Electric power grid resilience with interdependencies between power and communication networks – a review

Xin Liu, Bo Chen, Chen Chen, Dong Jin

1Department of Computer Science, Illinois Institute of Technology, Chicago, IL, USA
2Energy Systems Division, Argonne National Laboratory, Lemont, IL, USA
3School of Electrical Engineering, Xi’an Jiaotong University, Xi’an, Shaanxi, People’s Republic of China
E-mail: bo.chen@anl.gov

Abstract: Because of the development of smart grid technology, today’s power grid infrastructures are increasingly and heavily coupled with communication networks for many new and existing power applications. The interdependent relationship between the two systems, in which power control relies on the communication system to deliver control and monitoring messages and network devices require power supplies from the electrical grid, brings challenges in the effort to build a highly resilient integrated infrastructure. In this work, the authors summarise existing research on power grid resilience enhancement with the consideration of the interdependencies between power systems and communication networks. They categorise these works according to stages of resilience enhancement (i.e. failure analysis, vulnerability analysis, failure mitigation, and failure recovery) and methodologies (i.e. analytical solutions, co-simulation, and empirical studies). They also identify the limitations of existing works and propose potential research opportunities in this demanding area.

1 Introduction

Both power and communication systems are categorised as critical infrastructures by governments all over the world because their failure ‘would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters’ [1]. Therefore, these systems must maintain a high level of resilience in the face of various disturbances from either domain, such as power line trips and network congestion. The term ‘resilience’ is widely used in both power and network communities (and many other fields), but no universal definition exists across all domains or even within one domain. Wikipedia defines resilience in a computer network as ‘the ability to maintain service in the face of faults’, while in engineering and construction domain, resilience means the ‘ability to respond, absorb, and adapt to, as well as recover in a disruptive event’ [2]. In spite of the different definitions, there are extensive studies in both communities that focus on dealing with unavoidable failures in the systems. For example, how to use microgrids to improve service availability when substations fail or disconnect from the local area is a hot topic in the power system research community [3] and in the process of being an industry-standard [4]. The communication network community also studies network resilience in the face of link/node failures; these studies include, for example, new routing mechanisms to maintain end-to-end connectivity [5] and the multi-path TCP implemented as an industrial practice in Linux kernel stack [6].

However, a dependency/interdependency relationship exists between these two infrastructures, which have not drawn enough attention from academia and industry. Fig. 1 provides a high-level illustration of the architecture of power–communication systems. At the power transmission layer, to support wide-area control, protection, and monitoring of the transmission grid, fibre-optic networks and/or cellular networks are widely used to form a wide-area network (WAN) that serves the information exchange between control centre and intelligent electronic devices (IEDs) because these types of network technologies are suitable for long-distance, low-latency, and high-reliability message transmission. On the other hand, at the power distribution layer, Ethernet and/or wireless mesh network are often deployed by the utility companies to support their applications such as demand response, distribution automation, fast restoration, etc. These applications require the

Fig. 1 Illustration of the interdependent relationship between power and communication domains
underlying communication networks, neighbourhood-area networks/field-area network (NAN/FAN) to meet the requirements of moderate coverage range, high data rate, and high reliability. The lowest layer of communication networks, home-area networks (HANs), which is not shown in this figure are deployed within households to interconnect the smart meters and smart appliances. A comprehensive study of the communication network technologies of WAN, NAN/FAN, and HAN can be found in [7].

The concepts of dependency and interdependency between two infrastructures are defined in [8]; dependency refers to ‘a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other’, and interdependency stands for ‘a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other.’ Furthermore, this work categorises the interdependencies into four types: physical, cyber, geographic, and logical. Thus, the interdependency relationship of power–communication systems can be identified as (i) the communication system has physical dependency on electric power as it needs power supply to perform its data transmission functionalities, and (ii) the power system has cyber dependency on communication because, as a type of cyber-physical system (CPS), the state control of the power grid relies on the latter to deliver the monitoring data and control messages between the control entity and the field devices [9]. Furthermore, there is also a geographical interdependency between the two infrastructures, since the transmission line and optical fibre are usually located close to each other in the power transmission network, while the utility poles often carry both distribution lines and communication equipment on them. The power and information flow between the two infrastructures are also shown in Fig. 1.

The interdependent relationship creates an additional level of difficulty in enhancing the resilience of both infrastructures. When a large-scale natural disaster happens, due to geographical interdependency both power and communication systems might be damaged within a short period, and their physical and cyber dependencies will further propagate the failure to additional components that are NOT affected by the initial damage. To be more specific, Kwasinski [10] illustrates the power supply of typical public telecommunication equipment composed of the AC power line, onsite generator, and batteries in Fig. 2. Also, in [11], Cisco provides a FAN wireless network design guide with network equipment (IR510 distribution automation gateway) that requires DC power input with 12, 24, or 48 VDC. Kwasinski [10] observes from field investigations that ‘power outages are one of the main causes of communication network outages during natural disasters.’ When the electrical grid and power backup are damaged, the communication service will be interrupted and finally stopped when running out of battery or heat level is too high.

On the other hand, the control and monitoring applications of electrical grid rely on the communication infrastructure. In general, the smart grid control schemes can be categorised into short-term control schemes and long-term control schemes, depending on the time criticality of the control targets. Short-term control schemes have more direct dependencies on communication because it relies on sensor/actuator to perform local state control (e.g. voltage control). Thus, the communication service disruption will lead to the loss of information about grid state, which in turn greatly delay the failure detection and restoration process, in a sense that the system operation must dispatch crew members to manually retrieve the information and execute the control operations. Long-term control schemes normally involve a large number of sensors and actuators, such as economic dispatch and demand response. The interdependencies between cyber and physical in long-term control schemes are more complicated than short-term control schemes, in the sense that it may not only affect local control performance and sensor/actuator availability but also propagate to other elements. It is worth mentioning that the failure of sensors and actuators of control loops can be included in multiple control schemes. For example, the voltage sensor data collected from field devices can be used both by voltage regulators for local voltage control and by centralised system-level applications through the SCADA system.

The mutual impact of power and communication infrastructure leads to a closed-loop cascading failure scenario. For example, the authors of [12] investigated a hurricane event in Florida in 2004 and show that utility companies sent repairing crews and tree removal contractors to recover their distribution system; however, the process was hampered due to a lack of information exchange because the commercial cell phone service located in the same area was not functioning properly.

The examples above indicate that to improve the resilience of the interdependent systems, one must consider not only the individual infrastructures but also the influences they have on each other during the failures and the recovery process. Compared to the work on resilience enhancement in the power domain or the network domain, few studies have incorporated both domains together. The cross-domain nature of the topic leads the researchers in either domain to overlook the importance of the dependency/interdependency relationship. The relationship also introduces additional challenges in modelling and simulation, which we will further explain later. Fortunately, this issue has recently drawn great attention from the research community. In this survey, we collect and summarise the existing related research, and identify the advantages/disadvantages of those works as well as potential research directions in this area.

Prior to our work, two survey papers have focused on the same topic: Banerjee et al. [13] focus on the modelling perspective of the interdependencies between power and communication infrastructures and introduces five graph-based models in this area. Furthermore, this work identifies the limitations of these models and proposes a new modelling method based on Boolean expressions. Another survey, Martins et al. [14] summarise the existing studies that mostly focus on cascading failure effects due to interdependencies, especially under the assumption that the initial failure is due to weather-based disruptions. In this work, we conduct a comprehensive study of related literature that covers more aspects of different resilience studies and more types of modelling and simulation methodologies, and we analyse them at a deep level. Thus, we categorise the existing research based on two dimensions: objective and methodology.

The objective refers to the different stages of resilience enhancement. We adopt the definition in [15] that describes resilience in power grid as ‘the ability of a power system to recover quickly following a disaster, and more generally, absorb lessons for adapting its operation and structure for preventing or mitigating the impact of similar events in the future.’ Based on the definition, we consider resilience in the following stages:

• **Failure analysis:** This stage is to analyse the failure process, such as when the failure will stop, which components will be damaged, etc. Although this process actually does NOT count as part of the resilience enhancement study in our definition, it provides an understanding of the system behaviour when damage occurs, based on which actions for resilience enhancement can be applied.

• **Vulnerability analysis:** This stage focuses on identifying critical components in the system, whose failure is likely to propagate to the whole system. This stage could be based on either offline analysis or online analysis when the system is running in a normal state.

