IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 29, 2018, accepted July 3, 2018, date of current version August 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2855441

Cascading Failure Analysis of Cyber Physical Power System With Multiple Interdependency and Control Threshold

YU CHEN[1], YONG LI[1], (Senior Member, IEEE), WENGUO LI[1], (Senior Member, IEEE), XIAORUI WU[1], YE CAI[2], YIJIA CAO[1], (Senior Member, IEEE), AND CHRISTIAN REHTANZ[3], (Senior Member, IEEE)

[1]College of Electrical and Information Engineering, Hunan University, Changsha 410006, China
[2]Hunan Province 2011 Collaborative Innovation Center of Clean Energy and Smart Grid, Changsha University of Science and Technology, Changsha 410205, China
[3]Institute of Energy Systems, Energy Efficiency and Energy Economics, TU Dortmund University, 44227 Dortmund, Germany

Corresponding author: Yong Li (yongli@hnu.edu.cn)

This work was supported in part by the 111 Project of China under Grant B17016, in part by the National Natural Science Foundation of China (NSFC) under Grant 51520105011, in part by the Huxiang Youth Talent Program of Hunan Province under Grant 2015RS4022, in part by the Excellent Innovation Youth Program of Changsha of China under Grant KQ1707003, and in part by the National Natural Science Foundation of China (NSFC) under Grant 51607011.

ABSTRACT The traditional infrastructure in power system is undergoing a transition to the Smart Grid, in which the communication network and power grid will be integrated into a cyber-physical power system (CPPS). Although the traditional topological analysis reveals the mechanism of cascading failure between two networks, it ignores the control redundancy and standby lines from communication network to power grid. The robustness analysis in CPPS requires a more comprehensive model to analyze failure behavior in reality. Here, we propose a cascading failure model with one-to-multiple interdependency and a relevant theoretical framework to analyze CPPS cascading failure. In consideration of real CPPS, in the proposed model we introduce two robustness factors, the number of dependent links and control threshold, which can better describe the control function from communication nodes to power nodes. The remaining fraction under different initial attacking on high voltage transmission network, small world network, double star network, and the different topological combination of CPPS are analyzed. The results show that the proposed model and robustness factors can better reveal the robustness and the mechanism of two networks in cascading failure.

INDEX TERMS Cascading failure, control threshold, cyber physical system, percolation theory, robustness.

I. INTRODUCTION

With the development of communication and control technology, the traditional power grid is undergoing a change from a single power grid to an extremely large and complex multi-network coupled system (cyber-physical power system, CPPS) which composed of the traditional power grid and communication network [1]–[3], [33]–[35]. As a consequence, an initial disturbance or failure in power grid or communication network could trigger cascade failure, such as the 2003 North American blackout [4], the Italy blackout [5] and the 2004 Rome blackout [6]. Therefore, it is of much significance to analyze the mechanism of cascading failure in the cyber-physical system.

Traditional power flow methods are expanded to analyze the physical side of intra cascading failure. However, power flow calculation is more adopted in the preconceived power system accident analysis under N-1 contingencies. When it is carried out in the fast circulating state, the complexity is more difficult to handle. Although DC power flow methods is powerful for its balance between model complexity and system behavior approximation, compared to the AC flow models [7]–[10], the computing scenes number of cascading fault analysis still increases exponentially with the increase of nodes number. There are some models based on the whole system characteristic, such as the OPA (optimal power flow) model [11], CASCADE model [12], influence graph model [31], [32] and node dynamic model [13].

These methods have been studied intensively for some years, but research still focus on the single, non-interacting power grid. Whether these methods could be extended to the CPPS is still studied rarely.

The model of interdependent networks based on the complex networks theory develops a view of understanding cascading failures between the interdependent networks. Studies based on percolation theory show that the cascading failure transition in the one-to-one interdependent networks is first-order phenomena, while in isolated power networks, the cascading failure transition is second-order phenomena [14]–[16]. Then, different interface strategies such as random interface strategy, degree-to-betweenness interface strategy and topological centrality interface strategy are simulated. It shows that the more inter-similar between the two networks are, the more robustness of the network to cascading failures is [17]. The previous studies mostly are based on the one-to-one interdependent networks, that is, the number of nodes in the power network is equal to the cyber network, and one power node is only dependent on one cyber node. A theoretical framework for understanding the robustness of interdependent networks with a random number of support and dependence relationship was provided [18], which extends previous works on coupled networks from one-to-one support-dependence relation to multiple support-dependence relation. Reference [19] has observed that the interdependency between power grid and communication network is one to multiple. However, even after considering the multi-correspondence relationship, the coupling between the power system and the communication network is more complicated than the coupling between the two simple topologies. One important reason is that standby control lines exist in cyber-physical power system, and the communication node controls power node with some redundancy. There is little research on the relationship between this redundancy and system robustness.

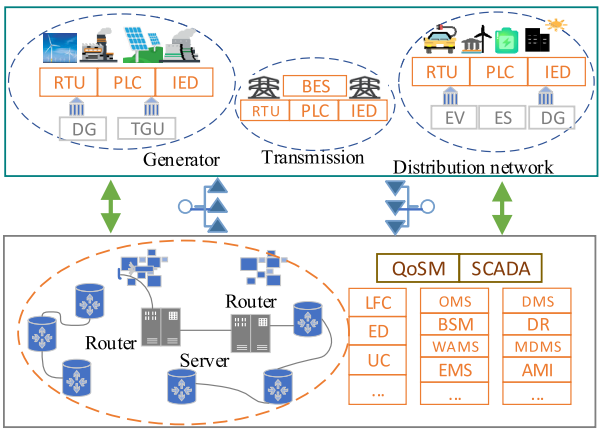
In this paper, we consider the more practical control situation. The cascading failure characteristic of whole interdependent system between actual power system and double star communication network are analyzed using interdependency theory and percolation theory. In the view of the fact that control standby lines exist, each node is considered to have control margin, they need the support of a minimum number of control supply nodes to remain function. For complex network structure of power system, the coupling relationship between communication network and power grid affects the robustness of whole system. Specially, the relationship between critical point and interdependent links are analyzed. On the other hand, the robustness is also influenced by the varying of control threshold. Therefore, a mathematical model of cascading failure considering two different situations, the varying of control threshold and the varying of interdependent number, are analyzed respectively.

