Study on cross-space risk interaction mechanism in CPS system under network attack

Zhentao Han¹, Kun Song¹, Zhuoran Song², Peng Chang³,⁴, Xin He¹ and Zhiyuan Duan³

¹State Grid Liaoning Electric Power Company Limited Economic Research Institute. Shenyang, China;
²State Grid Liaoning Electric Power Supply CO., LTD. Shenyang, China;
³College of Information Science and Engineering, Northeastern University, Shenyang, China
⁴Email: 1258911858@qq.com

Abstract. Power Information-Physical Systems are at risk of cyberattacks. Based on the interaction mechanism of power information-physical fusion system across space risks under network attack, this paper first analyzes the operational characteristics of power information-physical fusion system, and studies the operating characteristics and structural characteristics of the system before the attack occurs. Secondly, the topological model of power information-physical fusion system is established, and the influence of CPS system structure vulnerability on the spread of network attack security risk is analyzed from the characteristics of power grid topology, and a method of quantifying vulnerability nodes in network is established. At the same time, considering the evolution process of risk in the cross-space environment, combined with the operational characteristics of information-physical fusion system, this paper deeply studies the process of interactive transmission of power grid information-physical system security risk under cyber attack, and analyzes the alternating propagation process of information side risk penetrating physical boundary to trigger physical side risk and lead to further expansion of risk. Finally, the simulation analysis is carried out through the IEEE-57 node test system.

1. Introduction

Electric power is an indispensable basic energy source for modern life and plays an important supporting role in modern life and economic development. With the development of China's smart grid strategy, so that every link of development, transmission, distribution and use will have more complex and diversified intelligent information equipment access, grid control more dependent on the physical system and information systems between the cooperation. With the frequent interaction and close coupling between information flow and physical flow, the power grid is not simply a single system that considers physical flow, but a fusion system that covers information flow and physical flow, and gradually develops into a dependent coupling system, that is Cyber Physical System(CPS)[1].

However, with the wide application of information technology, the power CPS system will also face more uncertainty and complexity, which brings potential threats and challenges to the reliability and security of the system [2]. Because current state awareness and scheduling control require accurate and real-time data exchange, information system anomalies or network attacks can penetrate
the boundaries of information and physical systems to threaten the safe and stable operation of the power grid[3].

At present, there have been a number of accidents in power systems caused by information security problems. The most representative of these was the massive power outage in Ukraine at the end of 2015. At the end of 2015, Ukraine's power grid was hacked, causing malicious tripping of multiple substation switches at the bottom, while Ukraine's EMS system lost its awareness and control of physical systems due to the Black Energy virus, delaying the discovery and control of accidents. Eventually, the risk is alternating between information and physical space, triggering large-scale power outages[4]. In addition, it is not uncommon for network attacks to cause abnormal power grid operations[5], such as the 2011 Iran Stuxnet virus intruded on Iran's nuclear power plant facilities, the 2012 attack on Canada's TELVENT caused the SCADA system to collapse, and so on.

At present, some research progress has been made in the fields of information system interaction topology, discrete information state (information flow) and mutual drive of continuous power process (energy flow).

Reference[6] tries to put forward the hybrid computing technology of information flow and energy flow from the system operation level, puts forward a CPS fusion modeling concept, and applies it to the field of CPS security evaluation to improve the computing rate. Reference[7] in order to describe the interaction between CPS information flow and energy flow, the driving relationship between various kinds of events is constructed. Some documents discuss the process of information-physical interaction in the operation of CPS system from the actual business scenario. Reference[8] discusses the interaction topology between information space and grid physical systems from a topological perspective, and discusses the impact of dynamic changes in the interaction topology in typical scenarios.

However, none of the aforementioned literature considers the cross-space risk interaction mechanism due to cyber attacks. To address the above issues, this paper starts from the interactive mechanism of cross-spatial risk in power information-physical fusion system under cyber attack, considers the evolution of risk in cross-spatial environment with the operational characteristics of information-physical fusion system, and studies the process of security risk interaction and propagation of power grid information-physical system under cyber attack.

2. Power information-physical fusion system characterization

2.1. Power information-physical fusion system normal operation characteristics analysis

Grid CPS is a binary coupled heterogeneous network system that deeply integrates information and physical systems and thus constitutes a heterogeneous network system. Among them, information and energy flows have obvious heterogeneous characteristics, which have two main aspects.

First, the interaction between the discrete quantity of information system and the continuous quantity of physical system.