• **Failure mitigation:** This stage happens after the initial failure, either due to natural disasters or cyberattacks, to take action to
The methodology we encounter, expressed as different modelling communication network are indirect, and thus cannot be easily segregated the damaged component and prevent further cascading failures.

- **Failure recovery:** This stage aims to recover the damaged components, and more importantly restore services to customers.

Another dimension that we focus on in our review is the methodology applied to accomplish the objectives, because different authors may use different approaches to achieve common goals and similar methods could be used for different objectives. The methodology we encounter, expressed as different modelling approaches and the corresponding ‘solvers’ contains the following types:

- **Analytical models:** These models map the power and communication systems into mathematical structures (graphs, math equations, etc.) so that formal problems can be proposed in the context and solutions are developed using theoretical tools.

- **Executable models:** These models represent the system behaviour at a lower level, such as state machines or system dynamics, which can be ‘executed’ to obtain quantitative results under different parameter configurations. The results are often statistical and require a large number of repeated execution/simulations.

- **Empirical data:** Another collection of works conduct empirical studies about actual incidents that happened in the real world. They collect real data from field investigations and produce reports to illustrate the actual process of failure and recovery of interdependent power–communication systems. Although these data cannot be categorised as ‘models’ and are not suitable to directly acquire analytical solutions from them, they have the highest level of realism and can be used to validate other mathematical models proposed.

After reviewing and summarising the existing research, we found some limitations. For instance, although most of the works claim that they focus on the interdependency of the power and communication infrastructures, many of them only analyse the impact in one direction, from the cyber to power domain. Another challenge in this area is the difficulty of accurately modelling the interdependent relationship, since many impacts from the communication network are indirect, and thus cannot be easily quantified. Last but not least, existing research lack of efforts that address mitigation of and recovery from the failures, because they are considered less often with interdependencies. These insights provide potential research opportunities to focus on in this area.

The rest of the paper is organised as follows: Section 2 summarises the existing research according to modelling approaches; Sections 3 and 4 review the failure analysis and resilience enhancement studies, respectively, using the methods introduced in Section 2; Section 5 discusses the research reviewed and identifies the potential directions for future research; Section 6 concludes the paper.

---

2 Modelling and simulation of interdependent power–communication systems

To capture the interdependencies between power and communication networks, different approaches are applied to represent their relationship for different objectives. For the research that focuses on providing analytical results to a specific question (identify most critical components, produce fastest recovery plan, etc.), more abstract models are often used, such as graphs, Boolean predicates, etc. The simplicity of these models enables formalised problems to be defined and corresponding algorithmic solutions to be developed. On the other hand, for a different collection of studies that focus on a more realistic representation of the power and communication systems, executable (simulation) models are developed. These works often utilise existing simulation tools on power and communication communities and build a co-simulation platform to enable interoperability so that the interdependency relationship can be quantitatively investigated.

2.1 Analytical models

Most modelling techniques that aim at analytical results use multi-layer graph models. The basic idea is to use one graph to model the power system and another graph to model the communication system. There are additional edges connecting nodes in two graphs if a dependency relationship exists, as illustrated in Fig. 3. Under this general framework, existing works have different assumptions on the network topology, edge type (directed/undirected), failure process, and other properties.

The seminal work that brings attention to the role of interdependency in cascading failures is of Buldyrev et al. [16]. It assumes that two graphs (graph A for the power network and graph B for the communication network) have an identical number of vertices. Both graphs follow a scale-free topology. Regarding inter-edges, it is a one-to-one relationship between nodes in A and B, meaning for each node in either graph, there is and only one connected counterpart. The system failing process is modelled as (i) a node in A is removed at the initial stage, together with all the edges attached to it; (ii) the node in B that is attached to the removed interlink is also removed, together with all the edges attached to it; (iii) the edge removals might cause the graph to be isolated into multiple connected components – if two nodes in A are within the same component, but their counterpart in B is separated, then the edge between the two nodes in A are removed; (iv) the additional edge removal will cause new edge removals on the other side, and this iterative process terminates when all components are self-connected.

Huang et al. [17] follow similar assumptions about the internal topologies of both the power and communication networks to be scale-free graphs. However, it employs a different assumption about the interdependency relationship. Each power graph node stands for a generator or substation, while each communication graph node stands for an autonomous system (AS) where a control centre resides. The communication system's dependency on the power system follows a many-to-one mapping: each AS relies on one power source, while a power source may supply multiple ASs. On the other hand, among all the ASs it serves, a power source relies on one of them for control and monitoring. Thus, the edges between power graph nodes and communication graph nodes are directed. A power node has one incoming edge and multiple outgoing edges, while a communication node has one incoming edge and one outgoing edge. The failing process is more aggressive: (i) after initial removal of some nodes in the communication graph (and its outgoing edges), the power nodes losing their incoming edge (their control supply) will also be removed; (ii) the node removals will divide both graphs into multiple smaller components, and the ones that are disconnected from the giant component will be considered malfunctioning and removed also; (iii) the iterative process (with both edge and node removals in this case) will terminate when no more edges and nodes are removed.

Another graph-based modelling work is proposed by Parandehgheibi and Modiano [18]. In order to focus only on failure induced by interdependency, both the power and communication
networks are modelled as a star topology, where there is a centre node (power generator and control centre) on each side and other nodes (substations and routers) has one edge directly linked to their centre nodes. Thus, the node removals will NOT disconnect others from the centre node, which indicates that additional node/edge removal will be only caused by the inter-edges connecting the two graphs. Regarding inter-edges, this paper considers two scenarios: unidirectional case and bidirectional case. The latter assumes the interdependency is mutual, meaning if a router depends on a substation for power supply, the same substation communicates with itself, while the former case does not have this assumption.

There are several similar research works (e.g. [19, 20]) that use the graph as the system model to study the power–communication interdependent systems in impact or recovery perspective.

The graph models listed above are limited in that they can only provide abstract representations of the system components, as opposed to functional information, about the power and communication systems. Specifically, the node and links within either domain are indistinguishable, whereas, in reality, an entity in the power system could be a generator, a consumer, or a power switch and an entity in the communication system could be an end-host, a router, or a wireless base station. This coarse representation, the system failures and cascading failures can only be represented by structural changes such as node/link removal or disconnection from main components. To overcome this disadvantage, the authors of [21–23] combine graph-based models with power/information flow models. In these models, the nodes are assigned different properties, and the system states can be evaluated under certain assumptions. For example, Tootaghaj et al. [21] assign each node in the power graph as a generator, load, or junction node, and the power flow on each link can be calculated given an initial power input of the generators. Parandehgheibi et al. [22] directly incorporates the communication devices as ‘load’ entities into the power flow models and assigns constraints requiring that their demand must be satisfied first, in order to ensure the correct operation of the mitigation process. Similarly, Rosato et al. [23] models each node in the communication graph as the traffic origin, traffic destination, or routing device, the sending, receiving, and routing behaviours are modelled as stochastic processes, which enables the traffic delay to be evaluated through simulation. In this way, the status of the system components is no longer binary (on/off), but quantified within a range, which enables more complex interaction between the power and communication systems. However, heterogeneity also complicates the characterisation of the interdependency relationship. In simple graph models, the removal of a node on the power side ‘naturally’ causes the removal of its connected counterpart(s) in the other domain. However, in a more complicated model, how the state change of a node affects the state of the other node(s) in the other domain is not straightforward and may require further assumptions to be made.

In addition to graph-based models, other modelling methods are used in existing research. Banerjee et al. [13] point out that the graph models are limited to representing ‘conjunctive relationships.’ In other words, a power substation may be active only if multiple communication devices are ALL operating at the same time, and vice versa. To represent this conjunctive (or more complicated) dependency, this paper assigns each power or communication node a Boolean expression with other nodes as Boolean variables (i.e. True for active and False for failed) to represent this node's True/False status. When an initial failure happens, the corresponding variables are changed to False, and all other variables are recalculated according to their expressions. This calculating process stops when a fixed point is reached, where all the variables' states are the final outcome of this cascading failure. Wäfler and Heegaard [24] focus on the impact interdependency has on the power restoration process by modelling it as a stochastic activity network (SAN), where each power area’s recovery has five phases: detection (monitoring device notice the abnormal behaviours), administrative (design recovery plan and notify repair crew), logistics (gather materials and equipment), fault localisation (find the exact location and cause of the failure), and repair (bring back the normal operation of the devices). Fig. 4, acquired from their paper, illustrates this process. Among the above phases, detection, fault localisation, and repair (localisation) rely on the communication network to be completed in a timely manner. Thus, the communication infrastructure is assigned a timeout value that exceeds the value at which the device stops working because it runs of the backup battery. In addition, the repairing crew is considered short-handed and may not cover all failed areas when large-scale disasters happen.