The rest of this paper is organized as follows. First, the special framework of future CPPS and extended model of cascading failure are presented in Section II. Then, a measure called critical point is described in Section III. Simulations and a variety of results for different topological networks are shown in Section IV. The conclusion and future work are provided in Section V.

II. MODELING THE CASCADING FAILURE IN CPPS WITH CONTROL THRESHOLD

A. CASCADING FAILURE WITH ONE-TO-MULTIPLE INTERDEPENDENCY

The explicit modules of CPPS are shown as Fig. 1 [1], [21], [25]. In the view of complex networks, the nodes coupling is the simplicity of realistic system. There are two types of links in interdependent networks, connectivity link and interdependent link. Connectivity link represents the intra-interdependency of each network. The function of the nodes in both networks is maintained by connectivity link w [22], [23]. For the CPPS, connectivity link represents the transmission line in the power grid or the communication line in the cyber network, and the interdependent link realizes the exchange of energy or information between power grid and cyber network.



DG: Distributed Generation
TGU: Traditional Generating Unit
RTU: Remote Terminal Units
PLC: Programmable Logic Circuits
IED: Intelligent Electronic Devices
BES: Bulk Energy Storage
EV: Electric Vehicles
ES: Energy Storage
LFC: Load Frequency Control
ED: Economic Dispatch
UC: Unit Commitment
OMS: Outage Management System
BSM: Bulk Storage Management
WAMS: Wide-Area Monitoring System
EMS: Energy Management System
DMS: Distributed Management Systems
MDMS: Meter Data Management Systems
AMI: Advanced Meter Infrastructure

FIGURE 1. Illustration on control redundancy of CPPS.

Generally, both power grid and cyber network can be expressed as unweighted undirected graphs G and C, where G represents power grid and C represents communication network. $G = (U_G, E_G)$, $U = \{u_1, u_2, \ldots u_{NG}\}$ and $C = (V_C, E_C)$, $V = \{v_1, v_2, \ldots v_{NC}\}$ are the sets of each intra-network description respectively, $E = \{e_{ij}\}$ is the set of network connectivity links. In addition, the interdependent effects of power stations and information stations are established as set $E_I, E_I = \{E_{C-G}, E_{G-C}\}$, where E_{C-G} expresses the matrix of interdependent links that cyber layer depends on

$$g_G(p) = 1 - G_0^G[1 - p(1 - f_\infty^G)] \quad (3)$$

$$f_\infty^G = G_1^G[1 - p(1 - f_\infty^G)] \quad (4)$$

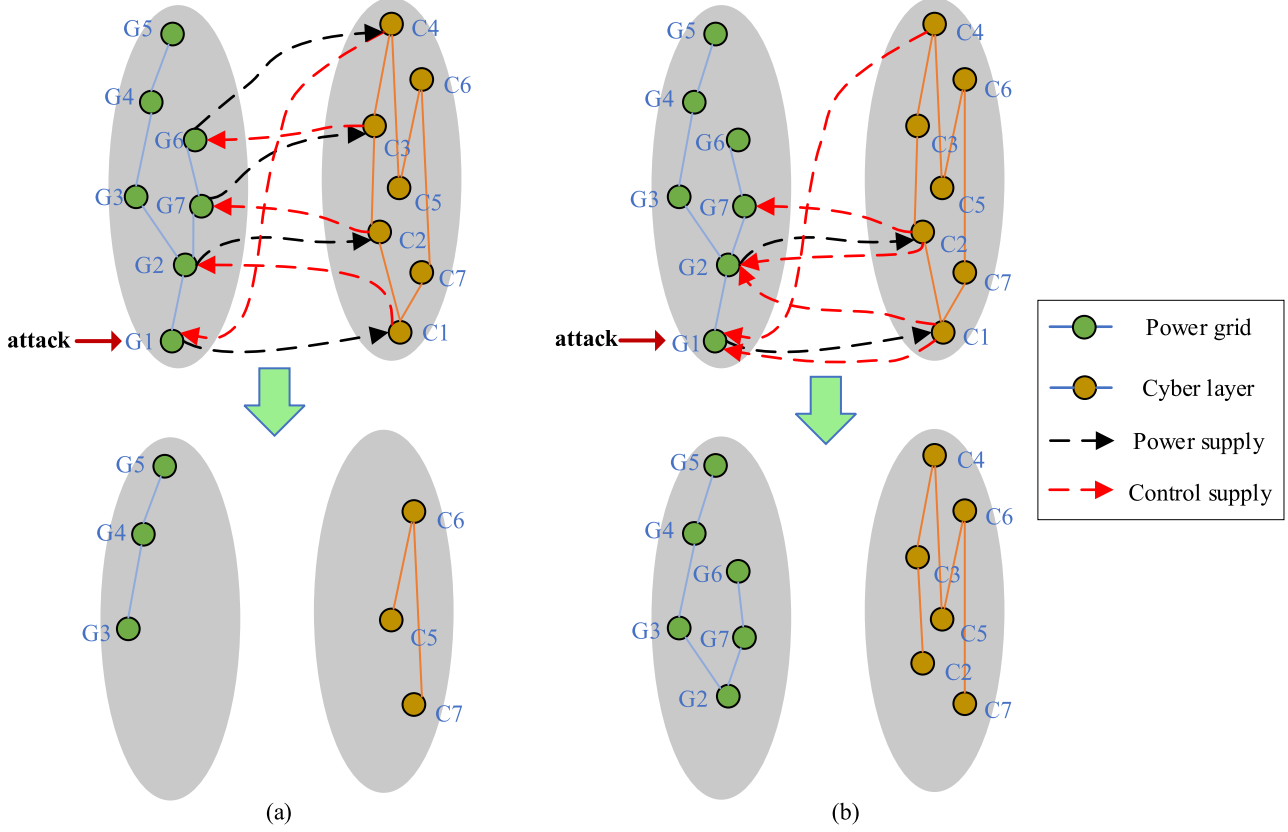


FIGURE 2. The cyber-physical network of (a) one control interdependency and (b) multiple control interdependency with initial attack.

the power grid. It represents cyber node u has failure without energy supply from power node v when $n_{C-G}(u, v) = 0$, where $n_{C-G}(u, v)$ is the number of interdependent links from node v in power grid to node u in communication network. The whole CPPS is expressed as set $\xi(G, C, E, E_I)$.

