristic is critical to resilient system design. Aminfar et al. [94] study the impact of wide-area measurement system (WAMS) monitoring/control malfunction on power systems based on an algorithm embedded optimal power flow function and optimal load shedding function on the cyber side, which quantifies the impact of cyber malfunctions by a load shedding metric. However, for the reliability of CPPSs, the impact of cyber contingencies on microgrids can be evaluated by the metric proposed by Wang et al. [95], which also applies vulnerability analysis of more severe malfunctions. Considering cyber contingencies, Xin et al. [96] display a vulnerability evaluation framework of hierarchical CPPSs. Furthermore, the vulnerability is compared

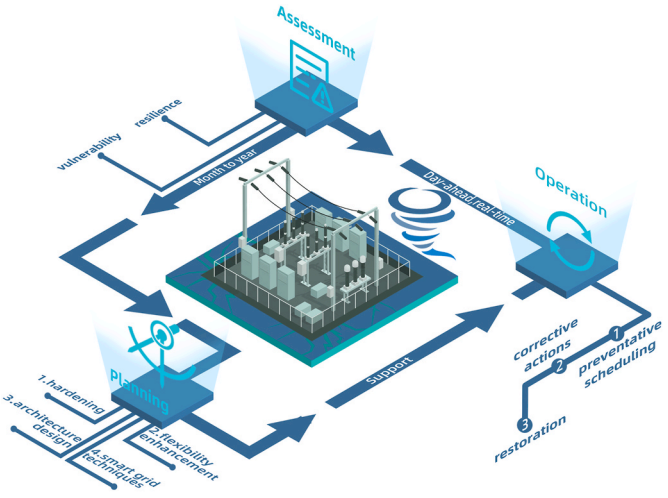


**Fig. 7.** The framework of resilience-oriented techniques of CPPSs against natural hazards.

between the centralized and distributed control mode in coordinated substation voltage control based on the proposed method. The results show that the distributed control mode has a better performance against various cyber contingencies in coordinated substation voltage control [97]. It is noteworthy that the interdependent network-based metrics concern the coupled topologies of CPPSs and less consider the functional interaction. Vice versa, the information-energy flow architecture [94–97] mainly focuses on the impact of cyber malfunction or cyber contingencies on the physical power systems without considering the spatially interdependent network and the impact of the physical side on the cyber side.

2) Resilience of CPPSs

Quantifying resilience helps to explore efficient techniques to improve the ability of systems to function in the face of natural disasters and extreme weather. For an infrastructure system, a "resilience triangle" index associated with a single event is presented by Tierney et al. [98], which depends on the integral of the deviation of system function from the moment of failure to the end of the restoration, that is, the area of the triangle. It assumes that the system function will suddenly fall to a trough when an extreme event occurs without considering one of the most critical characteristics of resilience: the resistance of the system against the fault. Hence, for better quantifying the resilience of a system, an improved "resilience trapezoid" introduced by Izadi et al. [1] and Panteli et al. [99] is more widely adopted to take into account the resistant resilience. Furthermore, for an interdependent infrastructure system, a quantitative resilience assessment method with a hybrid modeling approach for simulating cascading failures is developed by Nan et al. [100] considering three types of essential resilience (i.e., absorptive, adaptive, and restorative capabilities). Inspired by the "resilience trapezoid," the four-phase performance of a dynamic system function for defining the resilience based on the CPPS framework and key features in Section 3.1 is shown in Fig. 8. Here we note that the resilience describes the performance of the system in extreme scenarios, even the worst-case scenario.

Regarding the resilience of a CPPS, on the physical side, plenty of studies have explored the resilience assessment metrics of power systems in the face of natural disasters and extreme weather. For example, Ly et al. [101] study the resource resilience of power systems in extreme winter weather events by the reserve margin calculation. Panteli et al. [102,103] propose a resilience assessment framework for critical infrastructures of power systems against extreme weather events. A resilience achievement worth index is presented by Panteli et al. [103] based on a fragility model of transmission system and sequential Monte Carlo simulation, which can be used for identifying the critical network sections under extreme weather. Das et al. [104] systematically review the existing qualitative framework and quantitative metrics of the resilience of smart grids. It is also mentioned that the resilience

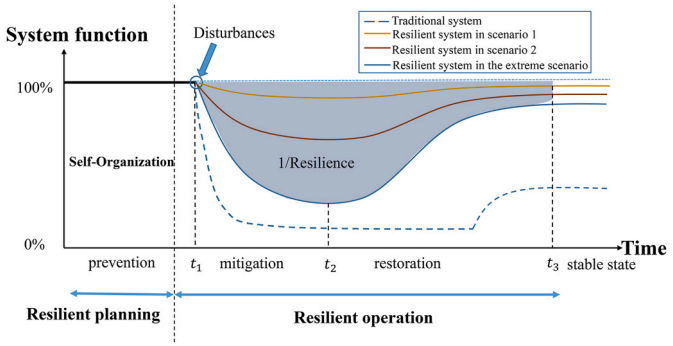


**Fig. 8.** Four-phase performance of a dynamic system function under several scenarios with disturbances.

assessment is far from being solved and there are still several factors that need to be further considered, such as operational factors in communication. This outlook also validates the necessity of studying the resilience of smart grids from the cyber-physical perspective, that is, the resilience of CPPSs.

Although cyber-physical resilience against malicious cyberattacks and its assessment metric have been studied by Clark et al. [37], a resilience assessment framework considering the impact of natural disaster-induced cyber-physical coupling failures of the interdependent topologies and functions still needs to be investigated.

*5.1.2. Resilience-oriented planning*

Resilience-oriented planning is the first step of a CPPS to resist natural disasters. Without the strong and resilient fundamentals of CPPSs, a resilient operating strategy cannot show its validity. We organize the resilience-oriented planning strategies into the following four types: 1) system hardening; 2) flexibility enhancement; 3) topology and architecture design; and 4) embedded smart grid technology. These four types of planning strategies are summarized in Table 3. We also further categorize the strategies into targeting on the physical side and targeting on the cyber side so as to explore the other potential methods to improve the resilience of CPPSs.

1) System hardening

Hardening the existing infrastructure of CPPSs is a cost-effective and efficient approach to cope with upcoming natural hazards. From the experience of previous widespread blackouts, we have learned that many power outages are induced by overhead line interruptions, such as line tripping in the 2016 Xiamen blackout caused by typhoons. For this reason, Panteli et al. [99] present several approaches to boost infrastructure resilience such as undergrounding overhead lines and relocating critical facilities. Although in practice undergrounding all overhead lines is beyond budget, this approach can be used for some critical tie-lines that are vulnerable to hazards. For example, Xiamen island in China has newly adopted submarine power cables to improve resilience against extreme weather. In Ref. [105], elevating substations, utilizing mobile transformers against floods, and managing vegetation to prevent short circuits are also listed as strategies to harden the system.

For distribution systems with multiple microgrids, Wang et al. [106] propose a two-stage robust optimization with the min-max-min objective for line hardening planning against worst N-k contingencies. Based on the operational subproblems with maximizing the load shedding cost, this two-stage planning can determine a robust line hardening strategy while minimizing the hardening cost to enhance the system resilience against natural disasters. In a similar tri-level defender-attacker-defender robust optimization form, Lin et al. [107] present an optimal hardening strategy for a distribution system considering reconfiguration and DG islanding capacity. For earthquakes, Oboudi et al. [108] propose a resilience enhancement optimization for retrofitting the critical components of substations in the form of a knapsack problem by using the pre-earthquake cost and the cost caused by earthquakes to quantify the system resilience. In addition, resilience strategies including line hardening and construction based on a data-driven transmission defense planning (DTDP) mode are proposed by Yan et al. [109], which show better performance in the face of extreme weather.

2) Flexibility enhancement

For short-term operational problems, making full use of system flexibility is beneficial for resisting extreme events under different states of a CPPS. For the planning of a CPPS, improving the flexibility of the system can reduce the uncertainty caused by intermittent renewable generation and allow higher penetration of renewable energy while guaranteeing that the system is sufficiently resilient to potential natural

**Table 3**
Resilience-oriented planning techniques for CPPSs.

| Taxonomy | Application to | Resilience against | Method/Technique | Targeting on | | Year | Ref. |
|---|---|---|---|---|---|---|---|
| | | | | Physical side | Cyber side | | |
| **System Hardening** | Transmission/ Distribution system | Extreme hazards (typhoon, earthquake) | Boosting the infrastructure resilience (e.g., undergrounding overhead lines and relocating) | ✓ | | 2017 | [99] |
| | Transmission/ Distribution system | Extreme weather | Hardening infrastructures and managing environment (e.g., vegetation) | ✓ | | 2010 | [105] |
| | Distribution system with multiple microgrids | N-k contingencies | Two-stage min-max-min robust optimization for line hardening planning considering N-k faults | ✓ | | 2019 | [106] |
| | Distribution system/ Microgrid | Natural disasters and man-made attacks | Tri-level optimization of reconfiguration and DG islanding | ✓ | | 2018 | [107] |
| | Substations | Earthquakes | Retrofit of substations' critical components in the form of a knapsack problem | ✓ | | 2020 | [108] |
| | Transmission system | Extreme weather | Line hardening and construction based on a data-driven transmission defense planning model | ✓ | | 2020 | [109] |
| **Flexibility Enhancement** | Transmission system | Extreme weather (heat waves and drought) | New units planning considering the operational flexibility against power fluctuation and extreme weather events | ✓ | | 2019 | [110] |
| | Transmission system | Natural disasters | Integrating planning of multi-energy system to share the potential enhancement of resilience | ✓ | | 2017 | [111] |
| | Transmission/ Distribution system | Natural disasters | Integrated restoration planning by using the iteration of mathematical programming and simulation | ✓ | | 2017 | [112] |
| | Distribution system | Random failures of cyber system | DG configuration and communication mode co-planning | ✓ | ✓ | 2020 | [113] |
| **Topology and Architecture Design** | Transmission system | Cascading failures caused by natural disasters | Resilient TEP minimizing the effects of cascading outages with resilience constraints | ✓ | | 2020 | [114] |
| | Distribution system/ Microgrid | Extreme events | Integrating controllable and islandable microgrids to improve the resilience of power grids | ✓ | | 2016 | [115] |
| | Distribution system/ Microgrid | Extreme events | Forming a networked microgrid cluster for resilience | ✓ | | 2017 | [116] |
| **Smart Grid Technology** | Transmission/ Distribution system | Extreme situations with cyber contingencies | SDN-based communication network | | ✓ | 2017 | [117] |
| | Distribution system/ Microgrid | Extreme natural disasters | AMI and PMU to enhance situational awareness for resilience | | ✓ | 2017 | [118] |
| | Distribution system/ Microgrid | Natural disasters | Ad hoc self-organized communication framework | | ✓ | 2020 | [119] |

hazards. To enhance the operational flexibility and the resilience against extreme heat waves and drought events, Abdin et al. [110] design a renewable generation unit planning framework considering the extreme effects on the performance of DG generation and load, where the resilient plan shows a lower load shedding rate, especially in an extreme scenario with low water availability.

Constructing a multi-energy system, also called Energy Internet, can improve not only the energy efficiency but also the flexibility of the entire system and can serve as a backup when a single system cannot withstand an extreme disturbance. For this purpose, a tri-level integrating planning method for the multi-energy system to share the potential enhancement of the resilience against extreme events is proposed by Shao et al. [111]. By fully developing the flexibility of the multi-energy system, the numerical results show that a smaller investment is needed to satisfy the requirements of the system's resilience. A resilient CPPS requires the ability to restore power services after extreme events. Considering that the restoration of the subsystems of a power system is designed in parallel, Qiu et al. [112] propose an integrated restoration planning focusing on generation restoration by using the iteration of mathematical programming and simulation to achieve a global optimal solution. For this restoration planning, the computations remain a challenge.

