Analysis of Failure Propagation in Cyber-Physical Power Systems Based on an Epidemic Model

Zhang, Haiyan; Teng, Yufei; Guerrero, Josep M.; Siano, Pierluigi; Sun, Xiaorong

Published in:
Energies

DOI (link to publication from Publisher):
10.3390/en16062624

Creative Commons License
CC BY 4.0

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
Zhang, H., Teng, Y., Guerrero, J. M., Siano, P., & Sun, X. (2023). Analysis of Failure Propagation in Cyber-Physical Power Systems Based on an Epidemic Model. *Energies*, *16*(6), Article 2624. https://doi.org/10.3390/en16062624

energies

MDPI

Article

Analysis of Failure Propagation in Cyber-Physical Power Systems Based on an Epidemic Model

Haiyan Zhang [1,*], Yufei Teng [2], Josep M. Guerrero [3], Pierluigi Siano [4,5] and Xiaorong Sun [1]

[1] College of Artificial Intelligence, Beijing Technology and Business University, Beijing 100048, China
[2] Power Internet of Things Key Laboratory of Sichuan Province, Chengdu 610072, China
[3] Department of Energy Engineering, Aalborg University, 9920 Aalborg, Denmark
[4] Department of Management & Innovation Systems, University of Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano, SA, Italy
[5] Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa
* Correspondence: haiyanzhang@btbu.edu.cn

Abstract: From the perspective of propagation dynamics in complex networks, failure propagation in cyber-physical power systems is analogous to the spread of diseases; subsequently, the cyber nodes and power nodes are regarded as individuals in each of their groups. In this study, a two-layer interdependent network model of the cyber-physical power system is proposed, where each subnetwork adopts the Susceptible-Infected-Susceptible (SIS) epidemic-spreading model. On this basis, we construct a failure cooperation propagation model of cyber-physical power systems. Furthermore, we introduce the node protection mechanism to ensure the normal operation of key nodes. The generated scale-free cyber network and IEEE118-bus power system are used for simulation to analyze the influence of the coupling effect between them on the final failure scale.

Keywords: cyber-physical power system; interdependent network; epidemic model; cooperation propagation; node protection

check for updates

Citation: Zhang, H.; Teng, Y.; Guerrero, J.M.; Siano, P.; Sun, X. Analysis of Failure Propagation in Cyber-Physical Power Systems Based on an Epidemic Model. *Energies* **2023**, *16*, 2624. https://doi.org/10.3390/en16062624

Received: 2 February 2023
Revised: 5 March 2023
Accepted: 6 March 2023
Published: 10 March 2023

1. Introduction

With the vigorous development and construction of smart grids and energy Internet, the power system and cyber network are deeply coupled and complementary, gradually developing into a new model of a cyber-physical power system [1]. The power grid provides a power supply for the nodes of the cyber network, while the real-time state sensing and control of the power grid is highly dependent on the normal operation of the nodes. On one hand, advanced information technology brings many conveniences to the power system, effectively enhancing controllability and observability [2]. On the other hand, because of the close interaction between the cyber network and the power network, there are certain security risks to the power grid. The dynamic propagation of failures in the two-layer coupled system is accelerated and becomes more extensive, and if a certain security boundary is exceeded, cascading failures will occur, leading to large-scale power outages [3]. Therefore, integrated modeling and vulnerability analysis of the cyber-physical power system to explore the coupling mechanism between the cyber and physical layers and analyzing the cascading failure propagation and dynamic evolution process are of great significance to ensure the safety and stability of the power grid [4].

In 2010, Buldyrev proposed the interdependent network model [5] that included two types of interdependent coupling, assortative coupling and random coupling, and found by comparison that the critical threshold of seepage at cascade failure in a one-to-one correspondent coupling network was lower than that of the random coupling network. The role of the load was considered in [6] and it was observed that the interlayer coupling in the interdependent network effectively enhanced the robustness of the network and was able to suppress the propagation of cascading failures, contrary to the results reported in the literature [7]. In [8], sparse coupling was proposed and it was found that increasing the coupling probability makes the interdependent network more robust to deliberate attacks, but increasing it again after reaching a certain coupling strength has the opposite effect. A non-uniform "one-to-many" and "partial coupling" cyber-physical power system model was constructed using the asymmetrical balls-into-bins method [9], and the risk propagation threshold was determined using percolation theory. In [10], the stability of this interdependent network was examined by modeling spatially embedded systems, such as power grids and cyber networks, as lattice networks. The literature [11] has been based on the ListNet learning-to-rank method for ranking critical nodes and tested on networks, such as the Western U.S. power grid, using the SIR (Susceptible-Infected-Recovered) contagion model to evaluate the propagation capability of critical nodes. In [12], an infectious disease-based model was used for power systems to perform predictive analysis of grid disturbance propagation.

Based on the above studies, we further explored the effects of coupled cyber and physical layers on power system vulnerability, especially on failure propagation. Dynamic models of network propagation, which have been developed in the last decade, are important tools for studying and mathematically describing actual propagation laws [13]. Failure propagation in power systems shares similarities with disease propagation in a population, as shown in Figure 1, resulting in large-scale propagation when the effective propagation rate exceeds a certain positive threshold.

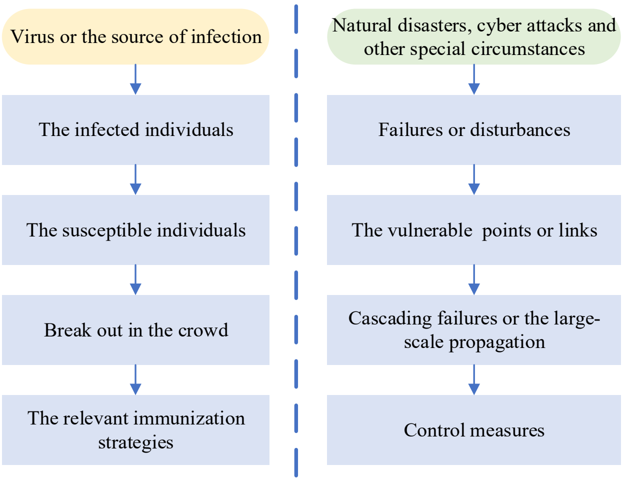
Virus or the source of infection
The infected individuals
The susceptible individuals
Break out in the crowd
The relevant immunization strategies
Natural disasters, cyber attacks and other special circumstances
Failures or disturbances
The vulnerable points or links
Cascading failures or the large-scale propagation
Control measures

Figure 1. Analogy between epidemic spread and failure propagation in power systems.

