


Modeling cascading failures and mitigation strategies in PMU based cyber-physical power systems

Yuqi HAN¹ , Chuangxin GUO¹, Shiyong MA², Dunwen SONG²



Abstract This paper presents a model of cascading failures in cyber-physical power systems (CPPSs) based on an improved percolation theory, and then proposes failure mitigation strategies. In this model, the dynamic development of cascading failures is divided into several iteration stages. The power flow in the power grid, along with the data transmission and delay in the cyber layer, is considered in the improved percolation theory. The interaction mechanism between two layers is interpreted as the observability and controllability analysis and data update analysis influencing the node state transformation and security command execution. The resilience indices of the failures reflect the influence of cascading failures on both topological integrity and operational state. The efficacy of the proposed mitigation strategies is validated, including strategies to convert some cyber layer nodes into autonomous nodes and embed unified power flow controller

(UPFC) into the physical layer. The results obtained from simulations of cascading failures in a CPPS with increasing initial failure sizes are compared for various scenarios. Dynamic cascading failures can be separated into rapid and slow processes. The interdependencies and gap between the observable and controllable parts of the physical layer with the actual physical network are two fundamental reasons for first-order transition failures. Due to the complexity of the coupled topological and operational relations between the two layers, mitigation strategies should be simultaneously applied in both layers.

Keywords Cyber physical power system, Cascading failure, Improved percolation theory, Interdependent network, Mitigation strategy

CrossCheck date: 5 March 2018

Received: 22 August 2017 / Accepted: 5 March 2018 / Published online: 30 July 2018

© The Author(s) 2018

✉ Yuqi HAN
hanyuqi@zju.edu.cn

Chuangxin GUO
guochuangxin@zju.edu.cn

Shiyong MA
mashiy@epri.sgcc.com.cn

Dunwen SONG
songdw@epri.sgcc.com.cn

¹ College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China

² China Electric Power Research Institute, Beijing 100192, China

1 Introduction

The secure and reliable operational requirements of modern power grids facilitate integration of the latest developments in communications and information technologies. Consequently, modern power grids are evolving into interdependent cyber-physical power systems (CPPSs) [1]. The architecture of a CPPS includes both physical and cyber layers. The physical layer refers to an electrical network that performs power generation, transmission, and distribution tasks, while the cyber layer refers to communications and computational nodes, which monitor, protect, and control the physical electrical layer. The nodes in the cyber layer require an energy supply extracted from substations located in the physical layer, while those in the physical layer are monitored, protected, and controlled by the cyber layer nodes.

The physical and cyber layers in a CPPS are increasingly interconnected and mutually interdependent, which

significantly increases the complexity of CPPSs and renders the coupled systems more vulnerable to cascading failures [2, 3]. Interdependent malfunctions of the cyber and physical layers have been the main triggers of, and contributors to, many of the big blackouts that have occurred recently. For example, blackouts in the US and Italy in 2003 can be summarized as malfunctions and defects in the cyber layer caused the failure situation in the physical layer to become increasingly unobservable and uncontrollable, which in turn allowed the failure to propagate and interact between the two layers and led to blackouts [4]. Traditional cascading failure models, such as OPA and CASCADE, focus on modeling the redistribution of power flows and enlargement of the failure scope by new tripping of over-loaded transmission lines, which can neither represent the interactions nor illustrate the process of failure propagating between the physical and cyber layers recursively. Therefore, it is critical to develop innovative models that reflect the interactions and cascading failure scenarios in coupled CPPSs.

Some recent studies have focused on this topic, including the complex system-based implicative interdependency model [5], the interdependent Markov-Chain approach [6], and the evil-rain model [7], which were proposed to analyze the interactions between coupled networks. In [2], percolation theory was introduced to analyze cascading failures in a one-to-one interdependent multi-layer model. Later studies [8–10] focused on the resilience of interdependent networks through complex network-based percolation theory, and showed that cascading failure transitions in interdependent networks are first-order phenomena in comparison to second-order phenomena in isolated power networks. A standard one-to-one interdependent model has been extended to a more complicated interdependent model to reflect configurations where physical nodes provide power to multiple cyber layer nodes, and vice versa. In the above study, a fundamental assumption made in normal operation is that cyber-physical system (CPS) nodes belong to a giant cluster of components in their own layer, while some recent studies [11, 12] consider the operation of small clusters. The interface strategy and dependency strength between mutually interdependent networks play important roles in the resilience of interdependent networks to withstand cascading failures [13–15]. The more inter-similarities there are between the two networks, the greater is their ability to withstand cascading failures [16, 17]. Purely topology-based percolation theory and interdependence strategies [2, 8, 9] can be used to model dynamic cascading failures in interdependent networks. However, the node failure interaction in these approaches is assumed as once the node fails, its interdependent nodes in the other layer fail immediately with a certain possibility value. The

possibility value was set as one in [8] and intermediate between zero and one in [13, 17]. The abovementioned studies overly neglected the specifics of power grids in CPPSs to provide an accurate and realistic model [18]. In addition, the indices representing the resilience of CPPSs to failures were only topological metrics in those approaches, and thus, could not measure the influence of cascading failures from an electrical perspective. To treat the cyber and physical layer operations as an indivisible whole, the reliability and contingency assessment frameworks were proposed in [19, 20] as pioneers in probing the assessment of risk factors in CPPSs. In [21], the cut of transmission lines was modeled by comparing the time needed for security controls to mitigate the failure and time for protection system to trip the overloaded line. Measurements from the sensors in the field, as well as commands from the control center, were relayed over the cyber layer [20]. Cascading failures in the physical layer were fueled by the latency of information package transmission in the cyber layer. Further research [22] proposed an interactive cascading failure simulation model and showed the self-organized characteristics in blackout probability and cyber layer network data transmission inefficiency. However, this study mainly discussed how the failure in a communication network influences the re-dispatch or corrective action, and did not probe the processes whereby failures develop recursively between the layers.

In our previous studies [23, 24], to integrate more physical operational specifics into the failure analysis method, we developed an improved percolation theory that divided the failures into different stages and considered the physical layer power flow analysis, security controls, and transmission line capacity checks to model cascading failures in a CPPS. However, the simple on/off two-state node model in our previous study only captured the linear direct interaction relation and neglected complicated indirect interactions between the two layers. Note that malfunctions of cyber layer nodes do not directly lead to the failure of physical nodes, but instead increase the risk of potential cascading failures. The indirect interaction mechanism of node failure in the two layers should be probed and modeled. Moreover, besides the power flow modeling for the physical layer, the key characteristics of topological and information flow analysis for the cyber layer are worth enough attention.

To mitigate the impact of cascading failures in power networks, blocking specific protective relays [25], allowing a certain minimum number of transmission lines to overload before protective relay acting, increasing generation margins [26], and embedding flexible AC transmission systems (FACTS) [27] have been incorporated into the power flow control method to relieve overloaded transmission lines and re-route power flows. As for the



mitigation of cascading failures in the context of CPPSs, current approaches focus primarily on network reformulation and improving the robustness of the cyber layers individually [28–30]. Note that flexible mitigation strategies adopted simultaneously in both layers have not received much attention in previous analyses.

