applied sciences

MDPI

Article

Vulnerability Assessment of Electrical Cyber-Physical Systems against Cyber Attacks

Yinan Wang [1,2,*], Gangfeng Yan [1,2] and Ronghao Zheng [1,3]

1 College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China; ygf@zju.edu.cn (G.Y.); rzheng@zju.edu.cn (R.Z.)
2 Huanan Industrial Technology Research Institute of Zhejiang University, Guangzhou 510535, China
3 Zhejiang Province Marine Renewable Energy Electrical Equipment and System Technology Research Laboratory, Zhejiang University, Hangzhou 310007, China
* Correspondence: 11410065@zju.edu.cn; Tel.: +86-136-3351-1992

Received: 16 April 2018; Accepted: 9 May 2018; Published: 11 May 2018

Featured Application: In this special issue, we proposed a MATLAB-based platform for offline simulation and analysis of the vulnerability of electrical cyber-physical systems with the advantages of easy programming, fast calculation, and the lack of damage to systems. The study is of significance to decision-makers as they can get specific advice and defence strategies about a special power system.

Abstract: The integration of modern computing and advanced communication with power grids has led to the emergence of electrical cyber-physical systems (ECPSs). However, the massive application of communication technologies makes the power grids become more vulnerable to cyber attacks. In this paper, we study the vulnerability of ECPSs and develop defence strategies against cyber attacks. Detection and protection algorithms are proposed to deal with the emergency of cascading failures. Moreover, we propose a weight adjustment strategy to solve the unbalanced power flows problem which is caused by splitting incidents. A MATLAB-based platform with advantages of easy programming, fast calculation, and no damage to systems is built for the offline simulation and analysis of the vulnerability of ECPSs. We also propose a five-aspect method of vulnerability assessment which includes the robustness, economic costs, degree of damage, vulnerable equipment, and trip point. The study is of significance to decision makers as they can get specific advice and defence strategies about a special power system.

Keywords: electrical cyber-physical system; protection procedure; vulnerability assessment; simulation platform

1. Introduction

Nowadays, cyber-physical systems (CPSs) are becoming increasingly pervasive across the critical infrastructures [1]. A cyber-physical system is an integration of computing and communication with physical systems [2]. Embedded computers monitor and control physical processes, usually with feedback loops, where physical processes affect computations and vice versa [3,4]. It dramatically enhances the controllability, adaptability, autonomy, efficiency, functionality, reliability, safety, and usability of the original system. Examples of CPSs include transportation systems [5], defensive weapon systems [6] industrial systems [7], and energy systems [8] (such as oil systems, water systems, and power systems).

However, cyber-physical attacks are posing great threats to the safety and security of cyber-physical systems. Cyber-physical interactions in the cyber-physical systems make cross-domain attacks, specifically, and cyber-physical attacks, possible. Attackers may use cyber attack techniques

(involving viruses, worms, and denial of service) in communication networks to cause damage to the physical system or use means of physical attacks in the physical system to cause disruptions in the communication network. In addition, these attacks can be applied comprehensively to achieve collaborative cyber-physical attacks. The objectives of cyber-physical attacks are usually achieved via threat propagation within the cyber and physical systems. According to the Industrial Control System Cyber Emergency Team reports [9], major cyber threats (such as cyber attacks and computer worms) against critical cyber-physical infrastructures have increased from 9 incidents in 2009 to 257 incidents in 2013.

The blackout of the Ukrainian power systems that happened in 2016 shows the fragility of the electrical cyber-physical systems (ECPSs) under cyber attacks [10]. The integration of traditional power grids and modern communication networks into ECPSs has improved the efficiency of the stand-alone power systems [11–13]. However, the introduction of communication makes power systems become vulnerable to cyber attacks, which has already been a serious problem and needs to be solved [14]. Thus, studying the vulnerability of ECPSs has become an important topic recently. On this issue, research efforts have been undertaken along three different approaches.

The first approach focuses on analyzing the vulnerability of ECPSs caused by safety loopholes based on a specific cyber attack, such as denial of service attacks [15], false data injection attacks [16], and undetectable cyber attacks [17]. Cardenas et al. [18] summarized that sensor measurements and control commands were avenues of cyber-physical attacks. Mo et al. [19] thought that existing security approaches were either inapplicable, not viable, insufficiently scalable, incompatible, or simply inadequate to address the challenges posed by highly complex environments such as the smart grid. Rahman et al. [20] pointed out that the vulnerability of ECPSs was caused by deceived bad data detection tests with attackers compromising some of the power grid measurements. Liu et al. [21] showed that the key real-time operational tools (for example, State Estimator) of the electric power grids were vulnerable to false data injection attacks. Based on these points, studies [22,23] improved the detection strategies in estimators. Pasqualetti et al. [24] studied attack detection for descriptor systems by geometric control theory. Pooranian et al. [25] proposed a random response approach to achieve strong privacy and minimize the privacy leakage based on data-deduplication. However, these strategies are only effective for a special attack or situation. If there are multiple attacks, these methods may not be helpful. Therefore, it is necessary to find a way which can deal with a more complex situation.

The second approach assesses the vulnerability of ECPSs based on models in order to enhance the system security. Buldyrev et al. [26] modeled ECPSs and quantized the vulnerability of the systems using the theory of complex networks. Shao et al. [27] described the relationship of communication networks and power grids with multiple support–dependence relations. Guo et al. [28] summarized the effectiveness indicators of power grids based on the topology information of ECPSs. Nezamoddini et al. [29] measured the damage of cyber attacks in terms of the load curtailment and addressed the problem of the transmission system security with an optimization model. Wei et al. [30] considered ECPSs multi-agent dynamic systems and proposed a flocking-based paradigm for security control. Chen et al. [31] introduced a two-player zero-sum game between the adversary and the defender to evaluate the performance of defense mechanisms with different network configurations. Although these models can be used to assess the vulnerability of ECPSs, the theory of complex networks can only be used to analyze the topological characteristics of ECPSs, not considering the electrical information. State equations of generators do not fit for analyzing large-scale transmission grids.

In the third approach, scholars concentrate on the development of smart grid cyber-physical system testbeds for vulnerability analyses. Carlini et al. [32] presented a cyber-physical power system framework based on the service-oriented architecture for experimental results. Wang et al. [33] provided a simulation environment to model the process of supervisory control and data acquisition (SCADA) system vulnerability exploitations. In Reference [34], the Optimized Network Engineering Tools (OPNET) was extended to simulate wide-area communication networks in power systems

where the power system dynamic simulation was simplified as a virtual demander. NS-2 [35] was also a popular and open source discrete-event simulator developed to facilitate the simulation of communication networks. In some of the testbeds [36,37], actual data acquisition and actuator components (remote terminal unit (RTU), phasor measurement unit (PMU), and intelligent electronic device (IED)) were integrated with the power system simulators using middleware to enable hardware-in-the-loop (HIL) simulations. In summary, different simulation platforms and approaches integrating existing simulators have been proposed with different purposes and limitations. Several simulation paradigms of communication networks (such as time delay or packet loss) are no longer a concern in smart grids.