Many scholars first studied viral transmission from the perspective of biology, summarizing the transmission law and modeling it mathematically. In fact, epidemic transmission models have been applied in many fields, such as the spread of computer viruses and the spread of rumors in society [14]. In this paper, when studying the failure propagation mechanism of information-physical power systems, we learned from the epidemic propagation model in complex networks and used it to explore cyber-physical power systems in an interdisciplinary endeavor. The primary aim of the propagation model is to analyze the failure propagation process of a two-layer coupled network to assess the impact of the coupling relation of cyber-physical power systems on the vulnerability of power systems.

In this study, the propagation of failures in a cyber-physical power system is assumed to be analogous to the propagation of a certain infectious disease in two populations, where the cyber network is scale-free and belongs to a heterogeneous network, while the power system exhibits small-world characteristics and belongs to a homogeneous network. Based on the theory of interdependent networks, a two-layer cyber-physical power system interdependent network model with a heterogeneous upper layer and a homogeneous lower layer is established. Based on the SIS model, a two-layer co-propagation network model is constructed, while different node protection mechanisms are introduced to analyze the influence of the coupling effect of the cyber layer and the physical layer on the failure propagation threshold and the impact of the eventual scale of the failure in the cyber-physical power system.

2. SIS Susceptible-Infected-Susceptible (SIS) Disease Propagation Model

The specific process of disease propagation is extremely complex; individuals may acquire immunity or may be infected once and still be re-infected. Moreover, different types of diseases spread in different ways, requiring different mathematical models to describe their transmission patterns. The most typical epidemic transmission models include the Susceptible-Infected (SI) model, SIS model, and Susceptible-Infected- Removed (SIR) model. The basic states involved are as follows: (1) Susceptible (S), which is the state of health in which infection can occur; (2) Infected (I), when the infected individual has infectious properties; and (3) Removed/Recovered (R), which is divided into two states, one in which the infected individual is cured and thus gains immunity, and the other in which the infected individual dies [15]. Individuals in the removed state are neither reinfected nor infectious and do not affect the dynamics of the system.

In this study, we mainly used the SIS disease propagation model shown in Figure 2. The SIS model is generally used to describe diseases, such as influenza, where individuals cannot gain immunity after being cured and can still be re-infected. In this case, individuals in a susceptible state have a probability α of contracting the disease and thus becoming newly infected, and the probability of an infected individual being cured is β. The mechanism of infection can be described as follows [16].

$$\begin{cases} S(i) + I(j) \xrightarrow{\alpha} I(i) + I(j) \\ I(i) \xrightarrow{\beta} S(i) \end{cases} \tag{1}$$

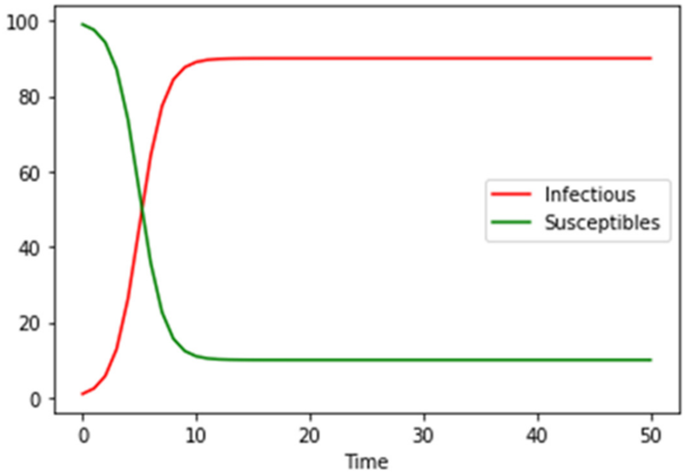

Figure 2. Diagram of the SIS model.

At moment t, the density of individuals in the susceptible state is $s(t)$, the density of individuals in the infected state is $i(t)$ and the set of dynamic equations for the SIS model is shown below.

$$\begin{cases} \frac{ds(t)}{dt} = -\alpha i(t)s(t) + \beta i(t) \\ \frac{di(t)}{dt} = \alpha i(t)s(t) - \beta i(t) \end{cases} \tag{2}$$

Therefore, let the effective transmission rate be $\lambda = \alpha/\beta$.

3. Two-Layer Interdependent Network Model

The cyber-physical power system is a deeply coupled cyber network and physical network with interdependencies as shown in Figure 3. Both the heterogeneity of the network and the homogeneity of the topology in this two-layer network have an important impact on the failure propagation behavior [17].

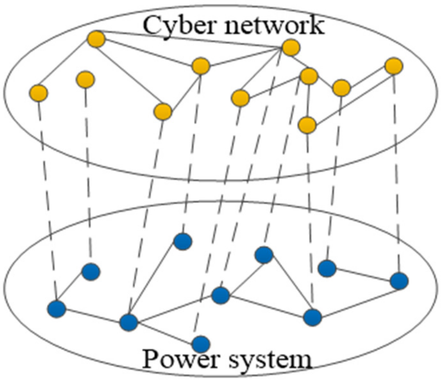

Figure 3. Double-layer network of the cyber-physical power system.

The topology of the physical network and cyber network is abstractly represented as undirected graphs G_P and G_C, where G_C denotes the cyber network and G_P denotes the physical network. Each single-layer network is $G = (V, E)$, where $V = \{n_i\}$ is the set of nodes in the network, and $E = \{e_{ij}\}$ denotes the set of internally connected edges in each layer of the network.