This paper first introduces an interdependence strategy based on the classification of nodes and their geographic closeness, as well as the three-state node model including normal, partial outage, and failure states. Then, an improved percolation theory is presented, which incorporates physical layer power flow analysis, cyber layer information transmission and delay analysis, and indirect interactions between coupled layers. Furthermore, cascading failure mitigation strategies are proposed from the network interdependence relation and physical layer operational perspectives. As the technical extensions of our previous study, the main contributions of this paper are as follows:

- 1) In establishing a complex network-based CPPS model, an interdependence strategy based on the classification of nodes and their geographic closeness is introduced. To take more CPPS actual operation specifics into modeling dynamic cascading failures, a three-state model is put forward to represent the normal state, partial outage state, and failure state of each node. In addition, the physical layer power flow analysis and edge capacity checks, cyber layer information transmission and delay analysis, and the indirect interaction mechanism between the two layers are incorporated into an improved percolation theory-based model.
- 2) Two mitigation strategies are put forward and validated, which include embedding UPFC in the physical layer and equipping the cyber nodes with a backup power source, thus transforming bidirectional interdependencies into unidirectional interdependencies.

The remainder of this paper is organized as follows. Section 2 introduces the system model of a CPPS and an interface strategy where the proposed improved percolation theory and mitigation strategies are applied. Section 3 formulates the improved percolation theory to analyze and model cascading failures in the CPPS. Mitigation strategies for the cascading failures are presented in Section 4. Case studies are discussed in Section 5, and the paper is concluded in Section 6.

2 System model

The architecture of a CPPS includes physical and cyber layers, neither of which can operate normally without the interdependencies from the other. The interdependencies

can be classified into two categories: energy support and 3C-function support (computation, communication, and control). Energy interdependence means that the power needed by the targeted cyber layer node is provided by the interconnected physical layer node, while 3C-function interdependence means that the targeted physical node is under the 3C-functional support of the interconnected cyber layer node.

2.1 Complex network-based model

The topologies and infrastructures of the cyber and physical layers in the CPPS are abstractly represented as nodes and edges, respectively; therefore, a complex network theory can be applied to CPPS modeling. The CPPS is modeled as a graph $G = \langle N_c, N_p, E_c, E_p \rangle$, where N_c, N_p are the sets of the cyber and physical nodes and E_c, E_p are the sets of the cyber and physical edges. The cyber layer is a combination of intelligent data collection and analysis devices, and includes an Ethernet-based communication interface, which links the 3C-function support to the corresponding physical layer. The nodes in the cyber layer include the abstracted 3C-function support devices and related data processing algorithms; the edge indicates the data transmission media. In the physical electrical layer, the nodes refer to the substations and generation plants, while the edges represent the transmission lines. The number of nodes within a cyber layer (i.e., the cyber layer network order) is k more than that in the corresponding physical layer.

$$D_c = D_p + k \quad (1)$$

where D_c is the order of the cyber layer; D_p is the order of the physical layer; and k is the number of control center nodes in the CPPS.

The intra-link connection relation within each layer can be represented by an adjacency matrix $A = (a_{ij})_{N \times N}$, where element a_{ij} is 1 if there is an edge node that directly connects node i to node j , and 0 otherwise.

The unidirectional and bidirectional interdependencies are of two common types. Considering the robustness of the actual situation, bidirectional interdependencies are adopted in the CPPS model [30], which means the cyber node provides 3C-function support to the physical node, while the physical node supplies power to the same cyber node. This mutual interdependence relation is illustrated in Fig. 1.

A core support for the 3C-function in the cyber layer is wide area measurement, protection and control system (WAMPCS). The WAMPCS master nodes are located in the nodes corresponding to the cyber layer control centers, and the WAMPCS slave nodes are located in other cyber

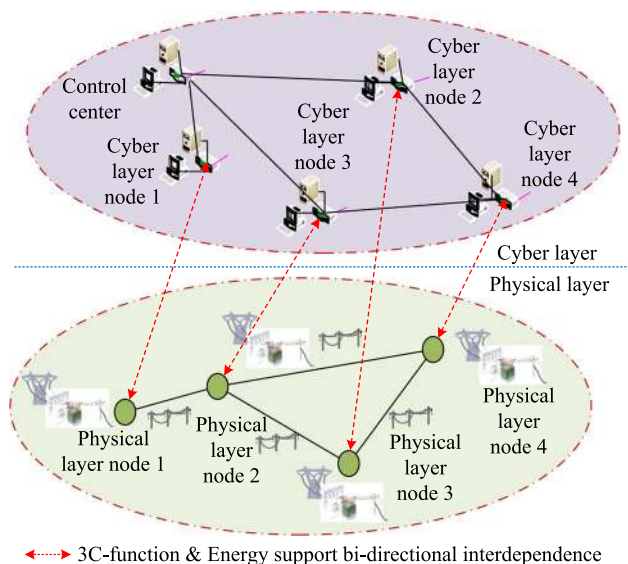


Fig. 1 Interdependencies within CPPS

layer nodes. To implement the 3C-function, the tasks of collecting measurements and distributing control signals to the actuators are performed by a PMU and intelligent electronic devices in WAMPCS. The PMU provides time-tagged information regarding the physical node and power flow measurements. There is a mimic diagram of the physical layer in the control center [31], which is based on the collected analog and digital measurement data from WAMPCS. The mimic diagram is the connection and operation mirror of the observable part of the physical power system. The control center in the cyber layer fulfils the functions of the WAMPCS master node and performs comprehensive CPPS operational computations, such as optimal dispatch or stability analyses. WAMPCS slave nodes perform the functions of measuring the PMU data, concentrating them, and signal communication. Considering the investment and operational costs of the CPPS, it is impractical to equip each cyber layer node with a PMU and synchronized GPS equipment under the current investment ability. The parameters of the transmission lines and other electrical infrastructure are already known in WAMPCS; thus, physical nodes are observable by their own PMU or through a transmission line based on their power flow relations [32]. Therefore, in the following analysis, a physical node is considered observable if its interdependent cyber node is equipped with a PMU, or at least one cyber node interdependent with its neighboring physical nodes is equipped with a PMU. The WAMPCS in the cyber layer is for both monitoring and control; thus, identifying the observable part also identifies the controllable part. The optimal PMU allocation can be formulated as an integer linear program model.

$$\min \left(\sum_{i=1}^n x_i \right) \tag{2}$$

$$x_i + \sum_{j \in i} x_j \geq 1 \tag{3}$$

where the binary variable x_i denotes the state of the PMU in the cyber layer WAMPCS node that is interdependent with physical node i , x_i is 1 if node i is equipped with a PMU and 0 otherwise, and j denotes the set of neighborhood physical nodes connected directly to node i .

The above formulation guarantees that all physical nodes are observable and controllable under normal conditions. For reliability, it is necessary for all physical nodes to be observable and controllable even when one set of PMUs is malfunctioning or is in outage. To meet the $N - 1$ criterion, the right part of (3) should be replaced with “2” which represents redundancy allocation.

2.2 Hierarchical architecture for cyber and physical layers

Generally, there are two types of electrical data networks, namely the double-star network and the mesh network [33], which are the archetypes of the cyber layer for a CPPS. The cyber layer is an Ethernet-based 3C network. It has been shown in the literature that Ethernet is a scale-free network, and that the degree of node distribution follows a power law distribution. In this paper, the cyber layer is modeled as a scale-free network using the Barabási–Albert model.

The cyber nodes are classified into three hierarchical categories depending on their operational and topological characteristics: control center or kernel nodes, backbone nodes, and accessing nodes [23]. Betweenness centrality [34] and shortest effective distance [35] are used to measure the importance of nodes in transmitting information. In particular, the shortest effective distance is the mean of the shortest distance of a node to the remaining nodes in a network, which indicates how quickly and easily the node can exchange information with others. Considering the critical role of CPPS control centers, the corresponding cyber layer nodes are located in the topological center of the cyber layer, thus are the top nodes in the sequenced list ranked by the shortest effective mean distance to other nodes. The nodes connected directly to the control centers, or those whose mean distances to other nodes are comparatively less than the diameter of the network, are called backbone nodes and the remaining nodes in the network are called accessing nodes. The physical nodes are classified into two categories in order to establish their interdependencies with the backbone and accessing nodes in the cyber layer, respectively. The classification criterion is that



if one of the following conditions is met, then the physical node is a backbone node in the physical layer and is interconnected with the backbone nodes in the cyber layer. Otherwise, the physical node is an accessing node and is interconnected with the accessing nodes in the cyber layer.

