A Stochastic Modeling Approach for Cascading Failures in Cyberphysical Power Systems

Gongyu Wu, *Member, IEEE*, Meiyan Li, and Zhaojun Steven Li, *Senior Member, IEEE*

***Abstract*—This article proposes an approach based on the stochastic process and approximate dynamic behavior for modeling cascading failures of the cyberphysical power system (CPPS) considering component multistate failures. Our approach focuses on modeling the coupling effects of interdependencies of the integrated power and communication networks, including control and power supply dependencies as well as the effects of the degradation of one network performance on the other. Nine failure states of each component and the performance/capacity degradation in different failure states are incorporated into the modeling approach. The state transitions between nine failure states are modeled as a discrete time Markov process whose transition probabilities are time-varying. In addition, the article proposes a new robustness measure for multistate CPPS, which integrates the information of the local and global topology, the damage state of components, as well as the performance degradation of the CPPS. The system that couples the IEEE 118-bus model with a small-world communication network is used as a testbed to demonstrate the feasibility and effectiveness of the proposed modeling approach, and the comparison with existing robustness measures shows the superiority of the proposed measure.**

***Index Terms*—Couplings, cybernetics, failure analysis, robustness, stochastic process.**

NOMENCLATURE

i_P	Index for nodes in the power network.
i_c	Index for nodes in the communication network.
i_{pc}	Index for all nodes in the power and communication networks.
j_p	Index for power transmission branches in the CPPS.
j_{pc}	Index for both power and communication transmission branches in the CPPS.
k	Index for all nodes and branches in the CPPS.
k_{pc}	Index for all power nodes, branches, and communication nodes in the CPPS.
ε	Constant coefficient used as the base of an exponential function.
ω	Constant coefficient used to calculate the state transition probability.
N_N^p	Total number of nodes in the power network.
N_N^{pc}	Total number of power and communication nodes in the CPPS.
N_B^{pc}	Total number of power and communication branches in the CPPS.
N_B^m	Number of branches on the island m.
N_L^p	Number of LNs in the power network.
Deg_m	Total degree of nodes on the island m.
$l_{j_p}(t)$	Power loads of the j_pth power transmission branch obtained by the power flow calculation at time t.
l_{i_p}	Loads received by the i_pth load node.
$r_{j_p}^A(t)$	Long term rating of the j_pth power transmission branch at time t.
$f_{\max}^O$	Short-time maximum allowable overload rate for each power transmission branch.
$I_{j_p}^O$	Impact of the factor of the overload on the mean of the damage distribution for the j_pth power branch at time t.
$I_{j_p}^N$	Impact of the factor of the network congestion on the mean of the damage distribution for the j_pth power branch at time t.
$I_{j_p}^D$	Impact of the factor of the operation in the damaged state on the mean of the damage distribution for the j_pth power branch at time t.
$\Gamma_C(j_p)$	Set of communication nodes in the network to which the power branch j_p belongs.
r_m	Number of remaining nodes in the CPPS after removing m nodes.
$\|\text{lcc}_m\|$	Number of nodes in the largest connected component after m nodes are removed.
$\overline{\kappa}(G)$	Average connectivity of the network G.
$\kappa_G(u,v)$	Connectivity between nodes u and v in the network G.
$a_{i_p i_c}^{\text{con}}(t)$	Element in the adjacency matrix of control dependencies at time t, indicating whether the power node i_p can be controlled by the communication node i_c, i.e., $a_{i_p i_c}^{\text{con}}(t)=1$, if it can be controlled; $a_{i_p i_c}^{\text{con}}(t)=0$, otherwise.
$S_{i_p}^{sp}(i_c,t)$	Binary variable which is used to indicate whether the shortest path of information transmission for the power node i_p passes through the communication node i_c at time t, i.e., $S_{i_p}^{sp}(i_c,t)=1$, if it passes; $S_{i_p}^{sp}(i_c,t)=0$, otherwise.

Manuscript received July 7, 2020; revised November 12, 2020 and March 9, 2021; accepted March 23, 2021. Date of publication April 23, 2021; date of current version March 24, 2022. *(Corresponding author: Zhaojun Li.)*

Gongyu Wu is with the School of Mechanical and Electrical Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: wu_gongyu@163.com).

Meiyan Li is with the Department of Industrial Engineering, Shandong University of Science, and Technology, Qingdao 266510, China (e-mail: limeiyanqdu@163.com).

Zhaojun Steven Li is with the Department of Industrial Engineering and Engineering Management, Western New England University, Springfeld, MA 01119 USA (e-mail: stevenli777@gmail.com).

Digital Object Identifier 10.1109/JSYST.2021.3070503

$S_k^C(t)$ Binary variable which is used to indicate whether the kth component is connected to the network at time t, i.e., $S_k^C(t) = 1$, if connected; $S_k^C(t) = 0$, otherwise.

Abbreviations and Acronyms

CPPS	Cyberphysical power system.
SN	Power supply node.
SLN	Both power supply and load node.
LN	Load node.
TN	Transformation node.
LCC	Local control center.
ALC	Area load dispatch center.
SLC	State load dispatch center.
RCC	Regional control center.

I. Introduction

THE cyberphysical system integrates computation, communication, and control systems for realizing the real-time perception and dynamic control between its physical and cybersystems. The smart grid, which is the integration of power (i.e., the physical system) and communication (i.e., the cybersystem) networks, is a typical CPS [1], i.e., cyberphysical power system (CPPS). The power network is monitored and controlled by control centers with smart devices, such as phasor measurement units (PMUs) and automatic generation controls (AGCs) [2]. These control centers can be divided into four levels, including local control centers (LCC), area load dispatch centers (ALC), state load dispatch centers (SLC), and regional control centers (RCC) [3]. Control centers at all levels can achieve the real-time data interaction through the communication network to continuously optimize the operation of the power network, which ensures a safe, efficient, and reliable power supply [4]. In turn, each control center needs to be powered by the power network.

The interdependencies of the CPPS can bring great values to the society. However, the CPPS is more vulnerable to disturbances due to such coupling dependencies [5]. When a node in one network fails, the nodes that depend on it in the other network may also fail, and vice versa. This process may continue recursively, resulting in cascading failures of the entire system, and eventually leading to large-scale blackouts. One of the well-known examples is the blackout happened in Italy in September 2003 [6]. The origins in this event came from two 400-KV high-voltage transmission lines interrupted by the heavy rain. These initial failures spread through power and communication networks and eventually affected about half the area of the country. Such cases are not rare. According to the United States records, such regional blackouts caused by extreme disasters account for 58% of total outages observed since 2003–2012, and cost 18 billion dollars a year [7]. As a result, the governments and researchers have realized the importance of the recovery strategies in face of such inevitable extreme events. The research emphasis has been placed on enhancing the CPPS resilience [8]–[10]. However, the propagation mechanism of failures within the CPPS (i.e., the cascading failure model of the CPPS), which is the critical foundation of developing recovery strategies and enhancing the CPPS resilience, is still not well investigated in the literature.

Most of the existing research on cascading failure models of CPPSs focuses on a single power network, rather than the interdependent CPPS. These models can be broadly divided into two categories. One is the complex network-based model [11], [12], the other is the approximate dynamic behavior-based model [13]–[15]. These models are of great importance for modeling cascading failures of a single power network. However, the actual power network is coupled with the communication network and cannot operate independently.

Existing research on cascading failure models, which takes into account the coupling effects of interdependencies within CPPSs, is very few. Buldyrev *et al.* [16] proposed a cascading failure model for the CPPS to study the vulnerability of the Italian power grid based on the penetration theory. The "one-to-one" interdependencies between the power and communication networks are considered in their model. Specifically, they assumed that each node has one and only one bidirectional dependence to the node of the interdependent network. If a node in the power network fails, the connected node in the communication network will also fail, and vice versa. One of the improved models based on the "one-to-one" interdependencies can be found in [17]. However, the power and control dependencies in the actual CPPS are usually interdependent and equipped with redundancies, which violates the "one-to-one" interdependency assumption [4].

Only a few researchers have explored the power and control dependencies in the CPPS. For example, Huang *et al.* [18] modeled the power and control dependencies separately as one-way dependencies. On the basis of their research, Chen *et al.* [19] introduced the control threshold of power network, that is, some nodes of the power network need to be controlled by multiple communication nodes, such as the multiple wide-area control. However, they ignored that only the distribution substations (i.e., load nodes) can provide power for the communication node in the actual CPPS. In addition, the structure and operating mechanism of the communication network are not involved in their research. For these reasons, Wang *et al.* [20] proposed a general communication network modeling method. The regional control methods for large-scale CPPSs are also considered in their research. Moreover, Guo *et al.* [21] modeled the communication nodes as three levels of nodes, including LCC, ALC, and RCC. In their model, random failures of power or communication nodes due to overload, hidden failures, and failures of control centers have been studied.