3.1. Cyber Layer Model

Information and communication networks are typical scale-free networks. The adjacency matrix is used to represent the connection between individual nodes of the cyber layer.

$$A_C = \left(a_{ij}\right)_{N\times N} \tag{3}$$

where $a_{ij} = 1$ denotes that the cyber nodes C_i and C_j are connected; otherwise, $a_{ij} = 0$.

It is constructed in the following way. Given the initial node m$_0$, a new node is added at each time step and m edges and, according to the preferred probability $p_i = \frac{k_i}{\sum_j k_j}$, is connected to the existing nodes. Here, k_i denotes the degree [18] of existing node i, and $\sum_j k_j$ is the sum of the degrees of all currently existing nodes.

3.2. Physical Layer Model

Physical grids are typically small-world networks, with power plants, substations, etc., and are represented using nodes where N denotes the total number of power nodes, while transmission lines are represented with connecting edges. The connections between load nodes in the power system can be represented by the adjacency matrix as

$$A_P = \left(a_{ij}\right)_{M\times M} \tag{4}$$

where $a_{ij} = 1$ denotes that the power nodes P_i and P_j are connected; otherwise, $a_{ij} = 0$.

3.3. Two-Layer Network Model of the Cyber-Physical Power System

The two topologically distinct subnetworks are described as $A = \left(a_{ij}\right)_{M\times M}$ and $B = \left(b_{ij}\right)_{N\times N}$. Assume that the cyber layer has N nodes $(C_1, C_2, \cdots, C_N)$ and the physical layer has M power nodes $(P_1, P_2, \cdots, P_M)$. The interdependence between the cyber communication network G_C and the physical power grid G_P corresponds to the dashed line in Figure 3. This is described by the adjacency matrix as $A_{C-P} = \{(n, m) | n \subset \mathrm{V_C}, m \subset \mathrm{V_P}\} \subset R^{N\times M}$ and referred to as the set of connection edges between two networks. $R^{N\times M}$ indicates the matrix of possible connection edges between the cyber network and the power system. The cyber-physical power system as a whole can be represented as

$$A = \begin{bmatrix} A_C & A_{C-P} \\ (A_{C-P})^T & A_P \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,N} & a_{1,N+1} & \cdots & a_{1,N+M} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{N,1} & \cdots & a_{N,N} & a_{N,N+1} & \cdots & a_{N,N+M} \\ a_{N+1,1} & \cdots & a_{N+1,1} & a_{N+1,N+1} & \cdots & a_{N+1,N+M} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{N+M,1} & \cdots & a_{N+M,N} & a_{N+M,N+1} & \cdots & a_{N+M,N+M} \end{bmatrix} \quad (5)$$

where if there is energy or information exchange between node n in the cyber network and node m in the power grid, i.e., there is an edge connection, then $A_{C-P}(n,m) = 1$; otherwise, $A_{C-P}(n,m) = 0$.

The dependency of assortative coupling is used in this section. Dependency of assortative coupling means that the cyber nodes are connected with the power nodes that have similar features. Here, the information nodes correspond to the power network nodes sequentially based on their degree. Indeed, there are multiple types of couplings, for example, one-to-one coupling, one-to-more coupling, more-to-more coupling, etc. In this paper, we adopt one-to-one coupling to keep the model simple, so that each cyber node connects one and only one power node.

First, all nodes in the two-layer network are arranged in descending order according to their degrees. A node with a higher degree occupies a more critical position in the topology. When an unexpected condition is encountered (for example, some cyber nodes are attacked or a part of the power loads fails), the entire system can still maintain normal operation as long as these critical nodes survive [19]. The degree of a node is denoted by d, $d_{C1} \geq d_{C2} \geq d_{C3} \geq \cdots \geq d_{CM}$ and $d_{P1} \geq d_{P2} \geq d_{P3} \geq \cdots \geq d_{PM}$ (if two nodes have the same degree value, they are further compared in terms of their betweenness centrality [18], which is denoted in the same order, from largest to smallest). Subsequently, the nodes in the cyber layer and the corresponding nodes in the physical layer are connected sequentially to form the symmetrical dependent network model presented in this section.

4. Collaborative Failure Propagation in the Cyber-Physical Power System

There are cases in the network where a node fails and returns to normal operations with a probability of β but does not gain immunity and may still be infected again [20]. Figure 4 shows a combination of the complex status of nodes during the operation of the cyber-physical power system.

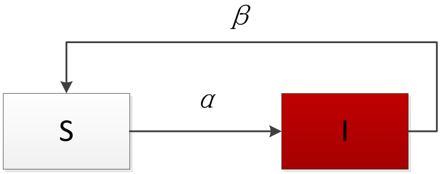

Figure 4. Status of nodes in the cyber-physical power system.

S indicates that the node is in a normal operating (susceptible) state, I indicates that the node is in a failure (infected) state, the probability of failure propagation (being infected) is α, and the probability of resuming operation (being cured) is β.

In the cyber-physical two-layer network model, a discrete SIS model is used for both subnetworks. The nodes in the network are in a normal operating state S or a failure state I, with the failures propagated through adjacent nodes (neighbor relationship). Thus, nodes in the normal operating state S will be infected by nodes in the failure state I in the same network layer or corresponding failure state node I in another network layer through inter-layer coupling [21]. Simultaneously, due to certain control measures or recovery mechanisms, the nodes in the failure state I return to the normal operation state S with a certain probability β.