Most of the research results of interdependent networks are based on the coupling ruler of one-to-one correspondence, as shown in Fig. 2(a). While in the realistic situation, there are multiple dependent links between electric power stations and communication stations. An electric power station can provide power for multiple information stations, and at the same time, an information station controls multiple power stations [24].

In the proposed model, each power node supplies the energy for each communication node, while each communication node controls multiple power node. The propagating process of initial attack is different between one control interdependency (Fig. 2(a)) and multiple control interdependency. The green nodes and brown nodes represent power nodes and communication nodes respectively. In one to one model (Fig. 2(a)), the power supply link goes from one green node and to one brown, controlling supply link is opposite with red dotted lines. From Fig. 2(b), one communication node has two controlling supply links which control two different power nodes. The power supply links have not changed. Hence, the number of nodes in cyber layer is equal to that in power grid. And the number of power supply-demand interdependent links is equal to the number of nodes in power grid. The number of controlling supply-demand links is two times larger than that in one-to-one model. In general, communication node will fail when it isn't connected with the power node and the same as power node. The cascading failure with initial attack in Fig. 2(a) propagates in the process of G1-C1-G2-C2-G7-C3-G6-C4, ending up in C4 because of the C4 control power node G1. While in Fig. 2(b), system has some difference from C1 to G2. Although supply control from C2 to G2 is fault, the standby link C2-G2 functionally works and supplies the necessary control. The number of interdependent links is no longer only 1. Hence the failure nodes are just G1 and C1.

B. CASCADING FAILURE WITH CONTROL THRESHOLD

Applying the one-to-multiple model to CPPS, the control threshold is considered. Industrial protocol such as IEEE 61850 and DNP3 have been proposed to standardize communication between control manage center and substation. New standard of PMU and PLC will also be established. The link cables are redundant because some of multiple modular achieve same function. The corresponding relationship of cyber layer and power grid is not must be so strict that

interdependent links can't break. SCADA system usually has standby communication lines for emergency control. Generally, the number of interdependent links from cyber layer to power grid has a certain redundancy in order to ensure the reliability of power supply system.

Both power grid and communication network are considered with N nodes respectively in real system. The initial failure nodes is 1-p fraction nodes, $(1\text{-}p)N$. Each node i in power grid has c_i control supply nodes from cyber layer. This node of power grid remains its function if the number of its functional supply nodes in the cyber layer remains greater or equal to its supply threshold $c_i^* \leq c_i$. The supply threshold is predefined as assumed for each node in power grid. In some case, some nodes in power grid are must controlled by multiple communication nodes such as multiple wide-area control. The control threshold represents the power nodes minimal necessary interdependent links from cyber layer.

Two conditions should be satisfied if a node in power grid works functionally.

1) The node belongs to the giant component in its own network.

2) There are at lease c_i^* control supply interdependent links of that node, where these links come from other functionally nodes in the cyber layer.

So the cascading failure model build firstly is that a random fraction 1-p of the nodes in power grid are attacked, then we calculate the giant component of power grid, then the failure judgment transfers to cyber layer. The cascading failure is divided into several steps. In the k step, we firstly judge the power grid

$$n_{G-C(i)}^k < c_i^* \tag{1}$$

where $n_{G-C(i)}^k$ is the number of real time interdependent links of node i in power grid supplied from cyber layer in failure process. That is, one power station is easier to break than they used to be when $c_i^* > 1$, since it needs control supply from more control stations. While the communication nodes in this paper is set to be supplied by single power station. Then the cyber layer is judged by

$$n_{C-G(i)}^k < 1 \tag{2}$$

Each node i in cyber layer has $n^{kC-G(i)}$ power supply nodes in the power grid that connected to node i by supply links.

III. ROBUSTNESS EVALUATION OF CPPS IN CASCADING FAILURE

The characteristic of cascading failure in two coupling networks are different from the second-order phase transition in single intra network. It is first-order phase transition [14]. At the ending of cascading failure, the probability of randomly selected node belonging to the giant component is μ.

We analyze the dynamic of cascading failure using percolation theory in this section. The power grid G and cyber layer C have the degree distribution $P_G(k)$ and $P_C(k)$, when 1-p of power nodes are randomly attacked, the exacerbation factor of power grid is

$$g_G(p) = 1 - G_0^G[1 - p(1 - f_\infty^G)] \tag{3}$$

where f_∞^G is the probability that satisfied the transcendental equation

$$f_\infty^G = G_1^G[1 - p(1 - f_\infty^G)] \tag{4}$$

And the communication network has the same form. The generating function of the degree distribution is $G_0^G(x) = \sum_k P_G(k)x^k$.Analogous, the generating function of excess degree distribution is $G_1^G(x) = G_0^{G'}(x)/G_0^{G'}$ [26], [27].