In summary, most of the existing research on cascading failure models of CPPSs focus on a single power network, rather than the interdependent CPPS. A few research works, which involves coupling effects of interdependencies within the CPPS, also considered simple abstractions or approximations of interdependencies, such as "one-to-one" interdependencies. Especially the impact of network congestion on the power network has not been well investigated. In addition, most existing researchers share the common assumption that the failure states of each component is binary, i.e., state is equal to 1, if working; state is equal to 0, otherwise. However, the failures of components usually present multiple states in the actual CPPS, and the impact of components in different failure states on the CPPS

performance is often unique. One of very few research that considers multistate failures mainly focuses on the state transitions from the perspective of the system, but did not consider the operating mechanisms of the CPPS and dynamic impact of the performance degradation of each component on the CPPS [22]. Therefore, the main contributions of this article are summarized as follows.

A stochastic modeling approach based on approximate dynamic behavior for cascading failures of CPPSs considering component multistate failures: Nine failure states of each component and the capacity degradation in different failure states are incorporated into the cascading failure model for the first time. The state transitions between nine failure states are modeled as a discrete time Markov process whose transition probabilities are time-varying and depend on the current failure states, time-varying failure rates, and the states of protection/isolation devices. During state transition processes, power and information flows are updated by the approximate dynamic behavior-based model and complex network-based model, respectively. Time-varying failures, which are caused by the overload, network congestion, and continuous operating in the damaged state, are modeled as stochastic processes. In addition, the response time of implementing artificial mitigation measures and the threshold of power required for each communication node are also included in our approach.

A new robustness measure for multistate CPPSs, which integrates the information of the local and global topology, the damage state of components, as well as the performance degradation of the CPPS. The local topology is quantified by the network average connectivity, which reflects the connectivity and redundancy of information and communication flows. The global topology is measured by Newman's modularity metric, which shows whether the system is divided into isolated islands, i.e., the presence of community structures. The performance degradation is evaluated by the rate of loads supplied, which can reflect the performance of the CPPS directly. The damage state of components is quantified by the average damage rate of all components in the CPPS, which can reflect the periods required for system repair after a disturbance.

The remainder of this article is structured as follows. Section II introduces the proposed modeling approach of cascading failures and robustness measure for CPPSs. In Section III, the CPPS, which couples the IEEE 118-bus with a small-world communication network, is used as a testbed to demonstrate the feasibility and effectiveness of the proposed modeling approach, and the comparison with existing robustness measures shows the superiority of the proposed measure. Section IV concludes this article.

II. Proposed Modeling Approach and Robustness Measure

A. Proposed Modeling Approach for Cascading Failures

1) Modeling the Physical Power Network: The power network is modeled as a weighted undirected graph with N_N^p nodes, where the weight represents the actual distance between nodes. Four categories of power nodes are considered: 1) power supply only node (SN); 2) load only node (LN); 3) both power supply and load node (SLN); and 4) transformation node (TN). In addition, these nodes are divided into multiple connected areas.

2) Modeling the Cybercommunication Network: The communication network is modeled as a weighted undirected graph with $N_N^p + 1$ nodes. Three levels of communication nodes, including LCCs, ALCs, and RCCs, are considered. Specifically, each power node is, respectively, configured with a unique communication node near it for monitoring and controlling [18]. These communication nodes can be LCCs or ALCs, but there is one and only one ALC in any power area. Each LCC sends the real-time status data of the power node it controls to the ALC, which manages this power area. The ALC makes use of the information obtained from LCCs to implement economic power dispatch and optimization for the power area managed by this ALC. Meanwhile, each ALC will interact with the highest level center (i.e., RCC) in real time for optimal dispatching power flows across areas.

The paths of the information uploading and distribution are assumed to be the same. Meanwhile, the information is always transmitted along the weighted shortest path. Specifically, the information always flows first through the nearest ALC, and is eventually uploaded to the RCC, and vice versa. The communication network can also operate normally when there is no RCC in this network, but each power area controlled by this communication network cannot interact with other power areas. In addition, at least one working ALC is required for a communication network to operate normally.

From the above, the information processing capacity of the i_cth communication node at time t, $c_{i_c}(t)$, can be calculated as in (1). The maximum capacity of the i_cth communication node at time t, $c_{i_c}^{\max}(t)$, are set to be 1.25 times its initial capacities $c_{i_c}(t)$ in our research, i.e., the initial capacity is about 80% of the maximum capacity.

$$c_{i_c}(t) = \begin{cases} \sum\limits_{i_p}^{N_N^p} a_{i_p i_c}^{\text{con}}(t), & \text{for LCCs} \\ \sum\limits_{i_p}^{N_N^p} S_{i_p}^{sp}(i_c, t), & \text{for ALCs and RCCs.} \end{cases} \tag{1}$$

3) Modeling Interdependencies Within the CPPS: The control and power supply dependencies between the power and communication networks can be modeled as the directed branch sets, respectively. Fig. 1 shows an example of the CPPS. Each power node depends on the control of the neighboring LCC or ALC. In contrast, each communication node is powered by the load node (i.e., LNs or SLNs) near it. Meanwhile, some critical communication nodes are equipped with emergency power supplies, and some critical power nodes are equipped with redundant control and monitoring branches. These critical nodes can be identified based on the degree, betweenness, or other importance measures. In addition, this article assumes that the power threshold required by each LCC for normal operation is T_p^{LCC} (any unit), and the power threshold required by both ALC and RCC is T_p^{AR} (any unit). These powers come from the dependent power nodes, emergency power supplies, or the combination of them.

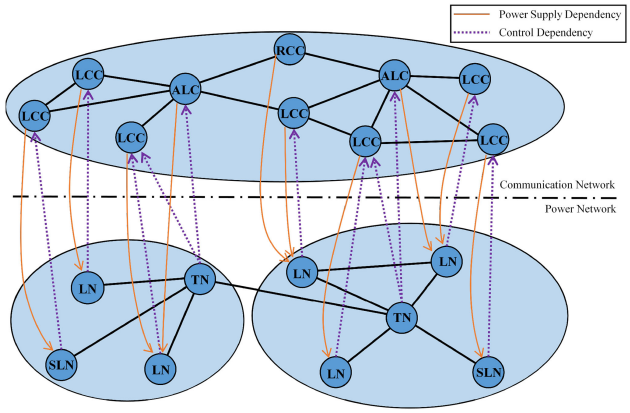

Fig. 1. Example of cyberphysical interdependencies in a two-area CPPS.

TABLE I
RELATIONSHIP BETWEEN THE DAMAGE RATE OF THE kTH COMPONENT, D_k, AND ITS NINE FAILURE STATES

No.	Failure State	Damage Rate (D_k)
1	Normal or Nearly Normal	$0\% \le D_k < 10\%$
2	Slightly Damaged	$10\% \le D_k < 20\%$
3	Moderately Damaged	$20\% \le D_k < 45\%$
4	Severely Damaged	$45\% \le D_k < 80\%$
5	Completely Damaged	$80\% \le D_k \le 100\%$
6	Normal or Nearly Normal (disconnected)	$0\% \le D_k < 10\%$
7	Slightly Damaged (disconnected)	$10\% \le D_k < 20\%$
8	Moderately Damaged (disconnected)	$20\% \le D_k < 45\%$
9	Severely Damaged (disconnected)	$45\% \le D_k < 80\%$

TABLE II
FOUR FUNCTIONAL TYPES OF COMPONENTS AND THEIR CRITICAL CAPACITY DEGRADATION

Functional Type	Components Involved	Capacities Degraded
Power supply	SN and SLN	The maximum/minimum reactive/active output
Load	LN and SLN	The reactive/active power demand
Power Transmission	All power transmission branches	The long/short term and the emergency rating
Information Processing	LCC, ALC, and RCC	The maximum information processing capacity

4) Multistate Failures and Performance/Capacity Degradation of Each Component: On the basis of our previous work [23], the failures of each component can be further divided into nine failure states based on their damage rates, maintenance modes, and the periods required for repair, which is described in Table I.

Similar to previous work [23], this article assumes that all nodes and branches in the CPPS have the same nine failure states as described in Table I, and the critical capacities for four functional types of components in failure state 3 will be degraded as described in Table II. The degraded capacities of each component can be calculated by the product of their initial capacities and damage rates.