The dynamic process of propagation between nodes in a two-layer cyber-physical power system is described as follows [21].

$$p_{1,i}(t+1) = (1 - p_{1,i}(t))(1 - q_{1,i}(t)) + (1 - \beta_1)p_{1,i}(t) + \gamma_1 p_{2,i}(t)(1 - p_{1,i}(t)) \tag{6}$$

$$p_{2,i}(t+1) = (1 - p_{2,i}(t))(1 - q_{2,i}(t)) + (1 - \beta_2)p_{2,i}(t) + \gamma_2 p_{1,i}(t)(1 - p_{2,i}(t)) \tag{7}$$

where $i\epsilon\{1, \cdots, N\}$, and $q_{1,i}(t)$ and $q_{2,i}(t)$ denote the probability that a node i will not be infected by neighboring failure nodes in the cyber and physical networks, respectively. On the contrary, $1 - q_{1,i}(t)$ and $1 - q_{2,i}(t)$ denote the probability of node i being infected by neighboring nodes in the cyber network and the physical network, respectively. Therefore, $(1 - p_{1,i}(t))$and $(1 - p_{2,i}(t))$ denote the probability that node i is in normal operation, the probability of being infected by neighboring nodes in the layer is $(1 - q_{1,i}(t))$ and $(1 - q_{2,i}(t))$, while $(1 - \beta_1)p_{1,i}(t)$ and $(1 - \beta_2)p_{2,i}(t)$ denote the probability that node i is infected with a failure at moment t and is not cured for resuming normal operations, and $\gamma_1 p_{2,i}(t)(1 - p_{1,i}(t))$ and $\gamma_2 p_{1,i}(t)(1 - p_{2,i}(t))$ denote the probability of node i being infected by a neighboring node in another layer of the network in a failure state.

The above aspects are defined as

$$q_{1,i}(t) = \prod_{j=1}^{N} (1 - \alpha_1 a_{ij} p_{1,j}(t)) \tag{8}$$

$$q_{2,i}(t) = \prod_{j=1}^{N} (1 - \alpha_2 b_{ij} p_{2,j}(t)) \tag{9}$$

From this, we can set different infection probabilities α and probability of cure β to analyze the dynamic propagation process in the two-layer cyber-physical network.

5. Node Protection Mechanism

In the two-layer cyber-physical power system, certain nodes are critical, as they play a major role in the spread and propagation of failures. Taking preventive measures in advance can effectively enhance the robustness of the network and is more practical than staging a recovery only after the entire network is down [22]. In cyber-physical power systems, both the cyber and physical nodes are protected based on node protection mechanisms for normal operating nodes in single-layer networks.

This subsection focuses on two different protection mechanisms: random recovery (equal probability of protection) and priority recovery (different probability of protection, which prioritizes the protection of nodes with high degree value or betweenness centrality).

5.1. Random Recovery

Random recovery is the simplest protection method. In this protection scheme, all nodes are treated equally, namely each normal operating node in the network has the same probability of being protected. Constantly counting the total number of normal operating nodes at the current moment is required and subsequently recalculating the protection probability. The probability is set as γ, s and can be adjusted as described below.

At moment t when failure in the network occurs, n_t nodes include normal working nodes that are treated indiscriminately and protected randomly. The probability of each node being selected for protection $1/n_t$ is presented in the following equation.

$$\mathrm{e}_i(t+1) = \begin{cases} 0 & \gamma > 1/n_t \\ 1 & \gamma \leq 1/n_t \end{cases} \tag{10}$$

where γ is a randomly generated number in the range (0, 1). When $\gamma \geq 1/n_t$, a node has a $1/n_t$ probability of changing from the unprotected state 0 to the protected state 1 at the $t+1$ time step.

5.2. Priority Recovery

Priority recovery is a form of weighted probability protection based on node weights, which mainly considers the differences between nodes in the topology, thereby treating normal nodes differently. The more important the node is in the network, the greater the scope of its impact after failure. To prevent the failure of critical nodes, priority should be given to protecting the critical nodes among all nodes, which is a different-probability protection mechanism that combines the results of node importance ranking. This is described as follows.

All normally working nodes in the network are ranked according to importance metrics (e.g., degree, betweenness, centrality metrics, PageRank, etc.; this study used degree value as the metric), which are combined with the probability of being protected. At moment *t*, if the node *j* is not protected, the state is $e_j(t) = 0$. Its importance is denoted by $I(j)$, and the ranking result is obtained according to the importance metric $1 \leq I(j) \leq N$, such that the sum is $\sum_{e_j(t)=0} I(j)$.

Therefore, at moment *t*, the probability of a failure node being protected is given as

$$g_t(i) = \frac{I(i)}{\sum_{e_j(t)=0} I(j)} \tag{11}$$

where all normal working nodes at moment *t* are ranked according to the important result from smallest to largest. $I(j) = 1$ indicates that the ranking is 1, where the importance metric is the largest and the node is the most important. When $I(j) = N$ time, the importance index is the smallest and the node is the least important. Therefore, to protect the most critical nodes in priority, they must be modified by taking the inverse sum, and the probability of a node being protected is given by the following equation.

$$r_t(i) = \frac{1/g_t(i)}{\sum_{e_j(t)=0} \frac{1}{g_t(i)}_{\ t}} = \frac{1}{g_t(i) \sum_{e_j(t)=0} \frac{1}{g_t(i)}} \tag{12}$$

After a failure is detected in the system, the normal node takes time to be protected, which is assumed to occur over a time step, and the node is added to the protected state at the next step $e_i(t+1) = 1$ with a probability of $r_t(i)$.

$$e_i(t+1) = \begin{cases} 1 & \tau \leq r_t(i) \\ 0 & \tau > r_t(i) \end{cases} \tag{13}$$

where τ is a randomly generated number between (0, 1). If $\tau \geq r_t(i)$, then the normal working node is added to the protected state at the next step $e_i(t+1) = 1$. If $\tau < r_t(i)$, then it remains in an unprotected state.

6. Simulation and Analysis

In this study, we used the IEEE 118 bus test system as the physical network. The IEEE 118 bus test case represents a portion of the American electric power system (in the mid-western US). It contains 19 generators, 35 synchronous condensers, 177 lines, 9 transformers, and 91 loads. In addition, the cyber network presents scale-free characteristics, in that most nodes in the network are connected only to a few nodes, and a few nodes are connected to a large number of nodes. Then we randomly generated a scale-free network with 118 nodes to represent the cyber layer. Each layer had a different subnetwork structure. All nodes in the two-layer network were arranged in descending order according to the size of the degree, and the corresponding nodes in the subnetworks were then connected in sequence. On this basis, with one-to-one coupling, a two-layer interdependent network model of

236 nodes, namely the cyber-physical power system model, was constructed. When a node was randomly infected, both subnetworks adopted the SIS disease propagation model, and the cyber nodes and physical grid nodes were considered as individuals in population 1 and population 2, respectively, to analyze the failure propagation process in the two groups. The flowchart is shown in Figure 5 below. The failure does not disappear in the cyber-physical power system at dynamic equilibrium. The main comparison is between the failure propagation rate and the recovery rate, and if both reach a certain ratio, the system enters a new stable state. The specific figures are shown in the following simulation results and analysis.