For simplicity, we assume that function $p_s(j, c)$ is a probability that a node with c supply links works functionally if j of its c supply nodes in the cyber layer work functionally, then a cumulative probability distribution of power grid is calculated

$$t_{sG}(j, c) = P(c_{sG}^* \leq j | c_{sG} = c) \tag{5}$$

where $P(|)$ is the conditional probability. The cumulative probability distribution of communication network is the same. From conventional homogeneous k-core percolation [20], [38]–[40], we introduce the function $H_{sG}(x)$, $H_{sC}(x)$, $L_{sG}(x)$, $L_{sC}(x)$.

$$H_{sG}(\gamma) = \sum_{c=0}^{\infty} P_{sG}(c) \sum_{j=0}^{c} \binom{c}{j} t_{sG}(j, c)\gamma^j(1-\gamma)^{c-j} \tag{6}$$

$$L_{sG}(\gamma) = \sum_{c=0}^{\infty} \frac{cP_{sG}(k)}{< c_s >} \sum_{j=0}^{c-1} t_{sG}(j+1, c)\gamma^j(1-\gamma)^{c-j} \tag{7}$$

where $H_{sG}(x)$ and $L_{sG}(x)$ are the k-core generating functions of degree distribution and excess degree distribution of supply links in power grid. The cumulative distribution of threshold in power grid is finally simplified to

$$t_{sG}(j, c) = \begin{cases} 0, & c_{sG}^* > j \\ 1, & c_{sG}^* \leq j \end{cases} \tag{8}$$

And that in cyber layer are

$$H_{sC}(\gamma) = \sum_{c=0}^{\infty} P_{sC}(c) \sum_{j=0}^{c} \binom{c}{j} t_{sC}(j, c)\gamma^j(1-\gamma)^{c-j} \tag{9}$$

$$L_{sC}(\gamma) = \sum_{c=0}^{\infty} \frac{cP_{sC}(c)}{< c_s >} \sum_{j=0}^{c-1} t_{sC}(j+1, c)\gamma^j(1-\gamma)^{c-j} \tag{10}$$

The cumulative distribution of threshold in communication network is given by

$$t_{sC}(j, c) = \begin{cases} 0, & j < 1 \\ 1, & j \geq 1 \end{cases} \tag{11}$$

We analyze the percolation step of failure propagation between power grid and communication network. In stage 1, after remove 1-p fraction of nodes, the surviving fraction of

power grid is determined by condition (1). It can be expressed in the closed-form expression

$$\mu_{G,1} = pg_G(p) \tag{12}$$

The probability of that random interdependent links are correspond to functionally work nodes in power grid is

$$f_{C,1} = \mu_{G,1} \tag{13}$$

In stage 1 it equals to the fraction of surviving power nodes. Then the remaining fraction of communication network is considered. The initial failure nodes in communication network caused by broke interdependent links is

$$y_{C,1} = H_{sC}(f_{C,1}) \tag{14}$$

The surviving fraction of communication network is

$$\mu_{C,1} = y_{C,1}g_C(y_{C,1}) \tag{15}$$

However, when the failure is re-propagated from communication network to power grid, it no longer simply follows the probability relationship of the probability $\mu_{C,1}$, so $f_{G,2} \neq \mu_{C,1}$. Because of the control margin, the situation that all the power nodes corresponding to the failed control links can't work no longer exists.

Therefore, we must first analyze the failure probability of interdependent links from communication network to power grid in stage 2. If one interdependent link corresponds to node i in power grid and node j in communication network, then the probability of its surviving depends on how many other links (belong to node i or j) survive. Then $f_{G,2}$ should multiply the generating function of excess degree distribution L_{sC}.

$$f_{G,2} = L_{sC}(f_{C,1})g_C(y_{C,1}) \tag{16}$$

The $f_{G,2}$ is calculated and then the probability of unfunctionally working power nodes caused by the out-of-order interdependent links can be calculated, just using generating function of degree distribution $H_{sG}()$, which is similar to stage 1.

$$y_{G,2} = pH_{sG}(f_{G,2}) \tag{17}$$

Then the size of finite components in power grid caused by its intra-dependency is

$$\mu_{G,2} = y_{G,2}g_G(y_{G,2}) \tag{18}$$

In same way, the recursion relations for the stages $n > 1$ are

$$f_{G,n} = L_{sC}(f_{C,n-1})g_C(y_{C,n-1}) \tag{19}$$
$$f_{C,n} = pL_{sG}(f_{G,n})g_G(y_{G,n}) \tag{20}$$

where

$$y_{G,n} = pH_{sG}(f_{G,n}) \tag{21}$$
$$y_{C,n} = H_{sC}(f_{C,n}) \tag{22}$$

The fractions of functional nodes at stage n in the cascade failure are

$$\mu_{G,n} = y_{G,n}g_G(y_{G,n}) \tag{23}$$
$$\mu_{C,n} = y_{C,n}g_C(y_{C,n}) \tag{24}$$

We have the obtained equation in terms of f_G at the steady state

$$f_{G,n} = f_{G,n-1} = f_G \tag{25}$$
$$f_G = L_{sC}(f_C)[H_{sC}(f_C)] \tag{26}$$

where

$$f_C = pH_{sG}(f_G)\, g_G[pH_{sG}(f_G)] \tag{27}$$

Graph solution is used to find the critical point p_c, which should satisfy

$$\frac{dF(f_A)}{df_A} = 1 \tag{28}$$

The Eqs. (26) and (28) can be used to calculated the critical point p_c.

The mechanism of cascading failure in section II can be analyzed through above formula. We measured the relationship between probability μ and initial remaining ratio p of nodes after attacked, shown as $p-\mu$ curve. Although the size of smart grid is not as large as complex network, this curve is still effective in the aspect of cascading failure. In the curve, μ changes obviously. When $p < p_c$, μ is approximately 0, and $p > p_c$ $\mu > 0$. Obviously, the critical point p_c is an index of the system robustness in cascading failure. The smaller critical point is, the more initial attacking ratio needs for whole system collapse [20].

IV. SIMULATION AND ANALYSIS

A. BENCHMARK POWEWR SYSTEM

Our tested power grid is taken from the High Voltage (HV) transmission system in Hunan Province, China, which has 241 nodes and edges. The details are described in Table 1. This network is one typical small world network. It satisfied

$$C \gg C_{random} \tag{29}$$
$$L \geq L_{random} \tag{30}$$

where C_{random} is the *Clustering Coefficient* in random network with the same nodes of the HV transmission system. L_{random} is the *Characteristic Path Length* in random network with the same nodes of the HV transmission system [28], [29]. For a general situation to reflect power grid, we used the small world with 2000 nodes to simulation. The details are shown as Table 1. N and M are the numbers of nodes and edges. $< k >$ is the average degree of the network.