For a cyber-physical active distribution system, constructing the integration and interconnection of DGs should consider not only the physical topology planning but also its communication network, especially for constructing a microgrid under fully distributed control architecture. Thus, Liu et al. [113] propose a DG configuration and communication mode co-planning approach for DG interconnection in a cyber-physical active distribution system. To improve the resilience against cyber failures, the Monte Carlo simulation is used to adjust the planning decision so as to obtain the final scheme considering cyber failures.

3) Topology and architecture design

In the resilience-oriented planning methods, expansion planning and architecture redesign offer an efficient long-term way to improve the resilience of a CPPS against various natural disasters. As conventional transmission expansion planning (TEP) does not consider the impact of failures on the power system, a resilient TEP proposed by Qorbani et al. [114] incorporates the resilience constraint to minimize the effects of cascading power outages that are estimated based on load curtailment calculated by a steady-state cascading failure analysis framework.

With the higher penetration of renewable generation and DG in modern power systems, traditional power grids tend to be decentralized and distributed. Liu et al. [115] show that integrating controllable microgrids with an option to function in the islanded model can greatly enhance the resilience based on the evaluation by four proposed resilience-quantifying metrics. Li et al. [116] present an illuminating framework for forming networked microgrid clusters to improve resilience against extreme events, which points out that a bulk power system or a smart city can achieve better performance through the deployment of networked microgrids.

4) Smart grid technology

The above planning and architecture design approaches are mainly focused on improving system resilience from the physical side. Considering the complex cyber-physical coupling characteristic of a CPPS, the resilience-oriented CPPS design can exploit the potential of an advanced

smart grid ICT on the cyber side for resilience enhancement. Ren et al. [117] establish a software-defined networking (SDN)-enabled microgrid. Due to the flexibility and controllability of this programmable SDN, faster failover and reconfiguration switching in SDN networks can be achieved under cyber contingencies. Real-time situational awareness of the physical system is a strong basis for operators to deal with extreme events. To battle the extreme events for a CPPS, among this ICT for smart grids, advanced metering infrastructure (AMI) and phasor measurement units (PMUs) can bring the ability of real-time situational awareness of power grids and power outage alerts [118]. In addition, due to the uncertainty of extreme natural disasters, it is not practical to excessively design strategies for various scenarios. When cascading failures occur, microgrids can provide localized support for loads, so it is critical to design a resilient and self-organized communication architecture for microgrids. In Ref. [119], an ad hoc self-organized communication framework is proposed for disaster response based on PLC media, which can support microgrid formation and topology identification on the cyber side.

### 5.1.3. Resilience-oriented operation

In the face of natural disasters, as shown in Fig. 8, the dynamics of a CPPS against a disturbance can be divided into three phases: 1) prevention; 2) mitigation; and 3) restoration. The operation strategies of a CPPS include day-ahead scheduling and recovery after disasters. Thus, according to the dynamics of CPPSs and the three phases of extreme events, the resilience-oriented operation strategies are reviewed in the following three aspects:

- Preventative scheduling: before events;
- Corrective actions: during events;
- Restoration strategies: after events.

Based on the above three aspects, the state-of-the-art operational techniques for CPPSs are organized in Table 4 and are discussed as follows.

1) Preventative scheduling: before events

Ahead of an extreme hazard, it is critical to accurately predict the impact of the hazard on a CPPS in advance, which provides a basis for the formulation of subsequent strategies. Nateghi et al. [120] propose a statistical model for incoming hurricanes and the corresponding impact on power outage durations, which are verified by several historical hurricanes. As mentioned before, an ice storm can directly strike a CPPS from the interdependent facilities and topologies level, and it is one of the disasters most likely to induce cascading failures of the CPPS. For incoming ice storms, Yan and Shahidehpour et al. [121] propose a two-stage optimization strategy with day-ahead and real-time power system dispatch. This strategy also integrates mobile de-icing device pre-positioning and real-time routing, which can be robust to the uncertainty of ice thickness. As mentioned in Ref. [111] regarding planning techniques, resilience-oriented planning for integrated energy systems can provide more flexibility for the entire system, thereby improving the performance against disasters. From an operation perspective, Yan and Shahidehpour et al. [122] also provide a resilience-oriented strategy by coordinating regional gas networks and the power grid for an integrated energy system in an energy hub form.

As for a CPPS facing an imminent disaster, optimally scheduling the

**Table 4**
Resilience-oriented operation techniques for CPPSs.

| Taxonomy | Application to | Resilience against | Method/Technique | Targeting on | | Year | Ref. |
|---|---|---|---|---|---|---|---|
| | | | | Physical side | Cyber side | | |
| **Preventative scheduling: before events** | Transmission system/ Distribution system | Extreme weather: hurricanes | Forecasting statistical model for power outages | ✓ | | 2014 | [120] |
| | Transmission system | Ice storms | Day-ahead and real-time power system dispatch integrating mobile de-icing device scheduling | ✓ | | 2019 | [121] |
| | Multi-energy system | Transmission line congestion | Two-stage robust preventative dispatch integrating gas and heating network | ✓ | | 2019 | [122] |
| | Transmission system | Cyber-physical failures | Redundant communication paths for building wide-area control resiliency | ✓ | ✓ | 2014 | [123] |
| | Transmission system | Cyber-physical coupling failures and uncertainties | Two-level robust optimization for routing of remedial control services considering cyber-physical interdependence | ✓ | ✓ | 2019 | [124] |
| | Transmission system | Cyber-physical failures | Prediction for cyber-physical risk area using Markov Chain and heuristic algorithm | ✓ | ✓ | 2020 | [125] |
| **Corrective actions: during events** | Transmission system | Natural disasters | Integrated resilience response framework with preventative dispatch and emergency load shedding | ✓ | | 2017 | [126] |
| | Transmission system | Extreme weather events | Sequential MDP-based generation redispatch | ✓ | | 2017 | [127] |
| | Distribution system | Extreme weather events | MDP state-based actions of on/off feeder lines | ✓ | | 2020 | [128] |
| | Distribution system/ Microgrid | Disasters | Dynamic self-healing microgrid formation during events | ✓ | | 2014, 2015 | [129], [131] |
| **Restoration strategies: after events** | Transmission system | Blackout caused by natural disasters | Black Start resource allocation for restoration | ✓ | | 2016, 2018 | [132], [133] |
| | Distribution system/ Microgrid | Natural disasters | Co-optimization of repair crew, mobile power resource, and microgrid formation for restoration | ✓ | | 2019, 2020, 2020 | [134], [135], [136] |
| | Distribution system/ Microgrid | Natural disasters | Multiagent coordination scheme -based microgrid formation for restoration | ✓ | ✓ | 2016 | [137] |
| | Distribution system/ Microgrid | Natural disasters | Radiality constraints on reconfiguration of distribution system and microgrid formation | ✓ | | 2020, 2020 | [138], [139] |
| | Distribution system/ Microgrid | Extreme weather events | Collaborative recovery strategy for both cyber and physical components | ✓ | ✓ | 2018 | [140] |
| | Distribution system/ Microgrid | Emergency conditions | Outage management system with switching strategies for both scheduled and unscheduled outages | ✓ | ✓ | 2018 | [142] |
| | Transmission system | Natural disasters | Rerouting recovery mechanism for survivability of communication network | | ✓ | 2020 | [143] |

physical power flow is not enough to compensate for the vulnerability of the cyber network. Zhang and Vittal [123] design redundant communication paths for providing more reliable damping control signals against system oscillations on the physical side and communication failures on the cyber side. To deal with potential cyber-physical coupling failures caused by natural disasters, Xu and Guo et al. [124] define an importance assessment approach for information flow based on cyber-physical sensitivity and propose a two-level robust optimization strategy for scheduling the main-alternative routings of remedial control services considering renewable generation fluctuation, which can give priority to ensuring the accessibility of critical information flows. Qu et al. [125] propose a prediction approach for cyber-physical risk areas based on the dependent Markov Chain and a heuristic algorithm against potential natural hazards.

Huang et al. [126] construct a prevention and real-time collaboration emergency strategy against natural disasters based on a three-level robust optimization model. In the preventative phase, the proposed response strategy not only considers the optimal scheduling of generators for resilience but also combines the topology switching of the out-of-services lines as an alternative.

2) Corrective actions: during events

The ability to rapidly respond to failures, especially cascading failures, determines the affected range of a CPPS. As previously stated, Huang et al. [126] provide an emergency response optimization strategy in the proposed integrated resilience response framework. Load shedding as an emergency response is taken into account in the subproblem of the two-stage robust optimization against the worst-case disaster scenario. Considering that the decision-making based on the current state affects both the current state and future states, Wang et al. [127] propose a proactive operation strategy for transmission systems that redispatches active power generation during natural hazards based on a Markov decision process (MDP) and a recursive model. Following this approach, Wang et al. [128] further develop a resilience enhancement strategy by modeling the on/off states of feeder lines as Markov states for the distribution system.

When cascading failures caused by catastrophic events cannot be contained, it is critical to ensure the electricity supply in other regions with temporary safety, such as by using dynamic microgrid formation strategies [129]. For this reason, Simonov [130] builds a dynamic partitioning of the distribution network into microgrids based on an event-driven approach, which can support the non-interruption of loads. In this field, Patsakis et al. [131] design a self-healing distribution system by sectioning the distribution system into multiple microgrids.

3) Restoration strategies: after events

A resilient system requires not only the ability to withstand extreme conditions but also the ability to recover quickly after disasters. Qiu et al. [132] propose a black start resource allocation optimization model for blackout restoration to minimize the total procurement cost within a tolerable recovery time for transmission systems. Patsakis et al. [133] further introduce a black start allocation optimization with consideration of the steps of the restoration sequence.

Repair crews and mobile power resources (MPSs) play an important role in the restoration of the distribution system after a natural disaster. Lei et al. [134] propose resilience-oriented co-optimization logistics with repair crew routing and mobile power resources dispatch for the power outage management of distribution systems, which can guide the microgrid formation in an emergency state. Combining a soft-open-point (SOP) technology, Ding et al. [135] provide a multiperiod restoration strategy with SOP-based microgrid reconfiguration, MPSs, and repair crew scheduling. Focusing on the seismic-resilient enhancement, Yang et al. [136] develop an MPS optimal scheduling strategy combined with dynamic network reconfiguration of distribution systems.

To pick up the critical load after natural disasters, Chen et al. [137] design a microgrid formation strategy with a multiagent coordination scheme to obtain global information using only local communications so that the formed microgrids can help the restoration of larger systems. To deal with radiality constraints for maintaining radial topology in reconfiguration problems of distribution systems, resilient reconfiguration for distribution systems after natural disasters is developed by Wang et al. [138] and Lei et al. [139], where the microgrid formation is also considered to enhance the flexibility for the reconfiguration. Considering the cyber-physical interdependence and cyber-physical coupling failures, Li and Shahidehpour et al. [140] propose a collaborative recovery strategy for both cyber and physical components in the distribution system of a CPPS, which mainly considers the remote terminal units and distribution control center constructing multiple cyber subsystems.

