Optimal Backup Power Deployment for Communication Network With Interdependent Power Network

PENG-YONG KONG®, (Senior Member, IEEE)
Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, United Arab Emirates
e-mail: pengyong.kong@ku.ac.ae

ABSTRACT

Smart grid has a power network with an interdependent communication network. In such a system, a node failure can lead to another failure in its dependent node in the other network. These inter-network failures can occur recursively in a cascading process, resulting in a complete system collapse. Such cascading failure process can be interrupted by providing backup power to communication nodes, so that they can continue operation when the power nodes they depend on have failed. It is costly to install a backup power unit at each communication node. We have used the two-stage percolation theory to determine the system robustness as a function of backup power deployment density and backup power unit capacity. Then, we propose a novel scheme to determine the optimal backup power deployment density and unit capacity, which can minimize the backup power deployment cost without compromising a desired system robustness. Through extensive simulations, we have found that when the probability of initial node failure is below its critical value, the deployment cost may decrease linearly with a smaller network size and may increase exponentially with a higher robustness requirement.

INDEX TERMS

Smart grid, interdependent network, backup power, cascading failure, cyber-physical system.

I. INTRODUCTION

Smart grid plays an important role in renewable energy integration into power network. With the support of an advanced communication network, smart grid can acquire an accurate status of the intermittently available renewable outputs. As the power output fluctuates, smart grid through the communication network may remotely control various components in the power network for a match between power supply and consumer demand [1]. This is a critical operation because an excessive power supply-demand gap can lead to a catastrophic breakdown in the power network. While the power network depends on the communication network for its stability, the communication network also depends on the power network for electricity supply to its equipments [2].

Typically, random failures are rare events in a well maintained smart grid system. According to [3], the average time to failure for a communication switch in IEC61850 communication network for a power grid can be 50 years. But, if they happen, such failures may inflict significant impact, which can be exacerbated by the interdependence between power network and communication network. As reported in a study which examines the causes of several major power blackouts in Europe and North America [4], power-communication network interdependence may reduce the smart grid system’s robustness against failures, natural hazards and malicious attacks. For instance, in the event of an attack or a random failure in one of the two networks, the failure can cause its dependent nodes in the other network to fail. This new failure can lead to further failures in the dependent nodes of the failed node. This process may continue in a recursive manner, triggering a cascade of failures between the two interdependent networks. Such cascading failures can potentially cause the entire smart grid to collapse [5]–[7].

This paper wants to minimize the negative impacts of network interdependence against an inter-network cascading failure process, which can be triggered by node failures in either a communication network or a power network. We propose a novel idea, which is to guard against a cascading failure process by interrupting it, through an optimal deployment of backup power units on communication nodes. Specifically, we interrupt the cascading failure process by installing...
backup power at communication nodes, so that the communication node can continue operation despite losing its primary electricity supply from the power node that it depends on. Since a failure in power node does not lead to a further failure in its dependent communication node, inter-network failure can be stopped from propagating.

Backup power is usually provided in the form of local energy storage or battery [8]. Each backup power unit has a cost, which is dependent on battery capacity. Therefore, it may become too costly to install a backup power unit at each node in the communication network. On the other hand, if some communication nodes are not installed with a backup power unit, the cascading failure process may continue for a few iterations before stopping at a steady-state, and this can reduce the system robustness, which is quantified as the fraction of power nodes that survive the cascade of failures [9]. In this paper, we first determine the smart grid robustness as a function of backup power deployment density and capacity of each backup power unit. Then, we propose a novel scheme to find the optimal backup power deployment density and backup power unit capacity, to minimize the backup power deployment cost without compromising a desired level of system robustness.

The rest of this paper is organized as follows. Section II is for a survey of related works. We introduce the system model in Section III, before developing an analytical model in Section IV to determine the system robustness. Section V describes the scheme for finding the optimal backup power deployment density and backup power unit capacity. Extensive performance evaluations are presented in Section VI, before the paper ends with concluding remarks in Section VII. For ease of reference, the main contributions of this paper are summarized as follows:

- Propose the novel idea to guard against a cascading failure process across interdependent power and communication network, by interrupting it, through an optimal deployment of backup power units on communication nodes.
- Develop an analytical model based on the two-stage percolation theory to determine the system robustness as a function of backup power deployment density and backup power unit capacity.
- Develop a novel scheme to determine the optimal backup power deployment density and unit capacity, which can minimize the backup power deployment cost without compromising a desired system robustness.

From the solutions given by the proposed scheme, the identified unit capacity indicates the required size of each backup power unit and the deployment density indicates the fraction of communication nodes that should be installed with a backup power unit of the given size. The scheme determines only the deployment density but not which particular communication nodes to be installed with the backup power units. Practically, given a deployment density, we envisage that the operator can pick the desired number of communication nodes randomly from all communication nodes for backup power installation. As an example, consider a smart grid with 100 power nodes and 200 communication nodes. Says, we want to achieve a robustness of 0.99. Hence, we can tolerate only failure of at most one power node at the end of a cascading failure process. To achieve this, says, the proposed scheme finds the optimal backup power unit capacity is five hours and the optimal backup power deployment density is 0.05. This solution means the operator can randomly pick 10 out of the 200 communication nodes to install a backup power unit, which can last for five hours.

II. RELATED WORK

The problem of cascading failures in interdependent networks has been presented in a survey in [10]. These existing works have adopted different levels of details on the physical characteristics of a power network. Some existing works such as [11] and [12], have considered a power network as a set of inter-connected nodes, just like a communication network. Without the specific physical characteristics of power flows in a power network, [13] has studied the system resilience by examining the impact of jointly induced cascading failures, which are caused by randomly disconnected power links and simultaneously broken communication nodes. Similarly, [14] has studied through computer simulations, the robustness of two interdependent networks under random failures and targeted attacks. In this simulation study, the power and communication network topologies are either random or scale-free.

The physical characteristics of a power flow as governed by the Kirchhoff’s law should be considered for an accurate study. In [15], the impact of communication latency on load-shedding in power network has been studied through simulations, where power flow takes the route with the smallest ohmic resistance. In [16], devices in communication network are treated as load in power network for accurate power flow calculation. The work [17] has quantified system robustness after considering failure of a power node will result in redistribution of its power flow to remaining nodes, upon which further failures in the power network may take place due to overloading. Here, the adoption of one-to-one interdependence model between networks has simplified the analysis, but is less realistic. Similar to [17], another work [18] has analyzed the system robustness with power flow redistribution after failures, but has used the percolation theory to model the behaviors of failure propagation. In both [17] and [18], the system robustness definition is the same as ours as described earlier. However, both works have not developed any method to improve or achieve a desired level of robustness.