- 1) The node load is large, which means that the node is located at the load center.
- 2) The generation node has a large reserve capacity, which plays an important role in voltage frequency control and dispatch.
- 3) If a generation node has a connected load, then the failure of that node leads to a loss of generating capacity, which directly causes load shedding and forces the system to operate at or beyond its limit.

In the following analysis, the general quantitative criteria for identifying a large load and large reserve capacity are that the load rate is more than 10 times the mean load rate and the reserve capacity is more than 15%. Specifically, the exact parameters in the above conditions can be adjusted within a small scope to ensure that the number of physical nodes that meet the condition and are interconnected to cyber layer backbone nodes is the same as the number of cyber layer backbone nodes.

2.3 Interdependence in CPPS

Information and energy are exchanged through the interdependence interface. The interdependencies are constructed based on certain strategies that can be classified as either topological, operational, or both. Many topological strategies have been formulated and compared in previous research; however, these typically neglect the geographical and engineering constraints in practical physical operational situations in a CPPS. An important constraint when allocating interdependencies is geographic closeness. For example, in a control and communication network, it is not feasible to receive electricity from a geographically distant node in the power grid due to the associated cost and physical constraints. Therefore, the interdependence strategy outlined in this paper is based on the classification of node categories and their geographic closeness, which include the control center, backbone, and accessing nodes. The physical nodes belonging to each category are interconnected with the corresponding cyber layer nodes belonging to the same category that have the shortest geographical distance. The control center nodes are autonomous, and there are no direct interdependencies between the control center and physical nodes. For a CPPS with sufficient geographic information, the nodes in each layer that belong to the same category are listed based on their geographic distance to the chosen reference location. Owing to the lack of actual geographic information regarding the IEEE standard power system, for

simulating the geographical distance, node numbers are used in this paper to represent the geographic distance to the chosen reference location. For this reason, the nodes belonging to the same category in each layer are relisted using the node number. The interdependencies are constructed by interconnecting the nodes in the same sequence for the backbone nodes and accessing nodes in cyber and physical layers.

2.4 Extended adjacency matrix of CPPS

To better analyze the model and clearly represent the interconnection relations in a CPPS, a matrix is formed to reflect the comprehensive topological relation, which includes information about the nodes, intra-links, and interconnections of the interdependencies. Similar to the definition of the adjacency matrix in Section 2.1, the extended adjacency matrix can be defined as:

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_p & \mathbf{A}_{p-c} \\ \mathbf{A}_{c-p} & \mathbf{A}_c \end{bmatrix} \quad (4)$$

where \mathbf{A}_p and \mathbf{A}_c are the adjacency matrices of the physical and cyber layers, respectively; \mathbf{A}_{c-p} is the cyber-to-physical interdependence matrix in which $\mathbf{A}_{c-p}(i, j)$ is 1 if there is 3C-function and energy interdependence between cyber layer node i and physical layer node j , and 0 otherwise; and \mathbf{A}_{p-c} is the physical-to-cyber interdependence matrix, which is the transpose of \mathbf{A}_{c-p} . The size of the extended adjacency matrix is $(N_p + N_c) \times (N_p + N_c)$ and those of \mathbf{A}_{c-p} and \mathbf{A}_{p-c} are $N_c \times N_p$ and $N_p \times N_c$, respectively. The diagonal sub-matrices of the extended adjacency matrix contain the topological information of each layer, and the off-diagonal sub-matrices contain the bi-directional interdependence relations between the two layers.

3 Improved percolation theory

Percolation theory is a probability-based analysis of structural connectivity in graphs. The process of percolation is similar to that of removing edges or nodes in cascading failures, and percolation state transitions are similar to the failure of the whole system at the end of the cascading failures. On this basis, percolation theory is adopted and improved according to the actual operation situation of the CPPS to model the dynamic development of cascading failures in coupled CPPSs.

3.1 States of CPPS nodes

The nodes in cyber and physical layers have three states: normal, partial outage, and failure. The requirements for

nodes in the normal state can be classified as intra-link and interdependence connections.

- 1) Intra-link connection: Cyber layer nodes should be able to access the control center or backup control center. Physical nodes belong either to the giant functioning cluster or to the self-supply small cluster, which means that the generators in the small cluster can satisfy either a portion of or the total load within the island.
- 2) Interdependence connection: Cyber layer nodes have at least one energy interdependence or are equipped with backup uninterrupted power source (UPS). Physical nodes are observable and controllable by the cyber layer.

If a physical node is in unobservable and uncontrollable state [33] but has not yet fully failed, then the node operates in a partial outage state. In this state, the node cannot evolve in the power flow re-dispatch and any new line capacity violation can trigger the protection system to cut the line, thus causing the node to enter the failure state if the new line cut renders the node totally isolated. For a failure in the physical node, the load that is more than its own generation capacity will be shed. The loss of energy interdependence causes the cyber nodes to transform from normal to partial outage state. For autonomous cyber nodes with their own backup power source (UPS), backup power maintains the core functions in the cyber nodes and the backup power is assumed to last for the duration of cascading failures. Consequently, if we do not differentiate between the impacts of various power sources on the operation performance of cyber nodes, the partial outage state and normal state can be simplified together for the autonomous cyber layer. However, if the cyber node is not equipped with backup power, the loss of energy interdependence causes the shutdown of the cyber nodes, and the partial outage and failure states can be simplified together.

3.2 Power flow analysis in physical layer

Considering the demands of computational time, and as this research is focused on (high-voltage) transmission grids, the linear DC power flow is a reasonable approximation. It provides a linear relation between the active power flowing through the line and the voltage phase at two ends of the line.

$$F_k = B_k(\theta_n - \theta_m) \tag{5}$$

where F_k is the power flow on transmission line k ; B_k is the admittance of line k ; and θ_n, θ_m are the voltage phases at two ends of line k .

Summing the power flow in all branches connected to node i , we obtain the power flow for node i . The physical network power flow can be presented in matrix form as:

$$P = B\theta \tag{6}$$

where P is the node power matrix; B is the network admittance matrix; and θ is the node voltage phase matrix.

During failures, security control is operated to ensure minimum operation cost of the system without violation of equality constraints and non-equality constraints. The objective function and constraints of the optimization are presented in (7) and (8), respectively.

$$\min_c = \min \sum_m c_{gm}(P_{gm}) + V \sum_n L_n \tag{7}$$

s.t.

$$\begin{cases} c_{gm}(P_{gm}) = a_m P_{gm}^2 + b_m P_{gm} + c_m \\ P_{gm}^{\min} \leq P_{gm} \leq P_{gm}^{\max} \\ -F_k^{\max} \leq F_k \leq F_k^{\max} \\ F_k - B_k(\theta_n - \theta_m) = 0 \\ \sum_{k \in in(n)} F_k - \sum_{k \in out(n)} F_k + \sum_{g \in g(n)} P_g = d_n - L_n \end{cases} \tag{8}$$

where L_n is the load shedding value at node n ; P_{gm} is the output of generator m ; $c_{gm}(P_{gm})$ is the cost for generator m ; a_m, b_m, c_m are the cost parameters; V is the penalty factor for load shedding; $P_{gm}^{\min}, P_{gm}^{\max}$ are its minimum and maximum values; F_k is the power flow on transmission line k ; F_k^{\max} is its maximum short-term rating; $\sum_{k \in in(n)} F_k$ is the sum

of transmission line power that flows into node n ; by the same token, $\sum_{k \in out(n)} F_k$ is the sum of transmission line power

that flows out of node n ; and d_n is the load connected to node n .