Tang and Ten et al. [141] provide a switching reconfiguration scheme to detect energy fraud in distribution systems embedded with AMI, which can improve the resilience of such systems with AMI under energy fraud. Further, Ten and Tang [142] systematically introduce an outage management system coordinating crew scheduling, switching steps, and a trouble call system for distribution networks, and they design practical switching strategies to improve system resilience against both scheduled and unscheduled outages. This work also introduces the distribution network communication architecture thoroughly, which is instructive for guiding the cyber-physical network configuration.

Survivability under extremely adverse conditions is a critical ability of a resilient communication network and has received wide attention in the ICT field. For critical services of a CPPS, when communication failures coupled with power outages occur, the availability of the routing of these real-time services should be guaranteed as much as possible by rapidly and automatically switching to alternate routing. Among various ICTs, self-healing rings in SDH and the automatically switched optical network technique in OTN can guarantee fast recovery from a single failure. Focusing on the fast recovery of control services, Liu et al. [143] propose a survivability-aware routing restoration strategy for the communication network of a CPPS under large communication failures caused by natural disasters.

#### 5.1.4. Discussion

From the above resilience assessment metrics and resilience-oriented planning and operation techniques, these cutting-edge studies use various resources of the CPPS from multiple aspects or introduce new architectures to enhance the system's resilience against natural disasters. However, from Tables 3 and 4, we can find that these studies mainly focus on one side of a CPPS (e.g., physical resilience-oriented transmission expansion planning on the physical side). Although the study by Liu et al. [113] is one of the few cyber-physical co-planning methods considering cyber failures, the resilience of the entire CPPS is not fully considered in the constraints of the planning model, especially regarding the impact of natural hazards. There are still many opportunities to improve the overall performance of the resilience of a CPPS. For example, the consistency of the topologies of the communication network and the power grid is a critical issue to be considered in the future planning of CPPSs. Moreover, the existing methods of using integrated energy systems to improve the flexibility and resilience of power systems have the potential to expand to cyber-physical multi--energy systems.

### 5.2. Attack-resilient techniques

With the deeper coupling of CPPSs and the growth of the multiagent trend, CPPSs will face more cyber threats in the future. In Section 3.3, we analyze the most advanced cyberattacks challenging the resilience of CPPSs from integrity and availability aspects in "CI&A". For the resilience of CPPSs against cyberattacks, the existing state-of-the-art

techniques target the following three critical issues:

- Prevention of cyberattacks from affecting CPPSs;
- Detection of stealthy cyberattacks that avoid prevention mechanisms or come from inside;
- Mitigation of the impact of cyberattacks on CPPSs.

The existing attack-resilient techniques, summarized in Table 5, are reviewed based on the above three issues. To be more explicit, the framework of the attack-resilient techniques of CPPSs is shown in Fig. 9.

*5.2.1. Prevention techniques*

The prevention techniques are particularly important as the first line of defense for CPPSs facing cyber threats. A well-designed prevention communication system or mechanism can fundamentally defend against most cyberattacks. For the security of the ICS, Genge et al. [144] propose an integer linear programming (ILP)-based approach that satisfies the state-of-the-art requirements of security zone sectionalizing and security conduit construction combined with a cyberattack impact assessment approach. The proposed method mainly focuses on cyberattacks against data integrity, such as crafted commands designed to remotely switch off breakers in power systems. Based on the SCADA communication network, Chalamasetty et al. [145] develop an improved architecture embedded with a trust-based prevention approach against DoS attacks. Aiming at the security issue of the smart distribution system based on the wireless meshed network, Wang et al. [146] design a smart tracking firewall for multiple cyberattacks against data availability, for example, dropping packets and disabling routings.

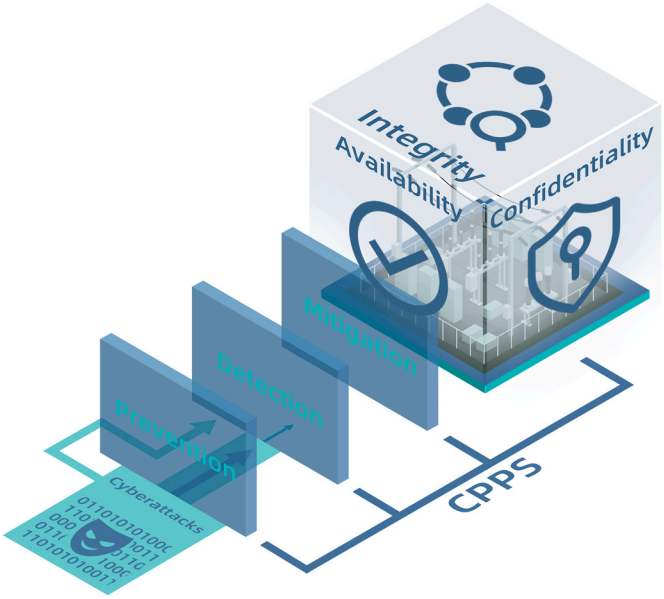


**Fig. 9.** The framework of the attack-resilient techniques of CPPSs.

In order to prevent cybercrime, such as ransomware targeting IoT-based CPPSs, well-developed crime prevention through environmental design (CPTED) is used by Joo et al. [147] combined with a factor

**Table 5**
Attack-resilient techniques for CPPSs.

| Taxonomy | Attack | Target | Method/Technique | Year | Ref. |
|---|---|---|---|---|---|
| **Prevention** | Attack against data integrity | ICS network | ILP optimization considering requirements of security zone sectionalizing and security conduits | 2017 | [144] |
| | DoS | SCADA system | Trust-based intrusion detection and prevention technology | 2016 | [145] |
| | Packet-related security attacks | Wireless smart distribution system | Smart tracking firewall | 2011 | [146] |
| | Cybercrime such as ransomware | IoT-based CPPS | Factor analysis of information risk model combined with CPTED | 2018 | [147] |
| | Malware and multiple cyberattack | SCADA/EMS | Firewall for separation of SCADA; PKI for all RIG-based devices | 2014 | [148] |
| | Attack targeting confidentiality | Smart meter data | Discounted differential privacy model for data-desensitization | 2021 | [149] |
| | | AMI networks | Homomorphic encryption | 2017 | [150] |
| | | Cloud-based EMS | Information masking without affecting the original optimal decisions | 2018 | [151] |
| **Detection** | FDIA | AC state estimation | KL distance-based detection for dynamics of measurement variations | 2015 | [152] |
| | | Cyber-physical DC microgrids | Detection by identifying variations in the set of estimated invariants | 2017 | [153] |
| | | WAMS | Bayesian-based approximated filter | 2016 | [154] |
| | | Electricity market | CLL-based detection of abnormal LMPs | 2020 | [155] |
| | RA/noise injection attack | AGC | Online detection method based on dynamic watermarking | 2018 | [156] |
| | Distributed stealthy data integrity attack | Distributed economic dispatch | Observation graph to estimate lower and upper bound of next step | 2018 | [157] |
| | DoS/DDoS | SCADA system | Model-free reinforcement learning for online detection | 2019 | [158] |
| | | 5G-enabled smart grid | Combining deep CNNs with real network data | 2020 | [159] |
| | Data availability attack | Microgrid | SDN embedded with intrusion detection systems | 2017 | [160] |
| | Bot attack | Microgrid | Host tracking in SDN | 2019 | [161] |
| **Mitigation** | FDIA | WAMS | Self-healing mechanism based on ILP model to minimize cost | 2018 | [162] |
| | | State estimation | Combining data-driven auxiliary model with compressive sensing regression | 2020 | [163] |
| | | DC/DC converter | Artificial neural networks to generate reference signals for outputs of controllers | 2020 | [164] |
| | Stealthy actuation attack | Distribution network | Adaptive attacker-defender model by deploying local reserved power injection resources | 2020 | [165] |
| | Distributed stealthy data integrity attack | Consensus-based economic distributed dispatch | Reputation-based neighborhood-watch mechanism | 2019 | [166] |
| | | Distributed DC-OPF | Use the estimated information to continue iteration | 2018 | [167] |
| | | VPP economic dispatch | Isolation of misbehaving DGs exceeds the estimated range | 2018 | [168] |
| | DoS/DDoS | LFC | Resilient event-triggering communication scheme | 2017 | [169] |
| | | LFC | Adaptive resilient event-triggering LFC | 2020 | [170] |
| | | Multiagent distribution network | Distributed confidence level manager | 2016 | [171] |
| | Time delay attack | LFC in distributed system | Time delay estimator with a buffer storing historical commands and an optimal controller | 2016 | [172] |
| | | PTP | Modified PTP with the designed guard clock | 2018 | [173] |
| | Coordinated cyber-physical attacks | Generation units, substations and SCADA systems | Bilevel NTO | 2020 | [174] |

analysis of information risk model for situational awareness of the environment of CPPSs, with which it is possible to reduce the risk of such cyberattacks. Isolating critical real-time control services can significantly reduce the losses caused by cyberattacks. California ISO (CAISO) [148] develops a dedicated communication network with high reliability called the Energy Communication Network (ECN). Both the logic and physical separation of SCADA devices from WAN/LAN are provided by a designed firewall. In addition, a public key infrastructure (PKI) for all remote intelligent gateway (RIG)-based devices in AGC can ensure secure communication by providing strong authentication.

As mentioned in Section 4.2, cyberattacks targeting confidentiality can also impair the resilience of a CPPS obliquely. Therefore, prevention techniques against confidentiality-oriented attacks are important for a resilient CPPS. Chhachhi and Teng [149] design a framework to evaluate the value of sharing privacy-protected smart meter data based on a discounted differential privacy model for data-desensitization, which can protect the data transaction privacy between consumers and producers in smart grids. To protect private information of smart metering data in AMI networks, Saxena et al. [150] provide a privacy-preserving scheme based on homomorphic encryption that can aggregate metering data without revealing real power system information. Xin et al. [151] design an information masking scheme for future cloud-based building EMS, virtual power plants management and multi-region coordinated dispatch, which can obscure private information without affecting the original optimal decisions.

#### 5.2.2. Detection techniques

Although there are some studies on practical applications of prevention techniques against cyberattacks, such as firewalls or information system separation, the detection of cyberattacks launched in a stealthy way or even implemented by internal operators remains a critical issue. For example, FDIA is proven to be injected in the form of a stealthy attack to evade the residue test for bad data detection in state estimation. Since integrity and availability are highly related to the resilience of CPPSs, cyberattack detection techniques center around integrity and availability.

1) Integrity

Aiming at the drawback of the residue test in AC state estimation, Chaojun et al. [152] develop a Kullback-Leibler distance -based detection mechanism for tracking the dynamics of measurement variations. Based on the Kullback-Leibler distance, the variation of probability distributions of measurement data caused by FDIA can be effectively captured. Due to the embedded power electronic controllers, the coupling at the facility level also causes CPSSs to face cyber threats. For the security of cyber-physical DC microgrids, a novel FDIA detection method that works by identifying variations in the set of estimated invariants is proposed by Beg et al. [153], where Simulink/Stateflow diagrams are designed to generate the candidate invariants in cyber-physical microgrids. To enhance the resilience of WAMS against cyberattacks, Khalid and Peng [154] design a Bayesian-based approximation filter in a distributed architecture, which can accurately extract the oscillatory parameters in manipulated PMU measurement data. Since LMPs in electricity markets are obtained based on the state estimation results, Zhang and Li et al. [155] propose a critical load level (CLL)-based detection of the abnormal LMPs. The developed risky CCL interval can detect LMP variation to determine a risky period for market-level defense analysis of operators.