System robustness can be achieved by fortifying or strengthening a set of critical nodes, removal of which can lead the system to complete collapse. Separately, [19] and [20] have proposed different methods to identify critical nodes. Instead of critical nodes, [21] has developed a method to identify the set of critical power lines and communication links, that can trigger a cascading failure process and result in a blackout when removed. The work [22] has found that
the communication network topology needs not be the same as the power network topology, and a slight change in the communication network topology can improve significantly the system robustness.

In [23], a scheme has been proposed to minimize the impact of cascading failures by optimally configuring the interdependence relations between power network and communication network. In a separate work, [24] has proposed a routing protocol for a communication network with interdependent power network. Here, communication routes are selected to minimize the impact of an inter-network cascading failure process between communication network and power network. The work [25] has formulated an integer linear program to find the desired number of interconnections between power network and optical communication network for resiliency against cascading failures initiated from a single node-failure. In [26], a communication-dependent cascading failure model has been proposed to capture the failure behaviors in a power network, where communication delay in delivering control commands plays a crucial role on the effectiveness of control strategies. Based on the model, a method has been designed to reduce the extension of a cascading failure process. In [27], cascading failures in interdependent networks are mitigated by dynamically readjusting generator dispatch and shedding loads, as the failures occur.

Based on the literature review above, as far as we know, there is no existing work that has proposed to deal with the problem of inter-network cascading failures in a smart grid through optimal deployment of backup power units in the communication network. This is a strong indication of the novelty of this work. This paper has proposed a novel scheme to identify the optimal backup power density and unit capacity that minimize the deployment cost without compromising a robustness requirement.

### III. SYSTEM MODEL

For ease of reference, we have summarized a list of symbols used in this paper in Table 1.

The system model consists of a power network and a communication network. The power network depends on the communication network to perform dynamic monitoring and control. Specifically, the communication network is needed to connect sensors and actuators which are installed at power nodes, to the control center. On the other hand, the communication network depends on the power network for electricity supply to operate various communication and computation equipments.

As illustrated in Figure 1, the communication network is modeled as a graph $\mathcal{G}_c = (\mathcal{V}_c, \mathcal{E}_c)$, where $\mathcal{V}_c$ is the set of communication nodes and $\mathcal{E}_c$ is the set of communication links. These communication nodes are routers that connect the sensors and actuators at power nodes to the control center.

The power network is modeled as a separate graph $\mathcal{G}_p = (\mathcal{V}_p, \mathcal{E}_p)$, where $\mathcal{V}_p$ is the set of power nodes and $\mathcal{E}_p$ is the set of power transmission lines. Each power node represents a small distribution network which is connected to one or more buses through substations. Within each distribution network, there are renewable power generators, load units and energy storage devices. As such, each power node can be a microgrid by itself.

| Symbol | Description |
|--------|-------------|
| $\mathcal{G}_c = (\mathcal{V}_c, \mathcal{E}_c)$ | $\mathcal{G}_c$ is the communication network, $\mathcal{V}_c$ is the set of communication nodes and $\mathcal{E}_c$ is the set of communication links. |
| $\mathcal{G}_p = (\mathcal{V}_p, \mathcal{E}_p)$ | $\mathcal{G}_p$ is the power network, $\mathcal{V}_p$ is the set of power nodes and $\mathcal{E}_p$ is the set of power transmission lines. |
| $P_{c,d}$ | Probability mass function of node degree $d$ for communication network. |
| $P_{p,d}$ | $P_{p,d}$ is the probability mass function of node degree $d$ for power network, with $\gamma$ as the node degree distribution coefficient. |
| $Q_{c,d}$ | Probability mass function of node degree $d$ for a neighbor node in communication network. |
| $\gamma$ | A communication node, which depends on power node $i$ for its electricity supply. |
| $h_i$ | A power node, which depends on communication node $i$ to as its gateway router to reach the control center. |
| $\rho$ | Backup power deployment density. |
| $\rho^*$ | Optimal backup power deployment density. |
| $\sigma$ | Probability of power node repair time exceeds backup power capacity. |
| $\sigma^*$ | Optimal probability of excessive power node repair time. |
| $T$ | Capacity of a backup power unit. |
| $\tau$ | Random variable representing repair time of a failed power node. Its probability density function is $f_T(x)$. |
| $S$ | Smart grid robustness. |
| $S_{min}$ | Smart grid robustness requirement. |
| $\psi_c$ | Probability of initial communication node failure. |
| $\psi_p$ | Probability of initial power node failure. |
| $\varphi_c$ | Critical probability of initial communication node failure. |
| $\varphi_p$ | Critical probability of initial power node failure. |
| $\phi_c$ | Probability of initial communication node survival. |
| $\phi_p$ | Probability of initial power node survival. |
| $u$ | Probability that the neighbor of a randomly selected communication network has been disconnected from the giant component at steady state, which is the state achieved at the termination of a cascading failure process. |
| $v$ | Probability that a power node has become non-functional, upon the termination of a cascading failure process. |
| $L$ | Random variable representing the load of a power node. Its probability density function is $f_L(x)$. |
| $Q$ | Random variable representing the generator’s set-point of a power node. Its probability density function is $f_Q(x)$. |
| $\alpha$ | Probability of load exceeds the uncontrollable generator’s set-point. |
| $\beta$ | Probability of load exceeds the island mode generator’s capacity. |
| $w_b$ | Cost of providing backup capacity of 1 hour to a communication node. |
| $\omega(\sigma, \rho)$ | Cost of providing backup power to communication network with deployment density $\rho$ and probability of excessive repair time $\sigma$. |
| $\lambda(a, b, c)$ | Function that determines the value of critical probability of initial power node failure when the probability of initial communication node failure is $a$, the probability of excessive repair time is $b$ and the backup power deployment density is $c$. |
| $\mu(a, b, c)$ | The inverse function of $\lambda(a, b, c)$ such that $\mu(a, b, \lambda(a, b, c)) = c$. Given a critical probability of initial power node failure $c$, $\mu(a, b, c)$ finds the corresponding backup power deployment density. |
For a randomly selected power node from $V_p$, its degree $d$ is a discrete random variable with probability mass function $P_{p,d}$. Similarly, we use $P_{c,d}$ to denote the probability mass function of degree $d$ for any randomly selected communication node from $V_c$.

Between $G_c$ and $G_p$, there are dependence links which indicate a need for support from one node to another node in a different network. Each power node $i \in V_p$ depends on a communication node $g_i \in V_c$ as its gateway router in a multi-hop path to reach the control center. Each communication node $i \in V_c$ depends on a power node $h_i \in V_p$ for its electricity supply. We do not assume the simplistic one-to-one interdependence relation, such as the one considered in [9] and [17]. In addition to the main electricity supply from power network, some communication nodes are also installed with a backup power unit to ensure continuous operation in case they lose their main electricity supply. We use $\rho$ to indicate the density of backup power deployment. Practically, $\rho$ indicates the fraction of communication nodes with a backup power unit, but not which specific node to deploy such a backup power unit. Given $G_c$, there are a total of $\rho|V_c|$ communication nodes, each with a backup power.