B. BENCHMARK COMMUNICATION NETWORK

To compare the influence of communication network topology on the cascading failure of CPPS, two topologies of communication network is simulated. The SW network in communication network has the same topology as the power grid. While the Double Star(DS) communication networks are the scale-free networks, whose degree distribution follows a power law, $P_C(k) \propto k^{-\gamma}$, where $P(k)$ is the probability that the degree of a node is k, γ is power law exponent. The details are shown as Table 2.

TABLE 1. Topology parameters in power grid.

	N	M	<k>	C	L
HV transmission system	241	371	3.08	0.19	5.87
Random network	241	365	3.08	0.0168	4.98
SW network in power grid	2000	3562	3.50	0.19	6.08

TABLE 2. Topology parameters in communication network.

	N	M	<k>	C	L
SW communication network	2000	3562	3.50	0.19	6.08
DS communication network	2000	3600	3.60	0.95	1.98

C. SIMULATION STEPS

When new failure occurs in the power grid, the intra dependency would be disrupted, and some power grid nodes need to be removed. Then the failure spread through interdependent links. The similar process occurs in communication networks. The interdependency from communication network to power grid makes the failure spread to power grid again. Specifically, the following simulating steps are performed.

Step 1: Generate random failure nodes in power grid. In each simulation, we vary the size of the initiating attacking proportion, 1-p, which the number of power nodes in the initial random failure is (1-p) $\times$ N.

Step 2: Calculate the remaining nodes in power grid. Because the nodes fault cause related links to break, the intra-dependencies work unfunctionally and the failure in power grid spreads. The remaining nodes after the intra failure are calculated according intra-dependent links.

Step 3: Judge whether the number of remaining nodes in power grid is 0 or it is equal to the number in last **step 2**. If true, the cascading failure ends. Else turn to **step 4**.

Step 4: Mark failure nodes in communication network for interdependent links fault and remove failure nodes in power grid. According to the supply relationship from power grid to communication network, if $n_{C-G(i)} < 1$, then the node i in communication network has fault. After the failure nodes are marked, remove the failure nodes of power grid in **step 2**.

Step 5: Calculate the remaining nodes in communication network. It is the same as **step 2**.

Step 6: Judge whether the number of remaining nodes in communication network is 0 or it is equal to the number in last **step 4**. If true, the cascading failure ends. Else turn to **step 7**.

Step 7: Mark failure nodes in power grid for interdependent links fault and remove failure nodes in communication network. According to the supply relationship from communication network to power grid, if $n_{C-G(i)} < c^*_{sG}$, then the node i in power grid has fault. After the failure nodes are marked, remove the failure nodes of communication network in step 5. Turn to step 2.

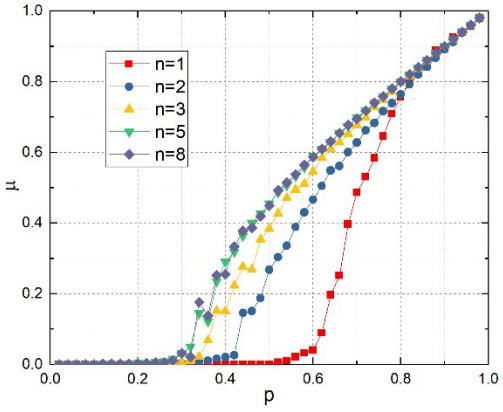


FIGURE 3. Robustness of SW-SW coupled networks to random failures, with varying numbers of interdependent links n.

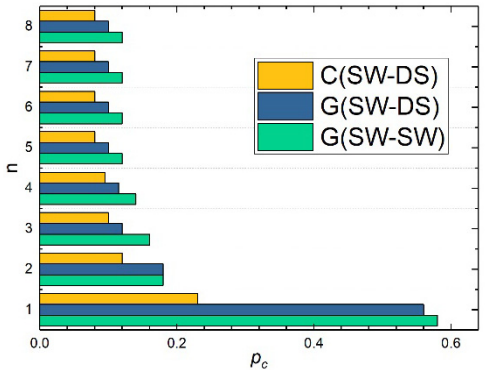


FIGURE 4. Critical point of three models, with varying numbers of interdependent links n.

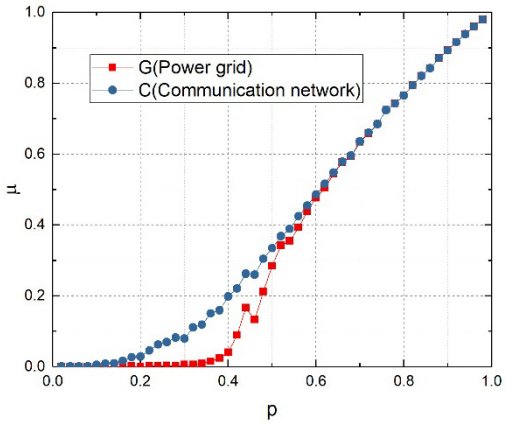


FIGURE 5. Robustness comparison between power grid and communication network in SW-DS model with $n = 2$.