5) Three Failure Causes and Their Probabilities During the Cascading Failure Propagation: When the capacities of one or multiple components are affected by a disturbed event, the power flows usually need to be redistributed to satisfy the end-user demand. The redistribution of power flows may cause overload of certain generating nodes (e.g., SN and SLN) or power transmission branches. These overloaded generating nodes will be protected and isolated from the network through the protective devices they are equipped with, such as breakers, if they cannot be regulated. The overloaded power transmission branches are allowed to continue to work for a short period without exceeding their short-time maximum allowable overload rate ($f^O_{\max}$) [21]. The overload rate of the j_pth power transmission branch at time t, $f^O_{j_p}(t)$, can be calculated as follows:

$$f^O_{j_p}(t) = \begin{cases} \frac{l_{j_p}(t) - r^A_{j_p}(t)}{r^A_{j_p}(t)}, \text{if } r^A_{j_p}(t) < l_{j_p}(t) \le r^A_{j_p}(t)(f^O_{\max}+1) \\ 0, \qquad\qquad \text{else.} \end{cases} \tag{2}$$

The overload will put power branches at risk of failures. In general, the higher the overload rate of a power transmission branch is, the higher the failure probability of this branch is and the faster its failure probability increases. This property of the power branch can be characterized by the exponential function. Hence, the failure probability of the j_pth power transmission branch caused by its overload at time t, $P^O_{j_p}(t)$, can be calculated by the following:

$$P^O_{j_p}(t) = \omega_1(\varepsilon_1^{f^O_{j_p}(t)} - 1),\ \varepsilon_1 > 1. \tag{3}$$

In terms of the communication network, the degradation or complete loss of the information processing capacity of any communication node may make it impossible to process the monitoring and control information in real time, resulting in network congestion. For example, if the ALC of an power area is completely failed, the power nodes in this area will be allocated to ALCs of other areas according to the weighted shortest path to control. In this case, if the capacity of an ALC is insufficient to process the information of the allocated power nodes, this ALC will become congested. The network congestion rate of the i_cth communication node at time t, $f^N_{i_c}(t)$, can be calculated as follows:

$$f^N_{i_c}(t) = \begin{cases} \frac{c_{i_c}(t) - c^{\max}_{i_c}(t)}{c^{\max}_{i_c}(t)}, & \text{if } c_{i_c}(t) > c^{\max}_{i_c}(t) \\ 0, & \text{else.} \end{cases} \tag{4}$$

The network congestion of communication nodes does not cause damage to the components in the CPPS directly, but such communication nodes will delay receiving and sending real-time monitoring and control information of the power nodes under control. The states of these power nodes affected by the network congestion are unnoticed and uncontrolled during the delay, and these affected power nodes continue to carry out the decisions given by the communication network before the congestion occurs. In this case, some undesirable events may happen, for example, the generation node does not adjust the output power as planned; the power network does not perform line switching properly; and the communication network makes and issues power control and dispatching decisions using outdated data of

the power network. Such events have the potential to overload each branch in the power network connected with congested communication nodes, thus, exposing these branches to the risk of failure and damage. The more the number of communication nodes is congested and the higher the congestion rate of each node is, the longer the delay is the higher the probability of the above-mentioned undesirable events occur. That is, it means that the higher the failure probability of this branch is the faster its failure probability increases. The influences of network congestion on the power network are complex and diversified, which can hardly be fully described. Hence, this article simplifies these influences to a scaling factor ω_2 to describe the average failure probability of the power branch due to network congestion. The network congestion rate and the failure probability caused by the network congestion of the j_pth branch in the power network at time t (i.e., $f_{j_p}^N(t)$ and $P_{j_p}^N(t)$) can be calculated by the following:

$$f_{j_p}^N(t) = \Psi(f_i^N(t)\,|i \in \Gamma_C(j_p)) \tag{5}$$

$$P_{j_p}^N(t) = \omega_2(\varepsilon_2^{f_{j_p}^N(t)} - 1),\ \varepsilon_2 > 1 \tag{6}$$

where $\Psi(\bullet)$ is an arbitrary monotone increasing function on the interval of $(0, +\infty)$, and its value is equal to 0 if all variables are 0. $\Psi(\bullet)$ is used to indicate that the combination of multiple congested communication nodes will have a greater impact on the j_pth power branch than that of any single congested node, but less than the sum of the respective impacts of these congested node on the power branch.

Another risk of failures for power nodes, branches, and communication nodes comes from their continuous operations in the damaged state. Specifically, slightly and moderately damaged components (i.e., power nodes, branches, and communication nodes in failure states 2 and 3) can keep in the operating state, but the damaged electrical equipment in these components are also at risk of deteriorating to their failure states. The higher the current damage rate of a component is, the higher the degradation probability of this component is and the faster its degradation probability increases. Note that if the failure of a node is not caused by the damage of its electrical equipment (e.g., the cyberattack on a communication node), the failure probability of this node caused by its continuous operation in the damaged state is equal to 0. The failure probability of the k_{pc}th damaged component caused by its continuous operating in the damaged state at time t, $P_{k_{pc}}^D(t)$, can be calculated as follows:

$$P_{k_{pc}}^D(t) = \begin{cases} \omega_3(\varepsilon_3^{D_{k_{pc}}(t)} - 1), & \text{if } 0.1 < D_{k_{pc}}(t) \le 0.45 \\ 0, & \text{else} \end{cases} \tag{7}$$

where ε_3 is greater than 1, i.e., $\varepsilon_3 > 1$.

The above-mentioned three failures are assumed to be independent. Components, which are actively disconnected by protective devices, are still functional and can be reconnected to the network at any time. In addition, the scaling factors ω_1, ω_2, and ω_3 are related to the failure probability of components, which can be estimated from the component's historical failure data using statistical methods.

6) Discrete Time Markov Process for Transitions Between Nine Failure States: The transitions between failure states of each component in the CPPS satisfy the Markov property since the next states of the components are only related to their current states [21], [22]. The transitions between nine failure states for each power transmission branch can be modeled as a discrete time Markov chain, as shown in Fig. 2. Our research focuses on the propagation of cascading failures, so recovery measures are not considered in Fig. 2.

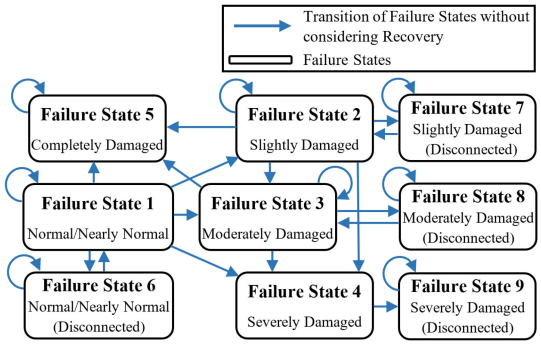

Fig. 2. Discrete time Markov process for transitions between nine failure states without considering recovery: for power transmission branches.

The four-parameter beta distribution has a finite domain, constrained between $D_k(t)$ and 1, which can be used to represent damage levels ranging from the current damage rate of a component to collapse. Second, the beta distribution is fully characterized by only two shape parameters and two bound parameters, and can flexibly model a broad variety of shapes, skewness, and curvature. In addition, through the extensive postearthquake damage data following the 2010 earthquake in Haiti, Lallemant and Kiremidjian [24] demonstrated that the beta distribution is suitable to model the damage distribution. For these reasons, the four-parameter beta distribution is chosen to establish the distribution of the damage rate $D_k(t)$ of each component. Specifically, two shape parameters of the beta distribution at time t, $\hat{\alpha}(t)$ and $\hat{\beta}(t)$, can be estimated by the mean μ and standard deviation σ from the real historical failure data

$$\hat{\alpha}(t) = \mu^{fr}\left[\frac{\mu^{fr}(1-\mu^{fr})}{(\sigma^{fr})^2} - 1\right] \tag{8}$$

$$\hat{\beta}(t) = (1-\mu^{fr})\left[\frac{\mu^{fr}(1-\mu^{fr})}{(\sigma^{fr})^2} - 1\right] \tag{9}$$

where

$$\mu^{fr} = \frac{\mu - D_k(t)}{1 - D_k(t)},\ \text{and}\ \sigma^{fr} = \frac{\sigma}{1 - D_k(t)} \tag{10}$$

where the purpose of (10) is to convert the mean and standard deviation to the form that is applicable to the four-parameter beta distribution. The μ and σ of damage distributions for different types of components can be calculated by the method-of-moments and maximum likelihood estimate-based formulations according to historical grouped categorical damage data [24]. The remainder of this section provides an estimation method for the μ and σ of damage distributions when there is insufficient historical data.