The capacity of a backup power unit is limited. Therefore, a communication node with backup power may still lose electricity supply if the power network is not restored fast enough. Let the backup power unit capacity be measured in terms of a supply duration $T$. We use $\tau$ to denote the power network repair time, which is a random variable with probability density function $f_\tau(x)$. Then, in the event of excessive repair time, a backup power unit will run out of its supply. The probability $\sigma$ of excessive repair time is determined as follows:

$$\sigma = \int_T^\infty f_\tau(x)dx.$$  

In probabilistic analysis of a power system, it is a common industrial practice to assume the repair time is an exponentially distributed random variable [28]. According to [29], this assumption is supported by data collected from Dutch and German power systems. Following the same assumption, $\tau$ is exponentially distributed with $f_\tau(x) = \overline{\tau}^{-1}e^{-x/\overline{\tau}}$, and $\overline{\tau}$ is mean value of $\tau$. As a result, $\sigma = e^{-T/\overline{\tau}}$.

### IV. NETWORK ROBUSTNESS WITH BACKUP POWER

Smart grid robustness measures the system resilience against initial removal of some nodes due to intentional malicious attacks or natural failures caused by hardware aging. A system is more robust if a larger part of the networks remain functional after a sequence of cascading failures which are triggered by the initial failures. In a smart grid, since the communication network plays only a supporting role to the power network, we quantify robustness $S$ as the fraction of power nodes that remain functional at the end of a dynamic cascading failure process. We develop a method to find $S$ in the rest of this section, and begin by deriving the probability of a communication node to become non-functional.

In a network, a connected component is a subset of nodes within which, each node is connected to all other nodes through a single-hop or multi-hop path. A network may have multiple isolated connected components. The largest connected component is called the giant component, which may or may not be the entire network. In the communication network analysis, a node is considered functional if and only if it is within the network’s giant component. This is a reasonable criterion for functionality because a communication node is a router. As long as the sensors and actuators of a power node are connected to a router within the giant component, they have a path to reach the control center which is assumed located within the component.

Let $\psi_c$ be the probability of initial communication node failure. Practically, $\psi_c$ is determined as the fraction of communication nodes that are removed (have failed) in the initial failure and $\psi_c = 1 - \phi_c$, where $\phi_c$ is the probability of initial communication node survival. Given $\phi_c$, we use the two-stage percolation theory [30] to determine the fraction of communication nodes that will remain in the giant component after a series of cascading failures. In the literature, percolation theory is an useful tool to study the statistical properties of failure propagation through a networked system of nodes and to analyze the fractal properties of percolating clusters [31].

According to percolation theory, at the steady-state, a communication node is in the giant component if it has not failed initially and not all its neighbors have been disconnected from the giant component. We use $u$ to denote the probability that the neighbor of a randomly selected communication node has been disconnected from the giant component at the steady-state, upon the termination of a cascading failure process. A neighbor communication node may have been disconnected from the giant component in the following cases:

- The node is one of the nodes in the initial failure. This case occurs with probability $1 - \phi_c$.
- All neighbors of the node have been disconnected from the giant component. Given \( P_{c,d} \) is the node degree probability mass function as defined earlier, the node degree probability mass function of the neighbor node’s neighbor, which is called the excess degree probability and has been determined in [32] as follows:

\[
Q_{c,d} = \frac{(d+1)P_{c,d+1}}{\sum_{i=0}^{\infty} P_{c,i}}.
\]

(2)

In the equation, summation in the denominator goes to infinity to account for the chance that a node’s neighbor’s neighbor having infinite number of neighbors. Given \( Q_{c,d} \), this case occurs with probability \( \sum_{d=0}^{\infty} Q_{c,d}u^d \).

- The node has lost its main electricity supply from power network and it has no backup power. We use \( v \) to denote the probability that a power node has failed, i.e., has become non-functional at the steady-state upon termination of the cascading failure process. A failed power node can no longer supply electricity to its dependent communication node. Thus, given the backup power deployment density \( \rho \), this case occurs with probability \( v(1 - \rho) \).

- The node has lost its main electricity supply from power network and it has backup power. But, the backup power has run out before the main electricity supply is restored. Given \( \sigma \) that has been determined earlier in (1), this case occurs with probability \( v\rho \sigma \).

Combining all the four cases above, probability \( u \) can be determined using the percolation theory [33] as follows:

\[
u = 1 - \phi_c + \phi_c \left( \sum_{d=0}^{\infty} Q_{c,d}u^d + v(1 - \rho + \rho \sigma) \right).
\]

(3)

Notice that (3) is a balance equation, which characterizes the smart grid steady-state which is reached at the end of a dynamic cascading failure process as exemplified in Figure 2. In the figure, with reference to the four cases presented above, failure propagates from a power node to its dependent communication node, if the communication node has no backup power unit, or it has backup power unit but the repair time has exceeded a limit.

In (3), we notice that the failure probability of a communication node depends on the failure probability of a power node. With interdependence between communication network and power network, failure probability of a power node also depends on that of a communication node. However, the failure criterion for power node is different from that of communication node. Specifically, a power node that is not a part of the power network’s giant component may remain functional. Recall that each power node is a distribution network which is connected to the main power network through at least one substation. Within the distribution network, there are generators, load units and energy storage devices. Here, the load may include but not solely, communication and computation equipments in the communication network. A power node is considered non-functional only if its load has no electricity supply and thus, cannot operate. As such, when a power node is disconnected from the power network, it may remain functional in island mode as long as its generator and energy storage can still provide sufficient electricity to supply its load. Following this same criterion, a power node is also functional even if its generator is broken, as long as it is still connected to the power network and its load may continue to operate with electricity supplied by other neighboring power nodes, which may not be within its immediate neighborhood.

Recall that, for a communication node with a backup power unit, the impact of failure in its electricity source can be deferred. Such deferment does not exist when a
communication node fails. Given the communication node repair time is a positive number larger than zero, a failure in a router will lead to an immediate loss of communication route of its dependent power node.