3.3 Data transmission analysis in cyber layer

The data in the cyber layer are transmitted step-by-step from the source node to the receiver node. At each step, the data packet is received and sent out only once by each cyber layer node. The time duration of the step is defined as the cyber layer unit time step. For each source node, it chooses one of its neighboring nodes based on the effective distance [21] to send out the data in the current unit time step, and this procedure goes on until all data have been received by the receiver nodes. The intermediate node is selected in accordance with certain route strategy. Inspired by the idea of OpenFlow in Soft-Defined Networks, in this paper, the route table is centrally derived by using the Floyd–Warshall algorithm [36]. The object function is the overall weighted shortest path from the source to receiver,



and the weight of the path is the number of datasets waiting in the node buffer.

$$\sum \min AN_k \quad (9)$$

where A is the $N \times N$ matrix, N is the number of functioning nodes in the cyber layer, A_{ij} demonstrates whether node j is chosen as the intermediate node for the data from source i ; and N_k is the $N \times 1$ vector of data waiting in the buffer.

The route table is updated at each unit time step and the number of datasets waiting in the node buffer for the next step is based on the current result. Within a unit time step, if the data needed to be transmitted are beyond the data-handling ability, then the data are saved in the buffer and wait to be sent out in the following unit time step until there are no data in the buffer. This procedure is illustrated in Fig. 2.

Therefore, the data congestion in some cyber nodes causes an increase in data transmission delay. Although the unit time step and delay are at the millisecond level, it does not mean that the delay has no influence on the cascading failure development. According to the TCP/IP protocol, if the transmission delay is beyond the round trip time (RTT) threshold, the data will be re-sent from the source. However, if the congestion situation is not mitigated and the delay is again beyond the RTT threshold, then that data would be lost and the receiver would not obtain the latest data.

3.4 CPPS cascading failure modeling

The cascading failures are triggered by initial failures, and then, evolve into a dynamic developing phase until the infected areas of the cascading failures remain constant and the failures terminate.

3.4.1 Initial failures

Indeed, initial malfunctions in the cyber layer do not directly cause failures in the physical layer. Few unobservable points will not cause any failure in the physical layer and the physical layer can operate normally until

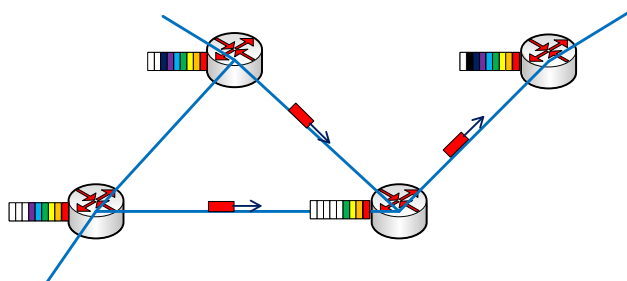


Fig. 2 Data transmission route in the cyber layer

failures occur within the physical system. However, the observability and controllability situations in the physical layer deteriorate. Many actual blackout cases proposed in recent years correspond to the circumstance where both cyber malfunctions and physical incidents have occurred, although there is no direct relation between them. In the initial state, there are defects or malfunctions in the cyber layer, including software malfunctions, PMU malfunctions, and communication transmission failures. Then, cascading outages are triggered by coincidental failures or faults in the unobservable part of the physical layer. Defects in the cyber layer cause the situation to become increasingly unobservable and uncontrollable. As a result, no security controls are taken, which in turn allow the failure to propagate between the two layers and lead to blackouts. Although the possibility of this circumstance is really low, it can lead to catastrophic results. This paper focuses on this low possibility, but worst result circumstance. Therefore, in the initial failure, the malfunctions in the cyber nodes and the failures in their corresponding physical nodes are assumed to occur simultaneously.

3.4.2 Interaction between cyber and physical layers

The failures in the cyber layer make their corresponding part in the physical layer unobservable and uncontrollable. Thus, in the mimic diagram of the physical layer, the unobservable and uncontrollable part should be removed from the optimal security and mitigation action calculation. The tripping of overloaded transmission lines generates new nodes in the physical layer disconnected from others and to be islands. The generator in a self-supply island can keep the energy interdependence still working, while that in a non-self-supply island can no longer keep the energy interdependence working, and thus, the cyber node is shut down. The state of a cyber node depends on whether the node is equipped with a backup power source. The failures that occur in the physical layer are unobservable, and thus, no effective security controls can be taken. For the observable and controllable part, the latest operation state data are sent to the control center in the cyber layer step-by-step. After the derivation of the security controls in the control center, the control data are sent back to the corresponding node to act correctly. If the data transmission delay is beyond the RRT threshold, the operation state or the control commands will not be executed accurately in the current stage.

3.4.3 CPPS cascading failure model based on improved percolation theory

The failures are developed recursively between the cyber and physical layers according to the interactive

mechanism after the initial failures. The dynamic development process can be divided into several stages, during which the operation state of the node needs to be updated. A flowchart describing the proposed improved percolation theory is illustrated in Fig. 3.

The initial failure is modeled as Stage 1, and the dynamic development of the cascading failure is modeled as the iterative process between Stages 2 and 3.

1) Stage 1: Initial malfunctioning nodes in the cyber layer and initial failed nodes in the physical layer

The cascading failure is triggered when several nodes in the cyber layer malfunction. As elaborated in the assumption, the malfunctions in the cyber nodes and failures in their corresponding physical nodes occur simultaneously as the initial failure. The sub-network obtained after removing the initial malfunctioning nodes in the cyber layer is expressed as:

$$C_1^{\sim} = C_u(\mu_1) \cap C \tag{10}$$

where set C denotes the entire set of nodes in the cyber layer; set μ_1 denotes the initial malfunctioning nodes; and C_u represents a function that returns the complementary of a set.

According to the operational conditions, the functioning nodes in set C_1^{\sim} can be expressed as set C_1 :

$$C_1 = F(C_1^{\sim}) \tag{11}$$

where $F(C_1^{\sim})$ represents the process of calculating the nodes in sub-network C_1^{\sim} , which have working intra-link connections to the control centers. The function $F(C_1^{\sim})$ is operated by calculating the shortest path from the node to the control centers by using the Floyd–Warshall algorithm. If there are no working intra-link connections to the control centers, then the distance from the node to the control centers will be infinitely large and there is no shortest path between them. As a result, that node will be excluded from C_1 .

The physical nodes interdependent with the malfunctioning cyber nodes are selected to be the initial failed physical nodes and need to be removed from the physical layer functioning set. The set of functioning nodes in the physical layer in Stage 1 is:

$$P_1^{\sim} = C_u(p_{\mu_2}) \cap P \tag{12}$$

where μ_2 is the set of physical nodes that are interdependent with initial malfunctioning cyber nodes; P is the set of all nodes in the physical layer; and p_{μ_2} is the ratio of initial failed nodes in set μ_2 , which can be adjusted according to the interdependent strength and ranges from 0 to 1.