Targeting replay attack (RA) and noise-injection attack against AGC systems, Huang et al. [156] propose an online detection framework based on dynamic watermarking techniques. As an active detection strategy, the dynamic watermarking techniques superimpose random independent detection signals on the controllers according to certain probability distributions and can reveal malicious tampering by tracing the significant deviation of the corresponding probability distribution around the control loop.

As mentioned in Section 4.3, multi-agent CPPSs are more susceptible to cyber threats, especially stealthy attacks against specific distributed algorithms. For consensus-based distributed economic dispatch, Zhang et al. [157] propose a stealthy attack detection strategy based on a defined observation graph where any agent can estimate the upper and lower bound to the next step of the iteration.

2) Availability

Kurt et al. [158] propose model-free reinforcement learning (RL) for the online detection of DoS attacks on meter measurements. The model-free method can overcome the drawback of the well-known cumulative sum test for its high requirement of an accurate model of the system and potential attack strategies. Under the background of the fast development of 5G technology, Hussain et al. [159] develop a DDoS detection strategy with tested 91% detection accuracy based on deep convolutional neural networks (CNNs) for 5G-enabled smart grids.

Toward the cybersecurity of microgrids, Jin et al. [160] design SDN-based microgrids. The SDN offers microgrids global visibility of data and supports the deployment of cost-effective intrusion detection systems at different locations based on its programmability. Li et al. [161] design a host status checker embedded in an SDN controller. The active synchronous detection in the proposed checker is verified to be a safeguard to microgrids against bot attacks.

#### 5.2.3. Mitigation techniques

Like restoration after power outages caused by natural disasters, mitigation of the impact of cyberattacks is an important ability of a resilient CPPS. Corresponding to the detection techniques, the mitigation techniques are also organized from the aspects of integrity and availability.

1) Integrity

To mitigate the FDIA attack on PMU/WAMS, Lin et al. [162] design a self-healing PMU network by accurately identifying the compromised PMU and reconnecting other normal PMUs to achieve self-healing and restore observability. An ILP model considering the self-healing mechanism is also developed to minimize the cost of the self-healing process. For improving the resilience of state estimation against FDIA, Anubi et al. [163] design a Gaussian process regression-based estimator combined with a data-driven auxiliary model. By taking the LMPs as the secondary information for the data-driven model, the resilience of the tested system against adversary attack can be remarkably enhanced. Furthermore, for the security of DC converters in microgrids, Habibi et al. [164] design a PI controller embedded with artificial neural networks to generate reference signals for the outputs of the controller. Srikantha et al. [165] introduce a type of stealthy actuation attack against distribution networks based on Stackelberg games, which can result in widespread disruptions by cumulatively violating the operational limitations such as triggering protection. Subsequently, an attack-resilient operation strategy is introduced by deploying local reserved power injection resources and actuating according to an optimal countermeasure problem.

To improve the resilience of multiagent CPPSs under distributed stealthy data integrity attacks, Duan et al. [166] present a neighborhood-watch mechanism for consensus-based economic distributed dispatch. The mechanism first verifies the correctness of the neighbors' information within two hops by the estimated upper and lower bound, then identifies the manipulated agents by updating reputation functions, and finally maintains the estimated information instead of the information from the manipulated agents. For the optimal power flow (OPF) problem in multiagent CPPSs, Duan et al. [167] also provide a distributed DC OPF algorithm targeted against distributed data integrity attacks by using estimated information to recover from

malicious effects. Since multiagent systems are more susceptible to cyberattacks, Li et al. [168] propose an attack-resilient distributed economic dispatch scheme for DGs aggregated into virtual power plants (VPP), which can isolate misbehaving DGs by estimating feasible ranges according to the property of the consensus algorithm and storing the latest connectivity information. It is noteworthy that due to the plug-and-play characteristic of the distributed scheme, accurately isolating the misbehaving agents can still converge to a consensus point.

2) Availability

For LFC to reduce the impact of DoS attacks with energy limitations, Peng et al. [169] design a resilient event-triggering communication scheme, which considers both DoS attacks and communication efficiency. Their work proposes a strategy to reduce the number of transmitted packets while ensuring the desired LFC performance, where the event-triggered condition depends on a threshold parameter. Furthermore, Lu et al. [170] propose a resilient LFC with an adaptive threshold parameter for the event-triggered condition, which shows better performance in communication resource saving while defending against DoS attacks. Moreover, Liu et al. [171] propose a cooperative control strategy for multiagent distribution networks with multiple DGs by designing a distributed confidence level manager that can cope with DoS attacks and communication failures. The strategy is also based on a consensus algorithm; when packet loss occurs, the corresponding neighbor's weight coefficient of an agent will be set as zero so that the iteration of this agent will not be affected and convergence can be achieved.

For time delay attacks on LFC in distribution systems, Sargolzaei et al. [172] propose a delay-resilient LFC method, which is adaptive to variable time delays and can successfully track the injected delay attack through an estimator with a buffer to store the historical commands and an optimal controller tracking a reference signal. The proposed method shows resilience to the latency in the observed state of LFC. Since precision time protocol (PTP) is a critical protocol for the time synchronization of a smart grid and proves to be vulnerable to time delay attacks, Moussa et al. [173] provide a detection and mitigation technique for PTP delay attacks in IEC 61850-based substations. The technique modifies the part of the PTP functionality to respond to the warning signal generated by the designed guard clock.

As mentioned before, cyber-physical coupling failures are extremely harmful to CPPSs and result in many widespread blackouts. Cyber-physical coordinated attacks also pose a great challenge to the security of CPPSs. For example, transmission facilities can be destroyed by a physical attack, and simultaneously a cyberattack may invade the SCADA systems of substations to disconnect the generators. To mitigate the impact of such cyber-physical attacks, Liu et al. [174] develop a bilevel network topology optimization (NTO) model for restoration after attacks. The NTO-based strategy reconfigures the system through transmission-switching and bus-splitting actions to minimize the total load shedding, which shows better performance compared with the conventional OPF and optimal transmission-switching strategy.

#### 5.2.4. Discussion

Cyberattack resilience research is accompanied by the interactive improvement of strategies for attacking and defending. Although Zhang and Li et al. [155] provide an efficient method for detecting abnormal LMPs, they also present a new stealthy FDIA against LMPs in real-time markets without a prevention method. In addition, data-driven methods and AI techniques are gradually being adopted in the detection and mitigation stages against cyberattacks with better adaptability and detection accuracy. A combination of model-driven and data-driven techniques for prevention, detection, and mitigation has the potential to adapt to different attacks with higher precision and thereby enhance the resilience of CPPSs against cyber threats in the future open network environment. Furthermore, cyberattack-resilient CPPSs should be based on composite techniques against cyberattacks targeting integrity, availability, and confidentiality. It is also noteworthy that cyber-physical coordinated attacks should be paid more attention in the future due to the catastrophic consequences they may cause. In response to such attacks, cyber-physical collaborative defense and restoration strategies remain to be further developed.

### 5.3. Cyber-physical-social perspective

In order to deal with the consequences of dispatchers' mistakes, a series of intelligent scheduling technologies, such as parallel scheduling of robots based on artificial societies and computational experiments [175], have been studied in recent years. The goal of these technologies is to learn a dispatcher's experience and knowledge using artificial intelligence so as to improve the reliability of the scheduling process [176]. However, this paper focuses on the effect of collective decision-making on the resilience of the social system. Human participation not only brings challenges to power system resilience but also brings more flexibility in resilience enhancement. The social system can assist in the operation of the cyber system and provide more information for a CPPS, and it can also provide the physical system with more flexibility from the demand-side through consumer demand response under certain incentive signals, as shown in Fig. 10. Thus, according to the targeting system, the human-in-the-loop resilience enhancement strategies are reviewed in the following two aspects:

- Their influence on the cyber system;
- Their influence on the physical system.

The state-of-the-art resilience enhancement techniques are summarized in Table 6 and discussed as follows.

#### 5.3.1. From social side to cyber side

As mentioned above, the integration of numerous sensors in a CPPS can monitor the power grid, with the intention being to raise the reliability of the network. However, the solution can be very costly and sensitive to cyber-physical attacks, thus increasing reliability and resiliency issues. Social media may present a solution to this problem as it is becoming more and more widely adopted. The data embedded within social media feeds include keywords, hashtags, geo-tag, time-tag, content, and sentiment. With the help of data-driven approaches, social

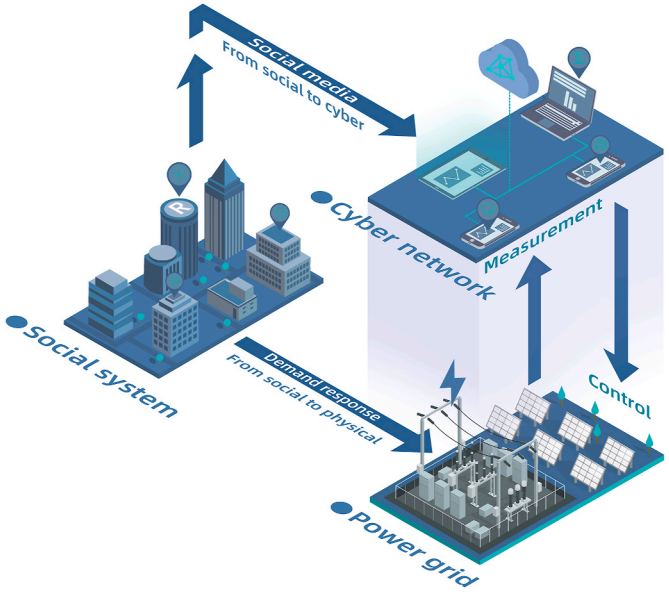


**Fig. 10.** The framework of the human-in-the-loop resilience enhancement strategies.

**Table 6**
Human-in-the-loop resilience enhancement in CPPSs.

| Taxonomy | Application | Against | Method/Technique | Human model | Targeting on | | Year | Ref. |
|---|---|---|---|---|---|---|---|---|
| | | | | | Physical side | Cyber side | | |
| **Temporal demand response** | Distribution system | Extreme weather | Real-time pricing framework based on program termed weather condition | Price elasticity | ✓ | | 2019 | [191] |
| | Distribution system | Natural disasters | Using parking lots and residential parking as distributed energy resources to restore critical loads | Demand-side management program | ✓ | | 2019 | [194] |
| **Spatial demand response** | Coupled power-traffic system | FCS fault | Reallocating the charging load through price adjustment incentives. | User equilibrium | ✓ | | 2020 | [89] |
| | Coupled power-traffic system | Local incidents | Pricing incentives in charging and taxi services | Discrete choice model | ✓ | | 2020 | [200] |
| **Social media** | Power system | Power outages | Utilizing information to plan and implement resources towards power grid resiliency | Social media | | ✓ | 2020 | [177] |
| | Power system | Hurricanes | Using social data source to model critical infrastructure behaviors | Publicly available social media | | ✓ | 2019 | [181] |

media could be utilized as social sensors, which have the potential to supplement existing data sources [177].

Exploiting this social data source may save the expense of physical sensors by serving as backup sensing and providing cross-validation for other data sources. In recent years, the applications of social media in various fields, such as power outage detection have been widely discussed [178]. Textual, temporal, and spatial information from social media are integrated to identify the event based on various predictive models, preprocessing techniques, and feature extraction methods [179,180]. Furthermore, social media can be regarded as a single data source from which knowledge about multiple infrastructures may be extracted to improve power grid resiliency from micro-level consumers to macro-level cities. The reliability of social sensors is based on two major aspects: the reliability of social sensors and the reliability of telecommunication networks. The steps of social media utilization include information extraction (location & problem), planning, and response actions [181].