The normal operation of the power CPS system is under the control of the discrete information flow of the physical flow of each link operation control, while the normal flow of information upstream and downstream can not be separated from the physical system's power support. Therefore, the normal operation of both is inseparable from the reliable operation of each other.

Secondly, the time cycle of the interaction between information flow and energy flow is different.

Although the two systems are coupled with each other to achieve a control goal, the time magnitude will be different because they are configured separately, and there is bound to be a time difference between the physical measurements or commands of the information system, so the complete synchronization and real-time performance between the two systems cannot be guaranteed.

2.2. Structural characterization of power information-physical fusion systems

(1) Characteristics of the information-physical network dual-layer structure
See Figure 1, the network topology is the most intuitive property of the system, and the network structure of the grid information-physical system can be considered as a complex network with 2 layers, i.e., interdependent networks. There are 2 forms of edges in its network: connected edges and coupled edges.

Figure 1. The topology model of power CPS system.

Due to the large differences among the sites in terms of device types, quantities, deployment methods, etc., from the point of view of simplifying the analysis, the information devices or physical devices in this paper mainly take the site as the unit of study.

(2) Topological coupling characteristics of information-physical network interaction

The coupled edge connection between information nodes and physical nodes in CPS is flexible and diverse, and its coupled connection modes are analyzed from the point of view of connection mode: 1. complete one-to-one coupling mode; 2. one-to-many coupling mode; 3. many-to-many coupling mode; analyzed from the point of view of connection state.

(3) Small-world and scale-free properties of single-layer networks

The small-world characteristic is the characteristic of a network having a small average path length and a large clustering coefficient, and was first proposed by Watts as a network between a regular network and a random network with the following topological characteristics:

$$\begin{cases} C >> C_{\text{random}} \\ L >> L_{\text{random}} \end{cases}$$

$C$ is the clustering coefficient of the network, $L$ is the average distance of the network, and $C_{\text{random}}$ and $L_{\text{random}}$ correspond to the corresponding parameters under the random network, respectively.

3. Security risk analysis of power information-physical converged system

3.1. Topological model of power information-physical fusion system

The power CPS system is a binary coupled interdependent network formed by the deep integration of the primary physical power grid and the secondary information network, in which the secondary information equipment collects and measures the operating information of the primary physical equipment, and sends the control commands from the control center to the primary physical equipment; the primary physical equipment provides power support for part of the secondary information equipment, so the CPS information nodes and the physical CPS information network are in close proximity to each other. There are many-to-many interdependencies between nodes.

In order to assess the structural impact on the nodes of the power grid after an attack, this paper models the topology of the CPS interdependence network as follows:

$$G_i = (V_i, E_i)$$  \hspace{1cm} (2)

$$A = \left[ a_{i,j} \right]_{N \times N}$$  \hspace{1cm} (3)

$$L = \{ S_{s-p} \}$$  \hspace{1cm} (4)

$$D = \{ F, Q \}$$  \hspace{1cm} (5)
In the above formula (2), \( x \in \{ p, c \}, G_p, G_c \) the two information and power physical networks are represented as separate powerless and directionless topographies, respectively, \( V = \{1, 2, \ldots, N\} \) is the set of nodes and \( E = \{e_{ij}\} \) is the set of edges of the single-sided network.

The above formula (3) represents the adjacency rights matrix of the unilateral networks based on their own characteristics of the information and physical single-layer networks, respectively, whose matrix elements are established based on the principle of the physical significance of the different networks.

The values of the matrix elements in the physical side adjacency matrix \( A_p \) are as follows:

\[
\begin{cases}
0, & \text{non-adjacent} \\
x', & \text{adjacent}
\end{cases}
\]

(6)

In the formula: \( x' \) is between nodes \( i \) and nodes \( j \) impedance scale of the transmission line \( 0 < x' < 1 \)

The matrix elements of the information-side adjacency matrix \( A_i \) are as follows:

\[
\begin{cases}
0, & \text{non-adjacent} \\
F_{ij}/F_{ih}, & \text{adjacent}
\end{cases}
\]

(7)

In the formula: \( F_{ij} \) is the sum of the information flows between information node \( i - j \) and \( F_{ij} \) is the sum of the information flows of all connected nodes of information node \( i \).

Equation (7) is a set of coupling relations for the connection of two interdependent networks. \( S_{c-p} \) matrix describes the virtual coupling dependence of the communication network on the physical network, when there is a link between information network node \( j \) and physical network node \( j \), coupling relationship matrix element \( s_{ij} = 1 \) otherwise \( s_{ij} = 0 \); \( S_{p-c} \) matrix describes the virtual coupling dependence of the physical network on the information network, when there is a link between physical network node \( i \) and information network node \( j \), \( s_{ij} = 1 \) otherwise \( s_{ij} = 0 \).