2) Stage 2: Failure in the physical layer

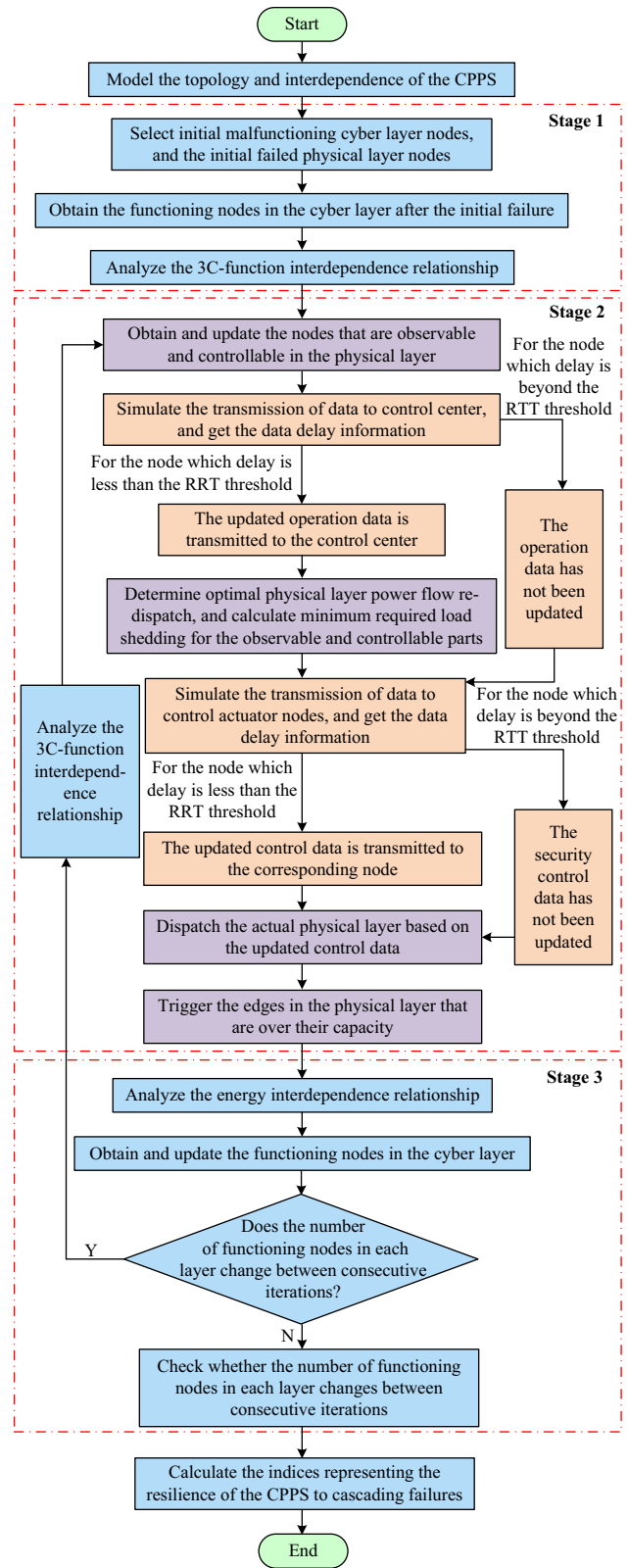


Fig. 3 Flowchart of the cascading failure model based on the improved percolation theory



In the physical layer, the nodes that belong to the observable and controllable part are included in set P_{2m} , which is derived by updating the functioning PMU in the cyber layer and selecting the nodes that correspond to the non-zero right column of (2) and (3). The actual operational physical nodes are expressed as set P_{2r} , which only removes the failed nodes and does not consider observation and control. Therefore, the set P_{2m} is a subset of P_{2r} .

$$P_{2m} \subseteq P_{2r} \tag{13}$$

In the first iteration, the expression of P_{2r} is the same as that of P_1^\sim .

$$P_{2r} = P_1^\sim = C_u(p_{\mu_2}\mu_2) \cap P \tag{14}$$

As presented in the purple blocks in Fig. 3, the effective security control of re-dispatching and load shedding are calculated on the observable and controllable mimic diagram of the physical layer in the control center. The optimal power flow for security control of the physical layer is calculated based on the network P_{2m} via (7) and (8). The results of the optimal dispatch command are applied to corresponding actuators in the actual operational physical layer P_{2r} . As presented in the orange blocks in Fig. 3, the simulation of data transmission would provide the data delay information. The data in which delay is less than the RRT threshold can be transmitted to control the center node on time; otherwise, the physical node operation information would not be updated in the control center or the corresponding actuators would not execute the security control command within the current stage. Besides, due to the gap between P_{2r} and P_{2m} , all constraints might not be satisfied in P_{2r} . Next, the capacities of the edges are checked and over-loaded edges are triggered. In terms of security and reliability, the maximum capacity of an edge in the physical layer is set as its emergency capacity. After the over-loaded edges are cut, the nodes in P_{2r} and P_{2m} should be re-calculated and updated.

3) Stage 3: Additional failures in the cyber layer

The failed nodes in Stage 2 can result in new nodes in the cyber layer losing their energy interdependence, and those without a power supply are in the failed state and need to be removed from the functioning cyber layer component set.

$$C_3^\sim = C_u(\mu_3) \cap C_1 \tag{15}$$

$$C_3 = F(C_3^\sim) \tag{16}$$

where μ_3 denotes the set of nodes that lose energy interdependence in the sub-network; and C_1, C_3 are the sub-network composed of functioning nodes in Stages 1 and 3.

The dynamic development of cascading failures in a CPPS is triggered by the initially malfunctioning and failed nodes as Stage 1. The recursive development of the cascading failure iterates from Stage 2 to 3 and then returns to Stage 2 to begin a new round of iterations. In the second round of iterations, P in (14) is replaced by P_{2i} , which is the functioning set of nodes in the physical layer at the end of the previous iteration. The subscript 2 in Stage 2 is replaced by $2i$ and the subscript 3 in Stage 3 is replaced by $2i + 1$, where i indicates iterations. The cascading failures terminate when the entire CPPS collapses or the number of nodes in the normal state in both layers remains unchanged over two successive iterations.

3.4.4 Cascading failure resilience indices

The indices used to represent the resilience of the CPPS to cascading failures are the ratio of the infected nodes (including partial failure and failure state) in both layers and that of load shedding in the physical layer at the end of cascading failures, which reflect the effects of failures from a topological integrity perspective and those of failures on the electricity yield and degree of load satisfaction from the operational perspective.

$$\begin{cases} R_c = (D_c - D_{c,2i+1})/D_c \\ R_p = (D_p - D_{p2i})/D_p \\ R_l = \sum_n^{D_p} L_n / \sum_n^{D_p} d_n \end{cases} \tag{17}$$

where D_c and D_p are the total number of nodes in the cyber and physical layers, respectively; i indicates the iteration; $D_{c,2i+1}, D_{p2i}$ represent the order of the functioning components in the cyber and physical layers when the cascading failures end, respectively; $\sum_n^{D_p} L_n$ is the total load shedding value at the end of the cascading failures; and $\sum_n^{D_p} d_n$ is the total load before the cascading failures.

4 Mitigation strategies for cascading failures

According to the cascading failure model described in Section 3, the iterations between Stages 2 and 3 reflect the effect of the interdependence relations on the failures in CPPS. Thus, studying mitigation strategies for cascading failures is critical. The strategies proposed in this paper are to be implemented at both layers in the CPPS. In the cyber layer, making the nodes autonomous requires them to be equipped with backup power sources (UPS). This means that the bidirectional interdependencies with the

corresponding physical nodes are transformed into unidirectional 3C-function interdependencies. The FACTS technology can effectively improve the operational conditions for a steady and transient states of power systems, and the mitigation control strategies can effectively relieve the overloads, increase the power-transfer capability, and keep power flowing through the designated routers. Thus, FACTS are embedded in the physical layer, and can be classified into three types: shunt, series, and unified controllers. The shunt controller controls the voltage of the node within a certain range. The series and unified controllers control the active and reactive powers on the transmission line by adjusting the transmission line impedance and injected power of the node. Considering the versatility and multi-controlled variables, as the transmission line impedance and injected node power of the unified power flow controller (UPFC), the UPFC represents FACTS. In addition, the requirement on the computational time for mitigation control is limited, and this paper discusses the application of UPFC for mitigating cascading failures in a DC optimal power flow environment. The control variables include the impedance of the transmission line embedded with the UPFC and the injected active power of the nodes at the two ends of the transmission line.