From the perspective of response speed, social media has been shown to provide valuable help in vehicle navigation by making route recommendations based on images uploaded by users related to such occurrences as traffic congestion, floods, and fire disasters. From the perspective of component importance, utility companies can preferentially offer immediate relief to social hotspots and dispatch their rescue teams and emergency resources considering the impact level of each area.

Despite the above benefits, the challenge of applying social media lies in its trustworthiness due to its data fragmentation, noise, and the possibility of false information. For instance, in June 2020, false claims about a communication blackout in Washington, D.C., were widely spread across Twitter. The "dcblackout" hashtag was first tweeted by an account that had three followers and then tweeted 500,000 times within 9 h of the initial post. In response, Twitter suspended hundreds of accounts associated with spreading this false claim [182].

Fortunately, the multi-source and massive community nature of social media data provides cross validation opportunities, which solves the above problems to some extent. Moturu and Liu [183] propose a framework to quantify the trustworthiness of health content in social media based on a two-step unsupervised, feature-driven approach. The proposed method has the potential to be applied to study the trustworthiness of electricity-related content in social media. Several other solutions are proposed in existing works toward truth discovery, i.e., ascertaining the correctness and reliability of social data sources. Diversified dimensions of social media data are exploited to achieve this goal, including claim hardness [184], personal sentiments [185], topic relevance [186], and attitude degree difference [187]. However, such works mainly lie in the general field of computer science, while how to identify trustworthy information when combining the data from cyber sensors and social sensors in CPPS is still a topic worthy of further exploration.

#### 5.3.2. *From social side to physical side*

As a typical technology of the smart grid, demand response is an effective measure to regulate the energy consumption behavior of customers through pricing or other incentives. With proper utilization, the flexibility from the social potential of customers could be exploited as a good supplement to the conventional resilience enhancement measures for critical conditions [188], e.g., extreme weather.

The demand response can be further divided into temporal and spatial responses. In the temporal demand response category, the deployment of demand-side management is utilized in network congestion management [189] and generation capacity adequacy [190], which presents the potential of resilience enhancement under extreme weather conditions. A demand-side management real-time pricing framework based on weather conditions is proposed by Li et al. [191] to adjust the energy consumption of users. The self-adaptive mechanism can generate demand-side management prices according to weather conditions, effectively tapping the potential of customer response characteristics. With more in-depth coupling between the power system and heating system, the power consumption of thermostatically controlled loads (TCLs) can be adjusted to a certain extent without affecting end-user comfort [192], which provides the attractive capacity in system restoration. Furthermore, TCLs offer energy storage and can be utilized in the form of batteries to enhance system resilience [193]. With the rapid growth of EVs, the aggregation of large numbers of EVs shows great capability of bidirectional power transfer, which can support critical load restoration in power distribution networks. EV parking lots are regarded as distributed energy resources in Ref. [194], where the demand response program is implemented.

Among spatial demand response resources, EVs can be regarded as transportable energy storage systems or mobile power sources [195]. Currently, transportable energy storage systems are utilized to enhance distribution system resilience. For example, the distribution system might form several islands after disasters, and mobile battery-toting vehicles could be dispatched quickly to supply critical loads [30]. Several studies [196–198] mainly focus on an integrated service restoration strategy to minimize the total system cost via the coordinated dispatching of repair crews, transportable energy storage fleets, microgrid resource, and distribution network reconfiguration. As traffic congestion may occur after natural disasters, the consideration of other travelers' responses behind the dynamic traffic state is necessary for the optimal dispatch (routing and charging) of mobile EVs for restoration [198,199]. With a higher penetration of EVs, the restoration service might be provided by more social vehicles instead of repair crews. Even if ordinary vehicles do not directly participate in the restoration process, the reasonable guidance of charging load redistribution in an emergency scenario can effectively reduce the system pressure. To solve the

potential threat from charging load redistribution due to FCS outage, Sheng et al. [89] propose a price-based preventative regulation method based on spatial demand elasticity to reallocate the charging load through price adjustment incentives. The regulation measure is implemented after the occurrence of regional FCS outage to prevent future overloading, which works as an auxiliary measure to generation adjustment. Furthermore, aiming at EV taxi fleets, a human-centric dynamic pricing scheme that broadcasts pricing incentives in charging and taxi services is proposed by Yang et al. [200] to improve the system performance by incentivizing human drivers and passengers to follow expected behavioral patterns. When an incident occurs in one area, the service demand and electricity baseload increase while the road capacity decreases, so dynamic pricing can help reduce operational pressure to meet the service demand in the transportation network and energy demand in the power network.

#### 5.3.3. Discussion

Cutting-edge studies have been conducted to study the utilization of human-in-the-loop potential in resilience enhancement. The social system can be regarded as a potential supplement to the cyber system, providing multi-source information for CPPSs. Furthermore, energy consumption behavior can be guided to regulate the temporal and spatial load distribution, which relieves the physical system operation pressure from the demand side. For future works, a comprehensive resilience enhancement framework that combines the CPPS model with human behavior will be an important research topic. The main challenge that remains is understanding the complex social behavior of massive human energy consumers. Some relevant questions are as follows: How can credible information be identified from the data of mass social sensors? How will personality characteristics and incentive forms influence consumer behaviors? How can human consumers participate in resilience improvement programs after disasters? The individual limited rationality and uncertainty of human perception, evaluation, and decision making need to be considered, which is difficult to express explicitly by mathematical models. Fortunately, based on the ubiquitous sensor network technology and data science technology, a large amount of historical behavior data about human consumers can be accumulated. On this basis, the "data enabling" method can be used to discover the statistical characteristics behind complex social behaviors and provide support for comprehensive optimization in system resilience.

## 6. Conclusion

The superposition of the vulnerability of cyber and physical spaces brings new challenge to the resilience of modern power systems such as CPPSs. By reviewing recent blackouts from a cyber-physical perspective, this study finds that cyber malfunctions coupled with physical incidents are the main cause of these widespread incidents due to the strong interdependence of CPPSs. To better study the resilience of CPPSs with such interdependence, this study presents a general system theory-based framework and three key features of hierarchy, self-organization, and vulnerability and resilience, where the difference between CPPS resilience and traditional power system resilience is also highlighted. On this basis, it reveals the bottom-up three-layer interdependences from facilities (e.g., inverter-based DGs), topologies (e.g., transmission lines and OPGWs), and functions (e.g., information-energy flow of the EMS).

To account for the complicated external environments of CPPSs, the three main categories of disturbances and security threats that challenge the resilience of CPPSs, including natural hazards, cyberattacks, and human behaviors, are also analyzed based on the framework and interdependences. Subsequently, literature proposing state-of-the-art resilience-oriented techniques to respond to these disturbances is thoroughly discussed in terms of different time scales and different phases of CPPSs against such high-impact, low-probability events. Based on the findings of our review, we conclude with some follow-up opportunities for the resilience enhancement of CPPSs:

- In response to natural disasters, the planning of CPPSs, especially expansion planning, should fully consider the topology interdependence of communication networks and power grids to enhance the resilience of entire systems. For the operational level, cyber-physical collaborative optimal dispatch and flexible resource allocation are critical strategies for the resilience of CPPSs.
- For the interactive improvement of attack/defend strategies, combining model-driven and data-driven models and exploring a comprehensive attack-resilient strategy including prevention, detection, and mitigation will be urgently needed in the future open network environment. In addition, to defend against cyber-physical coordinated attacks, cyber-physical collaborative mechanisms remain to be further developed.
- Considering the human-in-the-loop in the CPPS, the impact of massive user perception and decision making on system resilience needs to be fully considered, and the potential of a social system in resilience enhancement can be further tapped. For cyber systems, multi-source information can be provided through the social network as a reference. For the physical system, more flexibility from the demand side can be provided through the guidance of user behavior.

## Credit author statement

**Luo Xu**: Conceptualization, Writing – original draft, Visualization. **Qinglai Guo**: Conceptualization, Writing – review & editing, Supervision, Funding acquisition. **Yujie Sheng**: Writing, Writing – review & editing, Visualization. **S. M. Muyeen**: Writing – review & editing. **Hongbin Sun**: Supervision, Writing, Writing – review & editing.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

This work was partly supported by the joint project of NSFC of China and EPSRC of UK (No. 52061635103 and EP/T021969/1). The authors would also like to thank Fujian Electric Power Company, State Grid Corporation of China for providing the report of the 2016 Xiamen blackout.

## References

[1] Fang X, Misra S, Xue G, Yang D. Smart grid-the new and improved power grid: a survey. IEEE Commun Surv Tutor 2012;14(4):944–80.
[2] Bertalanffy von L. General system theory. New York: George Braziller; 1956.
[3] Colombo AW, Karnouskos S, Kaynak O, Shi Y, Yin S. Industrial cyberphysical systems: a backbone of the fourth industrial revolution. IEEE Ind Electron Mag 2017;11(1):6–16.
[4] Gunes V, Peter S, Givargis T, Vahid F. A survey on concepts, applications, and challenges in cyber-physical systems. KSII Trans on Internet Inf Syst 2014;8(12):4242–68.
[5] Yu X, Xue Y. Smart grids: a cyber–physical systems perspective. Proc IEEE 2016;104(5):1058–70.
[6] Xu L, Guo Q, Wang Z, Sun H. Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis. IEEE Trans Smart Grid 2021. in press.
[7] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature 2010;464(7291):1025–8.
[8] Arghandeh R, von Meier A, Mehrmanesh L, Mili L. On the definition of cyber-physical resilience in power systems. Renew Sustain Energy Rev 2016;58:1060–9.
[9] Li Z, Shahidehpour M, Aminifar F. Cybersecurity in distributed power systems. Proc IEEE 2017;105(7):1367–88.
[10] NCCIC/ICS-CERT. Cyber-attack against Ukrainian critical infrastructure. 2018. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01. [Accessed 29 December 2020].
[11] Chin W-L, Li W, Chen H-H. Energy big data security threats in IoT-based smart grid communications. IEEE Commun Mag 2017;55(10):70–5.
[12] Jifeng W, Yinsheng S. Practice and experience in dispatching of southern power grid during rare ice disaster at beginning of year 2008. In: 2011 international