Let \( \psi_p \) be the probability of initial power node failure. Practically, \( \psi_p \) is determined as the fraction of power nodes that are removed in the initial failure and \( \psi_p = 1 - \phi_p \), where \( \phi_p \) is the probability of initial power node survival. After completing a sequence of cascading failures, a power node may have lost electricity supply to its load in the following cases:

- The node is one of the nodes in the initial failure. This case occurs with probability \( 1 - \phi_p \).
- A power node may perform load shedding as a mechanism to protect the system from excessive loading. In a normal operating condition, excessive loading does not normally happen because generator output can be dynamically adjusted by the control center to match the load. These adjustments are done in the form of changing the generator’s operating set-point. When the power node loses its communication connection to the control center, the generator output is no longer remotely controllable through the secondary control. However, the generator can continue its operation with local primary (droop) control around an existing set-point. After the set-point becoming unchangeable by the control center, the generator is turned off and the load is shed. Let \( L \) be the load of a power node, and it is a random variable with probability density function \( f_L(x) \). Recall that generator output is dynamically adjusted to match the load. Therefore, we assume the generator output has a stochastic characteristic similar to that of the load. Let \( G \) be the last generator output set-point before the power node losing its communication path and thus, its probability density function \( f_G(x) = f_L(x) \). Then, after the loss of communication connection, the generator output remains at \( G \) while the load continues to vary. We define \( Z = L - G \) as the difference between load and generator output, and \( f_Z(x) \) is the probability density function of \( Z \). Then, load shedding is performed when \( Z \) is larger than zero. This probability \( \alpha \) of load exceeds the uncontrollable generator output is given as follows:

\[
\alpha = \int_0^\infty \int_0^y f_L(x+y)f_G(x)dx\,dy.
\]  

As one of the load models reviewed in [34], if \( L \) is exponentially distributed such that \( f_L(x) = \bar{L}^{-1}e^{-x/\bar{L}} \), where \( \bar{L} \) is the mean value of \( L \); then, \( f_Z(x) = (2\bar{L})^{-1}e^{-x/\bar{L}} \) and \( \alpha = 1/2 \). Recall that the probability of a power node losing its communication path equals the probability \( u \) of a communication node being not connected to the giant component. Hence, this case happens with probability \( au \).

- A power node may receive electricity from its neighbor nodes to supply its own load. This allows the load to remain functional after the local generator becoming broken. However, such support from neighbors is not available if all of the neighbors have shed their respective loads. Without electricity supply from neighbors, a power node must also shed its own load if the load \( L \) exceeds its local generator capacity \( C \). The probability \( \beta \) of a power node’s load exceeds its generator capacity is determined as follows:

\[
\beta = \int_C^\infty f_L(x)dx.
\]  

If \( L \) is exponentially distributed as in [34], with the mean load equals to \( \bar{L} \), then \( \beta = e^{-C/\bar{L}} \). Given \( P_{p,d} \), the probability that all the neighbors of a power node have shed their respective load is determined as \( \sum_{d=0}^\infty P_{p,d} v^d \). Then, this case occurs with probability \( \beta \sum_{d=0}^\infty P_{p,d} v^d \). Combining all the three cases described above, probability \( \nu \) of a power node can be determined using the percolation theory [33] as follows:

\[
\nu = 1 - \phi_p + \phi_p (\alpha u + \beta \sum_{d=0}^\infty P_{p,d} v^d).
\]  

Similar to (3), (6) is another balance equation, which characterizes the smart grid steady-state at the end of a dynamic cascading failure process. With reference to Figure 2 and the three cases presented above, failure propagates to a power node if it loses its communication route to the control center and its load has exceeded its previous operating set-point, or it operates in an island mode and its load has exceeded its generator capacity.

Both (3) and (6) are parallel equations that can be solved concurrently to find \( u \) and \( v \). Unfortunately, there is no closed form expression for the solutions, due to the existence of infinite summations in both equations. Also, there is no guarantee that a solution exists because (3) and (6) may not intersect for all values of \( u \) and \( v \) within the range of 0 to 1. The non-existence of a solution indicates inability of the cascading failure process in reaching a steady-state with some surviving nodes. Practically, this means a complete collapse where all nodes in the system will fail after a cascade of failures have been triggered by some initial node failures as specified by \( \psi_p \) and \( \psi_c \).

Imagine that if too many nodes have failed in the initial stage, it is likely that no node will survive at the end of a cascading failure process. Therefore, it is reasonable to think that the existence of solution to (3) and (6) depends on the values of \( \psi_p \) and \( \psi_c \). In the absence of closed form expressions for \( u \) and \( v \), we have made some coarse approximations in Appendix VII to linearize the infinite summations to show that there exist some critical upper limits for \( \psi_p \) and \( \psi_c \), denoted respectively by \( \psi_p' \) and \( \psi_c' \) as follows:

\[
\psi_p \leq \psi_p' = 1 - \frac{\rho(\sigma - 1) + q_1}{(1 - \alpha)(1 - \rho + \rho \sigma) - P_{p,1}(1 - q_1)},
\]
\[ \psi_c \leq \psi_c' = 1 - \frac{\alpha + P_{p,1}\beta - 1}{\alpha(\rho - \rho \sigma - Q_{c,0}) - Q_{c,1}(1-P_{p,1}\beta)}, \]  
(8)

where \( q_1 = Q_{c,0} + Q_{c,1} \). We call \( \psi_p \) and \( \psi_c' \) respectively the critical probability of initial power and communication node failure. We emphasize that these critical probabilities \( (\psi_p' \text{ and } \psi_c') \) of initial node failure are not the same as the probabilities of initial power node failure \( (\psi_p \text{ and } \psi_c) \). These critical probabilities are the upper limits of their respective initial failure probabilities. Given that the probability of initial node failure \( (\psi_p \text{ and } \psi_c) \) is below its critical value \( (\psi_p' \text{ and } \psi_c') \), respectively and thus, there is solution for \( v \), a complete system collapse can be avoided.

We have followed the existing literature in defining smart grid robustness as the steady-state fraction of surviving power nodes at the end of a cascading failure process. Then, given that there is no complete system collapse, the robustness is calculated as \( S = (1 - \psi_p)(1 - v) = \phi_p(1 - v) \). Specifically, it is the fraction of power nodes which have not failed initially and remain functional at steady-state.

V. BACKUP POWER COST OPTIMIZATION

Given a probability \( \psi_p \) of initial power node failure and a probability \( \psi_c \) of initial communication node failure, our objective is to minimize the cost of providing backup power to communication nodes without compromising the system robustness requirement \( S_{\text{min}} \), which is measured in terms of an acceptable fraction of surviving power nodes at the end of a cascading failure process. We begin by deriving the cost function.