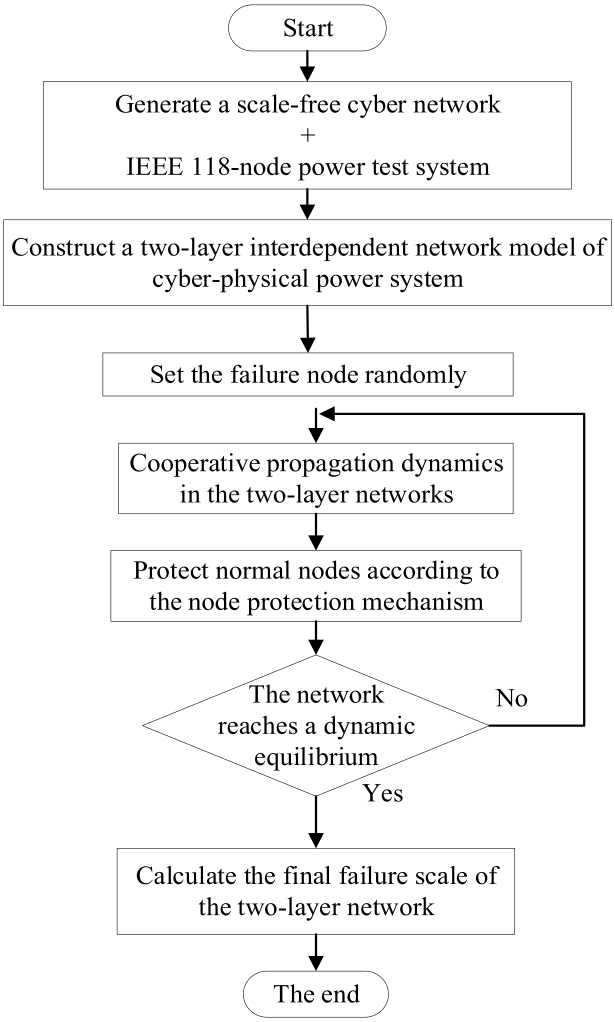
Start
Generate a scale-free cyber network
+
IEEE 118-node power test system
Construct a two-layer interdependent network model of cyber-physical power system
Set the failure node randomly
Cooperative propagation dynamics in the two-layer networks
Protect normal nodes according to the node protection mechanism
The network reaches a dynamic equilibrium
No
Yes
Calculate the final failure scale of the two-layer network
The end

Figure 5. Flowchart of simulation analysis.

The two networks were of equal size, $N_A = N_B = 118$, with the propagation parameters set as follows: the initially infected nodes were randomly selected; the number was 5% of the total number of nodes, and the step size was 0.025. For simplicity, we set the same recovery rate for both heterogeneous subnetworks [23], $\beta_1 = \beta_2 = 0.3$, and the infection rate between the subnetwork layers was set to be $\gamma_1 = \gamma_2 = 0.05$.

The four figures below (Figures 6–9) demonstrate the heterogeneous characteristics of the cyber and power networks and the coupling process of the two-layer network, respectively.

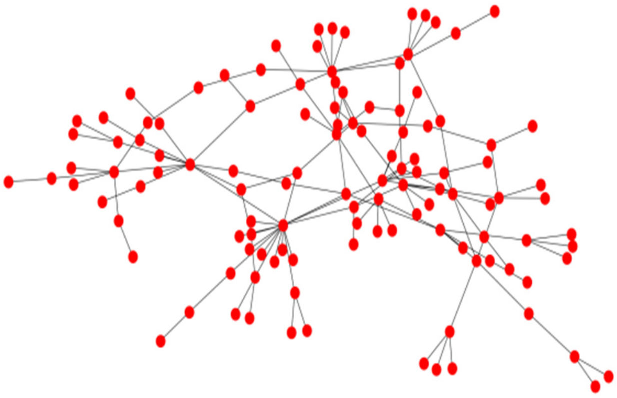

Figure 6. N = 118, m_0 = 3, m = 2 BA cyber network.

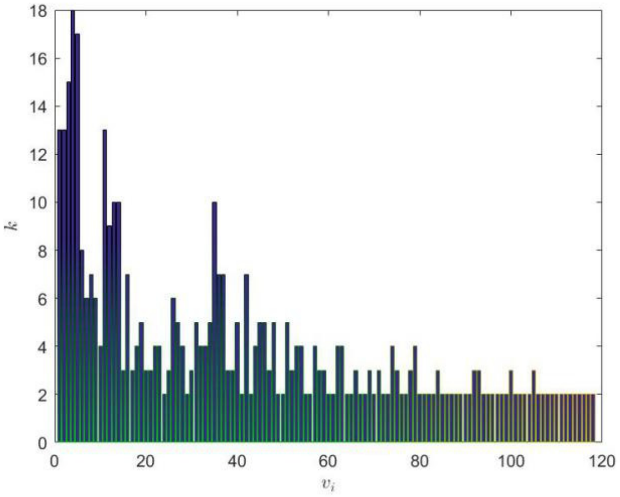

Figure 7. Degree value of nodes in the cyber network.