Falahati et al. [25, 26] propose a novel framework for assessing small-world interdependency with direct/indirect interdependency of cyber-power systems. In this framework, the secure servers’ failures are the direct interdependency, while other communication components are the indirect interdependency. Additionally, this framework assumes the power system to be a star topology, where there is a centre substation for power supply, the same substation communicates with itself, and vice versa. Compared to the previous models, this framework can be used to study the direct/indirect interdependency of cyber-power systems; however, the failure of a cyber component will directly cause the failure of power components; indirect interdependency means that the failure in the cyber components is going to affect the detection or recovery process of power components when future failure happens.

Simulation is another method used to study interdependencies between power and communication networks. A simulation is a process of executing a model to provide models for power controllers, generators, power switches, loads, transmission lines, etc., and calculate the system states (e.g. current, voltage, power) at each fixed time-step. On the other hand, simulation/emulation tools used widely in both power system and communication network communities, and provides an experimental environment in which to study properties of a model of the integrated system that would otherwise be too complex, expensive, or even infeasible to engage. Power grid simulators provide models for power controllers, generators, power switches, loads, transmission lines, etc., and calculate the system states (e.g. current, voltage, power) at each fixed time-step. On the other hand, simulation frameworks aim to provide realistic and executable models to study interdependencies between power and communication networks. A simulation is a process of executing a model to produce behaviours and to study the performance of an actual system. In this section, we overview a line of research on co-simulation frameworks that combine a power system and a communication network simulation platform [27–38]. The co-simulation frameworks aim to provide realistic and executable models to study the interdependent behaviours between the two systems. In contrast to the modelling techniques in Section 2.1, simulation can explore states that would not be possible in the original system.

The co-simulation framework integrates off-the-shelf simulation/emulation tools used widely in both power system and communication network communities, and provides an experimental environment in which to study properties of a model of the integrated system that would otherwise be too complex, expensive, or even infeasible to engage. Power grid simulators provide models for power controllers, generators, power switches, loads, transmission lines, etc., and calculate the system states (e.g. current, voltage, power) at each fixed time-step. On the other hand,
the communication network simulators build models for network devices, protocols, topologies, and traffic, and simulate the process of packet transmission to advance experiments. The cross-domain events include but are not limited to field devices emitting monitoring data to the control centre, control centre emitting control messages to the field devices, and arrivals of those messages. A special type of co-simulation frameworks, named real-time simulators or emulators, allows interaction with real power/communication hardware devices and software. Those hardware-in-the-loop testbeds provide high-fidelity analysis of the system to be studied, but on the other hand, imposes additional complexity for synchronisation between real and virtual devices. The interaction between simulators and external devices is illustrated in Fig. 5.

We focus on the following four features when reviewing the co-simulation frameworks in the literature and summarise the results in Table 2:

- **Simulators**: A co-simulation framework always contains widely used power system simulator(s) and a communication network simulator/emulator.
- **Synchronisation mechanism**: One key research challenge is to correctly enable the interaction between the two simulation systems. Specifically, a power simulator operates in continuous time while a communication simulator runs in discrete time.

### Table 1 Summary of analytical models for interdependencies

| Source | Objective | Modelling technique | Solution |
|--------|-----------|---------------------|----------|
| [16]   | failure propagation analysis | graph-based model | percolation theory |
| [17]   | failure propagation analysis | graph-based model | percolation theory |
| [18]   | critical component identification | graph-based model | graph-algorithms |
| [19]   | critical component identification | graph-based model | graph-algorithms |
| [20]   | failure restoration | graph-based model | integer linear programming |
| [21]   | failure mitigate and restoration | graph model and flow model | integer linear programming |
| [22]   | failure mitigation | graph model and flow model | integer linear programming |
| [23]   | perturbation effect evaluation | graph model and flow model | stochastic simulation |
| [13]   | failure propagation analysis | Boolean expressions | iterative Boolean simulation |
| [24]   | recovery process analysis | stochastic model | stochastic simulation |
| [25, 26] | reliability assessment | probability and power flow model | probability calculation and load calculation |

Researchers have explored different synchronisation schemes, which have a great impact on the accuracy and efficiency of the co-simulation framework.

- **Real-time simulation**: It is challenging to maintain temporal fidelity when allowing a virtual testbed to seamlessly interact with physical devices running the real world, such as control signals and monitoring messages for power system devices and network packets for network devices. People developed real-time simulators for both power and communication networks to address this challenge.
- **Use case**: Researchers often present case studies to demonstrate the usage of their co-simulation frameworks. We review the use cases presented in those works to understand how to utilise the co-simulators to study and evaluate system resilience, security, and interdependence.

As summarised in Table 2, 12 different combinations of power system and communication network simulators have been explored to build the co-simulation platforms. Regarding the power system simulation, PowerWorld [39] and OpenDSS [40] are the two most popular choices of power system simulator. In particular, PowerWorld and other tools including PSLF [41], PowerFlow [42], PSCAD/EMTDC [43], and Adevs [44] are applied to simulate the transmission networks, while OpenDSS and other tools including RTDS [45], GridLab-D [46], VTB [47], and Modelica [48] are used for simulating distribution networks in the platforms we reviewed. RTDS is the only real-time power system simulator.

Regarding the communication network simulation, NS2 [49], and OPNET [50] are the most popular choices. OPNET is capable of conducting real-time simulation experiments and of connecting to live network hardware and software applications through its System-In-The-Loop module. Similar simulators include NS3 [51], OMNet++ [52], Mininet [53], and RINSE [54]. Mininet is a container-based network emulation and RINSE has a parallel simulation kernel; both tools can support real-time simulation/emulation experiments as well. The authors of [29, 34] use the wireless network models offered in NS2 and OMNet++; all other co-simulation frameworks only utilise the wired network simulation models.

The objective of synchronisation in co-simulation is to enable the correct and efficient interaction (e.g. control and data message exchanges) between a power system simulator and a communication network simulator. In other words, when an event processed in one simulator triggers/produces events in the other simulator, we must ensure that the right event is generated at the right time in the target simulator. A co-simulation framework typically includes a translation module to convert event format in both directions. To achieve real-time performance, the translation process often requires great engineering effort to enable seamless messages interaction with physical devices.

In a co-simulation framework, it is important to ensure the timestamps of the events in both domains are appropriately synchronised and minimise the out-of-order events. The time advancement in [29, 34] is controlled by the communication network simulator; in other words, the power system simulator is
triggered by events generated from the communication network to perform a snapshot-based static calculation. In contrast, the authors of [33, 35, 36] use a time-stepped model, where the power and communication simulators capture their own evolving state as time advances, and both simulators stop at the predefined time instants to exchange information. This approach introduces causality issues because the actual timestamps of the cross-domain events are often different from the predefined synchronisation time points. Therefore, the authors of [31, 32, 38] take a more complicated approach that suspends the individual simulation processes to deal with cross-domain events so as to enhance the correctness of simulation results. To support real-time simulation, we not only need to ensure the correct time synchronisation between simulators, but also need to keep up the simulation models running in virtual time with the external devices running in wall-clock time. This challenging issue has not been fully addressed yet. For example, the authors of [27, 28, 37] apply the best-effort strategy to execute the simulation experiments as quickly as possible. On the other hand, Godfrey et al. [29] extend the Linux kernel with the functionality to pause/resume the system time so that the embedded devices [55] and containers [30] running real software applications now have the flexibility to slow down, speed up, or stop their own clocks when synchronising with the simulator.

All co-simulation frameworks except for [32] present use cases. The authors of [31, 33] are used to evaluate communication-based protection schemes of power systems. The authors of [34–36, 38] study the impacts of communication delay on various power control applications by comparing the power system states with and without considering the delay. The authors of [27, 28, 30, 37] investigate the impact of different cyberattacks on power systems. Finally, Godfrey et al. [29] focus on the solar ramping effect on wireless communication performance, and its impact on the backup storage dispatch. The details of the experiments are discussed in Section 3.2.