Our research focuses on establishing a complete evaluation procedure of vulnerability analysis with ECPSs considering cyber attacks. For this purpose, we have developed our study from three aspects in Figure 1: model, platform, and assessment. The model approach is suitable for large-scale systems (as shown in References [13,38]). In this paper, we will first go on with the study of the simulation platform with advantages of easy programming, fast calculation, and no damage to systems, and secondly, propose a convincing and comprehensive vulnerability assessment from five aspects.

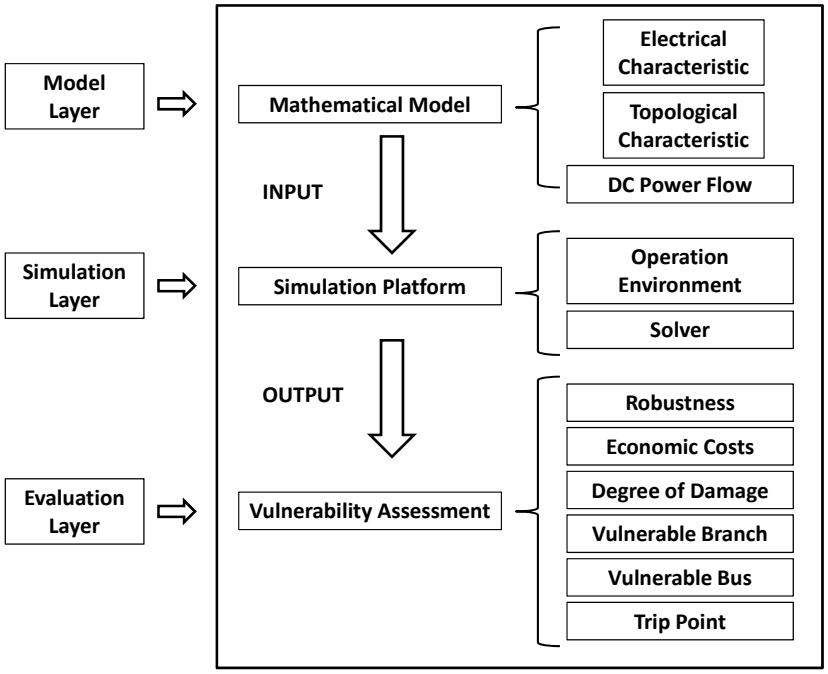

Figure 1. A complete evaluation procedure of vulnerability analysis.

This paper has two contributions. The first is a MATLAB-based platform (R2013a, The MathWorks, Inc., Natick, MA, USA, 2013) for the offline simulation and analysis of the vulnerability of ECPSs. This platform has advantages of easy programming, fast calculation, and no damage to systems. The protection procedure of ECPSs under cyber attacks and algorithms about detection and protection when dealing with a cascading failure are embedded by functions. The proposed simulation platform has great compatibility and expansibility in which operators can easily change the algorithm without changing the inputs.

Existing power simulation platforms and approaches integrating existing simulators like Matpower (V6.0, R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, Ithaca, NY, USA, 2017), PSCAD (X4, Manitoba-HVDC research centre, Winnipeg, MB, Canada, 2014), and PSASP (V7.0, China electric power research institute, Beijing, China, 2011) can be used for analyzing both steady states and transient states. However, when dealing with a simulation of the propagation of cascading failures, these simulators are not convenient because the topology of the power grid will be changed

after a splitting accident. Detailed comparisons with existing solution approaches of vulnerability analyses with ECPSs are shown in Table 1.

Table 1. The comparisons with existing solution approaches of vulnerability analyses with electrical cyber-physical systems (ECPSs).

Item	System Scale [1]	Algorithm Complexity [2]	Control Parameter	Platform Type	Considering Cyber Attack	Failure Propagation
Our	Large	Low	Bus/Branch/Power	Simulator	Yes/Multiple	Yes
[15]	Large	Medium	Control Command	Simulator	Yes/Single	No
[16,17]	Small	High	Angle/Frequency	Simulator	Yes/Single	No
[20–23]	Small	High	Control Command	Simulator	Yes/Single	No
[24]	Medium	Medium	Control Command	Simulator	Yes/Single	No
[26,27]	Large	Low	Node/Line	Simulator	Yes/-	Yes
[29]	Large	Low	Power	Simulator	Yes/Single	No
[30]	Small	High	Angle/Frequency	Simulator	No	No
[31]	Large	Low	Node	Simulator	Yes/Single	Yes
[32,33]	Small	-	-	Hardware	No	No
[34]	Medium	-	Angle/Frequency	OPNET	No	No
[35]	Medium	-	Pack loss/Delay	NS-2	Yes	No
[36,37]	Medium	-	Angle/Frequency	HIL	No	No

[1] System Scale (Small: nodes < 10; Medium: 10 < nodes < 40; Large: nodes > 40). [2] Algorithm Complexity (Low: DC power flow; Medium: Linear state equation; High: AC power flow/ Nonlinear state equation).

The second contribution is a comprehensive approach to vulnerability assessments. The five aspects of the vulnerability assessment include robustness, economic costs, the degree of damage, vulnerable equipment, and trip point. Associated with the simulation results obtained by our platform, we can have a thorough comprehension of the vulnerability in ECPSs. Additionally, decision-makers can get specific advice and defence strategies from this system against cyber attacks based on the results.

Existing indicators (such as node degree, cluster coefficient, and node betweenness) are mainly proposed in the research area of complex networks. These indicators cannot represent the relationship of power flows and topologies.

The rest of this paper is organized as follows. The modeling framework for ECPSs is presented in Section 2. Section 3 introduces the solution approaches for fault detections, protection procedures, and adjustment strategies. The aspects of vulnerability assessment and simulation platform are illustrated in Section 4. Section 5 analyzes the vulnerability with numbers of examples with the IEEE 39-bus system based on our proposed simulation platform. Section 6 concludes the paper. Section 7 discusses future works.

2. Framework of ECPSs

As we have introduced in Reference [13], the proposed framework compressively considers the characteristics of the power grids, communication facilities, and their interdependent relationships.

2.1. Model of ECPSs

Owing to the wide application of sensors, routers, controllers, and actuators in ECPSs, power grids and communication networks deeply interact with each other. According to Parandehgheibi's study [39], the topology of a power grid can be abstract as a graph $G(V, E)$, where V and E represent power buses and branches, respectively. Similarly, the topology of a communication network can be abstract as $G_c(V_c, E_c)$, where V_c and E_c represent communication nodes and lines, respectively.

In our framework, each bus or branch in a power grid is equipped with a controller and a sensor. That is to say, we consider a highly intelligent smart grid. Figure 2 shows the framework of

a regional ECPS. In this two-layer model, the upper layer with nodes numbered 1 to 10 represent a communication network, and C_k is the control center, while the lower layer with power nodes labeled A to E and breakers on branches labeled $b-1$ to $b-5$ represent a power grid. The dashed lines with double-sided arrows are information channels between the power grids and communication networks. In the real word, ECPSs in a large area can be divided into several regional ECPSs by physical distances or locations. In this paper, we consider each regional ECPS a local control center C_k with centralized control structures, while in large-scale areas, several regional ECPSs are controlled by a distributed control structures.