As mentioned in the previous section, the failures of power transmission branches are related to three factors, including the overload operation, network congestion, and continuous operation in the damaged state. In general, the higher the overload rate or damage rate of a power branch is, the more likely it is to deteriorate into a worse failure state (i.e., the closer the mean is to 1) and the faster the mean of the damage distribution for this branch increases. Then, the estimated value of the mean of damage distributions for the j_pth power transmission branch at time t, $\hat{u}_{j_p}(t)$, can be formulated as in the following:

$$\hat{u}_{j_p}(t) = D_{j_p}(t) + \omega_4[1 - D_{j_p}(t)]\Phi(S_f^O(t)I_{j_p}^O(t), S_f^N(t)I_{j_p}^N(t) \quad S_f^D(t)I_{j_p}^D(t)) \tag{11}$$

where

$$I_{j_p}^O(t) = \frac{\varepsilon_4^{f_{j_p}^O(t)} - 1}{\varepsilon_4^{f_{\max}^O} - 1},\ \varepsilon_4 > 1 \tag{12}$$

$$I_{j_p}^D(t) = \frac{\varepsilon_5^{D_{j_p}(t)} - 1}{\varepsilon_5 - 1},\ \varepsilon_5 > 1 \tag{13}$$

$$\Phi(\bullet) = \begin{cases} \Phi(\bullet), & \text{if } 0 \le \Phi(\bullet) \le 1 \\ 1, & \text{else} \end{cases} \tag{14}$$

where (11) ensures that the range of the mean is located in $(D_{j_p}(t), 1]$. $I_{j_p}^N(t)$ is assumed to be a constant in the range of (0,1] to represent the average impact. Equations (12) and (13) ensure that the ranges of $I_{j_p}^O(t)$ and $I_{j_p}^D(t)$ are located in (0,1]. $\Phi(\bullet)$ is an arbitrary monotone increasing function on the interval of [0,1], and its value is equal to 0 if all variables are 0. $\Phi(\bullet)$ is used to indicate that the combination of factors will have a greater impact on the mean than that of any single factor, but less than the sum of the respective impacts of these factors on the mean. Equation (14) restricts the result of $\Phi(\bullet)$ to the interval of [0,1]. The failure probability of the j_pth power branch at time t, $P_{j_p}^f(t)$, can be calculated as $1 - [1 - P_{j_p}^O(t)][1 - P_{j_p}^N(t)][1 - P_{j_p}^D(t)]$. $S_f^O(t)$, $S_f^N(t)$, and $S_f^D(t)$ are binary variables, which indicate that whether the failure is caused by corresponding factors, e.g., $S_f^O(t) = 1$, if the failure is caused by overload; $S_f^O(t) = 0$, otherwise. When a power branch fails, this failure may be caused by a single factor or a combination of multiple factors. These three failure factors can be grouped into seven different combinations of failure causes. The probability that the failure is caused by certain combination can be calculated by the probability formulas. For example, when a power branch that is affected by both overload and network congestion fails, the probability that this failure is caused by the branch's overload operation, i.e., $S_f^O(t) = 1$, $S_f^N(t) = 0$, and $S_f^D(t) = 0$, can be calculated as $P_{j_p}^O(t)(1 - P_{j_p}^N(t))(1 - P_{j_p}^D(t))$. After the probability of all combinations are calculated, the roulette wheel selection method is used to randomly select one of them as the failure cause of the failed power branch.

The standard deviation of damage distribution for power branches is also a variable. Taking the overload failure of power branches as an example, when a power branch with a low overload rate fails, the failure state of this branch tends to transfer to the adjacent state or stay at the current state. In contrast, when a component with a high overload rate fails, the failure state of this branch tends to transfer to one of the failure states between its current and the worst failure state. That is, the uncertainty of the damage rate of the power branch with a high overload rate is higher than that of the branch with a low overload rate. In order to characterize this property, the estimated value of the standard deviation for damage distributions of the j_pth power transmission branch at time t, $\hat{\sigma}_{j_p}(t)$, can be formulated as in the following:

$$\hat{\sigma}_{j_p}(t) = \frac{R_{j_p}[1-D_{j_p}(t)][\omega_5+(1-\omega_5)\Phi(I_{j_p}^O(t), I_{j_p}^N(t), I_{j_p}^D(t))]}{6} \tag{15}$$

where R_{j_p} represents the proportion of the maximum six sigma interval for the damage distribution of the j_pth power branch, and its value is located in (0,1). R_{j_p} can be estimated through historical data and experience. The purpose of the item $R_{j_p}(1-D_{j_p}(t))$ is to convert the applicable interval of R_{j_p} from [0,1] to $[D_{j_p}(t), 1]$. The item $\omega_5+(1-\omega_5)\Phi(I_{j_p}^O(t), I_{j_p}^N(t), I_{j_p}^D(t))$ ensures that the range of the standard deviation is located in $[\omega_5, 1]$.

The failures of power and communication nodes during cascading failures are caused by a single factor of the continuous operation in the damaged state. The Markov chain for power and communication nodes can also be expressed as the model shown in Fig. 2, but the links from failure state 1 to failure states 2, 3, 4, and 5 need to be removed. The estimated values of the mean and standard deviation for damage distributions of the i_{pc}th power or communication node at time t, i.e., $\hat{u}_{i_{\text{pc}}}(t)$ and $\hat{\sigma}_{i_{\text{pc}}}(t)$, can be formulated as in the following equations, respectively:

$$\hat{u}_{i_{\text{pc}}}(t) = D_{i_{\text{pc}}}(t) + \omega_6[1 - D_{i_{\text{pc}}}(t)]I_{i_{\text{pc}}}^D(t) \tag{16}$$

$$\hat{\sigma}_{i_{\text{pc}}}(t) = R_{i_{\text{pc}}}[1 - D_{i_{\text{pc}}}(t)][\omega_7+(1-\omega_7)I_{i_{\text{pc}}}^D(t)]/6. \tag{17}$$

The estimated values of mean and standard deviation can be substituted into (8)–(10) to obtain the damage distribution of each component at time t. Taking the power transmission branch in failure state 2 as an example, the calculation methods of states transition probabilities for the j_pth branch from failure state 2–3 and 7 at time t (i.e., $P_{j_p(23)}^p(t)$ and $P_{j_p(27)}^p(t)$), are shown as follows:

$$P_{j_p(23)}^p(t) = \frac{S_{j_p}^C(t)P_{j_p}^f(t)}{[1 - D_{j_p}(t)]^{\hat{\alpha}_{j_p}(t)+\hat{\beta}_{j_p}(t)-1}B(\hat{\alpha}_{j_p}(t), \hat{\beta}_{j_p}(t))} * \int_{0.2}^{0.45} [x - D_{j_p}(t)]^{\hat{\alpha}_{j_p}(t)-1}(1 - x)^{\hat{\beta}_{j_p}(t)-1}dx \tag{18}$$

$$P_{j_p(27)}^p(t) = 1 - S_{j_p}^C(t) \tag{19}$$

where $B(\alpha, \beta) = (\Gamma(\alpha) + \Gamma(\beta))/\Gamma(\alpha + \beta)$ is the beta function, and $\Gamma(\alpha)$ is the gamma function. The states transition probabilities of components in other failure states can be calculated in the similar methods using (18) and (19).

7) Proposed Cascading Failure Model of the CPPS: This article assumes that a response time (ΔT) is needed to implement artificial mitigation measures after a disturbance to

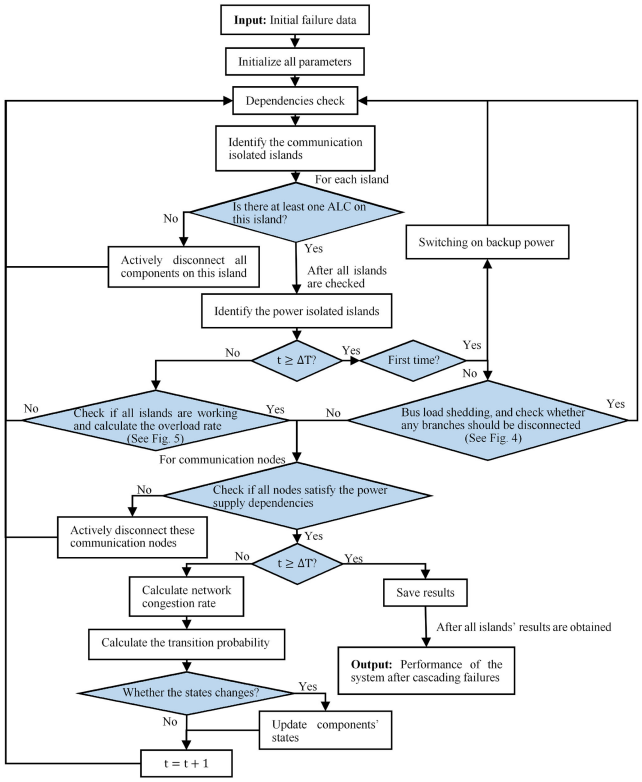

Fig. 3. Proposed cascading failure modeling procedure of the CPPS.