One observation is that most of the existing research focuses on the impact of communication network conditions (e.g. system failures or cyberattacks) on power system operations. Limited simulation models are proposed to study the interdependencies between the power system and communication network, except for Godfrey et al. [29], in which the power strength acts as a parameter to affect the signal to interference-plus-noise ratio (SINR) used in the wireless transmission, and a random variable is derived to indicate the failure probability of the dispatching command transmission. Further improvements could be made include introducing multiple base station interference and modelling the transmission process.

### 2.3 Comparison of different modelling approaches

In this section, we describe different modelling techniques for interdependent power–communication systems. Fig. 6 compares these models in terms of tractability and realism. The graph-based models are most tractable, because they represent the interdependency with edges between graphs, and failure/recovery process as node removal/activation. In this way, graph theory and algorithms can be utilised to analyse the topological properties of the systems. Another method used equation-based models, often combined with graph structure. These models have a higher level of realism because they first distinguish between different components’ behaviours, and then quantify the commodity (power flows and information flows) that is transmitted within the system using steady-state equations. In this way, system states can be studied quantitatively.

The previous two models, which we denote as analytical models, are suitable for quickly obtaining rigorous solutions with theoretical tools. On the other hand, executable models are often used as a validation method for the solution obtained by the

| Source | Simulators | Time synchronisation | Real-time | Use case |
| --- | --- | --- | --- | --- |
| [27] | PowerWorld, RINSE | best effort | yes (comm.) | DDoS attack |
| [28] | RTDS, OPNET | best effort | man-in-the-middle attack |
| [29] | OpenDSS, NS2 | static power side | no solar ramping |
| DSSNet | OpenDSS, Mininet | virtual time | yes (comm.) | DoS attack |
| Geo [31] | PSLF, NS2 | global event | delay on transmission protection |
| Fncs [32] | GridLab-D, PowerFlow, NS3 | barrier-based synchronisation | no | N/A |
| Epochs | PSCAD/ EMTDC, PSLF, NS2 | time-stepped model | delay on transmission protection |
| [34] | OpenDSS, OMNet++ | static power side | no delay on distribution control |
| Vpnet [35] | VTP, OPNET | time-stepped model | delay on boost converter |
| PowerNet [36] | Modelica, NS2 | time-stepped model | delay on power generator |
| TASSCS | PowerWorld, OPNET | best effort | HMI attack and DoS attack |
| [38] | Adevs, NS2 | global event | delay/throughput on generation control |

Fig. 6 Comparison between different modelling techniques

This is an open access article published by the IET under the Creative Commons Attribution -NonCommercial License (http://creativecommons.org/licenses/by-nc/3.0/)
analytical studies. The executable models represent the system's state changes with state machines and differential equations, and thus the system evolvement can be 'executed' throughout its whole life cycle. The high level of accuracy enhances realism, but in turns complicates the analysis of the system. Therefore, this type of model has lower tractability, since the overall behaviour cannot simply be described by equations. Finally, although not introduced in this section, we place empirical data in this chart as a baseline for the most real 'models' and related research works will be introduced in the next section.

A potential research direction is to combine the analytical and executable models to provide solutions with high fidelity. Real-time simulation can be incorporated into the resilience mechanisms. For example, to effectively restore power supply, a critical step is to recover certain selected wireless stations to support the underlying communication. When a smart grid application needs to choose among a number of wireless stations to recover, it can decide the importance of each station by conducting a simulation study to measure the impact on the control message delivery with/without these stations. The 'what-if' analysis at runtime helps control schemes to make decisions. For example, the graph-based method in [29] provides a high-level framework to generate an optimal sequence for fast restoration. However, the nodes and links in the graph model are oversimplified to represent the actual components in the power and communication systems and their interdependencies. Using co-simulation tools like [29], operators can conduct simulation experiments when a failure occurs, or a component gets fixed, and then update the corresponding graph-model. In this way, a more realistic and dynamic analytical model is constructed to optimise the restoration.

This section mainly introduces different types of models used to study the interdependent systems. How they are used for the failure analysis or resilience enhancement will be introduced in Sections 3 and 4.

3 Investigation of interdependent failures

3.1 Empirical studies

In addition to the modelling and simulation work mentioned in Section 2, a number of empirical studies investigate the real-world infrastructure failures that involve both power and communication systems. Table 3 summarises related works according to the year, place, source of failure, involved infrastructures, and their relationship to the events investigated.

Bigger et al. [12] first identifies the distinction between dependencies and interdependencies. The dependency of one system on the other means that the latter system provides products or services to the former and the failure of the latter system may cascade to the former. On the other hand, two systems are interdependent means that they both provide products or services to each other. Thus, one system's failure will cause the dependent system to fail, and in turn, bring more negative effect on itself. One example in this paper is the failure of a distribution system that leads to a cell phone service downgrade, thereby affecting the effectiveness of the repair crew from the utility company. Based on this definition, this paper lists all dependent and interdependent failures among multiple infrastructures (power, communication, water, and transportation) in the 2004 hurricane disaster in Florida. A squared matrix with each row/column to be each infrastructure is constructed to illustrate pair-wise dependencies and interdependencies.

Krishnamurthy et al. [56] follow a similar definition of dependency/interdependency and proposes two metrics to quantify the 'closeness' of two interdependent systems. In this work, the earthquakes that happened in 2010 at Maule, Chile, and in 2011 at Tohoku, Japan, are studied. Evidence shows that the source of failures of the communication infrastructures in both sites, among other reasons, includes power outages and a lack of onsite generators. In order to conduct quantitative analysis, the author's plot 'function restoration curves' for power and communication services in both events. A function restoration curve has time $t$ as the $x$-axis with units to be days, and $O(t)$, which stands for 'outage ratio at a time $t$', as the $y$-axis. The outage ratio is the ratio of the number of users out of power/communication services to the total number of users. Thus, this time-series curve decreases from 1 (all services out) to 0 (all services restored) as time advances. Fig. 7 is taken from [56] to show the function restoration curves collected from the earthquake event in Tohoku, Japan. $I$ shows the curves of power, landline telecommunication, mobile communication (Mob), and mobile communication with (destroyed) base station removed (Mob-brm).

Based on the acquired data above, the authors in [56] propose a metric called 'strength of coupling' to measure the strength of dependency/interdependency between two infrastructures' recovery processes. The metric is based on the cross-correlation function (CCF), $\gamma_{ij}(h)$, on any two of the curves $x_i(t)$ and $x_j(t)$ as follows:

$$\gamma_{ij}(h) = \frac{\sum_{t=0}^{N-h}[x_i(t+h) - \bar{x}_i][x_j(t) - \bar{x}_j]}{N}$$

(1)

In the equation above, $h$ stands for the lag time, $N$ is the total number of data points, and $\bar{x}_i$ and $\bar{x}_j$ are the mean values of the time-series $x_i$ and $x_j$, respectively. Readers can refer to [56] for more details. By applying this function and new formulations based on this function to the power and communication data, the conclusion is drawn that communication infrastructure is more dependent on the power grid than vice versa, due to the fact that the power grid at both sites is not quite 'smart' at the time of the events. In addition, landline and mobile systems are correlated with each other because of collocation.

According to the definition of dependency/interdependency in the previous works, the remaining four works focus more on how

| Year       | Location         | Source of failure | Infrastructures                      | Relationship          |
|------------|------------------|-------------------|--------------------------------------|------------------------|
| 2004       | Florida, USA     | hurricane         | power, communication, transportation, etc. | interdependency        |
| [56] 2010 & 2011 | Maule, Chile & Tohoku, Japan | earthquake | power, communication | interdependency |
| [57] 2008 | North China      | snowstorm         | power, communication, transportation, etc. | dependency             |
| [10] 2013 | East Coast, USA  | hurricane         | power, communication                | dependency             |
| [58] 2010 | Iran             | cyber attack      | nuclear, communication              | dependency             |
| [59] 2015 | Ukraine          | cyber attack      | power, communication                | dependency             |
the other infrastructures depend on the power system than vice versa. Rong et al. [57] conduct a field investigation in north China after the snowstorm disaster in 2008 and proposes a framework to evaluate the extremeness of the failure of various infrastructures, which was caused by the power failure. The framework contains two metrics, Impact and Extend, each on scales from 1 to 9, to evaluate the “duration and severity” and the “spatial extent and number of affected people”, respectively, of the dependent failures. This evaluation framework is applied to telecommunication, transportation, water, oil/gas, and other infrastructures using the data collected from the investigation. The results show that mobile/telephone systems, business retail industry, and transportation systems are the most affected by the outage, and both have high impact and high extent values.