D. CASCADING FAILURE WITH INTERDEPENDENT LINKS

First, we analyze the p-μ curve with the number of interdependent links in SW-SW coupling networks model. The result is shown as Fig. 3. The system's robustness increases with

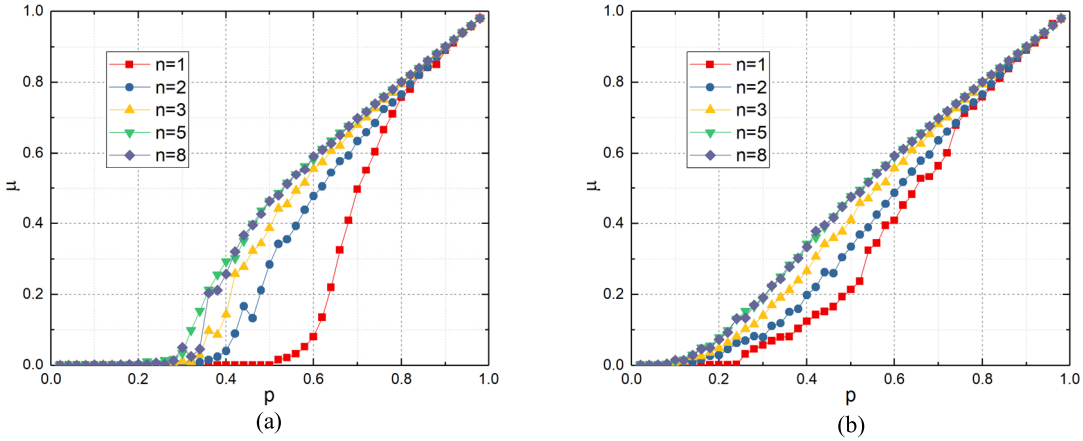


FIGURE 6. Robustness of SW-DS coupled networks to random failures in power grid(a) and communication network(b), with varying numbers of interdependent links n.

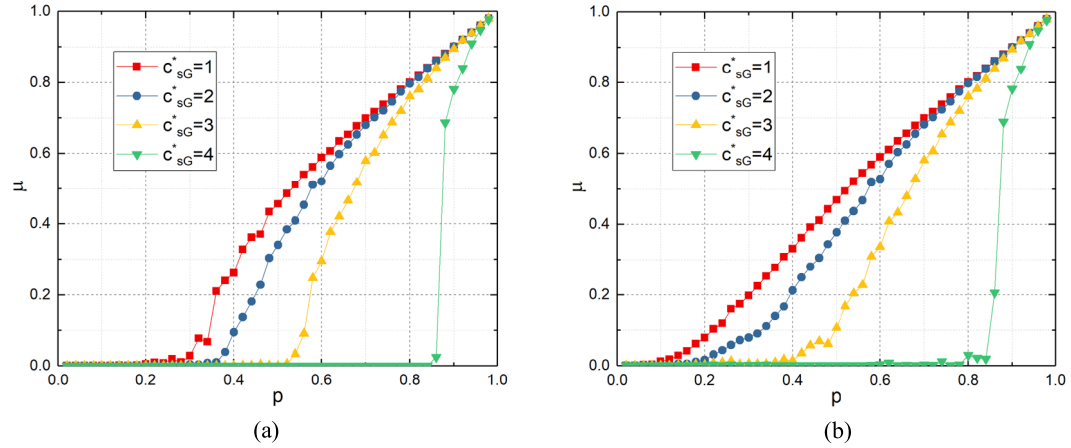


FIGURE 7. Robustness of SW-DS coupled networks to random failures in power grid(a) and communication network(b), with varying numbers of control threshold c^*_{sG}.

the increase of the number of interdependent links. Given the number of interdependent links with 1, 2, 3, 5 and 8, they respond on five p-μ curves. The critical point $p_c = 0.58$ when $n = 1$, and p_c is 0.32 when $n = 8$. On the other hand, there is saturation when the interdependent links reach to certain point. The difference of μ between $n = 5$ and $n = 8$ is negligible. The saturated value of interdependent links is 5 from the histograms of n-p_c in Fig. 4.

In addition to reflect the influence of networks topology on cascading failure, we compare the SW-SW networks and SW-DS networks. Double-star network is common in communication. When SW-SW model is simulated, both power grid and communication network have the same result shown as Fig. 3, although the interdependent from power grid to communication network and that from communication network to power grid are different. When SW-DS model is simulated, Fig. 6(a) reflects the curve of power grid while Fig. 6(b) reflects that of communication network. The p-μ curve between power grid and communication network are compared as shown in Fig. 5, when p is in a high interval, there are no difference of the μ value changing between power grid and communication network. The topology influences the low value interval of p.

DS communication network has the lower critical point 0.20. Obviously, in this model, the communication network is more robust to random failures than power grid.

Then the problem is which model is more resilience for power grid to random attacks? As shown in Fig. 4, the critical point p_c of power grid in SW-SW model is always larger than that in SW-DS model. The topology of communication network influences the critical point of whole systems in cascading failure. The double star network has more resilience for the whole system. The DS communication networks is a scale-free one and the operation centers which control power nodes and exchange information with other communication devices are some autonomous nodes [36], [37]. Thus, the double-star structure dispatching data network for the power system is better in case of random attacks.

TABLE 3. Different robustness to same redundant values.

	Redundant values in power grid			Redundant values in communication network		
Value	1	2	3	1	2	3
c^*_{sG}=1	0.860	0.510	0.380	0.830	0.400	0.210
n=5	0.180	0.120	0.115	0.12	0.100	0.095

E. CSACADING FAILURE WITH CONTROL THRESHOLD

In addition, Fig. 7 reflects the results when the control threshold is considered. Similar observation as the number of interdependent links can be found, the system robustness increases with the decrease of control threshold c^*_{sG}. However, the specific influence of the system robustness depends both on interdependency and control threshold. The control threshold subtracts from interdependent links number n-c^*_{sG} is the redundant value of lines. As shown in Table 3, although redundant values are same, different control thresholds and different interdependent links numbers still make different robustness to cascading failure.

V. CONCLUSION

In this paper, we introduce a model of cyber-physical system in cascading failure. By introducing the control threshold, the cascading failure model with the existence of redundancy and standby lines in control supply is developed. With the one-to-multiple interdependent relationship, the critical point based on percolation theory is measured to evaluate the robustness of CPPS. The topology simulator of HV transmission network with 241 nodes and 371 edges is implemented in Python. For further enhancing the application of the model in general power grid, we also analyze a SW network with 2000 nodes. For communication network, SW network and DS network are compared to find the robustness influence on topology, interdependent link and control threshold.