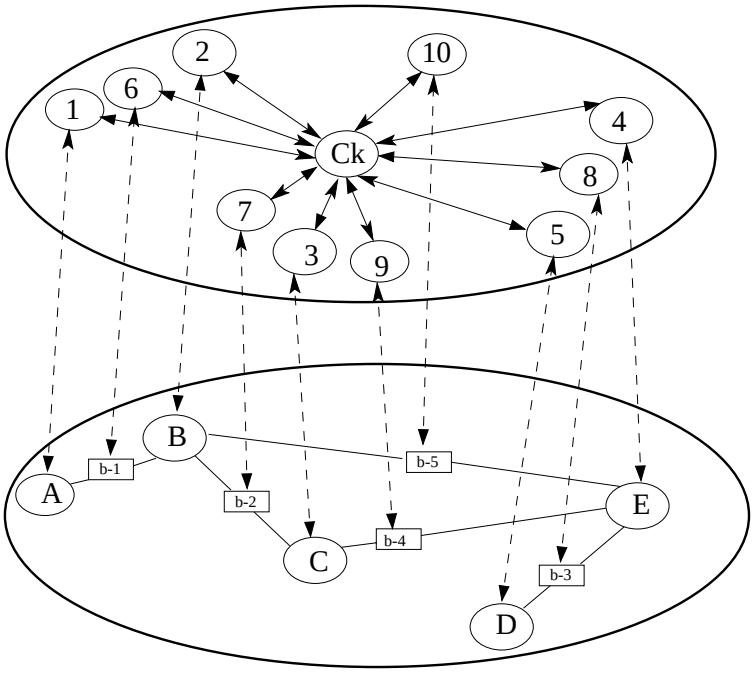

Figure 2. The framework of a regional ECPS.

2.2. DC Power Flow

The Direct Current (DC) power flow model [40] is used to calculate the distribution of power flows. The DC power flow model converts nonlinear problems into linear circuit problems. It clearly reflects the overload phenomenon but greatly reduces the calculation. Although the model has an error of generally 5%, it is acceptable when we estimate the performance of large-scale ECPSs.

Define $B \in R^{|V|\times|V|}$ as the conductance matrix associated with a power grid. Let θ and $p \in R^{|V|}$ be the phases and power injection at the buses, respectively. Let $F \in R^{|V|\times|V|}$ be the matrix of the power flows of the branches. Then a DC power flow model can be described as:

$$B\theta = p, \tag{1}$$

$$F(i,j) = B(i,j)\left(\theta_i - \theta_j\right), \tag{2}$$

where $i \neq j, i, j \in 1, 2, \ldots, |V|$.

As for communication networks, this paper is concerned more about the impacts of ECPSs under attack rather than the mechanism of different cyber attacks. So we define the relationships of communication networks to power grids to be the control function. A detailed solution approaching fault detections, protection procedures, and adjustment strategies will be introduced in the next section.

3. Solution Approach

In an ECPS, when a branch is tripped, the control center will first find out the possible faulty nodes, and then apply the procedure to protect the system. In this section, we first introduce algorithms for detection and protection and then propose methods for adjustment strategy.

3.1. Localization of Possible Faults

In a power grid $G = (V, E)$, let $V_G, V_L \subseteq V$ represent the set of generators and loads, respectively, and E represents the set of branches. If the system is attacked by uplink or downlink spoofing attacks, the control center cannot receive the alerting signal.

Definition 1. *The distance of Node i and j: the distance L_{ij} of node i and j is defined as the shortest path from node i to j.*

Definition 2. *The possible Fault Set of branch (i, j) : a set of nodes $S = \{g_1, g_2, \ldots, g_m, l_1, l_2, \ldots l_n\}$, $1 \leq m \leq |V_G|$, $1 \leq n \leq |V_L|$ is called a possible fault set of branch (i, j), if S satisfies the following two conditions simultaneously: (1) for $\forall g_k \in S$ and $\forall p \in V_G$, there are $g_k \in V_G$ and $L_{ig_k} \leq L_{ip}$ (or $L_{jgk} \leq L_{jp}$); (2) for $\forall l_w \in S$ and $\forall q \in V_L$, there are $l_w \in V_L$ and $L_{il_m} \leq L_{iq}$ (or $L_{jl_w} \leq L_{jq}$).*

Algorithm 1 is proposed to identify the possible fault set of branch (i, j).

Algorithm 1 Identify the possible fault set

1: Input the overloaded branch (i, j)
2: For $1 \leq r \leq |V_G|, r \neq i, j$
3: Calculate the distance L_{ri} and L_{rj}, respectively (not including the path (i, j))
4: Identify nodes that have the shortest distance with node i
5: Identify nodes that have the shortest distance with node j
6: End
7: For $1 \leq r \leq |V_L|, r \neq i, j$
8: Calculate the distance L_{ri} and L_{rj}, respectively (not including the path (i, j))
9: Identify nodes that have the shortest distance with node i
10: Identify nodes that have the shortest distance with node j
11: End
12: Combine steps 4, 5, 9, and 10, get the possible fault set S

Remark 1. *Algorithm 1 is used to deal with the situations in which an overload is caused by uplink or downlink spoofing attacks. It should be pointed out that Algorithm 1 will be used n times if there are n overloaded branches.*

3.2. Protection Procedure of ECPSs under Cyber Attacks

Based on Algorithm 1, in this section, we introduce the protection procedure of ECPSs considering cyber attacks. The procedure begins with a tripped branch and follows the steps below:

(a) Judge the connectivity of the system after cutting off a branch.

- (a-1) If there is a splitting incident, then go to step (b).
- (a-2) If there is no separation of the system, directly go to step (f).

(b) Identify the main area as the remaining system after splitting.

- (b-1) If there is a main area, go to step (c).
- (b-2) If there is no main area, go to step (i).

(c) Upload the changed topology and electrical information to the control center.

(d) Make decisions with the unbalanced power in the control center.
(e) Download and adjust the control strategies to the appointed generators.
(f) Update the topology and electrical information to the control center for calculation.
(g) Calculate the power flow.
(h) Search for the overloaded branches.

(h-1) If there are overloaded branches, cut off the branches and go back to step (a).
(h-2) If there is no overloaded branch, then go to step (i).

(i) End the procedure, record the loss.

In power systems, splitting incidents caused by cutting off the overloaded branches may lead to serious cascading failure propagation, especially in ECPSs. Owing to the topology change, related electrical information will be changed, which will consequently influence the stability, robustness, and safety margin of the system. Algorithm 2 is used to assess the damage degree of a system using tools from graph theory when there is an overloading incident. By analyzing the connectivity of the system, the splitting incident is considered a special situation. Let $L \in R^{|V|\times 1}$ be the area label vector, with $l_k \in L$ as the area label of node k, $k \in 1, 2, \ldots, |V|$.

Algorithm 2 Assess the damage degree

1: Input V, set $t = 1$ and $L = [0, 0, \ldots, 0]$.
2: For $i = 1 : |V|$
3: For $j = 1 : |V|$
4: If branch $(i, j) \in E$
5: If $l_i = l_j$
6: If $L(i) = 0$
7: Then $l_i = l_j = t$, $t = t + 1$;
8: End if
9: Else
10: If $l_i \cdot l_j \neq 0$
11: Then $l_i = l_j = \max\left\{l_i, l_j\right\}$;
12: Else
13: For $k = 1 : |V|$
14: If $L(k) = L(i)$
15: $L(k) = L(j)$;
16: End; end; end; end; end; end; end.
17: Output and count the number $n < |V|$ of areas.