Kwasinski [10] also focuses on the impacts of a power outage on the communication system. This work conducts field research of Hurricane Sandy, which affected the East Coast of the United States in 2012. It describes in detail, with photographic evidence, how wire-line networks, wireless networks, and cable television services were disrupted by the power failure due to the hurricane. Specifically, when misallocation of the backup power storage led to the damage of these power sources or additional difficulty in using them, the downtime of the communication services increased unnecessarily, because the failure drawn from these studies is that there is a need to increase the availability of the communication system through more advanced mitigation strategies such as microgrids.

In addition to previous works that investigate the impact from power grid on other infrastructures caused by natural disasters, the authors of [58, 59] study the impact of communication on other infrastructures caused by cyberattacks. Farwell and Rohozinski [58] describe an incident that happened in 2010 in which a sophisticated computer program called ‘Stuxnet’ penetrated into the Iran nuclear system and caused its motor to malfunction by alternating the frequency of the electrical current that powers the centrifuges. Instead of directly taking over the control system, attackers in [59] applied a false data injection attack to the Ukraine power grid in 2015. The false data (i.e. meter measurement data) caused the unwanted control actions to be performed, leading to outages of the power grid that affected 225,000 customers for several hours. The studies on these incidents indicate the importance of cybersecurity enhancement for critical infrastructures.

3.2 Quantitative studies with co-simulation

As pointed out in Section 2.2, the majority of the co-simulation works illustrate the usage of their tools by conducting experiments to analyse the impact of the communication network on the power grid. This is because all these tools aim to provide research tools for the smart grid community, where the communication infrastructure is considered a service layer underlying the power applications. A common framework in these experiments is (i) for power domain simulators, either distribution or transmission network, the power states are managed by some control applications; (ii) the control application takes power system state measurements from the communication network, which are affected by the incidents modelled in the communication domain simulator; (iii) the responding control messages deviate in a certain way, which results in disruption of the power states.

To be more specific, the authors of [27, 28] focus on how the failure-handling mechanisms in a power grid fail to take any action on a power failure due to cyber attack blocking/altering the monitoring data, resulting in cascading failures; Hannon et al. [30] illustrate how the load shifting module of renewable loads fails to achieve the load-balance because the denial-of-service (DoS) attack blocks the communication; Mallouhi et al. [37] evaluate their cyber protection system, Automatic Software Protection System, which provides protection by analysing MODBUS and TCP/IP protocols in the emulated packets in the OPNET emulator, by conducting a human–machine interface (HMI) compromise attack and DoS attack, to see whether they can be detected and be taken over the control system of the power grid.

The above experiments analyse how cyberattacks affect the states of the power systems, while the following experiments instead study the impact of network delay and throughput (thus not exactly communication failures). The authors of [31, 33] involve protection devices (i.e. backup relays in transmission systems) in their models and measures their performance (i.e. response time to a power failure) with the influence of packet delay; the authors of [34–36] plot the voltage fluctuation as the output of various voltage control devices under different communication delays, because they affect the time the sensor data are received; Nutaro et al. [38] evaluates the performance of an automatic generation control (AGC) by calculating the percentage of load served, where the parameters are delay and throughput of the communication network since they transmit the load monitoring information to the controller. It is worth noticing that [35] models the relationship between sensing data sampling rate and network performance; the high sampling rate could introduce heavy traffic into the communication system and cause congestion, and in turn affect the power control, which can be seen as a form of interrelated impact between two systems.

Although Li et al. [35] involve the impact from the power domain to the communication domain, it is not an interdependency relationship according to our definition, because it does not model how the network components are affected by their power supply. Godfrey et al. [29], on the other hand, model the probability of a wireless transmission failure as the equation below:

\[ P_{\text{fail}} = Pr(P_r - (P_N + P_h) < z_0), \]

where \( P_r \) is the receiving power, \( P_N \) is the noise power, and \( P_h \) is the interference power. When the receiving power minus noise and interference falls below a threshold \( z_0 \), the transmission is assumed to fail. The receiving power \( P_r \) in (2) is, in turn, expressed as

\[ P_r = P_i - L_{\text{path}} + X_{\text{shadow}} + X_{\text{fade}}. \]

which is the transmitting power \( P_i \) minus path loss \( L_{\text{path}} \) plus shadowing and fading effects as \( X_{\text{shadow}} \) and \( X_{\text{fade}} \).

After acquiring this relationship, the co-simulator evaluates the relationship between the transmitting power and the performance of a storage controller. The context of the experiment is that a distribution system involves photovoltaic power as part of the source, and a storage controller monitors the output voltage at a 1-second sampling rate. When a solar ramping event happens, the controller detects the voltage drop and issues the dispatch commands to the remote power storage units to discharge in order to maintain the voltage level. Thus, different transmitting power levels (400 and 30 mW in this experiment) at the controller are tested to evaluate how the resulting transmission of the command messages is going to affect the voltage fluctuation.

3.3 Quantitative studies with analytical models

The analytical works presented here study the system failures due to the interdependent relationship between the power and communication systems. Compared to the research in Section 4, the works in this section use similar analytical models but only focus on the failure process, instead of resilience enhancement works such as vulnerability analysis, failure mitigation, and failure recovery. However, the method obtained from these works can be used as a preceding step that helps identify the vulnerabilities in the system, since they provide a way to quantitatively evaluate the impact of the failures.

Two similar works that apply graph-based models to represent the power–communication systems and percolation theory to study the failure effect are given by the authors of [16, 17]. Percolation theory is a set of graph theories that investigate the relationship between the probability of giant component existence and the edge/node distribution in a random graph. In the original problem introduced in [60], given a three-dimensional network with \( n \times n \times n \) vertices and a probability \( p \) that two neighbouring vertices have ‘open bonds’ (i.e. they allow the liquid through), the problem
is to identify the probability that a path from top to bottom exists. In [17], based on the graph models for the power–communication system and the failing process defined in Section 2.1, they investigate a modified version of the problem, which is to evaluate the function $F(\phi, \lambda)$, where $\phi$ stands for the initial ratio of node existence (in other words, the initial failure has $(1 - \phi)N$ nodes removed from the graph, where $N$ is the total number of nodes); $\lambda$ stands for the power-law exponent of the edge distribution in both power and communication graphs; and $F(\phi, \lambda)$ is the fraction of nodes remains in the largest connected components when the cascading failure stops. By identifying the transcendental equations at each failure iteration and the convergence condition, a steady-state relationship can be expressed when the number of steps goes toward infinity.

The authors also conducted a simulation experiment to obtain the numerical value of $F(\phi, \lambda)$ as shown in Fig. 8. The horizontal axis is the ratio of remaining nodes after the initial failure, $\phi$, and the vertical axis is the fraction of the largest connected component’s size at a steady state, $F(\phi, \lambda)$. For instance, 0 indicates that all the nodes are removed at last, and 1 indicates that the whole network remains connected when the failure stops. $\delta$ and $\lambda$ are the power-law exponents in a power network ($\delta$) and communication network ($\lambda$), respectively. Finally, $\mu_{j+1}$ and $\mu_{j+1}$ are the fraction of nodes at the step $2j$ for power graph, and the step $2j + 1$ for communication graph, which is assumed to reach the convergence states. The result shows that the fraction of giant component is sensitive to the exponent value $\lambda$, and that the smaller the value (more likely to find a node with a large degree), the more robust the network is. Readers can refer to [17] for more technical details. Buldyrev et al. [16] apply similar techniques to identify the probability of giant component existence with different graph topology parameters.

As introduced in Section 2.1, Banerjee et al. [13] aim to provide a more comprehensive model to represent the interdependency relationship than the simple graph models that they reviewed in their work. The Boolean expression they propose in their work is able to represent the ‘conjunctive’ dependency of a power device on a set of communication devices (and vice versa). As illustrated in Table 4, which we take from their paper, each power network device $a_i$, and communication network device $b_i$ is assigned a Boolean expression, where the conjunctive and disjunctive relationship is represented by AND and OR operations. For example, the power device $a_i$ is active only if $b_i$, or $b_i$ is active, and $b_i$ is active only if both $a_i$ and $a_i$ are active.