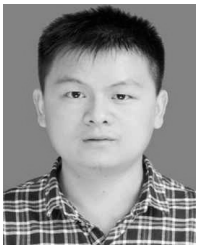
The simulation extends the robustness factors in cascading failure of CPPS. The control threshold presented in this paper can reflect the coupling strength from communication network to power grid. Both increasing the number of interdependent links and decreasing the control threshold have the saturation to enhance the robustness of CPPS. And as a common topology in communication network, we verify the DS communication network's effectiveness in resisting cascading failure both for the intra network and the whole system.

For the future work, we aware the mechanism in intra cascading failure in power grid is more complex than the intra-dependency. The development of power flow analysis [30] in intra cascading failure can extend the utilization of our approach with control threshold.

REFERENCES

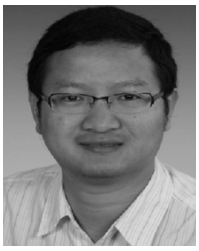
[1] K. Tomsovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose, "Designing the next generation of real-time control, communication, and computations for large power systems," *Proc. IEEE*, vol. 93, no. 5, pp. 965–979, May 2005.
[2] M. Amin, "Toward self-healing energy infrastructure systems," *IEEE Comput. Appl. Power*, vol. 14, no. 1, pp. 20–28, Jan. 2001.
[3] E. Nobile and A. Bose, "A new scheme for voltage control in a competitive ancillary service market," in *Proc. Power Syst. Comput. Conf.*, 2002, pp. 24–28.
[4] *Final report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power Syst. Outages Task Force, Washington DC, USA, 2004, pp. 1691–1702.
[5] S. Corsi and C. Sabelli, "General blackout in Italy sunday September 28, 2003, h. 03:28:00," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2004, pp. 1691–1702.
[6] A. Bobbio *et al.*, "Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network," *Rel. Eng. Syst. Saf.*, vol. 95, no. 12, pp. 1345–1357, 2010.
[7] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.
[8] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 285–297, Jan. 2015.
[9] S. Al-Takrouri, A. V. Savkin, V. G. Agelidis, "A decentralized control algorithm based on the DC power flow model for avoiding cascaded failures in power networks," in *Proc. Asian Control Conf. (ASCC)*, Jun. 2013, pp. 1–6.
[10] H. Cetinay, S. Soltan, F. A. Kuipers, G. Zussman, and P. Van Mieghem, "Comparing the effects of failures in power grids under the AC and DC power flow models," *IEEE Trans. Netw. Sci. Eng.*, to be published.
[11] S. W. Mei, Yadana, X. F. Weng, and A. C. Xue, "Blackout model based on OPF and its self-organized criticality," in *Proc. Chin. Control Conf.*, Harbin, China, 2006, pp. 1673–1678.
[12] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "An initial model fo complex dynamics in electric power system blackouts," in *Proc. 34th Hawaii Int. Conf. Power Syst. Sci.*, Jan. 2001, pp. 710–718.
[13] Y. Moreno, J. B. Gómez, and A. F. Pacheco, "Instability of scale-free networks under node-breaking avalanches," *EPL (Europhys. Lett.)*, vol. 58, no. 4, pp. 630–636, 2002.
[14] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, Apr. 2010.
[15] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3274–3284, Dec. 2014.
[16] C. D. Brummitt, R. M. D'Souza, and E. A. Leicht, "Suppressing cascades of load in interdependent networks," *Proc. Nat. Acad. Sci. USA*, vol. 109, no. 12, pp. E680–E689, 2012.
[17] M. Parandehgheibi, E. Modiano, and D. Hay, "Mitigating cascading failures in interdependent power grids and communication networks," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2016, pp. 242–247.
[18] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 83, no. 2, p. 036116, 2011.
[19] 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.*, Jun. 2013, pp. 1023–1028.
[20] D. Cellai, A. Lawlor, K. A. Dawson, and J. P. Gleeson, "Critical phenomena in heterogeneous k-core percolation," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 87, no. 2, p. 022134, 2013.
[21] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.
[22] A. Bose, "Power system stability: New opportunities for control," in *Stability and Control of Dynamical Systems With Applications*. Boston, MA, USA: Birkäuser, 2003, pp. 315–330.
[23] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2011.
[24] P. Palensky, E. Widl, and A. Elsheikh, "Simulating cyber-physical energy systems: Challenges, tools and methods," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 44, no. 3, pp. 318–326, Mar. 2014.
[25] C. A. Macana, N. Quijano, E. Mojica-Nava, "A survey on cyber physical energy systems and their applications on smart grids," in *Proc. IEEE PES Conf. ISGT LA*, Oct. 2011, pp. 1–7.

[26] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 9, pp. 1733–1740, Sep. 2004.
[27] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Initial evidence for self-organized criticality in electric power system blackouts," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2000, p. 6.
[28] L. Xu, X. Wang, and X. Wang, "Equivalent admittance small-world model for power system—I. Basic concepts and implementation," in *Proc. Asia–Pacific Power Energy Eng. Conf.*, Wuhan, China, Mar. 2009, pp. 1–4.
[29] M. Ding and P. Han, "Reliability assessment to large-scale power grid based on small-world topological model," in *Proc. Int. Conf. Power Syst. Technol.*, Chongqing, China, Oct. 2006, pp. 1–5.
[30] S. Mei, Y. Ni, G. Wang, and S. Wu, "A study of self-organized criticality of power system under cascading failures based on AC-OPF with voltage stability margin," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1719–1726, Nov. 2008.
[31] X. Wei, J. Zhao, T. Huang, and E. Bompard, "A novel cascading faults graph based transmission network vulnerability assessment method," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2995–3000, May 2018.
[32] X. Wei, S. Gao, D. Li, T. Huang, R. Pi, and T. Wang, "Cascading fault graph for the analysis of transmission network vulnerability under different attacks," *Proc. Chin. Soc. Elect. Eng.*, vol. 38, no. 2, pp. 456–474, Jan. 2018.
[33] J. Xia *et al.*, "Cache aided decode-and-forward relaying networks: From the spatial view," *Wireless Commun. Mobile Comput.*, vol. 2018, Art. no. 5963584, doi: 10.1155/2018/5963584.
[34] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 21879–21887, 2018.
[35] F. Shi, L. Fan, X. Liu, Z. Na, and Y. Liu, "Probabilistic caching placement in the presence of multiple eavesdroppers," *Wireless Commun. Mobile Comput.*, vol. 2018, Art. no. 2104162, doi: 10.1155/2018/2104162.
[36] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.
[37] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, Aug. 2017.
[38] S. Carmi, S. Havlin, S. Kirkpatrick, Y. Shavitt, and E. Shir, "A model of Internet topology using k-shell decomposition," *Proc. Nat. Acad. Sci. USA*, vol. 104, no. 27, pp. 11150–11154, 2007.
[39] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, "k-core organization of complex networks," *Phys. Rev. Lett.*, vol. 96, no. 4, p. 040601, 2006.
[40] A. V. Goltsev, S. N. Dorogovtsev, and J. F. F. Mendes, "k-core (bootstrap) percolation on complex networks: Critical phenomena and nonlocal effects," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 73, no. 5, p. 056101, 2006.