Remark 2. *Note that n is the number of different values of elements in L. If all the elements in L are the same, then there is no splitting and* $n = 1$.

Based on the results from Algorithm 2, we know whether there is a splitting incident and how many areas the system will be separated into when cutting off an overloaded branch. However, according to Kirchhoff laws, not every separated area can still be a functional subsystem. The control center needs to identify the main area of the system.

According to the results in Algorithm 2, assume that the power grid $G(V, E)$ is separated into $n (n \in Z)$ parts. The i^{th} part is abstracted as $G_i(V_i, E_i)$, $i \in 1, 2, \ldots, n$. Algorithm 3 is used to search for the main area after a splitting incident with the standard of the maximum numbers of generators and loads.

Let $K = [k_1, k_2, \ldots, k_n]$ and $M = [m_1, m_2, \ldots, m_n]$ be the vector of the number of generators and loads, respectively.

Algorithm 3 Search for the main area after splitting

1: Input n , $t = 0$, $j = 0$
2: For $l = 1 : n$, for $i = 1 : |V_l|$
3: Count k_i and m_i
4: if $k_i + m_i > t$
5: $j = i, t = k_i + m_i$
6: End if; end; end
7: Output j

So the j^{th} area is the main system after the splitting incident.

3.3. Method of the Control Center under Unbalanced Power

If an ECPS suffers a splitting incident, based on Algorithm 3, the remaining buses in the main area will lead to an unbalanced power distribution. The control center will collect the electrical information of the buses in the main area, calculate the unbalanced power, and adjust the outputs of each of the generators. The method proposed in this paper can be applied in three situations:

Situation I: If the splitting incident only causes the separation of generators, the remaining generators in this area must increase their outputs to keep the balance between supply and demand. The total amount of the increased power should be $\Delta P = \sum P^*_{gen}$, where $\sum P^*_{gen}$ is the sum of the lost generator outputs.

Situation II: If the splitting incident only causes the separation of loads, the remaining generators in this area must decrease their outputs to keep the balance between supply and demand. The total amount of the reduced power should be $-\Delta P = \sum P^*_{load}$, where $\sum P^*_{load}$ is the sum of the lost loads.

Situation III: If the splitting incident causes both the separation of generators and loads, the control center should first calculate the unbalanced power by $\Delta P = \sum P^*_{gen} + \sum P^*_{load}$. If $\Delta P > 0$, take the same strategy in Situation I; if $\Delta P < 0$, take the same strategy in Situation II; and $\Delta P = 0$, take no adjustment strategy.

Remark 3. *In the above generator power adjustment method, the distribution of the total unbalanced power to each generator should be decided in weighted terms. The specific distribution methods will be introduced in Algorithm 4.*

Algorithm 4 is used to calculate the weighted adjustment of each generator in the main area after the splitting incident. Generators near the tripped buses may be distributed with higher weighted terms. Let $V'_G \subset V'$ be the set of generators in the main area $G' = (V', E')$ after the splitting incident.

Algorithm 4 Calculate the weighted adjustment

1: Input G', ΔP and the tripped branch (i, j) with node m (generator or load bus)
2: Let $l = w = [0, 0, \ldots, 0]$, $S = 0$
3: For $k = 1 : \left|V'_G\right|$
4: Reconnect branch (i, j) to G', and calculate L_{km}, $l(k) = L_{km}$, $S = S + 1/l(k)$
5: End
6: For $k = 1 : \left|V'_G\right|$
7: Calculate the weight $w(k) = l(k)/S$ and the adjustment $P^w_k = \Delta P \cdot w(k)$
8: End

Remark 4. *If the adjusted output of a generator is beyond the output limit, then modify the output of this generator to the nearby limit. The rest of the total power adjustment value should be* $\Delta P' = (\Delta P - \sum P^w_i) + \sum (P^w_i - \Delta P^{\lim it}_i) = \Delta P - \sum \Delta P^{\lim it}_i$ *, where* P^w_i *is the weighted adjustment output of generator i and* $\Delta P^{\lim it}_i$ *is the actually adjustable output of generator i.*

Remark 5. *If there are n generators and loads tripped at a splitting incident, Algorithm 4 should be used for dealing with each tripped bus, respectively.*

4. Vulnerability Assessment and Simulation Platform

According to Section 3.2, it can be seen that, when dealing with a problem of overloading, every step will need the cooperation of sensors, routers, controllers, and actuators. However, the system is vulnerable because a small fault may lead to a serious cascading failure in ECPSs owing to the strong coupling between the power grids and the communication networks.

4.1. Vulnerability Assessment Aspects

In China, the data of the electrical communication systems in power grid systems are not open currently. These communication systems are equipped with special transmission lines which guarantee high bandwidth for data exchange. Hence, in the following discussion, we assume that bandwidth is not a concern. In this section, we assess the impacts of power grids in ECPSs.

In the power grids, the major electrical properties include node (generator or load) constraints, branch capacity limits, and flow direction. The major topological properties include numbers of nodes, connectivity, and the degree of nodes. All of these properties have an effect on the vulnerability of the power grids. Therefore, in this section, we propose thorough assessment procedures from five aspects which take the above properties into account.

(a) The stability and robustness of the system. In this procedure, we randomly cut off a branch, balance the power supplies and demands, redistribute the power flow, and count the number of remaining buses. At last, we calculate the proportion of the numbers of remaining buses. A system is said to have good stability against a single tripped branch if none of the nodes will be split during the procedure, while the system has bad stability if the system will suffer a cascading failure owing to the tripped branch. As for robustness assessment, the statistics show that a system has good robustness if the system is stable in most of the faulty situations, but not vice versa.

(b) The vulnerable branches which will cause higher economic costs. When a branch is randomly cut off from the grid, the consequential balance of power supplies and demands leads to economic cost. The economic cost can be represented by the sum of adjusted outputs of the generators (Algorithm 4) along the shortest path which is defined in Section 3. Generally speaking, the tripped branches which will lead to higher economic costs should be protected by some specific methods.

(c) The vulnerable branches which will lead to a serious damage. If we randomly cut off a branch, the degree of damage will be represented by the number of remaining buses or branches after cascading failures. The tripped branch which leads to less remaining buses or branches is more vulnerable.

(d) Vulnerable nodes against extra power injection. Randomly choose a power node (generator or load), inject the same amount of power, and recalculate the power flows on the branches. A node is vulnerable if the power injection will cause other lines to overload. The result is influenced by both the topological and electrical properties.

(e) The trip point of the cascading failure propagation. It reflects the controllability of a system. The trip point is the point when the number of remaining buses decreases the fastest. In a discrete system, the duration of cascading failures is replaced by the number of loops in the procedure. The system has more time to deal with the emergence if the trip point appears slowly.

4.2. Simulation Platform

In this section, we build a MATLAB-based platform for the offline simulation and analysis of the vulnerability of ECPSs from the five aspects in Section 4.1. The detailed system configuration we used is listed in Table 2.

Table 2. The system configuration.