Equation (8) represents the binary set of coupling strengths between information network and physical network nodes, \( F \) is the strength of the dependence of the coupling edge of information node \( i \) on the physical network, defining element \( F_i \) of it as follows.

\[
F_i = \frac{1}{N(S_{c-p})}
\]

(8)

\( N(S_{c-p}) \) is the number of physical nodes on which the information nodes corresponding to that coupled edge depend.

Similarly, the element of the coupled edge-weight matrix of the physical node to the information network is \( Q \), where element \( Q_i \) is defined as follows.

\[
Q_i = \frac{1}{N(S_{p-c})}
\]

(9)

\( N(S_{p-c}) \) is the number of information nodes on which the physical nodes connected by this coupled edge depend.

3.2. Impact of structural vulnerabilities of power information-physical convergence systems on security risks

Coupling between power and information networks is achieved due to the existence of interdependencies, while node vulnerability not only affects the survivability of a unilateral network under cyber attack [9], but also affects the survivability of the entire coupled network under cyber attack through interdependent edges.
The node vulnerability is mainly related to its location in the coupled network and the role between neighboring nodes. The location information of the node, i.e., global vulnerability, is measured using the efficiency value of the node, which is defined in the following equation.

\[
E_i^g = \frac{1}{N} \sum_{j \neq i} \frac{1}{d_{ij}}
\]

\(d_{ij}\) is the shortest path distance between \(i\) to \(j\) nodes in a single-sided network, measured by the number of sides passed.

The vulnerability transfer relationship between nodes is reflected in the impact of the attacked node on neighboring nodes, and when analyzing the vulnerability transfer relationship of a node, it should be combined with the efficiency value of the node, defining the node's local vulnerability contribution as.

\[
E_{j \to i}^v = \frac{a_i^j I_{j \to i} E_i^j}{(\bar{I}_i)^2}
\]

Combining the location of the node itself in the network and the vulnerability contribution of neighboring nodes to that node, an expression for the vulnerability of \(i\) nodes can be obtained.

\[
V_i = E_i^g \cdot \sum_{j \neq i} E_{j \to i}^v = E_i^g \cdot \sum_{j \neq i} \frac{a_i^j I_{j \to i} E_i^j}{(\bar{I}_i)^2}
\]

From the above equation, the critical node that affects the vulnerability of the network can be identified, which is also the main target of cyber attacks. Also, in order to measure the impact of the vulnerability node on the propagation of security risks, it can be determined by the transmission capacity degradation indicator of the network after the failure of the node[9], which is shown in the following equation.

\[
\Delta T_i^E = \frac{1}{N(N-1)} \sum_{\{i \neq j\}} \frac{1}{d_{ij}}
\]

4. Interaction mechanism for cross-spatial propagation of security risks to grid CPS systems under cyber attack

When the control center discovers the existence of an overrunning line, in order to ensure that the system can make quick decisions and ensure reliable power supply to users, the control center performs real-time optimization calculations on the current operating state of the CPS system by using the optimal current model. From the point of view of power supply reliability, it adopts the following tidal current model as equation (14).

\[
\min \sum_{\alpha \beta} P_{i,\alpha}^{\text{load}}
\]

\[
\begin{align*}
P_i(u, \bar{\delta}) + P_i^{\text{load}} - P_i^D &= 0 \\
Q_i(u, \bar{\delta}) - Q_i^D &= 0 \\
P_i^{\text{max}} &\leq P_i(u, \bar{\delta}) \leq P_i^{\text{max}} \\
Q_i^{\text{max}} &\leq Q_i(u, \bar{\delta}) \leq Q_i^{\text{max}} \\
0 &\leq P_i^{\text{load}} \leq P_i^D \\
u_i^{\text{min}} &\leq u_i \leq u_i^{\text{max}} \\
S_i^{\text{min}} &\leq S_i \leq S_i^{\text{max}}
\end{align*}
\]

In the formula: \(P_i^{\text{load}}\) is the amount of load cut on node \(i\); \(P_i^D\) is the amount of load carried by the node; \(P_i(u, \bar{\delta})\), \(Q_i(u, \bar{\delta})\) is the injected active power and injected reactive power of the node, respectively; \(u_i\) is the node voltage; \(S_i\) is the line transmission capacity.
5. Case analysis
This section uses the IEEE-57 node standard system to build the test system, the physical layer uses the IEEE-57 node system, the line tide capacity is set to twice the initial line tide in the normal operating state, the information side acquisition system can build a 58-node scale-free network through the Barabasi-Albert model, and the information layer has only one control center node. The physical and information side nodes of the CPS system are represented by $P_i$ and $C_j$.