The objective function of mitigation strategy model after embedding the UPFC is the same as (7), the constraints of that model are represented as follow:

$$\begin{cases} c_{gm}(P_{gm}) = a_m P_{gm}^2 + b_m P_{gm} + c_m \\ P_{gm}^{\min} \leq P_{gm} \leq P_{gm}^{\max} \\ -F_k^{\max} \leq F_k \leq F_k^{\max} \\ F_{\bar{k}} - B_{\bar{k}}(\theta_n - \theta_m) = 0 \\ B_{\bar{k}}^{\min} \leq B_{\bar{k}} \leq B_{\bar{k}}^{\max} \\ F_{\hat{k}} - B_{\hat{k}}(\theta_n - \theta_m) = 0 \\ \sum_{k \in in(n)} F_k - \sum_{k \in out(n)} F_k + \sum_{g \in g(n)} P_g + P_{F(n)} = d_n - L_n \end{cases} \quad (18)$$

where \bar{k} denotes the transmission line set with FACTS; \hat{k} denotes the transmission line set without FACTS; $B_{\bar{k}}$ is the adjustable impedance variable of the transmission line with FACTS; $B_{\hat{k}}$ is the impedance variable of the transmission line without FACTS; $B_{\bar{k}}^{\min}$, $B_{\bar{k}}^{\max}$ are the minimum and maximum values of the impedance range, respectively; $P_{F(n)}$ is the active power input of FACTS at node n .

The fourth equation of (18) is a nonlinear constraint obtained by the multiplication of $B_{\bar{k}}$ and θ . Therefore, the mitigation model becomes a nonlinear program (NLP) model. In [37], the NLP was first converted into a mixed-integer linear program (MILP), and then, the MILP was

reformulated as a two-stage linear program. However, this reformulation is based on the assumption that the adjustment of UPFC does not change the direction of the line's flow. Based on this assumption, the control scale of UPFC can be limited. Here we adopt the McCormick's envelopes [38] to obtain linear program (LP) relaxation. The optimal re-dispatch model with UPFC application of security control in Fig. 3 is based on (7) and (18).

The system overall resilience degradation index (SORDI) indicates the efficiency of the mitigation strategies. The SORDI for the CPPS from topological and operational perspectives indicates the mean of the removed nodes ratio and the physical layer load shedding ratio for simulation of the cascading failures, respectively.

$$SORDI = \begin{cases} \frac{1}{2j} \sum_j (R_c + R_p) & \text{in topological perspective} \\ \frac{1}{j} \sum_j R_l & \text{in operational perspective} \end{cases} \quad (19)$$

where j denotes the simulated number of cascading failures; R_c , R_p and R_l can be calculated using (17).

The efficiency of the mitigation strategy is defined in (20), which shows the extent of alleviating SORDI after the application of the cascading failure mitigation strategy.

$$M = (SORDI - SORDI_m) / SORDI \quad (20)$$

where M is the efficiency of the mitigation strategy; $SORDI_m$ represents the system's overall resilience degradation index after the application of the mitigation strategy. The values of M and $SORDI$ can be derived from either the topological or operational perspectives.

5 Case studies

In this section, CPPS network models are established based on the standard IEEE RTS-1996 system [39], which is a three-area IEEE RTS-1979 system connected through five tie lines. The node load is set as 200% of the default load given in [39]. The cyber layers are a scale-free network generated from the Barabási-Albert model, with two control center nodes, namely main and backup, in the cyber layer. There are bidirectional interdependencies between the physical and cyber layers, which mean that the cyber node provides 3C-function support to the physical node, while the physical node supplies power to the same cyber node. Then, the dynamic development of cascading failures is simulated based on the improved percolation theory. Different scenarios are further simulated and compared for the CPPS network model.



To model and compare the dynamic development of cascading failures under various initial failure sizes, five different sizes of initial malfunctioning cyber nodes are simulated for each CPPS network. The initial malfunctioning cyber nodes are chosen sequentially from the list in which the cyber nodes are ranked according to the number of nodes. In each simulation, it is assumed that all physical nodes corresponding to the malfunctioning cyber nodes have failed during the initial failure, which triggers the cascading failure. Thus, p_{μ_2} in (12) is set to one. According to the PMU allocation criterion, the PMUs are applied to the minimum number of cyber nodes to ensure that the system is fully observable and controllable. The cyber nodes corresponding to physical nodes 2, 10, 11, 17, 20, 24, 27, 28, 31, 34, 40, 45, 47, 50, 51, 55, 58, 64, 70, 71 are equipped with PMUs for the IEEE RTS-1996 system. The numbers of failed nodes at the end of each iteration until the cascading failures terminate are tabulated in Table 1.

Based on these results, the dynamic propagation of cascading failures can be classified as both rapid and slow processes. The second iteration following the initial failure illustrates the rapid process, during which most failed nodes in the cascading failures are infected and isolated from the remaining functioning networks. In the following iterations, the development of the cascading failures slows and the failures converge to a final state. The relation between the failure-infected node ratio in the final state and the initial failure size is nonlinear. To further investigate the nonlinear relation between them, the curves of the cascading failure indices versus the increasing initial failure sizes in various scenarios are illustrated and compared. In each of the following scenarios, the initial failure size is chosen from 5% to 100% at a discrete step of 5%, ranging from a small size to the whole network.

Scenario 1: Benchmark scenario

The PMUs are configured according to the fully observable and controllable criterion. The cascading failure simulation results are presented in Fig. 4.

The curve of load shedding ratio is beyond the infected nodes ratio. This is because the increased load pushes the

Table 1 Number of failed nodes in cyber and physical layers at the end of each iteration for the CPPS with 72 physical nodes

Iteration	Initial failure size				
	10%	20%	30%	40%	50%
1	8, 8	16, 16	30, 30	40, 40	53, 53
2	12, 12	26, 22	37, 33	54, 47	67, 61
3	–	29, 29	38, 38	60, 59	67, 67
4	–	–	–	61, 61	–

system to operate near its limit, and even a small disturbance can lead to large-scale load shedding. The failure transition pattern is a first-order transition and threshold values exist for the initial failure nodes. The index curves show a non-continuous relation in the curve between the initial failure size range and the cascading failure index range. The threshold values correspond to the steepest part of the curve. If the size of the initial failure nodes is close to the threshold value, the cascading failure indices are sensitive to the increase in the initial failure size. A small change in the initial failure size can lead to drastically different results. When the initial failure sizes range from 0.05 to 0.3, the failure of cyber nodes forces some of the data path to reselect the routine path, which can deteriorate the congestion situation of the functioning cyber nodes, and thus, increase data transmission delay. Consequently, the data in the control center and actuators have not been updated to the latest stage. Besides the increased transmission delay, the gap between P_{2r} and P_{2m} grows because the removed cyber nodes cause the physical nodes to enter unobservable and uncontrollable states, which further fuels the development of cascading failures and makes the curves steeper. The threshold value is around 0.35, which means that the remaining functioning nodes and interdependencies are affected, almost all nodes in the CPPS have failed, and all load has been shed by the time the cascading failures terminate.