conference on electric utility deregulation and restructuring and power technologies (DRPT). IEEE; 2011. p. 1869–74.
[13] Wang Y, Chen C, Wang J, Baldick R. Research on resilience of power systems under natural disasters—a review. IEEE Trans Power Syst 2016;31(2):1604–13.
[14] Mishra DK, Ghadi MJ, Azizivahed A, Li L, Zhang J. A review on resilience studies in active distribution systems. Renew Sustain Energy Rev 2021;135:110201.
[15] Izadi M, Hosseinian SH, Dehghan S, Fakharian A, Amjady N. A critical review on definitions, indices, and uncertainty characterization in resiliency-oriented operation of power systems. Int Trans Electr Energy Syst 2021;31:12680.
[16] Wang Y, Rousis AO, Strbac G. On microgrids and resilience: a comprehensive review on modeling and operational strategies. Renew Sustain Energy Rev 2020;134:110313.
[17] Ashok A, Govindarasu M, Wang J. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. Proc IEEE 2017;105(7):1389–407.
[18] Deng R, Xiao G, Lu R, Liang H, Vasilakos AV. False data injection on state estimation in power systems—attacks, impacts, and defense: a survey. IEEE Trans Ind Inform 2017;13(2):411–23.
[19] Mo Y, Kim TH-J, Brancik K, Dickinson D, Lee H, Perrig A, et al. Cyber-physical security of a smart grid infrastructure. Proc IEEE 2012;100(1):195–209.
[20] U.S. Department of Energy. August 2003 blackout. https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/august-2003-blackout. [Accessed 29 December 2020].
[21] Cleveland F. Enhancing the reliability and security of the information infrastructure used to manage the power system. In: 2007 IEEE power and energy society general meeting (PESGM). IEEE; 2007. p. 1–8.
[22] Owens C. Biggest blackouts in history: Italy 2003. https://www.theblackoutreport.co.uk/2020/09/28/italy-blackout-2003/. [Accessed 3 December 2020].
[23] Rosato V, Issacharoff L, Tiriticco F, Meloni S, De Porcellinis S, Setola R. Modelling interdependent infrastructures using interacting dynamical models. Int J Crit Infrastruct 2008;4(1):63–79.
[24] Bompard E, Huang T, Wu Y, Cremenescu M. Classification and trend analysis of threats origins to the security of power systems. Int J Electr Power Energy Syst 2013;50:50–64.
[25] Qingqian C, Xianggen Y, Dahai Y, Hui H, Guangyi T, Bo W, et al. Review on blackout process in China southern area main power grid in 2008 snow disaster. In: 2009 IEEE power and energy society general meeting. IEEE; 2009. p. 1–8.
[26] E-ISAC, SANS. Analysis of the cyber attack on the Ukrainian power grid: defense use case. https://ics.sans.org/duc5. [Accessed 29 December 2020].
[27] Liang G, Weller SR, Zhao J, Luo F, Dong ZY. The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans Power Syst 2017;32(4):3317–8.
[28] McDonell S. Typhoon Meranti mop up continues in southern China. https://www.bbc.com/news/av/world-asia-37372785. [Accessed 26 December 2020].
[29] Xie L, Mo Y, Sinopoli B. Integrity data attacks in power market operations. IEEE Trans Smart Grid 2011;2(4):659–66.
[30] Chen J, Xian Q, Zhang P. Buckling analysis of transmission tower considering ice load. In: IOP conference series: materials science and engineering. IOP; 2019. p. 12036.
[31] Meadows DH. Thinking in systems: a primer. Vermont: Chelsea Green; 2008.
[32] Wei J, Kundur D, Zourntos T, Butler-Purry KL. A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control. IEEE Trans Smart Grid 2014;5(6):2687–700.
[33] Cheng Z, Duan J, Chow M-Y. To centralize or to distribute: that is the question: a comparison of advanced microgrid management systems. IEEE Ind Electron Mag 2018;12(1):6–24.
[34] Dressler F. Self-organization in sensor and actor networks. John Wiley & Sons; 2008.
[35] Wang R, Li Q, Zhang B, Wang L. Distributed consensus based algorithm for economic dispatch in a microgrid. IEEE Trans Smart Grid 2019;10(4):3630–40.
[36] Kundur P, Balu NJ, Lauby MG. Power system stability and control. seventh ed. New York: McGraw-hill; 1994.
[37] Clark A, Zonouz S. Cyber-physical resilience: definition and assessment metric. IEEE Trans Smart Grid 2019;10(2):1671–84.
[38] Jianfeng D, Jian Q, Jing W, Xuesong W. A vulnerability assessment method of cyber physical power system considering power-grid infrastructures failure. In: 2019 IEEE sustainable power and energy conference (iSPEC). IEEE; 2019. p. 1492–6.
[39] Song Y, Hill DJ, Liu T, Zheng Y. A distributed framework for stability evaluation and enhancement of inverter-based microgrids. IEEE Trans Smart Grid 2017;8(6):3020–34.
[40] Wang Y, Chen Q, Hong T, Kang C. Review of smart meter data analytics: applications, methodologies, and challenges. IEEE Trans Smart Grid 2019;10(3):3125–48.
[41] Saleh SAM, Richard C, Onge XFS, McDonald KM, Ozkop E, Chang L, et al. Solid-state transformers for distribution systems–part i: technology and construction. IEEE Trans Ind Appl 2019;55(5):4524–35.
[42] Ilić MD, Xie L, Khan UA, Moura JMF. Modeling of future cyber–physical energy systems for distributed sensing and control. IEEE Trans Syst Man Cybern - Part Syst Hum 2010;40(4):825–38.
[43] Qi J, Hahn A, Lu X, Wang J, Liu C. Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys Syst Theory Appl 2016;1(1):28–39.
[44] He X, Wang R, Wu J, Li W. Nature of power electronics and integration of power conversion with communication for talkative power. Nat Commun 2020;11(1):1–12.
[45] Soulliere MJ. Optical parameters for SONET and the synchronous digital hierarchy. In: IEEE SONET symposium. IEEE; 1989. p. 43–9.
[46] Serizawa Y, Kitamura K, Myoujin M, Shimizu K, Matsushima T, Morimitsu M. SDH-based time synchronous system for power system communications. IEEE Trans Power Deliv 1998;13(1):59–65.
[47] Oliveira HMNS, Katib I, Fonseca NLS da, Medhi D. Comparison of network protection in three-layer IP/MPLS-over-OTN-over-DWDM networks. In: 2015 IEEE global communications conference (GLOBECOM). IEEE; 2015. p. 1–6.
[48] Ooura K, Kanemaru K, Matsubara R, Ibuki S. Application of a power line maintenance information system using OPGW to the Nishi-Gunma UHV line. IEEE Trans Power Deliv 1995;10(1):511–7.
[49] IEEE Standard. IEEE standard for medium frequency (less than 12 MHz) power line communications for smart grid applications. IEEE Std 1901 2018:1–192. 1–2018.
[50] Sun S, Wu Y, Ma Y, Wang L, Gao Z, Xia C. Impact of degree heterogeneity on attack vulnerability of interdependent networks. Sci Rep 2016;6(1):1–9.
[51] Xin S, Guo Q, Sun H, Chen C, Wang J, Zhang B. Information-energy flow computation and cyber-physical sensitivity analysis for power systems. IEEE J Emerg Sel Top Circuits Syst 2017;7(2):329–41.
[52] Kenward A, Raja U. Blackout: extreme weather, climate change and power outages. https://assets.climatecentral.org/pdfs/PowerOutages.pdf. [Accessed 18 December 2020].
[53] Haces-Fernandez F. Wind energy implementation to mitigate wildfire risk and preemptive blackouts. Energies 2020;13(10):2421.
[54] Wang Y, Chen C, Wang J, Baldick R. Research on resilience of power systems under natural disasters–A review. IEEE Trans Power Syst 2016;31(2):1604–13.
[55] Ravadanegh SN, Karimi M, Tabatabaei NM. Modeling and analysis of resilience for distribution networks. In: Tabatabaei NM, Ravadanegh SN, Bizon N, editors. Power systems resilience: modeling, analysis and practice. Springer; 2018. p. 3–44.
[56] Pittala F, Xie C, Clark D, Kuschnerov M, Stone C, Haddad A. Effect of lightning strikes on optical fibres installed on overhead line conductors. In: 2018 34th international conference on lightning protection (ICLP). IEEE; 2018. p. 1–5.
[57] Donaldson DL, Alvarez-Alvarado MS, Jayaweera D. Power system resiliency during wildfires under increasing penetration of electric vehicles. In: 2020 international conference on probabilistic methods applied to power systems (PMAPS). IEEE; 2020. p. 1–6.
[58] News Shenzhen. Large-scale outage of taxis caused by blackouts at charging stations in Shenzhen due to Typhoon Mangkhut. http://www.sznews.com/news/content/2018-09/16/content_21085714.htm. [Accessed 11 May 2021].
[59] Chi Y, Xu Y, Ding T. Coordinated VAR planning for voltage stability enhancement of a wind-energy power system considering multiple resilience indices. IEEE Trans Sustain Energy 2020;11(4):2367–79.
[60] Faheem M, Shah SBH, Butt RA, Raza B, Anwar M, Ashraf MW, et al. Smart grid communication and information technologies in the perspective of Industry 4.0: opportunities and challenges. Comput Sci Rev 2018;30:1–30.
[61] He H, Yan J. Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Phys Syst Theory Appl 2016;1(1):13–27.
[62] Higgins M, Teng F, Parisini T. Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems. IEEE Trans Inf Forensics Secur 2021;16:1275–87.
[63] Higgins M, Mayes K, Teng F. Enhanced cyber-physical security using attack-resistant cyber nodes and event-triggered moving target defence. IET Cyber-Phys Syst Theory Appl 2021;6(1):12–26.
[64] Ding D, Han Q-L, Xiang Y, Ge X, Zhang X-M. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing 2018;275:1674–83.
[65] Chen Y, Qi D, Dong H, Li C, Li Z, Zhang J. A FDI attack-resilient distributed secondary control strategy for islanded microgrids. IEEE Trans Smart Grid 2021;12(3):1929–38.
[66] Pillitteri VY, Brewer TL. Guidelines for smart grid cybersecurity. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf. [Accessed 28 December 2020].
[67] Tang Y, Chen Q, Li M, Wang Q, Ni M, Fu X. Challenge and evolution of cyber attacks in cyber physical power system. In: 2016 IEEE power & energy society Asia-pacific power and energy engineering conference (APPEEC). IEEE; 2016. p. 857–62.
[68] Liang G, Zhao J, Luo F, Weller SR, Dong ZY. A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid 2017;8(4):1630–8.
[69] Tajer A. False Data Injection attacks in electricity markets by limited adversaries: stochastic robustness. IEEE Trans Smart Grid 2019;10(1):128–38.
[70] Duan J, Chow M. A novel data integrity attack on consensus-based distributed energy management algorithm using local information. IEEE Trans Ind Inform 2019;15(3):1544–53.
[71] Kim J, Tong L. On topology attack of a smart grid: undetectable attacks and countermeasures. IEEE J Sel Area Commun 2013;31(7):1294–305.
[72] Yang Y, McLaughlin K, Littler T, Sezer S, Im EG, Yao ZQ, et al. Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems. In: 2012 international conference on sustainable power generation and supply; 2012. p. 1–8.
[73] Huseinovic A, Mrdovic S, Bicakci K, Uludag S. A taxonomy of the emerging denial-of-service attacks in the smart grid and countermeasures. In: 2018 26th Telecommunications forum (TELFOR); 2018. p. 1–4.
[74] Liu S, Liu XP, Saddik AE. Denial-of-Service (dos) attacks on load frequency control in smart grids. In: 2013 IEEE power & energy society innovative smart grid technologies conference (ISGT). IEEE; 2013. p. 1–6.