Recall that the probability \( \sigma \) of excessive repair time depends on the capacity \( T \) of a backup power unit. In order to achieve a smaller \( \sigma \), we need a bigger capacity for each backup power unit. For a target value of \( \sigma \), the cost of providing necessary backup power capacity is \( -w_b \ln \sigma \), where \( w_b \) is the cost of providing backup capacity of 1 hour to one communication node. The value of \( w_b \) can be changed according to the adopted backup power technology. Here, we consider only the cost of battery packs but no the supporting system and maintenance. Nevertheless, the cost formulation can be readily modified to account for such additional cost, which may be non-linear. This can be done by replacing the per unit cost \( w_b \) with a non-linear function \( w_b(\bar{T}) \). Given the backup power installation density \( \rho \), the total cost of providing backup power to the communication network is determined as follows:

\[ w(\sigma, \rho) = -\rho|V_c|w_b \ln \sigma. \]  
(9)

Given \( \psi_p, \psi_c \) and \( S_{\text{min}} \) as user-specify parameters, the minimization of backup power cost can be formulated as a constrained optimization below:

\[ \min_{\alpha, \rho} \quad w(\sigma, \rho), \]  
\[ s.t. \quad (1 - \psi_p)(1 - v) \geq S_{\text{min}}, \]  
\[ \sigma \leq \arg \min_b [\lambda(\psi_c, b, \rho) - \psi_p'], \]  
\[ \rho \geq \mu(\psi_c, \sigma, \psi_p). \]  
(13)

In this formulation, \( \sigma \) and \( \rho \) are the only optimization variables. According to (3) and (6), system robustness should also depend on \( \alpha \) and \( \beta \). However, we do not include \( \alpha \) and \( \beta \) as optimization variables because they are consumer’s load characteristics which are beyond the operator’s control. Constraint (11) enforces the robustness requirement through the three user-specify parameters. In this constraint, robustness depends not only on \( \psi_p \) but also on \( \psi_c \) through \( v \).

In constraint (12), \( \lambda(\alpha, \sigma, c) \) is a function that determines the value of critical probability \( \psi_p' \) of initial power node failure when the probability of initial communication node failure is \( a \), the probability of excessive repair time is \( b \) and the backup power deployment density is \( c \). Figure 3 illustrates an example of \( \lambda(\alpha, \sigma, c) \). From the figure and (7), we see that a higher backup power density can lead to a higher \( \psi_p' \). Therefore, with a higher backup power density, the system can tolerate a higher probability of initial node failure in avoiding a complete collapse, but this will also incur a higher cost. Ideally, we want \( \psi_p' \) to only equal to the given requirement \( \psi_p \), because a higher \( \psi_p' \) will incur a higher cost in providing additional robustness beyond the requirement. For this reason, the right hand side of constraint (12) finds the largest probability of excessive repair time such that the critical probability of initial power node failure is as close as possible to, but not smaller than \( \psi_p \). Then, this biggest probability of excessive repair time must not be exceeded by optimization variable \( \sigma \).

In constraint (13), \( \mu(\alpha, \beta, c) \) is the inverse function of \( \lambda(\alpha, \sigma, c) \) such that \( \mu(\alpha, \beta, \lambda(\alpha, \sigma, c)) = c \). Specifically, given a critical probability of initial power node failure \( c \), \( \mu(\alpha, \beta, c) \) finds the corresponding backup power deployment density. An example of \( \mu(\alpha, \beta, c) \) can be found in Figure 3. Right hand side of constraint (13) determines the smallest backup
power deployment density which is required when ψ' equals to the requirement ψ. Then, this smallest backup power deployment density forms the lower limit for any feasible value of the optimization variable ρ.

The is no closed-form expression for both function λ(a, b, c) and μ(a, b, e). We determine their values numerically. For a given set of three input variable values, a sequence of corresponding system robustness is determined by stepping through the probability of initial node failure. Then, the function value is determined as the largest value of the probability of initial node failure, beyond which the system robustness value becomes zero. As an example to find the function value is determined as the largest value of the ping through the probability of initial node failure. Then, of corresponding system robustness is determined by step-cally. For a given set of three input variable values, a sequence must not exceed the critical probability of initial power node failure. λ Then, too few in some cases. We need an efficient method to search met. This is because the number of surviving nodes can be there is no guarantee that the robustness requirement can be region, although a complete system collapse can be avoided, minimization (10) is not trivial partly due to the lack of closed form expressions for solution to (3) and (6). Within a solution region, although a complete system collapse can be avoided, there is no guarantee that the robustness requirement can be met. This is because the number of surviving nodes can be too few in some cases. We need an efficient method to search the region for a set of σ and ρ that meets the robustness requirement with minimum cost.

We notice that ψ' and ψ' are non-decreasing with respect to a decrease in σ or an increase in ρ. Hence, increasing ψ' implies an increase in backup power deployment cost. Therefore, with reference to Figure 4, the lowest cost can be achieved at the lower left or right corner of the solution region. There is no certainty that the lowest cost is at the left or right corner because the left corner has a smaller σ (need a bigger backup power capacity) as well as a smaller ρ (need fewer number of backup power units). We propose Algorithm 1 to search the region from the lower left or right corner, for the first set of σ and ρ that meets the robustness requirement.

Before describing the operational details, we present Figure 5 to illustrate the concept of Algorithm 1. The algorithm is recursive in nature, and each iteration anchors on three points at the solution region boundary. As depicted in Figure 5, these points are named A, B and C, respectively. Notice that point C of an iteration becomes point A of the next iteration. The first iteration starts at point A and B on the horizontal line ψ' = ψ, which is the lower boundary of the solution region. Through a sequence of successive iterations, the algorithm searches for a combination of σ and ρ, along the line between point A and B as well as the line between point B and C, in the direction of increasing backup power deployment cost.

In every iteration, each of the three points are defined by three variables namely xi, yi and zi for point i ∈ {A, B, C}. For a point i, xi indicates its values of the critical probability of initial power node failure, yi indicates its value of the probability of excessive repair time, and zi indicates its value of the backup power deployment density. For each iteration, these three points are inter-related. Specifically, point A and B have a same value of the critical probability of initial power node failure such that xA = xB. On the other hand, point B and C have a same value of the backup power deployment density such that zB = zC. Algorithm 1 begins the first iteration by defining point A with xA = ψ, yA = 0 and zA = μ(ψ, ψ, xA) in line 2. Based on this point A, the corresponding coordinate for point B can be determined in line 5 asxB = xA, xB = arg maxz [λ(ψ, c), yB = arg minz(λ(ψ, b, c) − ψ)], c = ψ] and xB = arg minz(λ(ψ, b, c) − ψ)]. After finding the coordinates of point A and B, the coordinate for point C is subsequently determined in line 6 as zC = xB, yC = yA and xC = λ(ψ, ψ, yC, zC).