YU CHEN was born in Changsha, Hunan, China, in 1993. He received the B.Sc. degree in electrical engineering from Central South University, Changsha, in 2016. He is currently pursuing the M.Sc. degree in electrical engineering with the College of Electrical and Information Engineering, Hunan University, Changsha.

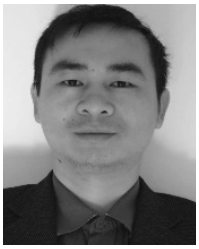
His recent research interests include the reliability of cyber physical power system and the modeling of cascading failure.



YONG LI (S'09–M'12–SM'14) was born in Xingyang, Henan, China, in 1982. He received the B.Sc. and Ph.D. degrees from the College of Electrical and Information Engineering, Hunan University (HNU), Changsha, China, in 2004 and 2011, respectively.

He received the second Ph.D. degree from TU Dortmund University, Dortmund, Germany, in 2012. Since 2009, he was a Research Associate with the Institute of Energy Systems, Energy Efficiency, and Energy Economics, TU Dortmund University. After then, he was a Research Fellow with The University of Queensland, Brisbane, Australia. Since 2014, he has been a Full Professor of electrical engineering with HNU. His current research interests include power system stability analysis and control, cyber physical systems, and analysis and control of power quality.

Dr. Li is the member of the Association for Electrical, Electronic and Information Technologies (VDE) in Germany. He is an Associate Editor of the *IET Power Electronics*.



WENGUO LI (S'09–M'12–SM'14) was born in Yiyang, Hunan, China, in 1977. He received the B.Sc. degree in circuit and system from Guangxi Normal University, Guilin, China, in 2005. He is currently pursuing the Ph.D. degree in electrical engineering with the College of Electrical and Information Engineering, Hunan University, Changsha, China.

He was an Assistant Professor with Hunan City University, Yiyang, China. Her current research interests include cyber-physical security in the smart grid and the application of complex networks in power systems.

XIAORUI WU was born in Guiping, Guangxi, China, in 1993. He received the B.Sc. degree in electrical engineering from Hunan University, Changsha, China, in 2016, where he is currently pursuing the M.Sc. degree in electrical engineering with the College of Electrical and Information Engineering.

His recent research interests include the reliability of cyber physical power system and the modeling of cascading failure.

YE CAI was born in Yiyang, Hunan, China, in 1988. She received the B.Sc. and Ph.D. degrees in electrical engineering and automation from the College of Electrical and Information Engineering, Hunan University, Changsha, China, in 2010 and 2015, respectively.

She was an Assistant Professor with the University of Science & Technology, Changsha, China. Her current research interests include cyber-physical security in the smart grid and the application of complex networks in power systems.

YIJIA CAO (M'98–SM'13) was born in Yiyang, Hunan, China, in 1969. He received the B.Sc. degree in mathematics from Xi'an Jiaotong University, Xi'an, China, in 1988, and the M.Sc. degree in computer science and the Ph.D. degree in electrical engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 1991 and 1994, respectively.

From 1994 to 2000, he was a Visiting Research Fellow and a Research Fellow with Loughborough University, Loughborough, U.K., the University of Liverpool, Liverpool, U.K., and the University of the West England, Bristol, U.K. From 2000 to 2001, he was a Full Professor with HUST, and from 2001 to 2008, he was a Full Professor with Zhejiang University, Hangzhou, China. He is currently a Full Professor and the Vice President of Hunan University, Changsha, China. His current research interests include power system stability control and the application of intelligent systems in power system.

CHRISTIAN REHTANZ (M'96–SM'06) was born in Germany in 1968. He received the Diploma and Ph.D. degrees in electrical engineering from TU Dortmund University, Dortmund, Germany, in 1994 and 1997, respectively. He received the *venia legend* in electrical power systems from the Swiss Federal Institute of Technology, Zürich, Switzerland, in 2003. In 2000, he joined ABB Corporate Research, Baden, Switzerland. He became the Head of the Technology for the global ABB business area of power systems in 2003, and the Director of ABB Corporate Research, Beijing, China, in 2005.

Since 2007, he has been the Head of the Institute of Energy Systems, Energy Efficiency and Energy Economics, TU Dortmund University. In addition, he has been a Scientific Advisor of ef.Ruhr GmbH, Dortmund, a joint research company of the three universities of Bochum, Dortmund, and Duisburg-Essen (University Alliance Metropolis Ruhr) since 2007. He is also an Adjunct Professor with Hunan University, Changsha, China. He has authored over 150 scientific publications, three books, and 17 patents and patent applications. His research interests include electrical power systems and power economics, technologies for network enhancement and congestion relief, such as stability assessment, wide-area monitoring, protection, coordinated network-control, and integration and control of distributed generation and storage.

Dr. Rehtanz received the MIT World Top 100 Young Innovators Award 2003.