[75] Huang K, Yang L, Yang X, Xiang Y, Tang YY. A low-cost distributed denial-of-service attack architecture. IEEE Access 2020;8:42111–9.
[76] Rahimi K, Parchure A, Centeno V, Broadwater R. Effect of communication time-delay attacks on the performance of automatic generation control. In: 2015 North American power symposium (NAPS); 2015. p. 1–6.
[77] Liu X, Li Z. False data attacks against AC state estimation with incomplete network information. IEEE Trans Smart Grid 2017;8(5):2239–48.
[78] Xue Y, Yu X. Beyond smart grid—cyber-physical-social system in energy future. Proc IEEE 2017;105(12):2290–2.
[79] Karakoc DB, Almoghathawi Y, Barker K, González AD, Mohebbi S. Community resilience-driven restoration model for interdependent infrastructure networks. Int J Disaster Risk Reduct 2019;38:101228.
[80] Karakoc DB, Barker K, Zobel CW, Almoghathawi Y. Social vulnerability and equity perspectives on interdependent infrastructure network component importance. Sustain Cities Soc 2020;57:102072.
[81] Raman G, Peng JC, Rahwan T. Manipulating residents' behavior to attack the urban power distribution system. IEEE Trans Ind Inform 2019;15(10):5575–87.
[82] Mohsenian-Rad A-H, Leon-Garcia A. Distributed internet-based load altering attacks against smart power grids. IEEE Trans Smart Grid 2011;2(4):667–74.
[83] Mishra S, Li X, Pan T, Kuhnle A, Thai MT, Seo J. Price modification attack and protection scheme in smart grid. IEEE Trans Smart Grid 2017;8(4):1864–75.
[84] Zhang X, Yang X, Lin J, Xu G, Yu W. On data integrity attacks against real-time pricing in energy-based cyber-physical systems. IEEE Trans Parallel Distr Syst 2017;28(1):170–87.
[85] Giraldo J, Cardenas A, Quijano N. Integrity attacks on real-time pricing in smart grids: impact and countermeasures. IEEE Trans Smart Grid 2017;8(5):2249–57.
[86] Tang D, Fang Y, Zio E, Ramirez-Marquez JE. Resilience of smart power grids to false pricing attacks in the social network. IEEE Access 2019;7:80491–505.
[87] Raman G, AlShebli B, Waniek M, Rahwan T, Peng JC-H. How weaponizing disinformation can bring down a city's power grid. PloS One 2020;15(8):0236517.
[88] Pan T, Mishra S, Nguyen LN, Lee G, Kang J, Seo J, et al. Threat from being social: vulnerability analysis of social network coupled smart grid. IEEE Access 2017;5:16774–83.
[89] Sheng Y, Guo Q, Yang T, Zhou Z, Sun H. A potential security threat and its solution in coupled urban power-traffic networks with high penetration of electric vehicles. CSEE J Power Energy Syst 2020. in press.
[90] Yang X, Li Y, Cai Y, Cao Y, Lee KY, Jia Z. Impact of road-block on peak-load of coupled traffic and energy transportation networks. Energies 2018;11(7):1776.
[91] Wei W, Wang J, Wu L. Quantifying the impact of road capacity loss on urban electrified transportation networks: an optimization based approach. Int J Transp Sci Technol 2016;5(4):268–88.
[92] Birkmann J. Measuring vulnerability to promote disaster-resilient societies: conceptual frameworks and definitions. In: Birkmann J, editor. Measuring vulnerability to natural hazards: towards disaster resilient societies. United Nations University Press; 2006. p. 9–54.
[93] Vespignani A. The fragility of interdependency. Nature 2010;464(7291):984–5.
[94] Aminifar F, Fotuhi-Firuzabad M, Shahidehpour M, Safdarian A. Impact of WAMS malfunction on power system reliability assessment. IEEE Trans Smart Grid 2012;3(3):1302–9.
[95] Wang C, Zhang T, Luo F, Li F, Liu Y. Impacts of cyber system on microgrid operational reliability. IEEE Trans Smart Grid 2019;10(1):105–15.
[96] Xin S, Guo Q, Sun H, Zhang B, Wang J, Chen C. Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. IEEE Trans Smart Grid 2015;6(5):2375–85.
[97] Xin S, Guo Q, Sun H, Wang J, Chen C. Cyber-physical assessment and comparison between centralized and distributed control mode in coordinated substation voltage control. In: 2016 IEEE power & energy society general meeting (PESGM). IEEE; 2016. p. 1–5.
[98] Tierney K, Bruneau M. Conceptualizing and measuring resilience: a key to disaster loss reduction. TR News 2007:14–7.
[99] Panteli M, Trakas DN, Mancarella P, Hatziargyriou ND. Power systems resilience assessment: hardening and smart operational enhancement strategies. Proc IEEE 2017;105(7):1202–13.
[100] Nan C, Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures. Reliab Eng Syst Saf 2017;157:35–53.
[101] Ly TC, Moura JN, Velummylum G. Assessing the bulk power system's resource resilience to future extreme winter weather events. In: 2015 IEEE power & energy society general meeting (PESGM). IEEE; 2015. p. 1–4.
[102] Panteli M, Mancarella P. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. IEEE Syst J 2017;11(3):1733–42.
[103] Panteli M, Pickering C, Wilkinson S, Dawson R, Mancarella P. Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures. IEEE Trans Power Syst 2017;32(5):3747–57.
[104] Das L, Munikoti S, Natarajan B, Srinivasan B. Measuring smart grid resilience: methods, challenges and opportunities. Renew Sustain Energy Rev 2020;130:109918.
[105] U.S. Department of Energy. Hardening and resiliency: U.S. energy industry response to recent hurricane seasons. http://www.oe.netl.doe.gov/docs/HR-Report-final-081710.pdf. [Accessed 26 December 2020].
[106] Wang X, Li Z, Shahidehpour M, Jiang C. Robust line hardening strategies for improving the resilience of distribution systems with variable renewable resources. IEEE Trans Sustain Energy 2019;10(1):386–95.
[107] Lin Y, Bie Z. Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding. Appl Energy 2018;210:1266–79.
[108] Oboudi MH, Mohammadi M, Trakas DN, Hatziargyriou ND. A systematic method for power system hardening to increase resilience against earthquakes. IEEE Syst J 2020. in press.
[109] Yan J, Hu B, Xie K, Tang J, Tai H. Data-driven transmission defense planning against extreme weather events. IEEE Trans Smart Grid 2020;11(3):2257–70.
[110] Abdin IF, Fang Y-P, Zio E. A modeling and optimization framework for power systems design with operational flexibility and resilience against extreme heat waves and drought events. Renew Sustain Energy Rev 2019;112:706–19.
[111] Shao C, Shahidehpour M, Wang X, Wang X, Wang B. Integrated planning of electricity and natural gas transportation systems for enhancing the power grid resilience. IEEE Trans Power Syst 2017;32(6):4418–29.
[112] Qiu F, Li P. An integrated approach for power system restoration planning. Proc IEEE 2017;105(7):1234–52.
[113] Liu W, Chen Y, Wang L, Liu N, Xu H, Liu Z. An integrated planning approach for distributed generation interconnection in cyber physical active distribution systems. IEEE Trans Smart Grid 2020;11(1):541–54.
[114] Qorbani M, Amraee T. Long term transmission expansion planning to improve power system resilience against cascading outages. Elec Power Syst Res 2021;1992:106972.
[115] Liu X, Shahidehpour M, Li Z, Liu X, Cao Y, Bie Z. Microgrids for enhancing the power grid resilience in extreme conditions. IEEE Trans Smart Grid 2017;8(2):589–97.
[116] Li Z, Shahidehpour M, Aminifar F, Alabdulwahab A, Al-Turki Y. Networked microgrids for enhancing the power system resilience. Proc IEEE 2017;105(7):1289–310.
[117] Ren L, Qin Y, Wang B, Zhang P, Luh PB, Jin R. Enabling resilient microgrid through programmable network. IEEE Trans Smart Grid 2017;8(6):2826–36.
[118] Bie Z, Lin Y, Li G, Li F. Battling the extreme: a study on the power system resilience. Proc IEEE 2017;105(7):1253–66.
[119] Al-Suwaidan HM, Mohagheghi S, Han Q. A communication framework for an ad-hoc microgrid for disaster response. In: 2015 IEEE international conference on smart grid communications (SmartGridComm). IEEE; 2015. p. 834–9.
[120] Nateghi R, Guikema SD, Quiring SM. Forecasting hurricane-induced power outage durations. Nat Hazards 2014;74(3):1795–811.
[121] Yan M, Ai X, Shahidehpour M, Li Z, Wen J, Bahramira S, 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 2019;34(4):2663–74.
[122] Yan M, He Y, Shahidehpour M, Ai X, Li Z, Wen J. Coordinated regional-district operation of integrated energy systems for resilience enhancement in natural disasters. IEEE Trans Smart Grid 2019;10(5):4881–92.
[123] Zhang S, Vittal V. Wide-area control resiliency using redundant communication paths. IEEE Trans Power Syst 2014;29(5):2189–99.
[124] Xu L, Guo Q, Yang T, Sun H. Robust routing optimization for smart grids considering cyber-physical interdependence. IEEE Trans Smart Grid 2019;10(5):5620–9.
[125] Qu Z, Xie Q, Liu Y, Li Y, Wang L, Xu P, et al. Power cyber-physical system risk area prediction using dependent Markov chain and improved grey wolf optimization. IEEE Access 2020;8:82844–54.
[126] Huang G, Wang J, Chen C, Qi J, Guo C. Integration of preventive and emergency responses for power grid resilience enhancement. IEEE Trans Power Syst 2017;32(6):4451–63.
[127] Wang C, Hou Y, Qiu F, Lei S, Liu K. Resilience enhancement with sequentially proactive operation strategies. IEEE Trans Power Syst 2017;32(4):2847–57.
[128] Wang C, Ju P, Lei S, Wang Z, Wu F, Hou Y. Markov decision process-based resilience enhancement for distribution systems: an approximate dynamic programming approach. IEEE Trans Smart Grid 2020;11(3):2498–510.
[129] Hussain A, Bui V-H, Kim H-M. Microgrids as a resilience resource and strategies used by microgrids for enhancing resilience. Appl Energy 2019;240:56–72.
[130] Simonov M. Dynamic partitioning of dc microgrid in resilient clusters using event-driven approach. IEEE Trans Smart Grid 2014;5(5):2618–25.
[131] Wang Z, Wang J. Self-healing resilient distribution systems based on sectionalization into microgrids. IEEE Trans Power Syst 2015;30(6):3139–49.
[132] Qiu F, Wang J, Chen C, Tong J. Optimal black start resource allocation. IEEE Trans Power Syst 2016;31(3):2493–4.
[133] Patsakis G, Rajan D, Aravena I, Rios J, Oren S. Optimal black start allocation for power system restoration. IEEE Trans Power Syst 2018;33(6):6766–76.
[134] Lei S, Chen C, Li Y, Hou Y. Resilient disaster recovery logistics of distribution systems: Co-optimize service restoration with repair crew and mobile power source dispatch. IEEE Trans Smart Grid 2019;10(6):6187–202.
[135] Ding T, Wang Z, Jia W, Chen B, Chen C, Shahidehpour M. Multiperiod distribution system restoration with routing repair crews, mobile electric vehicles, and soft-open-point networked microgrids. IEEE Trans Smart Grid 2020;11(6):4795–808.
[136] Yang Z, Dehghanian P, Nazemi M. Seismic-resilient electric power distribution systems: harnessing the mobility of power sources. IEEE Trans Ind Appl 2020;56(3):2304–13.
[137] Chen C, Wang J, Qiu F, Zhao D. Resilient distribution system by microgrids formation after natural disasters. IEEE Trans Smart Grid 2016;7(2):958–66.
[138] Wang Y, Xu Y, Li J, He J, Wang X. On the radiality constraints for distribution system restoration and reconfiguration problems. IEEE Trans Power Syst 2020;35(4):3294–6.