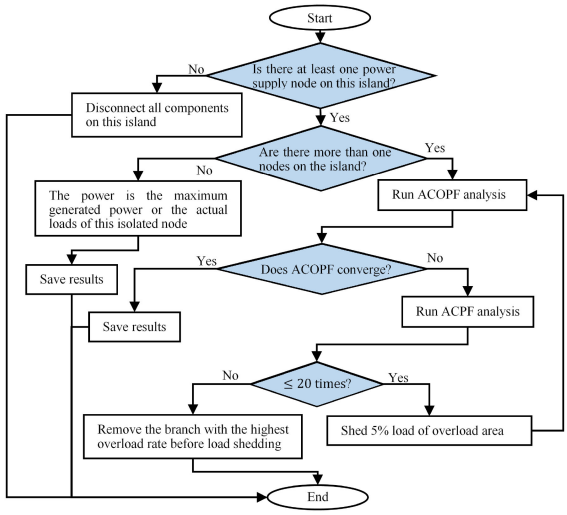

Fig. 4. Calculation method of power flows and self-optimization method for the power network with implementing mitigation measures.

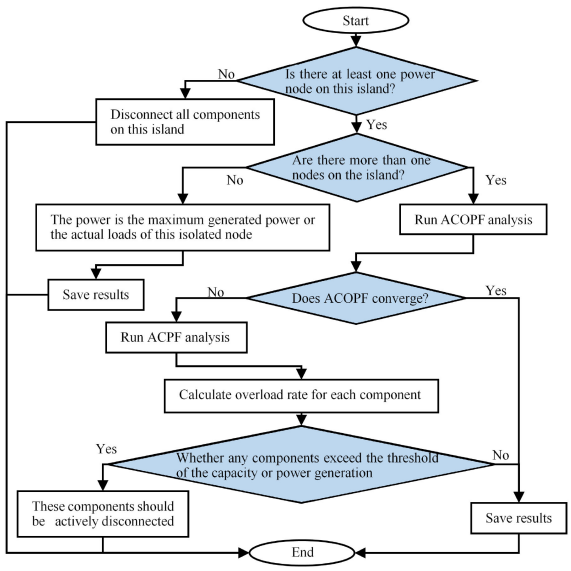

Fig. 5. Calculation method of power flows and self-optimization method for the power network without implementing mitigation measures.

restore the system to the safe and stable operating state. The implementation of such mitigation measures depends on subjective human decisions. For instance, the mitigation measures, such as initiating the standby servers or manually distributing congested information to the spare nodes, can effectively release the network congestion. In terms of the power network, the mitigation measures, such as switching on backup power or shedding the loads of certain node, can effectively ensure the safe and stable operation of the network. The proposed cascading failure modeling scheme of the CPPS considering component multistate failures is described in Fig. 3.

The steps of the proposed cascading failure modeling procedure are as follows: *S1:* Initialize all parameters, including parameters used in (2)–(17), the topology structure of the CPPS, as well as electrical parameters of the power network. *S2:* Check the dependencies of each component to disconnect or reconnect components. *S3:* Update the topological structure and identify communication isolated islands. *S4:* Check if there is at least one ALC on each communication island. If yes, go to *S5*; otherwise, all communication components on this island cannot work and return to *S2*. *S5:* Identify power isolated islands and check if mitigation measures have been implemented. If yes, go to *S6*; otherwise, go to *S8*. *S6:* Check if the backup power of the communication node has been switched ON. If yes, go to *S7*; otherwise, switch it ON and return to *S2*. *S7:* Perform the steps shown in Fig. 4 to calculate the power flows on each power island and check if any components need to be disconnected. If yes, return to *S2*; otherwise, go to *S9*. *S8:* Perform the steps shown in Fig. 5 to calculate the power flows on each power island, and check if any components need to be disconnected. If yes, return to *S2*; otherwise, go to *S9*. *S9:* Check whether there is sufficient power supply for each of the surviving communication nodes. If yes, go to *S10*; otherwise, disconnect the node whose power supply is insufficient, then return to *S2*. *S10:* Check if mitigation measures have been implemented. If yes, save the results and the iteration stops; otherwise, go to *S11*. *S11:* Calculate the network congestion rate according to (4) and (5). *S12:* Calculate the state transition probabilities for each component according to the approach proposed in Section III-A.6. *S13:* Update the failure states and the damage rates of components whose states changed. Then, execute $t = t + 1$ and return to *S2*.

Figs. 4 and 5 show the calculation methods of power flows and self-optimization methods for each isolated power island with and without implementing mitigation measures, respectively.

The steps of the method shown in Fig. 4 are as follows: *S7.1:* Check if there is at least one power supply node (i.e., SN or SLN) on each power island. If yes, go to *S7.2*; otherwise, all components on this island cannot work and save the results. *S7.2:* Check if there are more than one nodes on this island. If yes, go to *S7.3*; otherwise, the power on this island is equal to the smaller of the node's maximum generating power and actual load power. *S7.3:* An alternating current optimal power flow (ACOPF) analysis [25] is conducted for this island. Check if ACOPF converges. If yes, save the results; otherwise, it means that one or more components are overloaded. In order to identify the overloaded branches, *S7.4* is executed. *S7.4:* Conduct the alternating current power flow (ACPF) analysis [25] for this island. Referring to [13] and [26], the model sheds 5% loads in the area with the worst mismatches each time until convergence of the ACOPF is achieved. *S7.5:* If convergence has not been achieved after 20 load shedding steps, the system is deemed to have collapsed, and the branch with the highest overload rate before load shedding should be disconnected from the CPPS. The first three steps in Fig. 5 are the same as those in Fig. 4, and the remaining steps are as follows: *S8.4:* Conduct the ACPF analysis for each power island. Calculate the overload rate of each branch according to (2). *S8.5:* Check if any node's generating power exceeds its maximum output power or any branch's load exceeds its maximum overload rate $f^p_{\max}$. If yes, these overload components should be disconnected; otherwise, save the results of the ACPF analysis in *S8.4*.

B. Robustness Measures for the CPPS

1) Two Existing and Widely Used Robustness Measures: The R_n measure. This robustness measure is proposed by Schneider *et al.* [27], and has been proved to be effective for measuring the robustness of complex networks [28]

$$R_n = \frac{1}{N_N^{\text{pc}}} \sum_{m=1}^{N_N^{\text{pc}}} r_m. \tag{20}$$

The p^∞ measure. This robustness measure is based on the concept of the largest connected component [29], which denotes the isolated island containing the most nodes after the network is broken down into different isolated parts by disturbances. The p^∞ measure can be calculated as follows:

$$p^\infty = \frac{|\text{lcc}_m|}{N_N^{\text{pc}}}. \tag{21}$$

The p^∞ measure assumes the components only belonging to the largest connected component retain their functions. This measure is now widely used in research on the robustness of complex networks and CPPSs [30], [31].

The above-mentioned R_n measure evaluates the robustness by counting the number of surviving nodes after a given disturbance. The p^∞ measure only focuses on the number of remaining nodes, which belong to the largest connected component. However, these two robustness measures ignore whether there are power flows in the network. In the actual CPPS, even if the system is divided into multiple isolated islands, all of these components on each island have the potential to function as long as their dependencies are satisfied. In addition, the degradation of the network topology and the information of component's multistates failures cannot be reflected from these two measures.

2) Proposed Robustness Measure: The proposed robustness measure involves the information of the local and global topology, the damage state of components, as well as the performance degradation of the CPPS. Specifically, the local topology information is quantified by the network average connectivity [32], which can be defined as follows:

$$\overline{\kappa}(G) = \frac{\sum_{u,v} \kappa_G(u,v)}{\binom{N_N^{\text{pc}}}{2}} \tag{22}$$

where u and v represent two nodes in the CPPS. Note that only severely and completely damaged components (i.e., components in failure states are 4, 5, and 9) are removed from the network topology, since the components in other failure states are functional even if they cannot be connected to the network temporarily. The local topological structure of the CPPS can be better assessed by the average connectivity than other topological measures, such as the degree and betweenness measures, because the average connectivity is associated with redundancy in the transmission path of power and information flows. However, the average connectivity cannot capture the information of the breakdown of the network structure. That is, with average connectivity alone, it is difficult to identify whether the network is divided into isolated parts, i.e., global topological information. In general, even if the average connectivity of two networks is equal, the robustness of the undecomposed network is considered to be higher than that of the decomposed network.