Based on the ‘life equation’ above for each entity, the failure propagation is performed as triggering an initial variable from 1 to 0, and re-evaluate all the related variables. This process is repeated until a fixed-point is reached. This procedure could be used to identify the critical components in the system, whose failure will cause all other variables to be 0 eventually. However, we did not put address work in Section 4 because it does not provide an efficient solution to identify these critical components, other than running the iterative evaluation process.

Falahati et al. [25, 26] focus on providing a framework that quantifies the impacts of the communication network on the power grid. The common ideas of these works are to (i) identify the potential failures in the communication networks; (ii) map the each of the communication component failures to the corresponding power node failures and (iii) having the power failure information, based on the power flow model, formulate a minimisation problem to decide the minimum load reduction to maintain the power system operation. To be more specific, for step (1), both papers use a ‘probability table’ to represent the probability of each system state, which contains a vector of $N$ binary variables to indicate the $N$ devices’ ON/OFF status (for both power and cyber devices). Thus, the table contains $2^N$ rows and $N$ columns, and all the rows’ probabilities sum up to 1. To make the framework more scalable, some equivalent states can be combined to reduce the table size. Step (2) addresses how to model the dependency relationship of a power element $\delta$ on a cyber element $\gamma$, and a dependency link $D = (\gamma, \delta)$ is constructed in [25, 26], with different assumptions for direct and indirect influences. Then, step (3) is executed to calculate the actual value in load shedding caused by cyber failures.

Unlike the above two works, Rosato et al. [23] focus in the other direction, which is to quantify the impact from a power failure on the cyber network. A power failure is first triggered as a power line break and a minimisation problem similar to step (3) above is executed to calculate the load reduction. Then, communication devices (modelled as loads in the power network) are deactivated if their power supply is reduced below a certain threshold $\alpha$, which is a value between 0 and 1. Then, a flow-based simulation model of the communication network is executed to evaluate the change of quality of service (QoS) in telecommunication (TLC) due to the node failures. The QoS TLC is defined as follows:

$$QoS\ TLC = \frac{m/M}{(T_f)(T_c)}$$

(4)

where $m$ and $M$ stand for the number of packets generated and received, and $(T_f)$ and $(T_c)$ are the average packet delay of in the communication network obtained by simulation with and without failures, respectively. This metric is calculated to analyse its relationship to the power system QoS metrics under failures, and readers can look for more details in [23].

The authors of [23, 25, 26] give examples to quantitatively model the dependency relationship in details from either direction, and a potential research opportunity is to combine them to form a closed-loop, interdependent relationship of the power and communication systems.

4 Enhancement of resilience with interdependency

As mentioned in Section 1, we summarise resilience enhancement in the main categories: vulnerability analysis, failure mitigation, and failure recovery. In each area, we study the research that takes communication network interdependency into consideration (Fig. 9).

4.1 Vulnerability analysis

The vulnerability analysis is the process of identifying the vulnerabilities of the current system based on past experiences, and thus helping to detect and respond to certain future events that are similar. The authors of [18, 19] aim to identify the critical entity in both the power grid and communication networks, whose failures would cause the most damage to the whole system due to interdependency. As introduced in Section 2.1, Parandehgheibi and

| Table 4 | Boolean expression model modified from [13] |

| Power Network | Communication Network |
|---------------|-----------------------|
| $a_i \leftarrow b_i + b_2$ | $b_i \leftarrow a_i + a_{i0}$ |
| $a_i \leftarrow b_i + b_2$ | $b_i \leftarrow a_i + a_{i1}$ |
| $a_i \leftarrow b_i b_{i0}$ | $b_i \leftarrow a_i a_{i1}$ |
| $a_i \leftarrow b_i + b_2 + b_3$ | $b_i \leftarrow a_i a_{i2}$ |
Fig. 9 Three components of resilience

Modiano [18] use graph-based models to represent the systems, and the failure propagation is caused by the removal of a node in one domain that leads to its connected counterpart(s) also being removed. It formulates a minimum total failure removals (MTRF) problem, which identifies a minimum set of nodes that will cause the whole graph’s failure. Two separate cases are considered for this problem: if the dependencies are asymmetric, which means the interconnected edges are unidirectional, this MTRF problem is converted to an integer linear programming (ILP) problem and two heuristic algorithms (one based on node degrees and the other based on cycles) are proposed and compared to the optimal solution. If the dependencies are symmetric, meaning all interconnected edges are bidirectional, a polynomial-time algorithm is proposed to solve the problem. Nguyen et al. [19] define a similar optimisation problem, named interdependent power network disruptor (IPND), which aims to find a set of nodes \( T \) with a fixed size \( k \), whose removals will result in the minimum size of the largest connected components in the graph after failure propagation stops. This problem is first proved to be NP-complete by reduction from a maximum independent set (MIS) problem. Then, a set of greedy algorithms are proposed, where the nodes are chosen at each step according to the following three metrics: (1) maximise the number of failed nodes after the removal, (2) maximise the disconnected components after the removal, and (3) hybrid metrics that combine (1) and (2).

Unlike other graph-based approaches such as [16], the two works above not only study how the failure propagates, but also identify which part of the system is more vulnerable. Therefore, they help the resilience enhancement process to prioritise their protection planning.

4.2 Failure mitigation

Failure mitigation is the process of reducing the impact of a failure caused by certain events, by stopping the damage from propagating to the rest of the system. The interdependent relationship between power and communication systems creates difficulties in both the information gathering stage and the mitigation planning stage. Tootaghaj et al. [21] model the scenario as a ‘grey area’ in the power system that is the consequence of losing monitoring data. In their work, the power failures are assumed to be due to a broken transmission line, and the power network model contains three types of edges: broken edges, working edges, and unknown edges. However, when solving the optimisation problem for failure mitigation (to minimise the load reduction to satisfy the power flow condition), how the unknown edges are handled is not quite clear.

Parandehgheibi et al. [22] model the communication network differently. First of all, due to the interdependency, a certain part of the system cannot be recovered. For a power node to be working, it must be reachable from at least one generator and at least one communication node; for a network node to be working, it must be reachable from at least one control centre and at least one power node. The rest of the nodes are deemed failed and excluded from the graph. Then, a similar optimisation problem to [21] is modelled to minimise the load reduction to ensure the power flow constraints, with additional constraints that the communication loads (communication nodes acting as power loads) must be greater than the power they need to operate.

4.3 Failure recovery

To deal with failure recovery in power systems, a common approach is to maximise the load or number of served customers under various constraints. However, when communication network failures are taken into consideration, the timing issue also needs to be addressed because the recovery process involves interdependency between the two systems. Wäfler and Heegaard [24] capture the impact of communication service outages during the power recovery process that involves sending repairing crew to the disrupted sites. As illustrated in Fig. 4, they model the repairing process at each site as a stochastic process that involves five stages, the stage-completion times of which follow an exponential distribution. Among them, the detection phase, administrative phase, fault localisation phase, and repair phase have two different sets of mean waiting times from which to choose, depending on the availability of the communication services. For example, if the monitoring devices are not working due to a communication channel failure, the detection phase time increases from the order of seconds to order of minutes or even hours. Whether the communication systems are working at a certain time is decided by determining whether their backup batteries are depleted, since they are assumed to lose their regular power supply when the disaster happens. In addition, a blocking bar is placed at the administrative process to represent the waiting state for an available crew, because the authors assume the number of damaged sites may exceed the number of repair crews. Having the stochastic model, multiple simulations are run to evaluate the relationship between the recovery time (i.e. the time all five phases are completed) and the battery time of the communication devices, with other parameters including the number of failed sites, number of repair crews, etc. Their experiment results indicate that adding battery supply to the most critical parts of the system is an effective measure to reduce the repair time.