[139] Lei S, Chen C, Song Y, Hou Y. Radiality constraints for resilient reconfiguration of distribution systems: formulation and application to microgrid formation. IEEE Trans Smart Grid 2020;11(5):3944–56.
[140] Li Z, Shahidehpour M, Galvin RW, Li Y. Collaborative cyber-physical restoration for enhancing the resilience of power distribution systems. In: 2018 IEEE power & energy society general meeting (PESGM). IEEE; 2018. p. 1–5.
[141] Tang Y, Ten C-W, Brown LE. Switching reconfiguration of fraud detection within an electrical distribution network. In: 2017 Resilience week (RWS); 2017. p. 206–12.
[142] Ten C-W, Tang Y. Electric power: distribution emergency operation. New York: CRC Press; 2018.
[143] Liu BJ, Yu P, Xue-song Q, Shi L. Survivability-aware routing restoration mechanism for smart grid communication network in large-scale failures. Eurasip J Wirel Commun Netw 2020;1:1–21.
[144] Genge B, Haller P, Kiss I. Cyber-security-aware network design of industrial control systems. IEEE Syst J 2017;11(3):1373–84.
[145] Chalamasetty GK, Mandal P, Tseng TL. Secure SCADA communication network for detecting and preventing cyber-attacks on power systems. In: 2016 clemson university power systems conference (PSC). IEEE; 2016. p. 1–7.
[146] Wang X, Yi P. Security framework for wireless communications in smart distribution grid. IEEE Trans Smart Grid 2011;2(4):809–18.
[147] Joo M, Seo J, Oh J, Park M, Lee K. Situational awareness framework for cyber crime prevention model in cyber physical system. In: 2018 tenth international conference on ubiquitous and future networks (ICUFN). IEEE; 2018. p. 837–42.
[148] California ISO. CAISO information security requirements for the energy communication network (ECN). http://www.caiso.com/documents/californiaisoinformationsecurityrequirements_theenergycommunicationsnetwork.pdf. [Accessed 26 December 2020].
[149] Chhachhi S, Teng F. Market value of differentially-private smart meter data. In: 2021 IEEE power & energy society innovative smart grid technologies conference (ISGT). IEEE; 2021. p. 1–5.
[150] Saxena N, Choi BJ, Grijalva S. Secure and privacy-preserving concentration of metering data in AMI networks. In: 2017 IEEE international conference on communications (ICC). IEEE; 2017. p. 1–7.
[151] Xin S, Guo Q, Wang J, Chen C, Sun H, Zhang B. Information masking theory for data protection in future cloud-based energy management. IEEE Trans Smart Grid 2018;9(6):5664–76.
[152] Chaojun G, Jirutitijaroen P, Motani M. Detecting false data injection attacks in AC state estimation. IEEE Trans Smart Grid 2015;6(5):2476–83.
[153] Beg OA, Johnson TT, Davoudi A. Detection of false-data injection attacks in cyber-physical DC microgrids. IEEE Trans Ind Inform 2017;13(5):2693–703.
[154] Khalid HM, Peng JC-. A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks. IEEE Trans Smart Grid 2016;7(4):2026–37.
[155] Zhang Q, Li F, Cui H, Bo R, Ren L. Market-level defense against FDIA and a new LMP-disguising attack strategy in real-time market operations. IEEE Trans Power Syst 2021;36(2):1419–31.
[156] Huang T, Satchidanandan B, Kumar PR, Xie L. An online detection framework for cyber attacks on automatic generation control. IEEE Trans Power Syst 2018;33(6):6816–27.
[157] Zhang W, He X. Stealthy attack detection and solution strategy for consensus-based distributed economic dispatch problem. Int J Electr Power Energy Syst 2018;103:233–46.
[158] Kurt MN, Ogundijo O, Li C, Wang X. Online cyber-attack detection in smart grid: a reinforcement learning approach. IEEE Trans Smart Grid 2019;10(5):5174–85.
[159] Hussain B, Du Q, Sun B, Han Z. Deep learning-based DDoS-attack detection for cyber–physical system over 5G network. IEEE Trans Ind Inform 2021;17(2):860–70.
[160] Jin D, Li Z, Hannon C, Chen C, Wang J, Shahidehpour M, et al. Toward a cyber resilient and secure microgrid using software-defined networking. IEEE Trans Smart Grid 2017;8(5):2494–504.
[161] Li Y, Qin Y, Zhang P, Herzberg A. SDN-enabled cyber-physical security in networked microgrids. IEEE Trans Sustain Energy 2019;10(3):1613–22.
[162] Lin H, Chen C, Wang J, Qi J, Jin D, Kalbarczyk ZT, et al. Self-healing attack-resilient PMU network for power system operation. IEEE Trans Smart Grid 2018;9(3):1551–65.
[163] Anubi OM, Konstantinou C. Enhanced resilient state estimation using data-driven auxiliary models. IEEE Trans Ind Inform 2020;16(1):639–47.
[164] Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F. False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks. IEEE Trans Circuits Syst II Express Briefs 2021;68(2):717–21.
[165] Srikantha P, Liu J, Samarabandu J. A novel distributed and stealthy attack on active distribution networks and a mitigation strategy. IEEE Trans Ind Inform 2020;16(2):823–31.
[166] Duan J, Chow M. A resilient consensus-based distributed energy management algorithm against data integrity attacks. IEEE Trans Smart Grid 2019;10(5):4729–40.
[167] Duan J, Zeng W, Chow M. Resilient distributed dc optimal power flow against data integrity attack. IEEE Trans Smart Grid 2018;9(4):3543–52.
[168] Li P, Liu Y, Xin H, Jiang X. A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks. IEEE Trans Ind Inform 2018;14(10):4343–52.
[169] Peng C, Li J, Fei M. Resilient event-triggering H-infinity load frequency control for multi-area power systems with energy-limited DoS attacks. IEEE Trans Power Syst 2017;32(5):4110–8.
[170] Lu K, Zeng G, Luo X, Weng J, Zhang Y, Li M. An adaptive resilient load frequency controller for smart grids with DoS attacks. IEEE Trans Veh Technol 2020;69(5):4689–99.
[171] Liu Y, Xin H, Qu Z, Gan D. An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks. IEEE Trans Smart Grid 2016;7(6):2923–32.
[172] Sargolzaei A, Yen KK, Abdelghani MN. Preventing time-delay switch attack on load frequency control in distributed power systems. IEEE Trans Smart Grid 2016;7(2):1176–85.
[173] Moussa B, Debbabi M, Assi C. A detection and mitigation model for PTP delay attack in an IEC 61850 substation. IEEE Trans Smart Grid 2018;9(5):3954–65.
[174] Liu Z, Wang L. Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks. IEEE Trans Smart Grid 2021;12(2):1552–64.
[175] Yin L, Li S, Liu H. Lazy reinforcement learning for real-time generation control of parallel cyber-physical-social energy systems. Eng Appl Artif Intell 2020;88:103380.
[176] Cheng L, Yu T. Smart dispatching for energy internet with complex cyber-physical-social systems: a parallel dispatch perspective. Int J Energy Res 2019;43(8):3080–133.
[177] Heglund J, Hopkinson KM, Tran HT. Social sensing: towards social media as a sensor for resilience in power systems and other critical infrastructures. Sustain Resilient Infrastruct 2020;6(1–2):94–106.
[178] Bauman K, Tuzhilin A, Zaczynski R. Using social sensors for detecting emergency events: a case of power outages in the electrical utility industry. ACM Trans Manag Inf Syst 2017;8(2):1–20.
[179] Khan SS, Wei J. Real-time power outage detection system using social sensing and neural networks. In: 2018 IEEE global conference on signal and information processing (GlobalSIP). IEEE; 2018. p. 927–31.
[180] Sun H, Wang Z, Wang J, Huang Z, Carrington N, Liao J. Data-driven power outage detection by social sensors. IEEE Trans Smart Grid 2016;7(5):2516–24.
[181] Baidya PM, Sun W, Perkins A. A survey on social media to enhance the cyber-physical-social resilience of smart grid. 8th Renew. Power Gener. Conf. RPG 2019;2019:1–6.
[182] Bloomberg. Twitter suspends hundreds tweeting dcblackout during protests. https://www.bloomberg.com/news/articles/2020-06-02/twitter-suspends-hundreds-tweeting-dcblackout-amid-protests. [Accessed 11 May 2021].
[183] Moturu ST, Liu H. Quantifying the trustworthiness of social media content. Distributed Parallel Databases 2011;29(3):239–60.
[184] Marshall J, Syed M, Wang D. Hardness-aware truth discovery in social sensing applications. In: 2016 IEEE international conference on smart computing (DCOSS). IEEE; 2016. p. 143–52.
[185] Marshall J, Wang D. Towards emotional-aware truth discovery in social sensing applications. In: 2016 IEEE international conference on smart computation (SMARTCOMP). IEEE; 2016. p. 1–8.
[186] Huang C, Wang D. Topic-aware social sensing with arbitrary source dependency graphs. In: 2016 15th ACM/IEEE international conference on information processing in sensor networks (IPSN). IEEE; 2016. p. 1–12.
[187] Zhang DY, Han R, Wang D, Huang C. On robust truth discovery in sparse social media sensing. In: 2016 IEEE international conference on big data. IEEE; 2016. p. 1076–81.
[188] Kopsidas K, Abogaleela M. Utilizing demand response to improve network reliability and ageing resilience. IEEE Trans Power Syst 2019;34(3):2216–27.
[189] Shayesteh E, Moghaddam MP, Taherynejhad S, Sheikh-EL-Eslami MK. Congestion management using demand response programs in power market. In: 2008 IEEE power & energy society general meeting (PESGM). IEEE; 2008. p. 1–8.
[190] Huang D, Billinton R. Effects of load sector demand side management applications in generating capacity adequacy assessment. IEEE Trans Power Syst 2012;27(1):335–43.
[191] Li Y, Xie K, Wang L, Xiang Y. Exploiting network topology optimization and demand side management to improve bulk power system resilience under windstorms. Elec Power Syst Res 2019;171:127–40.
[192] Song M, Gao C, Shahidehpour M, Li Z, Yang J, Yan H. State space modeling and control of aggregated TCLs for regulation services in power grids. IEEE Trans Smart Grid 2019;10(4):4095–106.
[193] Song M, Gao C, Shahidehpour M, Li Z, Lu S, Lin G. Multi-time-scale modeling and parameter estimation of TCLs for smoothing out wind power generation variability. IEEE Trans Sustain Energy 2019;10(1):105–18.
[194] Momen H, Abessi A, Jadid S. Using EVs as distributed energy resources for critical load restoration in resilient power distribution systems. Transm Distrib IET Gener 2020;14(18):3750–61.
[195] Yang Z, Dehghanian P, Nazemi M. Seismic-resilient electric power distribution systems: harnessing the mobility of power sources. IEEE Trans Ind Appl 2020;56(3):2304–13.
[196] Yao S, Wang P, Zhao T. Transportable energy storage for more resilient distribution systems with multiple microgrids. IEEE Trans Smart Grid 2019;10(3):3331–41.
[197] Yao S, Wang P, Liu X, Zhang H, Zhao T. Rolling optimization of mobile energy storage fleets for resilient service restoration. IEEE Trans Smart Grid 2020;11(2):1030–43.

[198] Xu Y, Wang Y, He J, Su M, Ni P. Resilience-oriented distribution system restoration considering mobile emergency resource dispatch in transportation system. IEEE Access 2019;7:73899–912.
[199] Lei S, Chen C, Zhou H, Hou Y. Routing and scheduling of mobile power sources for distribution system resilience enhancement. IEEE Trans Smart Grid 2019;10 (5):5650–62.
[200] Yang T, Guo Q, Xu L, Sun H. Dynamic pricing for integrated energy-traffic systems from a cyber-physical-human perspective. Renew Sustain Energy Rev 2021;136: 110419.