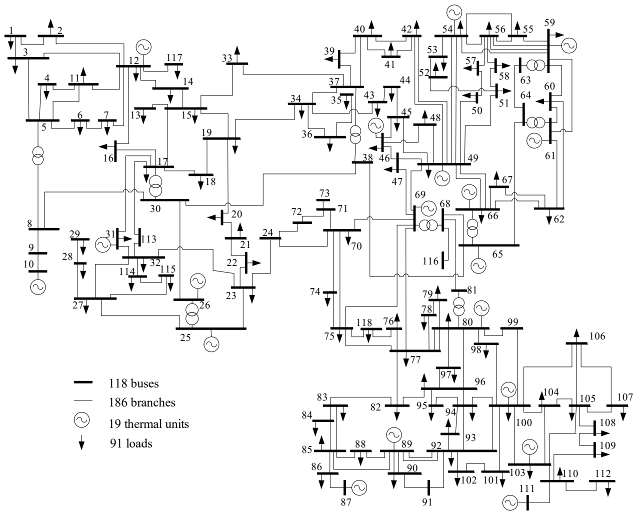

Figure 8. N = 118 topology of the power grid.

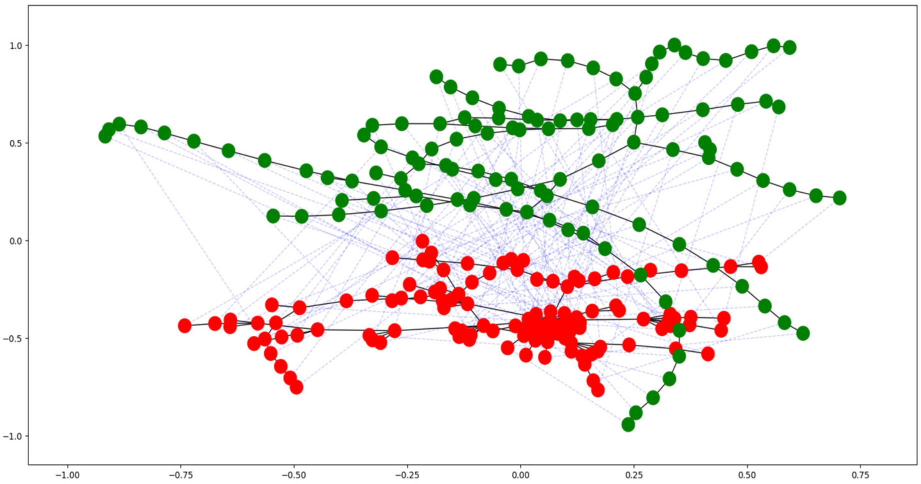

Figure 9. Cyber-physical power system with an assortative link and 236 nodes.

In Figure 9, the solid lines refer to the actual edges in the subnetwork, the dashed lines are the inter-layer coupling edges, the red nodes indicate the cyber network, and the green nodes indicate the power network.

For the same number of nodes randomly selected as the initial source of infection (failures), the propagation pattern varied between different network topologies. Figure 10 shows the change of steady-state probability density of failure nodes with λ. The main figure shows that for the cyber network, a scale-free network if the primary infection probability is greater than 0, the primary infection will keep propagating and eventually reach a stable state.

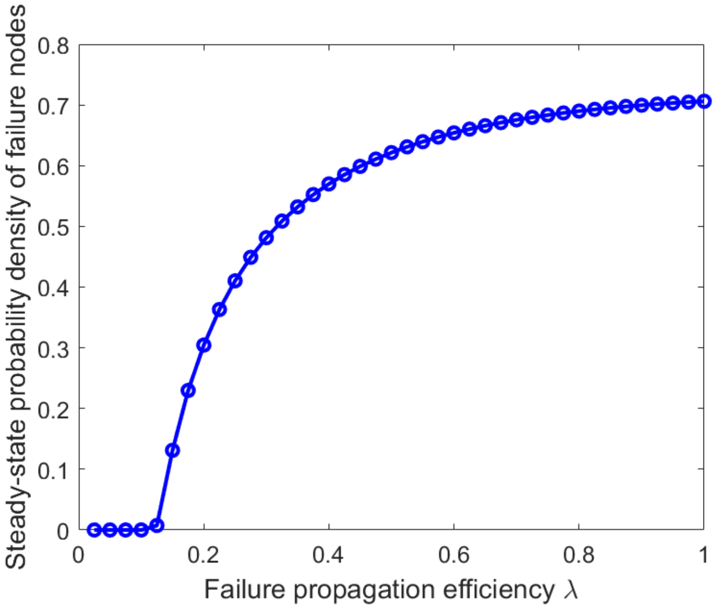

Figure 10. Propagation process of failure in a cyber network based on the SIS model.

Figure 11 shows the change of steady-state probability density of failure nodes with λ. As power systems have certain small-world characteristics, failures do not last long without long-range random propagation.

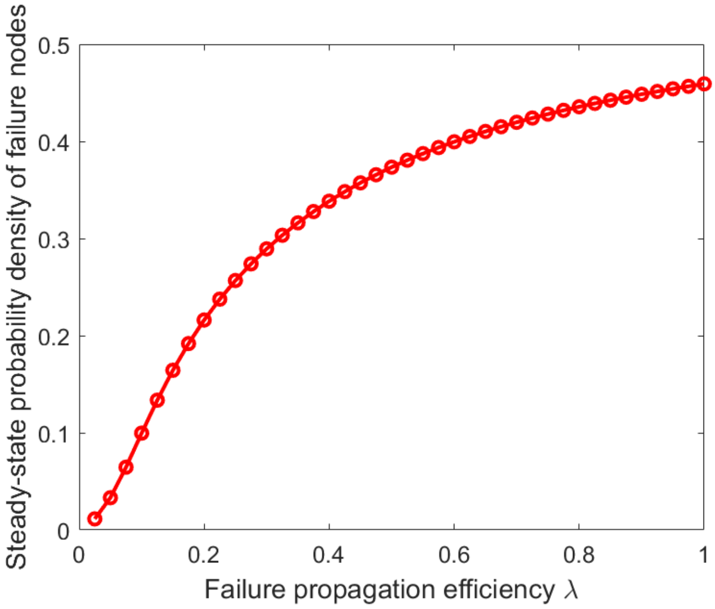

Figure 11. Propagation process of failure in 118-node power grid based on the SIS model.

The synergistic propagation of failures in the overall cyber-physical power system is shown in Figure 12 by the change in infected density (Count%) with time (T). Failures spread rapidly and reached a maximum at $t \approx 50$, then eventually converged to a more stable state. The sum of failure nodes and normal operating nodes is the total number of nodes, 2N, in the two-layer system.