Item	Content
Operating system	Windows 7/10, Mac OS X 10.11
CPU	Intel (R) Core (TM) i7-4790, 3.60 GHz
RAM	8.00 GB
System Type	64-bit
Software	MATLAB 2012a

Three necessary settings are required before the simulation: (i) input the topology of a power grid and related electrical information; (ii) input the locations of sensors, routers, and actuators; and (iii) specify the initial tripped branch (or the amount of power injection and the ID of a power node) and the protection algorithms. Then the proposed program will give vulnerability assessments of the system based on the simulation results.

In the simulation, the IEEE 39-bus system (including 10 generators, 21 loads, and 46 branches) is used as an example (Figure 3). We assume that the sensors, routers, and actuators are located at each bus and branch.

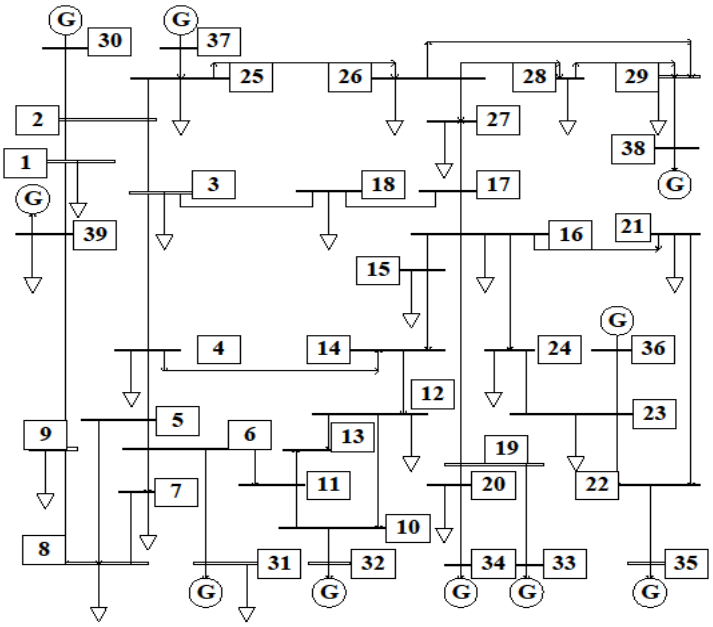

Figure 3. The topology of the IEEE 39-bus system.

Figure 4 shows the flowchart of the platform for the offline simulation of the performance of ECPSs under different faults. The program begins with a situation selection. In CASE 1, the program user randomly selects a power node and sets the amount of the power injection and the program searches for the overloaded lines at first. In CASE 2, the user randomly selects a branch (i, j) as the initial triggering event and trip the line in CASE 2, the ECPS will suffer a protection and control procedures.

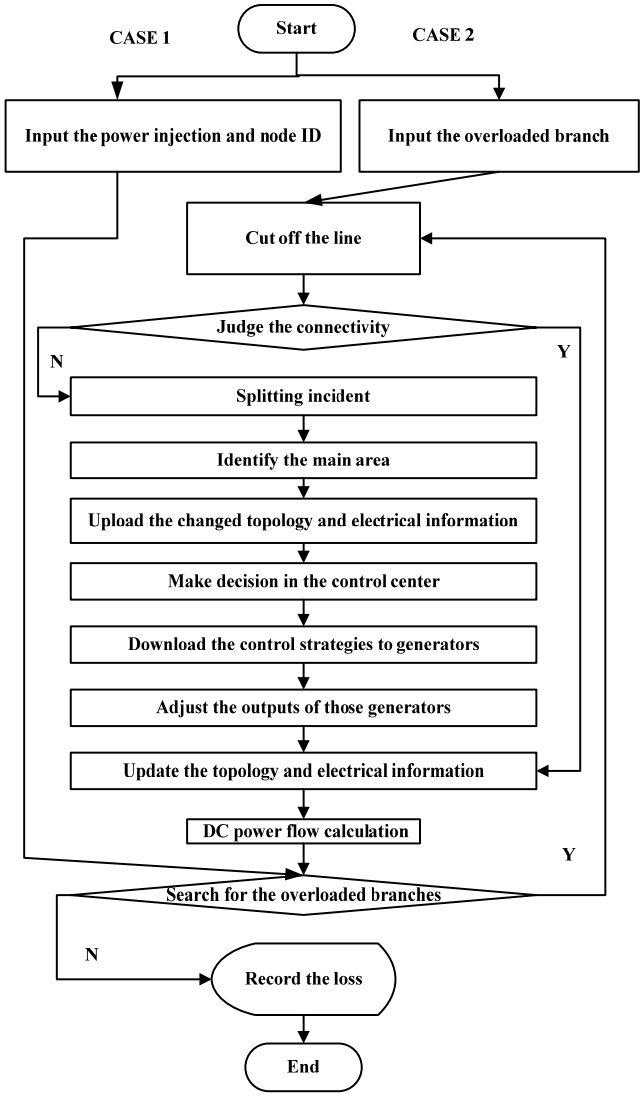

Figure 4. The flow chart of the simulation platform.

5. Discussion

In this section, we assess the vulnerability of the ECPSs and provide protection suggestions based on the simulation results provided by the simulation platform developed in this work.

In CASE 1, we set the initial power injection as $\Delta P = \{50, 100, 150, 200, 250MW\}$. The extra injection of the power can successfully be injected into a power bus if ΔP is within the capacity limitation. When $\Delta P > 250MW$, almost half of the loads are beyond the limitation. Table 3 shows 8 situations in which the extra injection will cause an overloading incident. Table 3 also lists the IDs of possible fault power nodes based on Algorithm 1.

Remark 6. *The upper right mark '$(*)$ ' on node ID represents the different power injection. For example, ID = $25^{(3-5)}$ means that the node with ID = 25 will cause a line overload with $\Delta p_3 = 150$, $\Delta p_4 = 200$, and $\Delta p_5 = 250$.*

Four important conclusions are made based on the simulation results. First, buses 12, 20, 21, 23, 25, 26, 28, and 29 are vulnerable buses against a single power injection, and bus 20 is the most vulnerable bus in the system. Second, the overloaded branches such as $(6, 11)$, $(16, 19)$, $(21, 22)$, and $(23, 24)$ are

vulnerable to power flow change. The two possible explanations include the initial higher load rate Q (such as $Q_{(6,11)} = 70.4\%$, $Q_{(16,19)} = 76.7\%$, $Q_{(21,22)} = 67.7\%$, and $Q_{(23,24)} = 59\%$ ($Q_{average} = 35.9\%$)) and the unreasonable partial design of topology (like branches $(2, 25)$ and $(28, 29)$). Third, in this system, the branches near the generators have higher capacity limitations with no generator node being vulnerable. This partial design is worth learning. Last, the results in Table 1 also demonstrate the efficiency of Algorithm 1. In seven of eight situations with ten overloaded branches, the accuracy of the proposed algorithm is 90%.

Table 3. The CASE 1 result.