It is not certain that point A has a lower or higher cost than point B because while point A has a smaller ρ, it has also a larger σ. From line 7 to 11, Algorithm 1 first finds the lower cost point between A and B. This lower cost point is called the start point and the other point is called the
Algorithm 1 Recursive Search Algorithm for Optimal $\sigma$ and $\rho$

1: SolutionFound = false.
2: $x_C = \psi_p, y_C = 0$ and $z_C = \mu(\psi_c, y_C, x_C)$.
3: while SolutionFound is false do
4:   Define point A: $x_A = x_C, y_A = y_C$ and $z_A = z_C$.
5:   Define point B: $x_B = x_A$.
6:      $z_B = \arg\max\{\lambda(\psi_c, \arg\min_b\{\lambda(\psi_c, b, c) - 
7:       \psi_p\}^+, c) = \psi_p\}$ and
8:      $y_B = \arg\min_b\{\lambda(\psi_c, b, z_B) - \psi_p\}^+$.
9:   Define point C: $z_C = z_B, y_C = y_A$ and
10:      $x_C = \lambda(\psi_c, y_C, z_C)$.
11: if A has lower cost than B then
12:   A is start point and B is end point.
13: else
14:   SolutionFound = false.
15: end if
16: if start point meets robustness requirement then
17:   $\sigma^* = \psi_{\text{start point}}$.
18:   $\rho^* = \psi_{\text{start point}}$.
19: else if end point meets robustness requirement then
20:   Perform linear search from start point to end point on the line connecting the two points, to find the first $\rho$ that meets the robustness requirement, and mark this found $\rho$ the $\rho^*$.
21:    $\sigma^* = \arg\min_b\{\lambda(\psi_c, b, \rho^*) - x_A\}^+$.
22: else if point C meets robustness requirement then
23:   Perform linear search from point B to point C on the line connecting the two points, to find the first $\psi_p^*$ that meets the robustness requirement, and mark this found $\psi_p^*$ as $\psi_p^*$.
24:    $\sigma^* = \arg\min_b\{\lambda(\psi_c, b, z_B) - \psi_p^*\}^+$.
25: end if
26: else
27:   SolutionFound is false.
28: end while
29: cost = $-\rho^*|\psi_c|w_b\tilde{r}\ln\sigma^*$.

end point. They are literally the start and end point of a search process for solution. If the start point can meet the robustness requirement $S_{\text{min}}$, it will lead to the minimum cost and the algorithm terminates. Upon termination as expressed between line 13 to 15, the optimal backup power deployment density $\rho^*$ equals to $z_i$ of the start point $i$, and the optimal probability of excessive repair time $\sigma^*$ equals to $y_i$ of the start point $i$. If the start point cannot satisfy the robustness requirement, the algorithm examines three different possible cases as follows:

- **Case-1: End point satisfies robustness requirement.**
  Line 16 to 18 performs linear search for a solution from the start point to the end point, on the line connecting the two points. Find the first backup power density that satisfies the robustness requirement, as the optimal backup power deployment density $\rho^*$. Given $\rho^*$, determine the corresponding optimal probability of excessive repair time as $\sigma^* = \arg\min_b\{\lambda(\psi_c, b, \rho^*) - x_A\}^+$.

- **Case-2: End point does not satisfy robustness requirement but point C does.**
  Line 19 to 22 marks the optimal backup power deployment density $\rho^* = z_B$. Perform linear search for a solution from point B to point C on the line connecting the two points. Find the first critical probability of initial power node failure that satisfies the robustness requirement, as the optimal critical probability of initial power node failure $\psi_p^*$. Given $\psi_p^*$, determine the corresponding optimal probability of excessive repair time as $\sigma^* = \arg\min_b\{\lambda(\psi_c, b, \rho^*) - \psi_p^*\}^+$.

- **Case-3: Both end point and point C do not satisfy robustness requirement.**
  Line 24 starts a new iteration.

In the new iteration, line 4 to 6 makes the current point C as the new point A and then, find the corresponding new point B and point C, using the same method described above for the first iteration. In short, point A and B are on a same horizontal line, while point B and C are on a same vertical line, in the solution space.

The recursive process will eventually terminates with a set of $\rho^*$ and $\sigma^*$ identified as the solution that satisfy the robustness requirement $S_{\text{min}}$. Then, the backup power deployment cost is determined in line 27 as $-\rho^*|\psi_c|w_b\tilde{r}\ln\sigma^*$.

In Algorithm 1, the number of iterations is upper bounded, because the solution region as illustrated in Figure 4 and Figure 5, is bounded. In the worst case, the final iteration will have only Point A and Point B, on the horizontal line with the critical probability of initial power node failure equals to 1. In this final iteration, there is no Point C because the critical probability cannot exceed 1. We quantify complexity of the proposed Algorithm 1 based on the number of times the robustness requirement is checked upon. Let $I$ be the maximum number of iterations. In each iteration, the robustness requirement is checked as many as $\Delta_{AB}/\delta$ times between point A and point B, where $\Delta_{AB}$ is the difference in backup power density between the two points and $\delta$ is the search step size. Similarly, the number of checks between point B and point C is $\Delta_{BC}/\delta$, where $\Delta_{BC}$ is the difference in critical probability of initial power node failure between the two points. In the worst case, the maximum number of robustness requirement checks in each iteration is $\Delta_{AB}/\delta + \Delta_{BC}/\delta$. Since both the backup power density and critical probability of initial power node failure are limited within 0 and 1, we find $I \times \Delta_{AB} \leq 1$ and $I \times \Delta_{BC} \leq 1$. Therefore, the maximum number of robustness requirement checks across all iterations is $2/\delta$. As such, the complexity of the big O notation is $O(1/\delta)$.

VI. PERFORMANCE EVALUATION

We have performed extensive simulations to evaluate the proposed backup power deployment scheme. In these evaluations, the following parameter values are assumed unless
stated otherwise: $|V_p| = 500, |V_c| = 500, \rho = 1, \sigma = 0, \alpha = 0.5, \beta = 0.5, \phi_p = 1$ and $\phi_c = 1$. For interdependence relation of each communication node, its electricity source is randomly selected from the power nodes within a coverage radius. Similarly, for each power node, its communication gateway is randomly selected from the communication nodes within a coverage radius. This is a very pragmatic consideration because in a real-world situation, a communication node will not draw its electricity supply from a faraway power node, and a power node will not connect to the communication network through a router that is not within its reach.

Following the practice in [9] and [14], the communication network is modeled as a random network. According to [35] and [36], the power network is scale-free with power-law node degree distribution, such that $P_{p,d} \sim d^{-\gamma}$, and $2 < \gamma < 3$. The scale-free power network is generated using the Barabasi-Albert (BA) algorithm [37]. In the algorithm, nodes are successively added to the network until the desired network size is achieved. For each added node, $m$ edges are generated. For these new edges, the endpoints are selected from the existing nodes in the network, with a bias towards the nodes with a high degree. With BA algorithm, we cannot specify a desired power-law exponent $\gamma$, but parameter $m$ will affect $\gamma$. Through a series of simulations, we have determined the value $m$ which should be used for a desired $\gamma$. For simplicity, we do not present these simulation results here. In short, an increasing $m$ can lead to a larger $\gamma$ and we use $m = 3$ to achieve $\gamma = 2.5$ unless stated otherwise.