Unlike Wäfler and Heegaard [24], which focus on detailed modelling of the repairing process, Baidya and Sun [20] apply a high-level graph model to represent the power–communication system recovery. In their model, the recovery of a power/communication entity is represented by activating the node from OFF to ON state. For a pair of mutually dependent nodes (power and communication nodes that connected to each other), they are assumed to be activated together if the power node’s neighbour is ON. On the other hand, a power node can be recovered only if at least one of its neighbours is activated AND at least one of the communication nodes that point to itself is activated. Thus, the system recovery process is step-by-step and an optimal sequence of recovery needs to be found to minimise the recovery time. To address this issue, the authors formulate a mixed-integer linear programming problem where the decision variable is each power/communication node/link’s ON/OFF (i.e. 1 and 0) state at each time \( t \), and the objective is to maximise the value of the summation of the variables across the whole time, plus the power load of the whole system. Notice that maximising the timed-states summation indicates minimising the restoration of the whole system. The interdependency constraints are expressed as a power node being stateless or equal to the summation of its dependent communication nodes’ states, and vice versa.

5 Discussion

In this section, we identify the limitations of the existing research that we discussed in this review. We then propose future research directions to address these issues to improve the resilience study of interdependent power–communication systems.

**Dependency versus interdependency:** As defined in Section 1, the term dependency describes how one system’s state is impacted...
by the other one's state, and the term interdependency refers to a mutual impact. In the papers we review, although some claim to consider interdependency, most indeed only focuses on the impacts of communication networks on power systems. For example, most co-simulation works conduct experiments to illustrate how cyber failures change the behaviour of control mechanisms, but not the other way around. This is because most smart grid research considers the communication infrastructure as an underlying layer that serves the information exchange of power components, and ignores the potential influence in the opposite direction. Thus, modelling of this relationship is needed to fully address the resilience of interdependent systems; Godfrey et al. [29] provide an example to model the relationship between the power supply and wireless signal strength.

Modelling of interdependencies: Related to the previous issue, another reason that the interdependency is NOT intensively studied is the difficulty of modelling it. Most related works that involve the actual mutual influence are graph-based models, where the dependency is represented by directed/undirected edges. This method has the advantage of being able to quickly identify the components in different domains that affect each other so that failure propagation can be easily represented in the model by node/edge removals. However, in reality, the influences between the two infrastructures are quite subtle. As pointed out in [26], a communication network failure may not directly impact some specific power system components but will cause problems when future power incident happens. For example, the failure to deliver monitoring information quickly to the control centre will delay failure detection in the power system, which leads to the propagation of initial damage. This observation is further proved in many of the co-simulation works whose experiments fall within this scenario. Thus, a more detailed quantitative analysis framework of the interdependent failure and recovery is needed. A potential direction that we found promising is to combine the equation-based modelling in both power and communication systems, such as [23, 25], to form a feedback loop of the whole interdependent systems.

Failure analysis versus resilience: Another limitation of existing works is that most of them focus on failure analysis, and there are limited efforts on resilience, especially failure mitigation and recovery. Specifically, in graph-based model studies, only one (i.e. [20]) improves restoration efficiency, while the others analyse the outcome of cascading failures and identify the critical components as vulnerabilities. In addition, only two works (i.e. [21, 22]) focus on failure mitigation of the power system with communication network taken into consideration. Thus, a potential research opportunity is to design and implement new frameworks to improve the mitigation and recovery processes with the presence of interdependencies.

6 Conclusion
In this paper, we summarise the existing research on interdependencies in the power and communication systems, which create challenges for enhancing the resilience of these two critical infrastructures. We categorise studies based on objective (failure mitigation, vulnerability analysis, failure mitigation, and failure recovery) and methodology (graph-based models, equation-based models, and executable models). We found there is a tradeoff between realism and tractability across the modelling techniques, and more efforts should be put into studying the interdependent relationship to develop accurate and efficient models. In addition, in comparison to failure analysis, the resilience aspect of power–communication systems is not fully studied. This paper provides several potential directions for future research into the resiliency enhancement of interdependent infrastructures.

7 Acknowledgments
This work was partly sponsored by the Air Force Office of Scientific Research (AFOSR) under grant YIP FA9550-17-1-0240 and the Maryland Procurement Office under Contract no. H98230-18-D-0007. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of AFOSR and the Maryland Procurement Office. This material is partially based upon work supported by the U.S. Department of Energy’s Office of Energy Efficiency and Renewable Energy (EERE) under Solar Energy Technologies Office (SETO) Agreement Number 34230, and the U.S. Department of Energy’s Office of Electricity (OE) under Agreement Number 31278.

8 References
[1] Moteff, J., Copeland, C., Fischer, J.: ‘Critical infrastructures: What makes an infrastructure critical?’. Library of Congress (Congressional Research Service), Washington DC, 2003
[2] Wikipedia: ‘Resilience – wikipedia, the free encyclopedia’, 2019, accessed 05 July 2019. Available at http://en.wikipedia.org/wiki/index.php?title=Resilience
[3] Farzin, H., Fotuhi-Firuzabad, M., Moemie-Aghaie, M.: ‘Enhancing power system resilience through hierarchical outage management in multi-energy networks’, IEEE Trans. Smart Grid, 2016, 7, (6), pp. 2869–2879
[4] Bui, D.M., Lien, K.Y., Chen, S.L., et al.: ‘Standards commonly used for microgrids – research project to develop an industry microgrid standard in Taiwan’, Electr. Power Compon. Syst., 2016, 44, (19), pp. 2143–2160. Available at https://doi.org/10.1080/15325008.2016.1216203
[5] Atlas, A.K., Zinin, A.: ‘Basic specification for ip fast reroute: loop-free alternates’, 2008
[6] Ford, A., Raiciu, C., Handley, M.: ‘Architectural guidelines for multipath TCP development’, IETF, Inf. RFC 2011, 6182, pp. 1–28
[7] Kuzlu, M., Pipattanasomporn, M., Rahman, S.: ‘Communication network failures change the behaviour of control mechanisms, but not the recovery. Specifically, in graph-based model studies, only one’
[8] Baidya, P.M., Sun, W.: ‘Effective restoration strategies of interdependent power grids and communication networks’, Proc. IEEE, 2016, 104, (5), pp. 1058–1070
[9] Kwasiinskii, A.: ‘Lessons from field damage assessments about communication networks power supply and infrastructure performance during natural disasters with a focus on hurricane sandy’. FCC Workshop Network Resiliency, Brooklyn, NY, USA, 2013
[10] ‘Distribution automation – feeder automation design guide’, Cisco Systems, 2019. Available at https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Feeder-Automation/DS/DA-FA-DA-FA-DX.pdf
[11] Bigger, J.E., Willingham, M., Kringsdol, F., et al.: ‘Consequences of critical infrastructure interdependencies: lessons from the 2004 Hurricane season in Florida’, Int. J. Critical Infrastruct., 2009, 5, pp. 199–219
[12] Barnerjes, J., Das, A., Sen, A.: ‘A survey of interdependency models for critical infrastructure networks’, arXiv preprint arXiv:170102547, 2017
[13] Martins, L., Girao-Silva, R., Jorge, L., et al.: ‘Interdependence between power grids and communication networks: a resilience perspective’. 13th Int. Conf. DRCN 2017-Design of Reliable Communication Networks, Munich, Germany, 2017, pp. 1–9
[14] Pantelli, M., Mancarella, P.: ‘The grid: stronger, bigger, smarter?’; presenting a conceptual framework of power system resilience’, IEEE Power Energy Mag., 2015, 13, (3), pp. 58–66
[15] Baidya, P.M., Sun, W.: ‘Effective restoration strategies of interdependent power system and communication network’, J. Eng., 2017, 2017, (13), pp. 1760–1764
[16] Tootaghaj, D.Z., Bartolini, N., Khamsfroush, H., et al.: ‘Controlling cascading failures in interdependent networks under incomplete knowledge’. 2017 IEEE 36th Symp. on Reliable Distributed Systems (SRDS), Hong Kong, China, 2017, pp. 54–63
[17] Huang, Z., Wang, C., Rui, S., et al.: ‘Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory’. 2013 IEEE 8th Conf. on Industrial Electronics and Applications (ICIEA), Melbourne, VIC, Australia, 2013, pp. 1023–1028
[18] Parandehgheibi, M., Modiano, E.: ‘Robustness of interdependent networks: the case of communication networks and the power grid’. 2013 IEEE Global Communications Conf. (GLOBECOM), Atlanta, GA, USA, 2013, pp. 2164–2169
[19] Nguyen, D.T., Shen, Y., Thai, M.T.: ‘Detecting critical nodes in interdependent power networks for vulnerability assessment’, IEEE Trans. Smart Grid, 2013, 4, (1), pp. 151–159
[20] Baidya, P.M., Sun, W.: ‘Effective restoration strategies of interdependent power system and communication network’, J. Eng., 2017, 2017, (13), pp. 1760–1764
[21] Tootaghaj, D.Z., Bartolini, N., Khamsfroush, H., et al.: ‘Controlling cascading failures in interdependent networks under incomplete knowledge’. 2017 IEEE 36th Symp. on Reliable Distributed Systems (SRDS), Hong Kong, China, 2017, pp. 54–63
[22] Parandehgheibi, M., Modiano, E., Hay, D.: ‘Mitigating cascading failures in interdependent power grids and communication networks’. 2014 IEEE Int. Conf. on Smart Grid Communications (SmartGridComm), Venice, Italy, 2014, pp. 242–247
[23] Rosato, V., Issacharoff, L., Tiririco, F., et al.: ‘Modeling interdependent infrastructures using interacting dynamical models’, Int. J. Crit. Infrastruct., 2008, 4, (1–2), pp. 63–79
[24] Wäfler, J., Heegaard, P.L.: ‘Interdependency in smart grid recovery’. 2015 7th DRCN 2017-Design of Reliable Communication Networks, Munich, Germany, 2017, pp. 1–9
[25] Falahati, B., Fu, Y., Wu, L.: ‘Reliability assessment of smart grid considering direct cyber-power interdependencies’, IEEE Trans. Smart Grid, 2012, 3, (3), pp. 1518–1524