No.	Extra Injection Node ID	Overloaded Branch	Possible Gen ID	Possible Load ID
1	$12^{(3–5)}$	6–11	31/32	7/12
2	$20^{(1–5)}$	16–19	33/35/36	15/20/24
3	$21^{(4–5)}$	16–21	33/35	16/21
4	$23^{(4–5)}$	21–22, 23–24	33/35/36	16/21/23
5	$25^{(3–5)}$	2–25	30/37	1/25/26
6	$26^{(5)}$	2–25	30/37	1/25/26
7	$28^{(5)}$	2–25	30/37	1/25/26
8	$29^{(5)}$	2–25, 28–29	30/37/38	1/25/26/28/29

In CASE 2, the simulation program begins with a tripped branch. Table 4 presents 20 possible simulation results which will cause cascading failures, with the ID of the initial faulty branch, the number of remaining branches and buses, the economic cost, and running time in the table. Table 3 does not include the situations if cutting off branches will not disturb the original operation. In order to verify the superiority of Algorithm 4, we take the strategy using average adjustments for comparison. Note that 'A' represents the average adjustments and 'W' represents the weighted adjustments.

Table 4. The CASE 2 results.

Faulty Branch	Remaining				Cost		Running Time	
	Branch		Bus		(100 MVA)			
	A	W	A	W	A	W	A	W
2–30	45	45	38	38	2.50	2.50	1	1
4–14	21	21	20	20	6.74	6.74	3	3
6–31	14	17	14	17	26.53	16.75	7	5
6–11	21	6	18	6	8.13	18.88	5	5
10–11	13	13	13	13	28.68	27.18	7	7
10–32	13	13	13	13	28.68	27.18	6	6
10–13	22	22	21	21	13.22	11.77	5	5
13–14	19	19	18	18	13.12	11.80	5	5
16–21	7	8	8	9	20.70	18.71	7	6
16–19	42	11	35	11	4.60	24.36	1	6
19–33	9	13	10	13	35.99	27.60	6	5
19–20	42	11	35	11	7.86	17.76	2	7
20–34	45	10	38	10	5.08	32.32	1	5
21–22	0	8	0	9	20.32	18.44	7	6
22–35	12	13	12	13	23.38	17.96	6	5
23–24	7	8	8	9	20.70	18.80	7	6
23–36	10	10	10	10	35.18	32.86	5	5
25–37	45	45	38	38	5.40	5.40	1	1
26–27	37	37	33	33	5.18	5.18	2	2
29–38	45	45	38	38	8.30	8.30	1	1

Based on the simulation results, Figure 5 shows the stability of the system. It can be seen that among the 46 branches, if a branch is randomly tripped, the system is still stable with a probability of

57%. In the other 43.7%, the system will suffer a splitting incident, while the probability of causing serious cascading failures (less than 20 buses remained) is 31%.

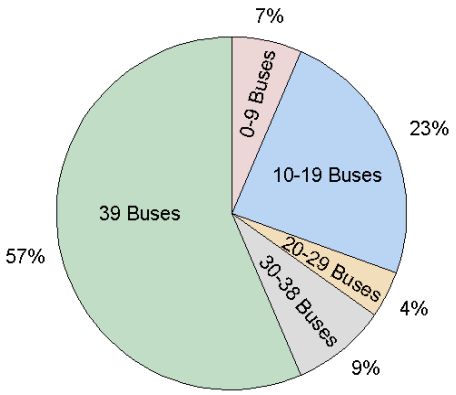

Figure 5. The performance of the system under faults.

Figure 6 presents the vulnerability from the aspect of economic costs. Strategies of average and weighted adjustments are shown together (the black line with circle marks represents for costs with weighted adjustments, while green line with star marks represents the costs with average adjustments). The X-axis is the ID of the initial tripped branch. It can be seen from Figure 4 that if branches $(10, 11)$, $(10, 32)$, $(19, 33)$, $(20, 34)$, or $(23, 36)$ are cut off at the beginning, the government will pay much more for repairing the system after the cascading failures. Comparing these two lines, we can also make a conclusion that the weighted adjustment in Algorithm 4 is more economical than the average one. A significant advantage against the average strategy is that the system with a weighted strategy can largely ease the degree of severe cascading failures (such as branch $(16, 21)$, $(21, 22)$, and $(23, 24)$).

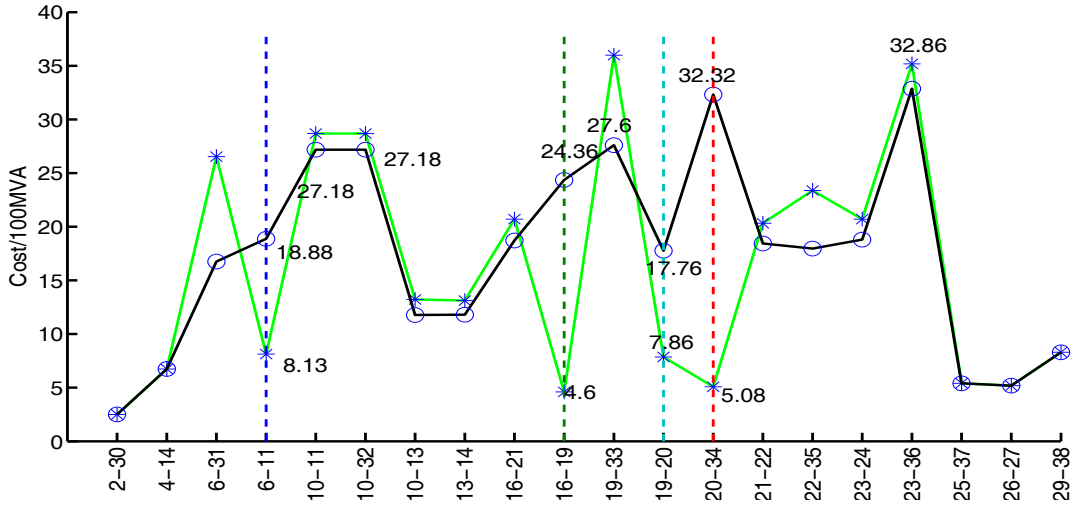

Figure 6. The economic costs of protection.

However, in this example, there are four situations in which cutting off a branch with the weighted adjustment will aggravate the cascading failures compared with average adjustment. We have marked these four situations (branches $(6, 11)$, $(16, 19)$, $(19, 20)$ and $(20, 34)$) with the dashed lines in Figure 7. Inspired by CASE 1, we find that these four lines have high initial load rates Q ($Q_{(6,11)} = 52.4\%$, $Q_{(16,19)} = 42.9\%$, $Q_{(19,20)} = 49.8\%$, and $Q_{(20,34)} = 70.5\%$ ($Q_{average} = 35.9\%$)). Branches $(6, 11)$ and $(16, 19)$ are also vulnerable lines in CASE 1. This phenomenon reflects a limitation of our proposed

algorithm. If the branches near the tripped power node have a high initial load rate, the weighted adjustment based on the distance may have a higher probability to cause a severe failure.