Figure 6 compares the simulation results with theoretical results. For these comparisons, the theoretical values are calculated using the average value of $\gamma$ for the simulated networks with corresponding $m$. In the figure, we notice that the theoretical and simulation results follow a same trend quite closely to each other. Nevertheless, the theoretical values are lower bounds to the simulation values. This is because the theoretical results are calculated using the average value of $\gamma$ while the simulations are performed by setting $m$ in the BA algorithm. As such, the theoretical calculations have underestimated the number of nodes with high degree of a few tens. With a significant number of nodes with some high degrees, more communication nodes remain in the giant component and fewer power nodes disconnect their load.

Thus, the simulated system is more robust compared to the theoretical model. Figure 6 shows only results for $\rho = 1.0$ and $\rho = 0.5$. For smaller values of $\rho$, it is more likely that the theoretical results will show a complete system collapse while there are still surviving nodes in the simulations.

In Figure 6, we confirm the argument by (7) and (8) that there exists a critical value of the initial node survival probability, below which the system will collapse all together with no power node survives at the end of a cascading failure process. For example, in Figure 6(c) for $\rho = 0.5$ and $\phi_c = 0.7$, robustness is equal to 0 for probability of initial power node survival smaller than 0.86. In this case, if there are more than 13% of power nodes fail in the initial stage, the whole system will collapse. As indicated by (7) and (8), this critical probability of initial node failure depends on the system configurations. Comparing Figure 6(b) and Figure 7, we notice that an increase in $\sigma$ due to a reduction in backup power unit capacity for potential cost saving, will lead to a lower robustness.

Figure 8 shows the critical probability of initial power node failure for various configurations. In the figure, increasing probability $\sigma$ of excessive power node repair time will lead to a lower critical probability of initial failure. For example, in Figure 8(b), when $\sigma$ increases gradually from 0.0 to 0.1 and finally to 0.2, the critical probability of initial failure decreases from 0.4 to 0.3 for $\rho = 0.6$. This means the system can tolerate a smaller number of initial node failures for a...
larger $\sigma$. In applying these results, we should understand that the critical probability of initial failure indicates only the existence of a non-zero robustness if the actual initial failure probability is lower than the critical value, but not the robustness itself. For example, we know that there will be a non-zero robustness if the initial failure probability is lower than 0.4 for $\rho = 0.6$ and $\sigma = 0.0$, but we cannot tell from the figure the actual robustness value, which can be a very small number.

Figure 9 shows the normalized backup power deployment cost. It is a normalized cost because we let $w_b = 1$ for ease of comparison. In the figure, the cost increases when there is an increase in the probability of initial node failure in either the communication network or the power network. Comparing Figure 9(a) to Figure 9(b), there is an increase in the cost for a larger network. While the robustness requirement remains unchanged, the trend in the cost increment is simply a linear scaling of the network size. This is consistent with the cost function developed in Section IV. When the network size remains unchanged, given a larger probability of initial node failure, an increase in the robustness requirement can significantly increase the cost, as indicated by a change in the cost trend between Figure 9(a) and Figure 9(c). Specifically, compared to a robustness requirement 0.1 in Figure 9(a), the cost for larger values of initial node failure probability, has increased exponentially in Figure 9(c) for robustness requirement 0.5. Based on Figure 9(c), for a case with 25% of power nodes and 15% of communication nodes fail initially, a total deployment cost of 998.76 times $w_b$ is needed for a system of 100 communication nodes, to achieve a robustness of 0.5, which means half of all power nodes should survive at steady-state. From Figure 9(a), the deployment cost is only 96.88 times $w_b$ for the same system configuration but with a lower robustness requirement of 0.1.

Figure 10 compares with backup power deployment cost achieved by the proposed scheme against that of a full deployment. For the full deployment, each backup power unit can last as long as 2 times the average repair time of a power node. For this comparison, the probability of initial power node failure is 0.05.

Figure 10 demonstrates the benefits of the proposed scheme over a full deployment. The proposed scheme significantly reduces the cost, especially for higher failure probabilities. For instance, at 20% initial failure probability, the cost for the proposed scheme is only 10% of the full deployment cost.
power node failure is 0.05, but similar results are seen for other initial power node failure probabilities. The proposed scheme can achieve a noticeably lower cost compared to full deployment, and the cost advantage is clearer for a smaller probability of initial communication node failure. This is because the proposed scheme can find the smallest cost in fulfilling the robustness requirement given some operating conditions, while the full deployment method is incapable of exploiting a favorable operating condition to lower its cost.

VII. CONCLUSION

We have proposed installing backup power units at communication nodes to interrupt inter-network failure propagation. We have used two-stage percolation theory to model the cascading failure process. Based on the model, we can find the critical probability of initial node failure. We have confirmed that if the probability of initial node failure exceeds the corresponding critical probability, the system will end in a complete collapse. If the critical probability is not exceeded, the cascading failure process can reach a steady-state with some surviving power nodes. At the steady-state, system robustness is a function of backup power deployment density and backup power unit capacity. We have proposed a scheme to find the optimal backup power deployment density and backup power unit capacity to minimize the backup power deployment cost, without compromising a desired level of system robustness. Simulation results confirm that an increase in network size will only increase the cost linearly. On the other hand, an increase in robustness requirement can lead to an exponential increase in cost.

APPENDIX

In this appendix, we show that there is a maximum value for the probability of initial node failure, above which there is no solution to equations (3) and (6). We begin by making the approximation \( \sum_{k=0}^{\infty} P_{p,k}u^k \approx P_{p,0} + P_{p,1}v \) and \( \sum_{k=0}^{\infty} Q_{c,k}u^k \approx Q_{c,0} + Q_{c,1}u \). These approximations consider only the first two terms of an infinite summation. As illustrated in Figure 11, the approximations are more accurate for smaller values of \( u \) and \( v \). More specifically, for \( v = 0.01 \), the approximated value account for more than 99% of the actual value. With the approximations, we can rewrite (3) and (6) as follows:

\[
\begin{align*}
    u &= 1 - \phi_c + \phi_c(Q_{c,0} + Q_{c,1}u + (1 - \rho + \rho\sigma)v), \\
    v &= 1 - \phi_p + \phi_p(\alpha u + \beta(P_{p,0} + P_{p,1}v)).
\end{align*}
\]

From (14),

\[
    v = \frac{\phi_c(1 - Q_{c,0}) + (1 - \phi_c Q_{c,1})u - 1}{\phi_c(1 - \rho + \rho\sigma)}. \tag{18}
\]

Substituting (18) into (15) and knowing that \( P_{p,0} = 0 \), we can obtain the equation (16), as shown at the bottom of the page, for \( u \). As a probability, \( u \leq 1 \) and thus, we further derive the inequality (17), as shown at the bottom of the page.