Scenario 2: All cyber layer nodes are equipped with PMUs and increased data transmission ability

In this scenario, each node in the cyber layer is equipped with a PMU and a synchronized GPS unit. Therefore, in each iteration of cascading failures, every functioning physical node is observable and controllable. The set of P_{2r} fully overlaps P_{2m} . In addition, with the increased data transmission ability in the cyber layer node, more than one

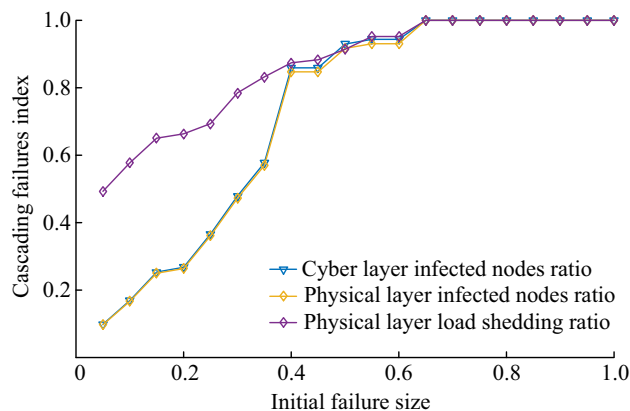


Fig. 4 Cascading failure curves for Scenario 1

data package can be handled within each unit time step simultaneously. The corresponding curves are presented in Fig. 5.

While the failure transition pattern is still a first-order transition, the curves are below that of the benchmark scenario when the initial failure size is not large. This phenomenon illustrates the importance of observability and controllability and the necessity of timely and accurate data, which is consistent with that in our previous research. The fully observable and controllable and decreased delay avoids gaps between P_{2r} and P_{2m} , which ensures that the security control from the cyber layer is optimized for the actual situation in the physical layer, and the control signals no longer cause new unintended violations and tripping of the transmission lines. If the initial failure size is beyond 0.2, the curves overlap, which implies that less data are needed to be transmitted with more nodes into the failure state. Therefore, the increasing data transmission ability makes almost no difference in delay.

Scenario 3: Application of mitigation strategies

The mitigation strategies include Strategy A: transforming the cyber layer nodes into autonomous nodes, and Strategy B: embedding UPFC in the physical layer. Twenty UPFCs are allocated uniformly on branch 1–100. The efficiencies of the mitigation strategies are listed in Table 2.

The efficiency of Strategy A is demonstrated mainly from both the topological perspectives, while that of Strategy B is manifested mainly from the operational perspective. This is fair as Strategy A transforms some of the bidirectional interdependencies into unidirectional interdependencies, which changes how the two layers interact.

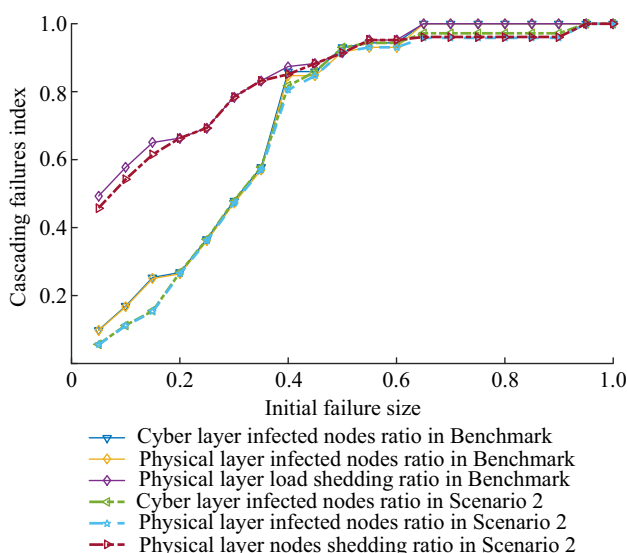


Fig. 5 Cascading failure curves for Scenario 2

Strategy B cannot cause fundamental changes in the development of cascading failures; however, it can control the active and reactive power on the transmission line and keep power flowing through the designated routes. Consequently, load shedding in the physical power flow analysis stage is reduced. The combination of these two strategies exhibits greater efficiency than they do individually, which illustrates the complex coupled relation between the topology and operation of the two layers.

The curves for the Benchmark scenario and the scenario where in both mitigation strategies are applied are compared in Fig. 6.

When the initial failure size interval ranges from 0.1 to 0.5, the mitigation strategies are more effective. When the dotted curves are compared with their solid counterparts, the indices on the dotted curves are reduced for the same initial failure sizes and the curves follow a more continuous second-order failure transition characteristic. The nodes infected ratio in Scenario 3 exhibits a second-order transition characteristic, which can be ascribed to the fact that bidirectional interdependencies have become unidirectional interdependencies and the operation of the cyber layer nodes does not depend on the states of the coupled physical layer. This phenomenon illustrates that, in

Table 2 Efficiencies of the mitigation strategies

Mitigation efficiency	Topological perspective (%)	Operational perspective (%)
Strategy A	8.62	2.40
Strategy B	3.04	10.57
Both strategies	8.72	11.94

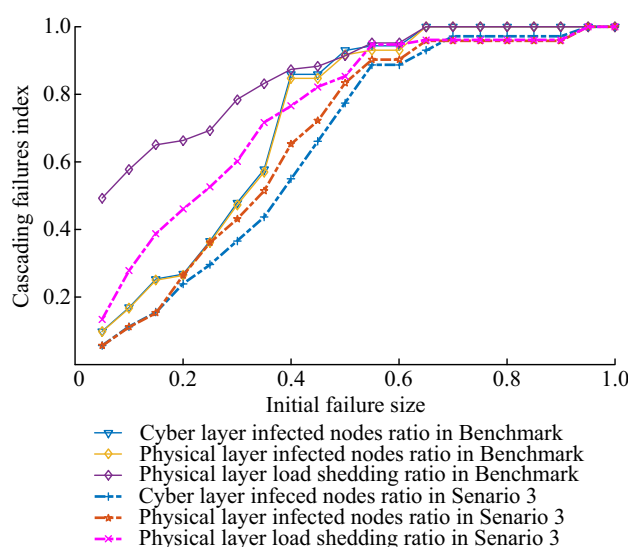


Fig. 6 Cascading failure curves for Scenario 3



interdependent networks, the interdependencies are the corridors through which the failures develop between the layers and exacerbate the propagation size of cascading failures. Meanwhile, the difference between the physical layer load shedding ratio and that in the benchmark scenario is the largest in this scenario. For the initial failure size that ranges from 0.05 to 0.2, the physical layer load shedding ratio decrease from more than 0.5 to less than 0.4. The application of UPFC expands the controllable variables in security control and improves the physical layer's operation limit.

6 Conclusion

This paper introduces an interdependence strategy based on node classification and geographic closeness. To model cascading failures in a CPPS, we propose an improved percolation theory in which the operational analysis and simulation of both layers and the role of indirect interaction mechanism in failure propagation are taken into account. In addition, two cascading failure mitigation strategies are presented from both a network interdependence relation perspective and a physical layer operational perspective. Cascading failures in a CPPS with increasing initial failure sizes are then simulated for different scenarios.

The results demonstrate that the fundamental reasons for the first-order transition of cascading failures are the interdependence relation and the gap between the observable and controllable physical layer and the actual operational one. Because of the complex coupled topological and operational relations between the two layers, these mitigation strategies should be applied simultaneously to alleviate the influence of cascading failures. This is especially true when decreasing the physical layer load shedding ratio and transitioning the failures to have more continuous second-order transition characteristics.

Acknowledgements This work was supported by the National Natural Science Foundation of China (No. 51537010), the National Key Basic Research Program (973 Program) (No. 2013CB228206) and the project of "The up layer design for DC-AC hybrid grids system protection" (No. XT71-16-053).