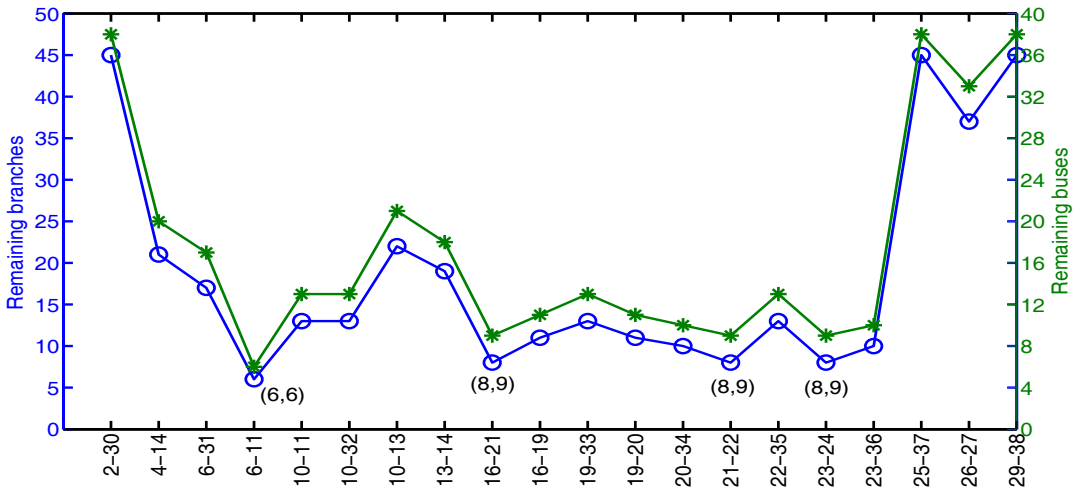

Figure 7. The remaining buses and branches in the system.

Figure 7 shows a positive relationship between the remaining branches (blue line with circle marks) and buses (dark green line with star marks) of the system with a weighted adjustment strategy. From the figure, we can find the vulnerable branches which will lead to a serious damage. Cutting off branches $(6, 11)$, $(16, 21)$, $(21, 22)$ or $(23, 24)$ will lead to a rapid decrease of the node scale, which means a serious cascading failure.

Figure 8 gives us a deep understanding of the relationship between the trip point and cascading failure propagation caused by splitting incidents. Each shape of mark and its related color line in the figure represent a vulnerable branch. We pick up 9 of the vulnerable branches mentioned above and count the remaining buses after each split and protection procedure. It can be seen that the relationship of time and propagation of cascading failures is nonlinear, but with the increase of loops, the system may suffer a jump point (blue dashed line), in which the size decreases rapidly.

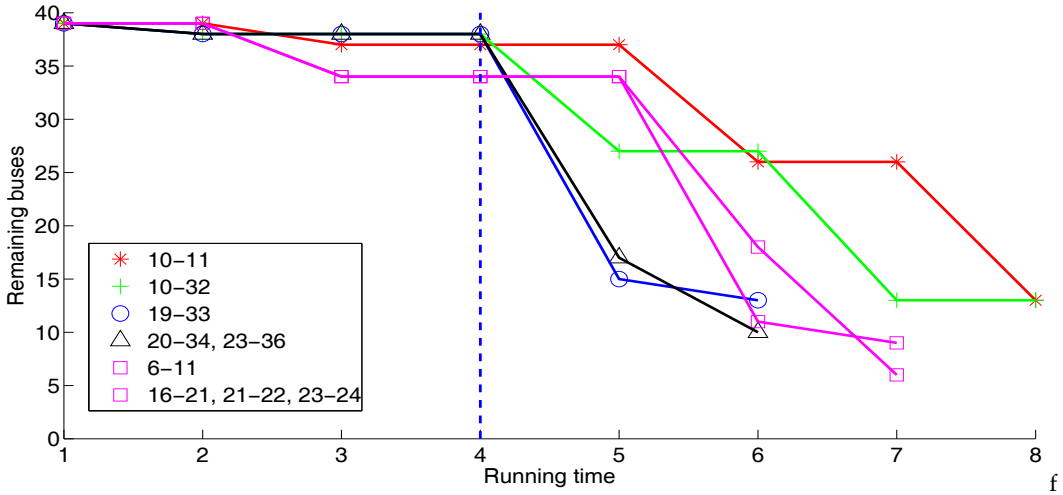

Figure 8. The propagation of cascading failures.

6. Conclusions

In this paper, we have established a complete evaluation procedure of vulnerability analysis with ECPSs considering cyber attacks. Firstly, a MATLAB-based platform for the offline simulation and analysis of the vulnerability of ECPSs was proposed. This platform has advantages of easy programming, fast calculation, and no damage to the systems. The protection procedure of ECPSs under cyber attacks and algorithms about detection and protection when dealing with a cascading failure are embedded by functions. Compared with the existing power simulation platforms and approaches integrating existing simulators like Matpower, PSCAD, or PSASP, our platform has a higher performance when dealing with the propagation of cascading failures.

Secondly, this paper has presented a comprehensive approach to vulnerability assessment. Existing indicators (such as node degree, cluster coefficient, node betweenness) are mainly proposed in the research area of complex networks. These indicators cannot represent the relationship of power flows and topologies. Our proposed indicators of vulnerability assessment include robustness, economic costs, the degree of damage, vulnerable equipment, and trip point. Associated with the simulation results obtained by our platform, we can have a thorough comprehension of the vulnerability in ECPSs. Additionally, decision-makers can get specific advice and defence strategies of this system against cyber attacks based on the results.

7. Future Works

In the future, based on this platform, we will focus on studying fault detection and the prediction of ECPSs using the algorithm of Neural Networks. We may replace the DC power flow model with an AC power flow model in order to get a higher precision.

Author Contributions: Y.W. and G.Y. conceived and designed the experiments; Y.W. performed the experiments, analyzed the data, and wrote the paper; R.Z. checked the language and grammars of the paper. Part of this work was presented by Y.W. in IEEE IECON 2017-43rd Annual Conference.

Funding: The financial support for this research is supported by (1) the National Basic Research Program (863) of China (No. 2015AA050202); (2) the Science and Technology Project of State Grid (WBS: 52110417001B); (3) National Natural Science Foundation of China (No. 61503335); and (4) The National Key Research and Development Program of China (No. 2018YFB0904900).

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Liu, X.; Zhang, J.; Zhu, P. Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory. *Int. J. Crit. Infrastruct. Prot.* **2017**, *16*, 13–25. [CrossRef]
2. Bordel, B.; Alcarria, R.; Robles, T.; Martín, D. Cyber–physical systems: Extending pervasive sensing from control theory to the Internet of Things. *Pervasive Mob. Comput.* **2017**, *40*, 156–184. [CrossRef]
3. Lee, E.A. The past, present and future of cyber-physical systems: A focus on models. *Sensors* **2015**, *15*, 4837–4869. [CrossRef] [PubMed]
4. Lee, E.A. Cyber-physical systems-are computing foundations adequate. In Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation. *Technol. Roadmap* **2006**, *2*, 1–9.
5. Xiong, G.; Zhu, F.; Liu, X.; Dong, X.; Huang, W.; Chen, S.; Zhao, K. Cyber-physical-social system in intelligent transportation. *IEEE/CAA J. Autom. Sin.* **2015**, *2*, 320–333.
6. Lee, E.A. Cyber Physical Systems: Design Challenges. In Proceedings of the IEEE International Symposium on Object Oriented Real-Time Distributed Computing, Orlando, FL, USA, 5–7 May 2008; pp. 363–369.
7. Javanmardi, S.; Shojafar, M.; Shariatmadari, S.; Ahrabi, S.S. Fr trust: A fuzzy reputation–based model for trust management in semantic p2p grids. *Int. J. Grid Util. Comput.* **2014**, *6*, 57–66. [CrossRef]
8. Kleissl, J.; Agarwal, Y. Cyber-physical energy systems: Focus on smart buildings. In Proceedings of the 47th Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; ACM: New York, NY, USA, 2010; pp. 749–754.