In order to capture the global topological information of the CPPS, the Newman's modularity measure [33] is introduced to identify the network's community structures (i.e., isolated islands), which can be defined as follows:

$$Q = \sum_{m=1}^{M} \left[\frac{N_B^m}{N_B^{\text{pc}}} - \left(\frac{\text{Deg}_m}{2N_B^{\text{pc}}} \right)^2 \right] \tag{23}$$

where M is the number of isolated islands. The value of Q ranges from 0 to 1, i.e., $0 \le Q < 1$. $Q = 0$ indicates that all nodes in the CPPS belong to a single network, and the high value of Q means that there are more isolated islands in the CPPS.

The damage state of components can be quantified by the average damage rate of all components in the CPPS, which can be expressed as in (24). This measure can reflect the periods required for system repair after a disturbance. Note that the damage rates of components in failure states 1 and 6 are not counted in this measure since these components are regarded as normal and do not need to be repaired.

$$\bar{D} = \frac{\sum_{i_{\text{pc}}=1}^{N_N^{\text{pc}}} D_{i_{\text{pc}}} + \sum_{j_{\text{pc}}=1}^{N_B^{\text{pc}}} D_{j_{\text{pc}}}}{N_N^{\text{pc}} + N_B^{\text{pc}}} \tag{24}$$

where

$$D_k = \begin{cases} D_k, & \text{if } 0.1 \le D_k \le 1 \\ 0, & \text{else.} \end{cases} \tag{25}$$

From the perspective of system performance, the ultimate goal of the CPPS is to transmit electricity the end-users (i.e., load nodes) to meet their demand. As a result, the amount of the loads supplied by the CPPS can reflect the performance of the CPPS directly, which can be formulated as follows:

$$L=\sum_{n=1}^{N_L^p} l_{i_p}. \tag{26}$$

Based on the above-mentioned discussions, the proposed robustness measure for the CPPS is formulated as follows:

$$R = [\lambda_1(1-Q)+\lambda_2\frac{\bar{\kappa}(G')}{\bar{\kappa}(G)} + (1-\lambda_1-\lambda_2)(1-(\bar{D}')^{\eta})]^{\gamma}\left(\frac{L'}{L}\right)^{1-\gamma} \tag{27}$$

where λ_1, λ_2, and γ are three weighting factors that serve for relative weighting between four factors. Based on (24), the change in the average damage rate is much smaller than those in other three factors due to the large number of components in the system. Therefore, a positive number of η less than 1 is used to adjust the magnitude of the rate of change between the average damage rate and the other three factors. $\kappa(G)$ and $\overline{\kappa}(G')$ represent the average connectivity of the CPPS before and after the system is disturbed, respectively. L and L' represent the amount of the loads supplied by the CPPS before and after the system is disturbed, respectively. $\bar{D}'$ denotes the damage state of components after the system is disturbed. The multiplication sign in front of the item L'/L means that even though the components in the CPPS are interconnected, all components in this system are considered to be inactive if there is no power flow in this system, i.e., the system has collapsed. The values of the proposed robustness measure ranges from 0 to 1, i.e., $0 \le R \le 1$. $R = 1$ shows that the system has high robustness and is not affected by disturbances, and $R = 0$ indicates that the system has collapsed due to the disturbances.

III. Numerical Example and Simulation Results

A. Test System Introduction

1) Physical System Model: The physical system of the test CPPS is represented by the IEEE 118-bus model, whose initial network and electrical data are extracted from the source code package of MATPOWER v7.3 MATLAB [25]. A total of 54 power generation nodes, i.e., SNs and SLNs, 54 LNs, 10 TNs, and 179 undirected branches are included in this power network. The ratings of these 179 power branches are not provided in the literature. Hence, the long-term ratings of all power branches in the CPPS were set to be 1.25 times its loads calculated by the ACPF analysis of the initial power network.

2) Cybersystem Model: The data of the actual communication network are difficult to obtain due to its confidentiality. The communication network in the literature is usually modeled as a complex network model, such as random networks, scale-free networks, and small-world networks. Chen *et al.* [19] indicated that the CPPS shows the higher robustness than others when the communication network is modeled as a small-world network. Similar to their approach, the communication network is modeled as a small-world network with the rewiring probability 0.2. Specifically, there are 119 nodes and 238 branches in this network, among which the 119th communication node c_{119} is the RCC, and three ALCs, including c_{18}, c_{49}, and c_{77}, manage three power network areas, respectively. Of these 118 communication nodes, four critical nodes, including c_{18}, c_{49}, c_{77}, and c_{119}, are equipped with emergency power supplies.

3) Interdependencies Within the CPPS: The power supply and control dependencies consist of 119 and 177 directed branches, respectively. The network structure diagram of the test CPPS, which couples the IEEE 118-bus with a small-world communication network, is shown in Fig. 6.

TABLE III
Parameters Used in the Proposed Cascading Failure Model

Parameter Name	Value	Parameter Name	Value	Parameter Name	Value
$f_{\max}^{O}$	1	ω_1	0.05	ω_2	0.01
ω_3	0.035	ω_4	0.95	ω_5	0.1
ω_6	0.95	ω_7	0.1	T_p^{LCC}	1
T_p^{AR}	1.5	λ_1	1/3	λ_2	1/3
η	0.5	γ	0.5	$I_{j_p}^{N}(t)$	0.3
ε_k	e	ΔT	5	R_k	0.6

B. Simulation Results

Table III describes a list of 18 parameters used in the proposed cascading failure model. Functions $\Psi(\bullet)$ and $\Phi(\bullet)$ are set to have the same expression, i.e., $({x_1}^2+{x_2}^2+\cdots+{x_n}^2)^{(1/2)}$.

In order to verify the feasibility and effectiveness of the proposed modeling approach, two of the most representative and common phenomena in the actual CPPS are simulated and explained through the proposed cascading failure model, including: 1) the large blackouts are generally caused by the occurrence of one or a small set of power contingencies (e.g., tree branches flashing on overhead lines); and 2) the failure of even one or a small set components in cybersystem has the potential to cause the large blackout, e.g., a malicious cyberattack on a cybernode. At first, the power branch between power nodes 37 and 38 and the power branch between power nodes 30 and 38, denoting as $B(p_{37}, p_{38})$ and $B(p_{30}, p_{38})$, respectively, are assumed to be broken by tree branches. Then, the simulation result is shown in Fig. 7.

The propagation process of cascading failures in Fig. 7 is as follows: at first, the disconnection of branches $B(p_{37}, p_{38})$ and $B(p_{30}, p_{38})$ caused the output power of five generation nodes to exceed their allowable upper limits. Meanwhile, the loads of 16 power branches exceed their allowable maximum overload rates ($f_{\max}^{O}$). In order to protect these overloaded components, they were actively disconnected from the network by circuit breakers. Next, the disconnection of these overloaded components resulted in 12 communication and 12 power nodes losing power supply or control dependencies. Meanwhile, 3 generation nodes and 12 power branches were severely overloaded and protected by circuit breakers. Then, 12 communication and 20 power nodes lost their coupling dependencies and could not operate. These disconnected components caused 9 of the