Simultaneous setup of destructive events occurring in the system i.e. simultaneous cyber attacks on the information and physical layers generating failed nodes. Analyze the risk interaction of the CPS system under different attack scenarios.

Simulates what happens when the information layer fails massively due to an attack, i.e., a network attack spreads latently in the information layer for a certain amount of time and then begins to explode with a failure attack, resulting in the failure of the information side node $C_1$, $C_5$, $C_{18}$, $C_{35}$ and $C_{38}$ and the simultaneous failure of lines 13-15. The red node shown in Figure 2 is the bus node where the monitoring function fails, and the dashed line indicates the line that cannot be monitored and controlled.

![Figure 2](image)

**Figure 2.** Situation of IEEE-57 bus system attacked by a large-scale of network attack.

Figure 3 that the tidal reduction on the physical side of the network branch. The situation shows that the more the number of failed nodes on the information side of the CPS system, the greater the amount of load loss caused by unexpected failures on the physical side of the network or disconnected failures caused by network attacks, so the study of intrusion-tolerant defense strategies against failure attacks on the CPS system is very important to improve system reliability.

![Figure 3](image)

**Figure 3.** Comparison of branch power flow before and after network attacks in case 3
6. Conclusions
This paper analyzes the cross-space risk interaction mechanism in the distribution network information-physical fusion system, firstly, it analyzes the operational characteristics of the power information-physical fusion system, and studies the operational and structural characteristics of the system before the cyber attack occurs. Secondly, the topological model of the power information-physical fusion system is established, and the structural vulnerability of the CPS system is analyzed from the characteristics of the power grid topology on the risk impact on the security propagation of cyber attack, and a quantification method of the vulnerability nodes in the network is established. Again, the process of the interactive propagation of security risks of the information-physical system of a power grid under cyber attack is studied in depth. The alternate propagation process in which the information-side risk penetrates the physical boundary to trigger the physical-side risk and leads to further expansion of the risk is analyzed. Finally, the above risk interaction process of the cyber attack is verified by the IEEE-57 node example analysis.

Acknowledgments
This work is supported by the science and technology project of STATE GRID CORPORATION OF CHINA-Research and Application of Smart Grid Rapid Detection and Response Method under Malignant Data Injection Attack (SGLNJY00GHJS2000044)

References
[1] Rajkumar R, Lee I, Sha L, et al 2010 Cyber-physical systems: the next computing revolution [C]//Proceedings of the 47th ACM/IEEE Design Automation Conference. Anaheim, CA, IEEE 731-736
[2] Wei Zhinong, Chen Hesheng, Ni Ming, Sun Guoqiang, Sun Yonghui, Li Chao 2016 Malignant data definition, construction and defense challenges in power information physical systems [J]. Power System Automation 40(17) 70-78
[3] Li Tian, Su Sheng, Yang Hongming, Wen Fuxuan, Wang Dongqing, Zhu Lin 2017 Attack behavior and security protection of power information physical systems [J]. Power System Automation 41(22) 162-167
[4] Guo Qinglai, Xin Shujun, Wang Jianhui, Sun Hongbin 2016 A comprehensive safety assessment of information energy systems as seen from the Ukrainian blackout [J]. Power System Automation 40(05) 145-147
[5] Liu Nian, Yu Xinghuo, Zhang Jianhua 2016 Collaborative cyberattack: extrapolation and insights from the Ukrainian blackout [J]. Power System Automation 40(06) 144-147
[6] Guo Qinglai, Xin Shujun, Sun Hongbin, et al 2016 Power system information-physical fusion modeling and integrated security assessment: driving force and research concept [J]. Chinese Journal of Electrical Engineering 36(6) 1481-1489
[7] Yin Zhonghai, Zhang Kaisheng, Du Huahu, et al 2015 Event-driven modeling of information-physical fusion systems [J]. Microelectronics and Computers 32(12) 126-129
[8] Buldyrev S V, Havlin S, Parshani R, et al 2010 Catastrophic cascade of failures in interdependent networks [J]. Nature 464(7291) 1025-1031
[9] Dong Zhengcheng, Fang Yanjun, Tian Meng 2017 A Review of Interdependent Network Destructibility Research[J]. Complex Systems and Complexity Science 14(03) 30-44