9. Peterson, D. *Ics-Cert: Stuxnet Lessons Learned*; Digital Bond: Sunrise, FL, USA, 2010.
10. Guo, Q.; Xin, S.; Wang, J.; Sun, H.B. Comprehensive Security Assessment for a Cyber Physical Energy System: A Lesson from Ukraine's Blackout. *Autom. Electr. Power Syst.* **2016**, *40*, 145–147.
11. Moslemi, R.; Mesbahi, A.; Velni, J.M. A Fast, Decentralized Covariance Selection-based Approach to Detect Cyber Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2017**, *99*. [CrossRef]
12. Shakeruzzaman, A.; Akter, M.N.; Nasiruzzaman, A. Power Grid Connectivity Monitoring by Identifying Critical Transmission Lines Based on Network Flow. In Proceedings of the IEEE International Conference on Electrical, Computer and Communication Engineering, Cox's Bazar, Bangladesh, 16–18 February 2017; pp. 235–238.
13. Wang, Y.N.; Lin, Z.Y.; Liang, X.; Xu, W.Y.; Yang, Q.; Yan, G.F. On modeling of electrical cyber-physical systems considering cyber security. *Front. Inf. Technol. Electron. Eng.* **2016**, *17*, 465–478. [CrossRef]
14. Xiang, Y.; Wang, L.; Liu, N. A Robustness-Oriented Power Grid Operation Strategy Considering Attacks. *IEEE Trans. Smart Grid* **2017**, *99*. [CrossRef]
15. Zhang, H.; Cheng, P.; Shi, L.; Chen, J. Optimal DoS attack scheduling in wireless networked control system. *IEEE Trans. Control Syst. Technol.* **2016**, *24*, 843–852. [CrossRef]
16. Teixeira, A.; Sou, K.C.; Sandberg, H.; Johansson, K.H. Secure control systems: A quantitative risk management approach. *IEEE Control Syst. Mag.* **2015**, *35*, 24–45. [CrossRef]
17. Zhao, T.; Xu, Y.; Wang, Y.; Lin, Z.; Xu, W.; Yang, Q. On Identifying Vulnerable Nodes for Power Systems in the Presence of Undetectable Cyber-Attacks. In Proceedings of the IEEE Conference on Industrial Electronics and Applications, Hefei, China, 5–7 June 2016; pp. 1062–1067.
18. Cardenas, A.A.; Amin, S.; Sastry, S. Secure Control: Towards Survivable Cyber-Physical Systems. In Proceedings of the IEEE International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500.
19. Mo, Y.; Kim, T.H.J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber–physical security of a smart grid infrastructure. *Proc. IEEE* **2011**, *100*, 195–209.
20. Rahman, M.A.; Mohsenian-Rad, H. False Data Injection Attacks with Incomplete Information against Smart Power Grids. In Proceedings of the IEEE Global Communications Conference, Anaheim, CA, USA, 3–7 December 2012; pp. 3153–3158.
21. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst.* **2011**, *14*, 13. [CrossRef]
22. Gu, C.; Jirutitijaroen, P.; Motani, M. Detecting False Data Injection Attacks in AC State Estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483.
23. Teixeira, A.; Amin, S.; Sandberg, H.; Johansson, K.H.; Sastry, S.S. Cyber Security Analysis of State Estimators in Electric Power Systems. In Proceedings of the IEEE Conference on Decision and Control, Atlanta, GA, USA, 15–17 December 2010; pp. 5991–5998.
24. Pasqualetti, F.; Dorfler, F.; Bull, F. Cyber-Physical Security via Geometric Control: Distributed Monitoring and Malicious Attacks. In Proceedings of the IEEE Conference on Decision and Control, Maui, HI, USA, 10–13 December 2012; pp. 3418–3425.
25. Pooranian, Z.; Chen, K.C.; Yu, C.M.; Conti, M. RARE: Defeating Side Channels based on Data-Deduplication in Cloud Storage. In Proceedings of the Infocom Workshop, Honolulu, HI, USA, 15–19 April 2018; pp. 660–665.
26. 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] [PubMed]
27. Shao, J.; Buldyrev, S.V.; Havlin, S.; Stanley, H.E. Cascade of failures in coupled network systems with multiple support-dependence relations. *Phys. Rev. E* **2011**, *83*, 036116. [CrossRef] [PubMed]
28. Guo, J.; Wang, D.R. Vulnerability analysis on power communication network based on complex network theory. *Telecommun. Electr. Power Syst.* **2009**, *30*, 6–10.
29. Nezamoddini, N.; Mousavian, S.; Erol-Kantarci, M. A risk optimization model for enhanced power grid resilience against physical attacks. *Electr. Power Syst. Res.* **2017**, *143*, 329–338. [CrossRef]
30. Wei, J.; Kundur, D.; Zourntos, T.; Butler-Purry, K.L. A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control. *IEEE Trans. Smart Grid* **2014**, *5*, 2687–2700. [CrossRef]
31. Chen, P.Y.; Cheng, S.M.; Chen, K.C. Smart attacks in smart grid communication networks. *IEEE Commun. Mag.* **2012**, *50*, 24–29. [CrossRef]

32. Wang, C.; Fang, L.; Dai, Y. A simulation environment for SCADA security analysis and assessment. In Proceedings of the IEEE International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, 13–14 March 2010; pp. 342–347.
33. Carlini, E.M.; Giannuzzi, G.M.; Mercogliano, P.; Schiano, P.; Vaccaro, A.; Villacci, D. A decentralized and proactive architecture based on the cyber physical system paradigm for smart transmission grids modelling, monitoring and control. *Technol. Econ. Smart Grids Sustain. Energy* **2016**, *1*, 5. [CrossRef]
34. Li, W.; Zhang, X.; Li, H. Co-simulation platforms for co-design of networked control systems: An overview. *Control Eng. Pract.* **2014**, *23*, 44–56. [CrossRef]
35. Li, W.; Zhang, X. Simulation of the smart grid communications: Challenges, techniques, and future trends. *Comput. Electr. Eng.* **2014**, *40*, 270–288. [CrossRef]
36. Vaccaro, A.; Popov, M.; Villacci, D.; Terzija, V. An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification. *Proc. IEEE* **2011**, *99*, 119–132. [CrossRef]
37. Morris, T.; Srivastava, A.; Reaves, B.; Gao, W.; Pavurapu, K.; Reddi, R. A control system testbed to validate critical infrastructure protection concepts. *Int. J. Crit. Infrastruct. Prot.* **2011**, *4*, 88–103. [CrossRef]
38. Huang, P.; Wang, Y.; Yan, G. Vulnerability analysis of electrical cyber physical systems using a simulation platform. In Proceedings of the IEEE the 43rd Annual Conference, Beijing, China, 29 October–1 November 2017; pp. 489–494.
39. Parandehgheibi, M.; Modiano, E.; Hay, D. Mitigating cascading failures in interdependent power grids and communication networks. In Proceedings of the IEEE International Conference on Smart Grid Communications, Venice, Italy, 3–6 November 2014; pp. 242–247.
40. Stott, B.; Jardim, J.; Alsaç, O. DC power flow revisited. *IEEE Trans. Power Syst.* **2009**, *24*, 1290–1300. [CrossRef]