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- [1] Han Y, Wen Y, Guo C et al (2015) Incorporating cyber layer failures in composite power system reliability evaluations. *Energies* 8(9):9064–9086
- [2] Buldyrev SV, Havlin S, Parshani R et al (2010) Catastrophic cascade of failures in interdependent networks. *Nature* 464(7291):1025–1028
- [3] Huang Z, Wang C, Stojmenovic M et al (2013) Balancing system survivability and cost of smart grid via modeling cascading failures. *IEEE Trans Emerg Topics Comput* 1(1):45–56
- [4] Andersson G, Donalek P, Farmer R et al (2005) Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Trans Power Syst* 20(4):1922–1928
- [5] Das A, Banerjee J, Sen A (2014) Root cause analysis of failures in interdependent power-communication networks. In: Proceedings of IEEE military communications conference, Baltimore, USA, 6–8 October 2014, pp 910–915
- [6] Rahnamay-Naeini M, Hayat M (2016) Cascading failures in interdependent infrastructures: an interdependent Markov-Chain approach. *IEEE Trans Smart Grid* 7(4):2340–2350
- [7] Rahnamay-Naeini M (2016) Designing cascade-resilient interdependent networks by optimum allocation of interdependencies. In: Proceedings of international conference on computing, networking and communications, Kauai, USA, 15–18 February 2016, pp 1–7
- [8] Huang Z, Wang C, Ruj S et al (2013) Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory. In: Proceedings of IEEE industrial electronics and applications, Melbourne, Australia, 19–21 June 2013, pp 1023–1028
- [9] Huang Z, Wang C, Stojmenovic M et al (2015) Characterization of cascading failures in interdependent cyber-physical systems. *IEEE Trans Comput* 64(8):2158–2168
- [10] Shao J, Buldyrev SV, Havlin S et al (2011) Cascade of failures in coupled network systems with multiple support-dependence relations. *Phys Rev E Stat Nonlinear Soft Matter Phys* 83(3 Pt 2):1127–1134
- [11] Huang Z, Wang C, Nayak A et al (2015) Small cluster in cyber physical systems: network topology, interdependence and cascading failures. *IEEE Trans Parallel Distrib Syst* 26(8):2340–2351
- [12] Muro MAD, Buldyrev SV, Stanley HE et al (2016) Cascading failures in interdependent networks with finite functional clusters. *Phys Rev E* 94:1–9
- [13] Liu RR, Li M, Jia CX (2016) Cascading failures in coupled networks: the critical role of node-coupling strength across networks. *Sci Rep* 6:1–6
- [14] Liu RR, Li M, Jia CX et al (2016) Corrigendum: cascading failures in coupled networks with both inner-dependency and inter-dependency links. *Sci Rep* 6:1–9
- [15] Parshani R, Rozenblat C, Ietri D et al (2011) Inter-similarity between coupled networks. *EPL* 92(6):2470–2484
- [16] Ranjan G, Zhang ZL (2011) How to glue a robust smart-grid: a "finite-network" theory for interdependent network robustness. The workshop on cyber security and information intelligence research. ACM, 2011
- [17] Wang H, Li M, Deng L et al (2015) Percolation on networks with conditional dependence group. *PLoS ONE* 10(5):e0126674
- [18] Cuadra L, Salcedo-Sanz S, Ser JD et al (2015) A critical review of robustness in power grids using complex networks concepts. *Energies* 8(9):9211–9265

- [19] Xin S, Guo Q, Sun H et al (2015) Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. *IEEE Trans Smart Grid* 6(5):2375–2385
- [20] Davis KR, Davis CM, Zonouz SA et al (2015) A cyber-physical modeling and assessment framework for power grid infrastructures. *IEEE Trans Smart Grid* 6(5):2464–2475
- [21] Cai Y, Cao Y, Li Y et al (2016) Cascading failure analysis considering interaction between power grids and communication networks. *IEEE Trans Smart Grid* 7(1):530–538
- [22] Cai Y, Li Y, Cao Y et al (2017) Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids. *Int J Electr Power Energy Syst* 89:106–114
- [23] Han Y, Guo C, Zhu B et al (2016) Model cascading failures in cyber physical power system based on improved percolation theory. *Autom Electr Power Syst* 40(17):30–37
- [24] Han Y, Li Z, Guo C et al (2016) Improved percolation theory incorporating power flow analysis to model cascading failures in cyber-physical power system. In: *Proceedings of IEEE power and energy society general meeting, Boston, USA, 17–21 July 2016*, pp 1–5
- [25] Qi J, Sun K, Mei S (2015) An interaction model for simulation and mitigation of cascading failures. *IEEE Trans Power Syst* 30(2):804–819
- [26] Newman DE, Carreras BA, Lynch VE et al (2011) Exploring complex systems aspects of blackout risk and mitigation. *IEEE Trans Reliab* 60(1):134–143
- [27] Xiao Y, Song YH, Sun YZ (2002) Power flow control approach to power systems with embedded FACTS devices. *IEEE Trans Power Syst* 17(4):943–950
- [28] Schneider CM, Yazdani N, Araújo NA et al (2013) Towards designing robust coupled networks. *Physics* 3(24):1–7
- [29] Wang J (2012) Mitigation of cascading failures on complex networks. *Nonlinear Dyn* 70(3):1959–1967
- [30] Yağan O, Qian D, Zhang J et al (2012) Optimal allocation of interconnecting links in cyber-physical systems: interdependence, cascading failures, and robustness. *IEEE Trans Parallel Distrib Syst* 23(9):1708–1720
- [31] Aminifar F, Fotuhi-Firuzabad M, Shahidehpour M et al (2012) Impact of WAMS malfunction on power system reliability assessment. *IEEE Trans Smart Grid* 3(3):1302–1309
- [32] Dehghani M, Goel L, Li W (2014) PMU based observability reliability evaluation in electric power systems. *Electr Power Syst Res* 116(116):347–354
- [33] Li GW, Ju WY, Duan XZ et al (2012) Transmission characteristics analysis of the electric power dispatching data network. *Proc CSEE* 32(22):141–148
- [34] Yong L, Li W, Yi T et al (2017) Hierarchical decomposition for betweenness centrality measure of complex networks. *Sci Rep* 7:1–12
- [35] Brockmann D, Helbing D (2013) The hidden geometry of complex, network-driven contagion phenomena. *Science* 342(6164):1337–1342
- [36] Pradhan A, Mahinthakumar G (2013) Finding all-pairs shortest path for a large-scale transportation network using parallel Floyd–Warshall and parallel Dijkstra algorithms. *J Comput Civ Eng* 27(3):263–273
- [37] Sahraei-Ardakani M, Hedman KW (2015) A fast LP approach for enhanced utilization of variable impedance based FACTS devices. *IEEE Trans Power Syst* 21(3):2204–2213
- [38] Wen Y, Li W, Huang G et al (2016) Frequency dynamics constrained unit commitment with battery energy storage. *IEEE Trans Power Syst* 31(6):5115–5125
- [39] Grigg C, Wong P, Albrecht P et al (1999) The IEEE reliability test system-1996: a report prepared by the reliability test system task force of the application of probability methods subcommittee. *IEEE Trans Power Syst* 14(3):1010–1020

Yuqi HAN is currently a Ph.D. candidate in Zhejiang University. He obtained bachelor and master degrees in Electrical Engineering at Nanchang University (2012) and Georgia Institute of Technology (2014). His research interests include cyber-physical power system reliability, cyber-physical power system cascading failures.

Chuangxin GUO received the Ph.D. degree in electrical engineering from Huazhong University of Science and Technology, Wuhan, Hubei, China (1997). He is currently a Professor and the Vice Dean with the College of Electrical Engineering, Zhejiang University, Hangzhou, Zhejiang, China. His research interests include smart grid, power system reliability and power system data communication system.

Shiying MA is currently a senior engineer in China Electric Power Research Institute. His research interests include power system analysis and simulation, also power system voltage stability and reactive power control.

Dunwen SONG is currently a senior engineer in China Electric Power Research Institute. His research interests include power system stability analysis and control, also power system simulation tools development.