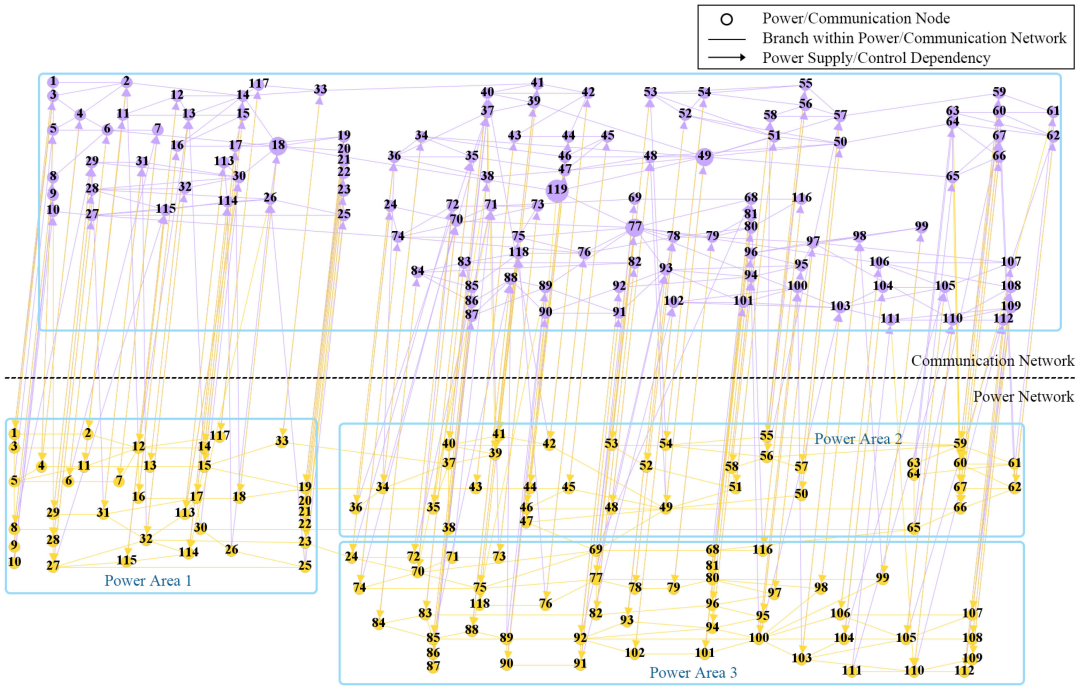

Fig. 6. Test CPPS which couples the IEEE 118-bus with a small-world communication network.

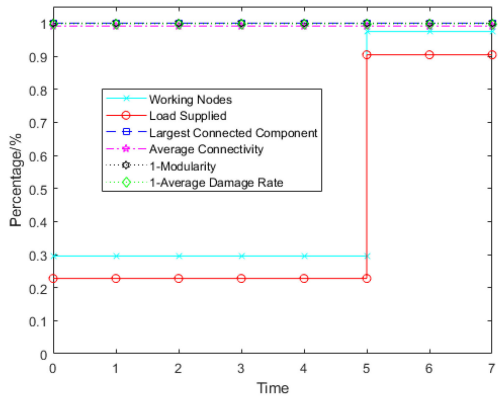

Fig. 7. Change of the system performance, topological information, and average damage rate during cascading failures when branches $B(p_{37}, p_{38})$ and $B(p_{30}, p_{38})$ are accidentally broken by tree branches.

remaining power branches to be disconnected since their loads exceeded their allowable limits. Finally, only 35 power and 35 communication nodes survived, and the power supply rate of the system was also reduced to 22.76%. After mitigation measures are implemented, i.e., after $t = 5$, 161 nodes were reconnected to the network, and the power supply rate of the system was restored to 91.41%. In order to demonstrate and simulate the other phenomenon that the failure of even one or a small set components in cybersystem has the potential to cause the large blackout, the communication node c_{18} is assumed to lose 40% of its capacity due to a malicious cyberattack, i.e., $D_{18} = 0.4$, whose simulation result is shown in Fig. 8.

The communication node c_{18} cannot process data of all power nodes in the power area 1 in time due to the degradation of its information processing capacity. That is, the network congestion with a congestion rate of 0.3333 occurs in the communication network. During the period $t = 1$, the congestion of the communication network caused damages to two branches, including $B(p_{59}, p_{61})$ and $B(p_{85}, p_{88})$, by 34.75% and 21.23%, respectively. The capacity degradation of these two damaged branches did not affect the operation of the system. During the period $t = 2$, the other four branches, including $B(p_{45}, p_{46})$, $B(p_{42}, p_{49})$, $B(p_{85}, p_{89})$, and $B(p_{27}, p_{115})$, were affected by the congested communication network. A total of 88 power nodes and 88 communication nodes were disconnected from the network by circuit breakers, and the power supply rate of the system was reduced to 31.12%. Through the implementation of artificial mitigation measures, i.e., after $t = 5$, 64 power nodes and 65 communication nodes were reconnected to the network, and the power supply rate of the system increased to 77.13%.

From the simulation results in Figs. 7 and 8, the proposed modeling approach can be considered to be feasible and effective for modeling cascading failures in the CPPS, which can well explain the cascading failure phenomenon in the actual CPPS.

C. Comparison of Robustness Measures

The superiority of the proposed measure in evaluating the robustness of the multistate CPPS is verified by comparing with the p^{∞} measure. As it can be seen from the simulation results in Figs. 7 and 8, the power supply rate decreased significantly in these two cases after disturbance events. However, the evaluation result of the p^{∞} measure shows that the system is not affected by disturbances in these two casesm i.e., $p^{\infty} = 1$, which indicates that the p^{∞} measure is not sufficient for the multistate CPPS. The p^{∞} measure only focuses on the number of nodes belonging to the largest connected component, while ignoring the power flows

TABLE IV
COMPARISON RESULTS BETWEEN p^{∞} AND THE PROPOSED ROBUSTNESS MEASURE ACCORDING TO THREE CASES FROM FIGS. 7–9

No.	Failed Component	Amounts of Islands	Load Supplied (100%)	Average Damage Rate (100%)	Working Node (100%)	Average Connectivity (100%)	Modularity	p^{∞}	Proposed Measure (R)
1	$B(p_{37}, p_{38})$ and $B(p_{30}, p_{38})$	1	0.9041	0.0021	0.9747	0.9910	0	1	0.9493
2	c_8 (damage rate 40%)	1	0.7713	0.0024	0.7975	1	0	1	0.8781
3	Isolated power area 1 and its connected cyber network	2	0.9946	0.0074	0.9916	0.5902	0.4198	0.6962	0.8478

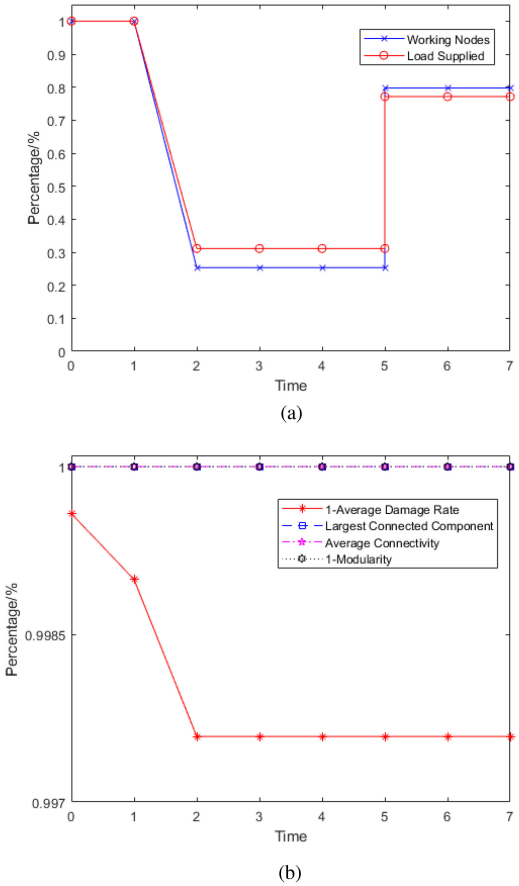

Fig. 8. Simulation results of cascading failures when the communication node c_{18} lost 40% of its capacity due to a malicious cyberattack. (a) Change of system performance and topological information during cascading failures. (b) Change of average damage rate during cascading failures.

in the CPPS as well as the degradation of capacity/performance of components with multistate failures. In order to further demonstrate the superiority of our proposed robustness measure, power area 1 and its connected communication network are isolated from the CPPS. Thus, the system is divided into two isolated islands. The simulation result is shown in Fig. 9.

It can be seen from the simulation results in Fig. 9 that even though the system is divided into two isolated islands (i.e., 70 and 165 nodes), all nodes on these two islands can continue to operate normally, and loads in the system are still fully supplied. However, eight power branches in the power area 1 are at risk of failures since their loads exceed their long-term ratings but less than their emergency rating. At time $t = 5$, the nodes p_{33} and c_{33} are disconnected from the system temporarily to ensure

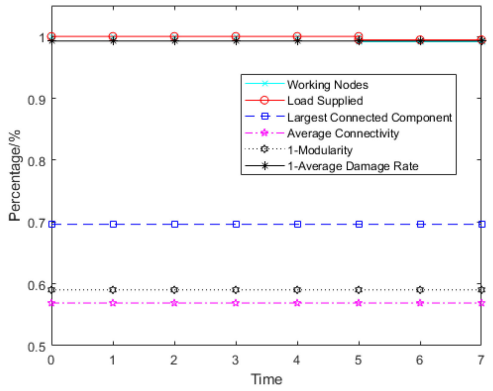

Fig. 9. Change of the system performance, topological information, and average damage rate during cascading failures when the power area 1 and its connected communication network are isolated.

the safe and stable operation of other nodes on this island. The power supply rate of the system is reduced to 99.46%.