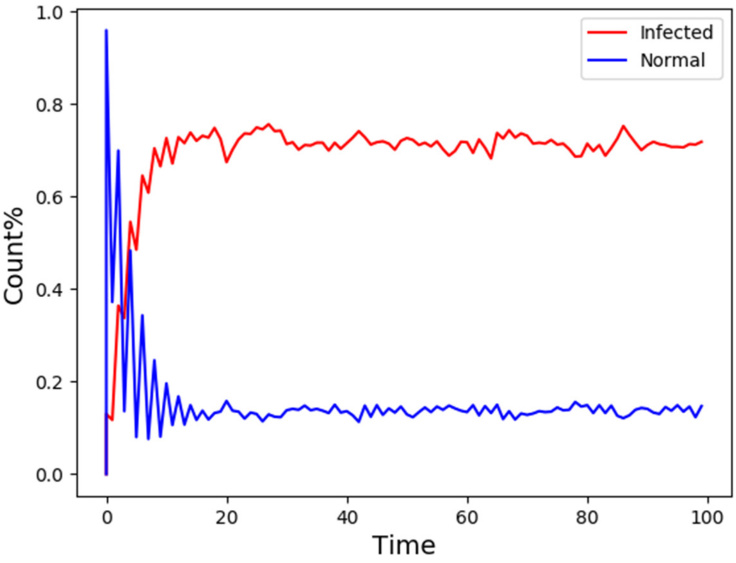

Figure 12. Propagation process of failure in cyber-physical power system based on the SIS model.

Furthermore, we explored and compared the final failure scale of the single-layer network and double-layer network with the same probability of infection. The final failure scale was approximately 77% for the individual power system and it was 83% for the cyber-physical power system, as shown in Figure 13. It indicates that in the two-layer interdependent network, that is, the cyber-physical power system, the coupling relationship between two networks created conditions for failure propagation that will lead to a larger final failure size under the same failure propagation probability.

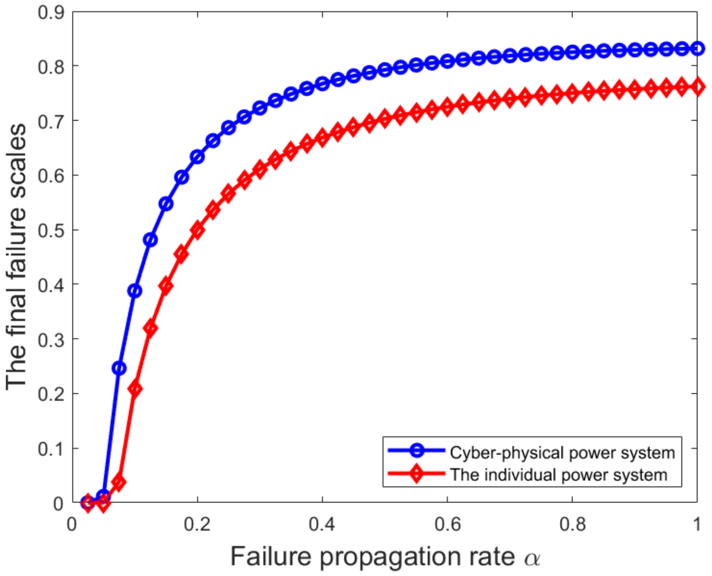

Figure 13. Comparison of final failure scales.

Failed nodes were randomly selected from the global scope and 10% of normal operating nodes were protected. The average failure scale of the cyber-physical power system with different node protection mechanisms was analyzed.

The three curves in Figure 14 illustrate the number of failure nodes that converged to a regular number after some time had elapsed. The overall final failure scale with no protection taken for the cyber-physical power system was approximately 83%. With random recovery, the final failure size was approximately 52%, and with priority recovery, the final failure size was approximately 30%. The use of priority recovery was more effective than random recovery, significantly reducing the overall failure scale of the system.

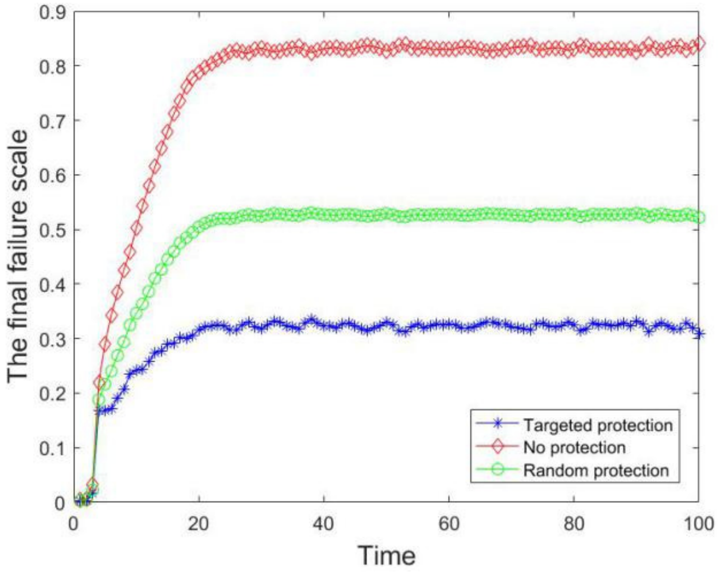

Figure 14. Failure scales under different node protections.

7. Conclusions

In this study, we used the epidemic propagation model in complex networks to explore coupled cyber-physical power systems, mainly from the perspective of propagation models, in analyzing the failure propagation process of two-layer interdependent networks. Considering the deep coupling between layers in cyber-physical power systems, a heterogeneous two-layer interdependent network model with a heterogeneous upper layer and a homogeneous lower layer was constructed based on complex network theory. The subnetworks adopted the SIS disease propagation model, which forms the basis of the dynamic failure propagation model in the interdependent network. It was proved through simulation that the coupling relationship between the cyber layer and the physical layer promoted failure propagation. The failure scale of the cyber-physical power system was higher than that of the single-layer power system under the same propagation rate. In addition, different node protection strategies were introduced, and the results verified that the use of priority recovery was more effective than random recovery, thereby significantly reducing the overall failure size.