From (17), it is trivial that \( \phi_c \) must be larger than 0 because if the probability of initial communication node survival is zero, there will be no surviving node for the whole system as soon as the failure process starts. From the second factor on the left hand side,

\[
    \phi_p \geq \frac{Q_{c,0} + Q_{c,1} + \rho(\sigma - 1)}{(1 - \alpha)(1 - \rho + \rho\sigma) - \beta P_{p,1}(1 - (Q_{c,0} + Q_{c,1}))}. \tag{19}
\]

This inequality states the minimum probability of initial power node survival that is necessary to avoid a complete system collapse. In (19), the denominator must be positive and thus, \( (1 - \alpha)(1 - \rho + \rho\sigma) \) must be greater than \( \beta P_{p,1}(1 - (Q_{c,0} + Q_{c,1})) \). Then, it is reasonable that a smaller probability of initial node survival will require a larger backup power deployment density \( \rho \). In the same line of thought, it is feasible to tolerate a larger probability \( \sigma \) of excessive repair time only if there are more nodes that have survived in the initial failure stage. Since the probability of initial power node failure \( \psi_p = 1 - \phi_p \), we have the followings:

\[
\begin{align*}
    \psi_p \leq & 1 - \frac{Q_{c,0} + Q_{c,1} + \rho(\sigma - 1)}{(1 - \alpha)(1 - \rho + \rho\sigma) - \beta P_{p,1}(1 - (Q_{c,0} + Q_{c,1}))}, \tag{20}
\end{align*}
\]

\[
\begin{align*}
    u &= \frac{1 + \phi_p(1 - \phi_p)(1 - \rho + \rho\sigma) + \phi_p\beta P_{p,1}(1 - Q_{c,0} - 1)}{(1 - \phi_c Q_{c,1})(1 - \phi_c \beta P_{p,1}) - \alpha \phi_c \phi_p(1 - \rho + \rho\sigma)} - \phi_c (1 - Q_{c,0}) - (1 - \rho + \rho\sigma)(1 - \phi_p) - \phi_p\beta P_{p,1}(1 - Q_{c,0}) - Q_{c,1} + Q_{c,1}\phi_p\beta P_{p,1} - \alpha \phi_p(1 - \rho + \rho\sigma) \geq 0. \tag{17}
\end{align*}
\]
Using the same approach presented above for \( p_i \), we can show that the probability \( \psi_i \) of initial communication node failure is also upper bounded as follows:

\[
\psi_i \leq 1 - \frac{\alpha + p_{i,1}^\beta - 1}{\alpha + p_{i,1}^\beta - 1} \left( \rho_{i,0} - \sigma_{i,0} - Q_{i,0} - (1 - p_{i,1}^\beta) \right). \tag{21}
\]

REFERENCES

[1] S. Liu, P. X. Liu, and A. E. Saddik, “Modeling and stability analysis of automatic generation control over cognitive radio networks in smart grids,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 45, no. 2, pp. 223–234, Apr. 2015.

[2] The Emerging Interdependence of the Electric Power Grid & Information and Communication Technology, document PNNL-24643, Pacific Northwest National Laboratory, Aug. 2015.

[3] J.-C. Tournier and T. Werner, “A quantitative evaluation of IEC61850 process bus architectures,” in Proc. IEEE PES Gen. Meet., Jul. 2010, pp. 1–8.

[4] G. Andersson, P. Donalek, R. Farner, N. Hatzigiayriou, I. Kanwra, P. Kundur, N. Martins, J. Paschina, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, “Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance,” IEEE Trans. Power Syst., vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[5] R. Mattioli and K. Moulinos, “Communication network interdependencies in smart grids: Methodology for the identification of critical communication networks links and components,” Eur. Union Agency Netw. Inf. Secur. (ENISA), Athens, Greece, Tech. Rep., 2015.

[6] P.-Y. Kong, “Cost efficient data aggregation point placement with interdependent communication and power networks in smart grid,” IEEE Trans. Smart Grid, vol. 10, no. 1, pp. 74–83, Jan. 2019.

[7] M. Rahnamay-Naeini and M. M. Hayat, “On the role of power-grid and communication-system interdependencies on cascading failures,” in Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP), Dec. 2013, pp. 527–530.

[8] Z. Ma, J. Eichman, and J. Kurtz, “Fuel cell backup power system for grid-service and micro-grid in telecommunication applications,” J. Energy Resour. Technol., vol. 141, no. 6, Jun. 2019, Art. no. 62002.

[9] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” Nature, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.

[10] X. Liu, B. Chen, C. Chen, and D. Jin, “Electric power grid resilience with interdependencies between power and communication networks—A review,” IET Smart Grid, vol. 3, no. 2, pp. 182–193, May 2019.

[11] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, “Networks formed from interdependent networks,” Nature Phys., vol. 8, no. 1, pp. 40–48, Jan. 2012.

[12] X. Yuan, Y. Hu, H. E. Stanley, and S. Havlin, “Eradicating catastrophic collapse in interdependent networks via reinforced nodes,” Proc. Nat. Acad. Sci. USA, vol. 114, no. 13, pp. 3311–3315, Mar. 2017.

[13] J. Wang, S. Pambudi, W. Wang, and M. Song, “Resilience of IoT systems against edge-induced cascade-of-failures: A networking perspective,” IEEE Internet Things J., vol. 6, no. 4, pp. 6952–6963, Aug. 2019.

[14] Robustness in Interdependent Networks, Oxford Univ., Oxford, U.K., Mar. 2014.

[15] E. Zio and G. Sansavini, “Vulnerability of smart grids with variable generation and consumption: A system of systems perspective,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 43, no. 3, pp. 477–487, May 2013.

[16] M. Parandehgheibi, E. Modiano, and D. Hay, “Mitigating cascading failures in interdependent power grids and communication networks,” in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Oct. 2014, pp. 242–247.

[17] Y. Zhang and O. Yagan, “Robustness of interdependent cyber-physical systems against cascading failures,” IEEE Trans. Autom. Control, vol. 65, no. 2, pp. 711–726, Feb. 2020.

[18] Z. Huang, C. Wang, T. Zhu, and A. Nayak, “Cascading failures in smart grid: Joint effect of load propagation and interdependence,” IEEE Access, vol. 3, pp. 2520–2530, 2015.

[19] D. T. Nguyen, Y. Shen, and M. T. Thai, “Detecting critical nodes in interdependent power networks for vulnerability assessment,” IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 151–159, Mar. 2013.