This is an open access article published by the IET under the Creative Commons Attribution -NonCommercial License (http://creativecommons.org/licenses/by-nc/3.0/)
Falibati, B., Fu, Y.: ‘Reliability assessment of smart grids considering indirect cyber-power interdependencies’, IEEE Trans. Smart Grid, 2014, 5, (4), pp. 1577–1585.

Davis, C., Tate, J., Okhravi, H., et al.: ‘Scada cyberspace security testbed development’. 2006 38th North American Power Symp., Carbondale, IL, USA, 2006, pp. 483–488.

Chen, B., Butler-Parry, K.L., Goulart, A., et al.: ‘Implementing a real-time cyber-physical system test bed in rtds and opnet’. 2014 North American Power Symp. (NAPS), Pullman, WA, USA, 2014, pp. 1–6.

Godfrey, T., Mullens, S., Griffith, D.W., et al.: ‘Modeling smart grid applications with co-simulation’. 2010 first IEEE Int. Conf. on Smart Grid Communications, Gaithersburg, MD, USA, 2010, pp. 291–296.

Hannon, C., Yan, J., Jin, D.: ‘Dssnet: A smart grid modeling platform combining electrical power distribution system simulation and software defined networking emulation’. Proc. of the 2016 ACM SIGSIM Conf. on Principles of Advanced Discrete Simulation, Banff, Alberta, Canada, 2016, pp. 131–142.

Lin, H., Veda, S.S., Shukla, S.S., et al.: ‘Geoo: global event-driven co-simulation framework for interconnected power system and communication network’, IEEE Trans. Smart Grid, 2012, 3, (3), pp. 1444–1456.

Ciraci, S., Daily, J., Fuller, J., et al.: ‘Pneo: a framework for power system and communication networks co-simulation’. Proc. of the Symp. on Theory of Modeling & Simulation-DEVIS Integrating, Tampa, Florida, USA, 2014, p. 36.

Hopkinson, K., Wang, X., Giovanini, R., et al.: ‘Epoch: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components’, IEEE Trans. Power Syst., 2006, 21, (2), pp. 548–558.

Lévesque, M., Xu, D.Q., Joines, G., et al.: ‘Communications and power distribution network co-simulation for multidisciplinary smart grids experiments’. Proc. of the 45th Annual Simulation Symp., Orlando, Florida, USA, 2012, p. 2.

Li, W., Monti, A., Luo, M., et al.: ‘Vpnet: A co-simulation framework for analyzing communication channel effects on power systems’. 2011 IEEE Electric Ship Technologies Symp., Alexandria, VA, USA, 2011, pp. 143–149.

Libratore, V., Al-Hhamouri, A.: ‘Smart grid communication and co-simulation’. IEEE 2011 EnergyTech, Cleveland, OH, USA, 2011, pp. 1–5.

Gadalouhi, M., Al-Hamouri, A., Cox, D., et al.: ‘A toolset for analyzing security of scada control systems (tasscs)’. ISGT 2011, Anaheim, CA, USA, 2011, pp. 1–7.

Naturo, J., Kuruganti, P.T., Miller, L., et al.: ‘Integrated hybrid-simulation of electric power and communications systems’. 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 2007, pp. 1–8.

‘Powerworld corporation’, accessed 20 June 2019. Available at https://www.powerworld.com/products/features/powerflow.

‘Powerflow load flow analysis software’, accessed 20 June 2019. Available at https://www.powerworld.com/products/features/powerflow.

Manitoba, H.: ‘Research centre’, PSCAD/EMTDC: Electromagnetic transients program including dc systems, 1994.

‘Adevs: A discrete event system simulator’, accessed 20 June 2019. Available at https://web.ornl.gov/~nutarojj/adevs/.

‘Rtsd technologies’, accessed 20 June 2019. Available at http://www.rtsd.com/.

Chassin, D.P., Fuller, J.C., Dijalli, N.: ‘Gridlab-d: an agent-based simulation framework for smart grids’, J. Appl. Math., 2014, pp. 1–12.

Brice, C.W., Gökdere, L.U., Dougall, R.A.: ‘The virtual test bed: an environment for virtual prototyping’. Proc. of Int. Conf. on Electric Ship, Istanbul, Turkey, 1998, pp. 27–31.

Tillier, M.: ‘Introduction to physical modeling with modelica’, vol. 615, (Springer Science & Business Media, USA, 2012).

‘Ne2 simulator’, accessed 20 June 2019. Available at http://nnsam.sourceforge.net/wiki/index.php/Main_Page.

‘Opnet technologies’, accessed 20 June 2019. Available at https://www.riverbed.com/products/steelcentral/opnet.html?redirect=opnet.

Henderson, T.R., Lucage, M., Riley, G.F., et al.: ‘Network simulations with the ns-3 simulator’, SIGCOMM Demonstration, 2008, 14, (4), p. 527.

Varga, A.: ‘Omnet+++, in ‘Modeling and tools for network simulation’ (Springer, Germany, 2010), pp. 35–59.

Lantz, B., Heller, B., McKeown, N.: ‘A network in a laptop: rapid prototyping for software-defined networks’. Proc. of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, New York, NY, USA, 2010, p. 19.

Liljenstam, M., Liu, J., Nicol, D., et al.: ‘Rinse: the real-time immersive network simulation environment for network security exercises’. Workshop on Principles of Advanced and Distributed Simulation (PADS’05), Monterey, CA, USA, 2005, pp. 119–128.

Hannon, C., Yan, J., Liu, Y.A., et al.: ‘A distributed virtual time system on embedded Linux for evaluating cyber-physical systems’. Proc. of the 2019 ACM SIGSIM Conf. on Principles of Advanced Discrete Simulation. SIGSIM-PADS ’19, Chicago, IL, USA, 2019, pp. 37–48. Available at http://doi.org/10.1145/3316800.3322895.

Krishnamurthy, V., Kwasiński, A., Duemas-Quites, L.: ‘Comparison of power and telecommunications dependencies and interdependencies in the 2011 Tohoku and 2010 Maule earthquakes’, J. Infrastruct. Syst., 2016, 22, (3), p. 04016013.

Rong, M., Han, C., Liu, L.: ‘Critical infrastructure failure interdependencies in the 2008 Chinese winter storms’, 2010 Int. Conf. on Management and Service Science, Wuhan, China, 2010, pp. 1–4.

Farwell, J.P., Rohozinski, K.: ‘Stuxnet and the future of cyber war’, Survival, 2011, 53, (1), pp. 23–40.

Liang, G., Weiler, S.R., Zhao, J., et al.: ‘The 2015 Ukraine blackout: implications for false data injection attacks’, IEEE Trans. Power Syst., 2016, 32, (4), pp. 3317–3318.

Wikipedia: ‘Percolation theory – wikipedia, the free encyclopedia’, 2019. Accessed 02 July 2019. Available at en.wikipedia.org/wiki/index.php?title=Percolation%20theory&oldid=900882642.