Author Contributions: Conceptualization, H.Z. and X.S.; methodology, H.Z.; software, H.Z.; validation, H.Z., Y.T. and X.S.; formal analysis, Y.T.; investigation, H.Z.; resources, H.Z.; data curation, X.S.; writing—original draft preparation, H.Z.; writing—review and editing, P.S. and J.M.G.; visualization, H.Z.; supervision, P.S. and J.M.G.; project administration, H.Z. and X.S.; funding acquisition, H.Z. and Y.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Opening Fund of Power Internet of Things Key Laboratory of Sichuan Province, grant number PIT-F-202206. This research was also supported by the Research Foundation for Youth Scholars of Beijing Technology and Business University, grant number 19008022160.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Qin, B.Y.; Liu, D. Research progresses and prospects on analysis and control of cyber-physical system for power grid. *Proc. CSEE* **2020**, *40*, 5816–5826.
2. Wu, Z.T.; Du, W.; Liu, L.L.; Lin, Y.H.; Liu, J. Risk propagation model of power coupled networks under malicious attack. *Power Syst. Technol.* **2020**, *44*, 2045–2052.
3. Wu, L.J.; Zou, Y.L.; Wang, R.R.; Yao, F.; Wang, Y. Comparison of cascading failures between power information interdependent networks and single-layer power grids. *Complex Syst. Complex. Sci.* **2018**, *15*, 11–18.
4. Che, L.; Liu, X.; Ding, T.; Li, Z.Y. Revealing Impacts of Cyber Attacks on Power Grids Vulnerability to Cascading Failures. *IEEE Trans. Circuits II Express Briefs* **2019**, *66*, 1058–1062. [CrossRef]
5. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [CrossRef]
6. Peng, X.Z.; Yao, H.; Du, J.; Wang, Z.; Ding, C. Load-induced cascading failure in interdependent network. *Acta Phys. Sin.* **2015**, *64*, 355–362.
7. Gao, J.X.; Buldyrev, S.V.; Stanley, H.E.; Havlin, S. Networks formed from interdependent networks. *Nat. Phys.* **2012**, *8*, 40–48. [CrossRef]
8. Tan, F.; Xia, Y.X.; Zhang, W.P.; Jin, X.Y. Cascading failures of loads in interconnected networks under intentional attack. *Eur. Phys. Lett.* **2013**, *102*, 28009. [CrossRef]
9. Qu, Z.Y.; Zhao, T.Y.; Zhang, Y.; Qu, N.; Liu, Y.Q.; Sun, J. A method for determining risk propagation threshold of power cyber physical system network based on percolation theory. *Autom. Electr. Power Syst.* **2020**, *44*, 16–23.
10. Bashan, A.; Berezin, Y.; Buldyrev, S.V.; Havlin, S. The extreme vulnerability of interdependent spatially embedded networks. *Nat. Phys.* **2013**, *9*, 667–672. [CrossRef]
11. Han, Z.M.; Wu, Y.; Tan, X.S.; Duan, D.G.; Yang, W.J. Ranking key nodes in complex networks by considering structural holes. *Acta Phys. Sin.* **2015**, *64*, 429–437.
12. Wu, Q.; Zhang, D.X.; Ling, X.F.; Liu, D.W.; Qi, Y.Z.; Ma, S.Y.; Zheng, C.Y. Dynamic analysis of disturbance propagation in power grid based on an epidemic model. *Proc. CSEE* **2019**, *39*, 4061–4069.
13. Siettos, C.I.; Russo, L. Mathematical modeling of infectious disease dynamics. *Virulence* **2013**, *4*, 295–306. [CrossRef] [PubMed]
14. Zhan, X.X.; Liu, C.; Zhou, G.; Zhang, Z.K.; Sun, G.Q. Coupling dynamics of epidemic spreading and information diffusion on complex networks. *Appl. Math. Comput.* **2018**, *332*, 437–448. [CrossRef] [PubMed]
15. Allen, L.J.S. Some discrete-time SI, SIR, and SIS epidemic models. *Math. Biosci.* **1994**, *124*, 83–105. [CrossRef]
16. Li, J.Q.; Ma, Z.E.; Brauer, F. Global analysis of discrete-time SI and SIS epidemic models. *Math. Biosci. Eng.* **2017**, *4*, 699–710.

17. Jiang, L.R.; Xu, Q.Y.; Ouyang, B.; Lang, Y.; Dai, Y.; Tong, J. Epidemic Spreading in Interdependent Networks. *Math. Probl. Eng.* **2018**, *2018*, 9374039. [CrossRef]
18. Newman, M.E.J. *Networks: An Introduction*; Oxford University Press: Oxford, UK, 2010; pp. 125–193.
19. Guo, H.D.; Yu, S.S.; Herbert, H.C.; Fernando, T.; Zheng, C.Y. A complex network theory analytical approach to power system cascading failure-From a cyber-physical perspective. *Chaos* **2019**, *29*, 053111. [CrossRef]
20. Li, X.L.; Xu, R.J.; Lou, J.; Xu, X.J. Social contagions on duplex networks. *Complex Syst. Complex. Sci.* **2019**, *16*, 13–18.
21. Li, J.Y.; Luan, Y.Y.; Wu, X.Q.; Lu, J. Synchronizability of double-layer dumbbell networks. *Chaos* **2021**, *31*, 073101. [CrossRef]
22. Tootaghaj, D.Z.; Bartolini, N.; Khamfroush, H.; La, P.T. Mitigation and recovery from cascading failures in interdependent networks under uncertainty. *IEEE Trans. Control Netw.* **2019**, *6*, 501–514. [CrossRef]
23. Wei, X.; Wu, X.Q.; Chen, S.H.; Lu, J.; Chen, G. Cooperative epidemic spreading on a two-layered interconnected network. *Siam. J. Appl. Dyn. Syst.* **2018**, *17*, 1503–1520. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.