Based on the simulation results of Fig. 9, the p^{∞} measure is calculated to be 0.6962. The p^{∞} measure assumes the components only belonging to the largest connected component retain their functions, i.e., only the island with 165 nodes is functioning. However, it can be seen that all nodes in these two islands are working. In addition, the degradation information of topological structure due to the system division is also ignored in the p^{∞} measure. The comparison of simulation results of three cases are summarized in Table IV.

From the above-mentioned discussion and the comparison results in Table IV, it can be seen that the proposed robustness measure, which integrates the information of the local and global topology, the damage state of components, as well as the performance degradation of the CPPS, is more reasonable and effective in evaluating the robustness of the multistate CPPS.

IV. CONCLUSION

This article proposed an approach for modeling cascading failures of the CPPS considering component multistate failures. The stochastic process, the approximate dynamic behavior-based model, as well as nine failure states of each component are incorporated in our approach. According to the application of the proposed modeling approach in the test CPPS, which couples the IEEE 118-bus model with a small-world communication network, it can be seen that the propagation process of cascading failures in actual CPPS can be well simulated and explained by the proposed modeling approach. In addition, a robustness measure, which integrates the information of the local and global

topology, the damage state of components, as well as the performance degradation of the CPPS, is proposed. The comparison with p^{∞} measure indicates that the proposed measure is more effective in evaluating robustness of the multistate CPPS.

In terms of the scalability of the proposed modeling approach, the modeling procedure in Fig. 3 is based on the system model shown in Fig. 1. This system model is a graph theory-based abstraction of the real CPPS, and consisted of communication nodes, power nodes, and the corresponding topological relations, which makes it possible to build models for larger-scale CPPSs by adding more edges and nodes. Thus, the scalability of the proposed modeling approach would not be a challenge, and the application of the proposed modeling approach can scale up to larger CPPSs. However, larger-scale real-life CPPSs modeling may incur extra computation efforts.

The computational complexity of the proposed modeling approach for cascading failures is heavy due to the power flow calculation process based on approximate dynamic behavior-based methods, e.g., the ACPF and ACOPF analyses. The high computational cost results in that the proposed modeling approach may be most applicable to certain problems with low requirements for real-time response, such as the critical node identification problem and the decision problem of optimal recovery sequence of components. The complex network-based methods, which are the alternative methods for the power flow calculation, can update power flows more efficiently at the cost of larger errors. To this end, how to balance the approximate dynamic behavior-based and complex network-based methods to reduce the complexity in the power flow calculation process within an acceptable error range is one of our future research directions.

REFERENCES

[1] D. Gürdür and F. Asplund, "A systematic review to merge discourses: Interoperability, integration and cyber-physical systems," *J. Ind. Inf. Integr.*, vol. 9, pp. 14–23, 2018.

[2] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, "A realistic model for failure propagation in interdependent cyber-physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 2, pp. 817–831, Apr.–Jun. 2020.

[3] S. Ankaliki, "Energy control center functions for power system," *Int. J. Math. Sci., Technol., Humanities*, vol. 2, pp. 205–212, 2012.

[4] L. Shi, Q. Dai, and Y. Ni, "Cyber-physical interactions in power systems: A review of models, methods, and applications," *Elect. Power Syst. Res.*, vol. 163, pp. 396–412, 2018.

[5] A. Vespignani, "Complex networks: The fragility of interdependency," *Nature*, vol. 464, no. 7291, pp. 984–985, 2010.

[6] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *Int. J. Crit. Infrastruct.*, vol. 4, no. 1-2, pp. 63–79, 2008.

[7] W. House, "Economic benefits of increasing electric grid resilience to weather outages," Washington, DC, USA: Executive Office of the President, 2013.

[8] U. S. Department of Homeland Security, "National infrastructure protection plan (NIPP) 2013: Partnering for critical infrastructure security and resilience," Washington, DC, USA: Office of the Secretary of Homeland Security, 2013.

[9] U. S. Department of Homeland Security, "The 2014 quadrennial homeland security review (QHSR)," Washington, DC, USA: Office of the Secretary of Homeland Security, 2014.

[10] C. Alcaraz, "Cloud-assisted dynamic resilience for cyber-physical control systems," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 76–82, Feb. 2018.

[11] G. A. Pagani and M. Aiello, "The power grid as a complex network: A survey," *Phys. A: Statistical Mechanics Appl.*, vol. 392, no. 11, pp. 2688–2700, 2013.

[12] B. Stott, J. Jardim, and O. Alsaç, "DC power flow revisited," *IEEE Trans. Power Syst.*, vol. 24, no. 3, pp. 1290–1300, Aug. 2009.

[13] D. P. Nedic *et al.*, "Criticality in a cascading failure blackout model," *Int. J. Elect. Power Energy Syst.*, vol. 28, no. 9, pp. 627–633, 2006.

[14] B. Li, K. Barker, and G. Sansavini, "Measuring community and multi-industry impacts of cascading failures in power systems," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3585–3596, Dec. 2018.

[15] M. Khederzadeh and S. Zandi, "Enhancement of distribution system restoration capability in single/multiple faults by using microgrids as a resiliency resource," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1796–1803, Jun. 2019.

[16] S. V. Buldyrev *et al.*, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[17] H. Pan, H. Lian, C. Na, and X. Li, "Modeling and vulnerability analysis of cyber-physical power systems based on community theory," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3938–3948, Sep. 2020.

[18] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," in *Proc. IEEE 8th Conf. Ind. Electron. Appl.*, 2013, pp. 1023–1028.

[19] Y. Chen *et al.*, "Cascading failure analysis of cyber physical power system with multiple interdependency and control threshold," *IEEE Access*, vol. 6, pp. 39353–39362, 2018.

[20] Y. Wang *et al.*, "On modeling of electrical cyber-physical systems considering cyber security," *Frontiers Informat. Technol. Elect. Eng.*, vol. 17, no. 5, pp. 465–478, 2016.

[21] H. Guo *et al.*, "A complex network theory analytical approach to power system cascading failure-from a cyber-physical perspective," *Chaos*, vol. 29, no. 5, 2019, Art. no. 0 53111.

[22] L. K. C. and G. Vandana, "Modeling cyber-physical attacks based on stochastic game and Markov processes," *Rel. Eng. Syst. Saf.*, vol. 181, pp. 28–37, 2018.

[23] G. Wu and Z. S. Li, "A cascading failure model of power systems considering components' multi-state failures," in *Proc. Prognostics Syst. Health Manage. Conf.*, 2019, pp. 1–6.

[24] D. Lallemant and A. Kiremidjian, "A beta distribution model for characterizing earthquake damage state distribution," *Earthq. Spectra*, vol. 31, no. 3, pp. 1337–1352, 2015.

[25] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[26] J. Li *et al.*, "AC power flow importance measures considering multi-element failures," *Rel. Eng. Syst. Saf.*, vol. 160, pp. 89–97, 2017.

[27] C. M. Schneider *et al.*, "Mitigation of malicious attacks on networks," *Nat. Acad. Sci.*, vol. 108, no. 10, pp. 3838–3841, 2011.

[28] M. Gong *et al.*, "Enhancing robustness of coupled networks under targeted recoveries," *Sci. Rep.*, vol. 5, 2015, Art. no. 8439.

[29] M. E. Newman, A. L. E. Barabási, and D. J. Watts, *The Structure and Dynamics of Networks*. Princeton, NJ, USA: Princeton Univ. Press, 2006.

[30] X. Liu *et al.*, "Onion structure optimizes attack robustness of interdependent networks," *Physica A: Statistical Mechanics Appl.* vol. 535, 2019, Art. no. 122374.

[31] Z. Wang, D. Zhou, and Y. Hu, "Group percolation in interdependent networks," *Phys. Rev. E*, vol. 97, no. 3, 2018, Art. no. 032306.

[32] L. W. Beineke, O. R. Oellermann, and R. E. Pippert, "The average connectivity of a graph," *Discrete Math.*, vol. 252, no. 1–3, pp. 31–45, 2002.

[33] V. D. Blondel, J. L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *J. Statist. Mech.*, vol. 10, 2008, Art. no. P10008.