Energy Internet Security Risk Evaluation Index System

Jing Li¹, Zhijie Shang¹, Ren Qiang²*, Jin Pang¹, Han Guo¹, Jingchu Wang¹ and Haihang Niu³

¹Information and Communication Branch of State Grid Corporation of China, Xicheng District, Beijing, 100032, China
²Beijing Engineering Research Center of Energy Electric Power Information Security, North China Electric Power University, Changping District, Beijing, 102206, China
³Institute of Software Chinese Academy of Sciences, Haidian District, Beijing, 100089, China

*Corresponding author’s e-mail: 120202201291@ncepu.edu.cn

Abstract. As the construction of the Energy Internet has launched into a novel method, the dependence on energy and information networks has been greatly increased. The interaction of energy and information flow has become recurring, and the deep coupling of energy and information flow has been realized. As a result, security risk factors have increased substantially. Given that, this article from the perspective of energy and information flow, combined with the “Source-Grid-Load-Storage” coordination scenario of the energy Internet and the actual development needs of the information network, this article proposes a risk assessment for many security risks that threatens the stable construction of the energy Internet Index system and corresponding index analysis.

1. Introduction

All parts of the world are facing the dilemma of uneven energy distribution. Many developed countries and regions have a large amount of electric energy surplus, while some backward countries and regions lack a stable electric power supply for a long time [1]. Because of this, the rational allocation and utilization of energy have become an urgent problem for people to solve, and the construction of the energy Internet has become an effective way to meet global electricity demand. Informatization is one of the indispensable factors of the Energy Internet. Open interaction and interconnection are the most significant features of the Energy Internet [2]. This clearly provides many malicious attackers with more diversified means to threaten the Energy Internet. Therefore, while vigorously building the Energy Internet, it is urgent to discover and protect its security risks. For which, building an energy Internet security risk evaluation index system has become the primary task.

Security risk assessment [3], as the main means for operation and maintenance personnel to identify safety risks, can realize rapid diagnosis of weak links in the Energy Network, and provide an effective basis for operation and maintenance personnel to take timely measures to avoid operational risks. Integrating various types of security risks and constructing a scientific and rigorous security risk assessment system is of great significance for guiding the effective construction of the Energy Internet and ensuring its safe and stable operation.
2. Energy Internet architecture and security risks

2.1. Concept of Energy Internet
In the general terms, the Energy Internet can be divided into three modes: Global Energy Internet, Internet + Energy, and regional Energy Internet [4]. The Global Energy Internet is a global Energy Network structure that uses the UHV (Ultra-High Voltage) transmission and distribution network as the backbone network, which covers the transmission methods of large-scale new energy sources, and is supplemented by global interconnection features. For Internet + Energy, there are essentially two modes. One is Internet + new energy power generation, through information technology such as cloud computing, big data, and blockchain, the energy system can achieve the purpose of configuration optimization, efficient operation, and safety and control; The second is Internet + conventional energy, through in-depth cooperation between several Internet companies such as Alibaba and Baidu and some large energy companies such as State Grid Corporation of China and China National Petroleum Corporation, the use of the network channel obtains user data information and further promotes the vigorous development of new business models. Regarding the Regional Energy Internet, it is essentially a comprehensive energy service model based on multiple forms of industrial capacity complementation, using multi-energy coupling and smart energy technology to provide an integrated energy service system such as electricity, heat, etc. for one region or multiple regions.

Energy Internet can be regarded as a form of energy application development entering a high-quality stage, based on the practice of applying multi-energy coupling energy Internet technology to energy development links. The Energy Internet architecture model includes the physical layer of multi-energy coupling, the information layer of open interconnection and intelligent intercommunication, and the business layer of high-demand service users. The multi-energy coupling is reflected in the vertical "Source-Grid-Load-Storage" system optimization mode and horizontal power supply, heating and cooling and other energy supply coupling modes, give full play to the interaction of energy flow and information flow of the Energy Internet, drive a substantial increase in energy utilization efficiency, and greatly increase the value of the energy industry.

2.2. Energy Internet security risks
With the development of information technology and the continuous evolution of information security policies in various countries, the trend of nationalization of network attacks [5] has increased significantly, and attacks on the vulnerability of power network systems have become an important form of political and economic struggle. Also, the continuity, concealment, and destructiveness of information security attacks have been significantly enhanced, greatly increasing the difficulty of information security protection, making the power network system face new network and information security risks in all aspects of power generation, transmission, transformation, distribution, utilization, and dispatch. The Energy Internet security risk diagram is demonstrated in Figure 1.
Energy Internet has the characteristics of informatization, automation, and interaction, and the energy flow and information flow are deeply integrated. Here, the network and information security risks faced by the power network system in the generation, transmission, transformation, distribution, utilization, and dispatching links are sorted out. Summarized into three categories.

(1) Intelligent business faces the risk of power failure. The intelligent development of power network systems has further revealed the risk of power outages. The control functions of power monitoring systems such as smart substation systems, power distribution automation systems, and load control systems rely more on information and communication technology. At the same time, security attacks are combined with specific services, showing a customized development trend. Suffering from network and information security attacks such as control instruction tampering and business logic destruction, causing business failure or abnormal control instruction settings, resulting in an increased risk of power outages.

(2) The network security boundary faces the risk of blurring and uncontrollable. The original relatively closed power system gradually adopts general network transmission protocols and multiple different network transmission channels, and multiple communication methods such as wireless local area networks, mobile communication networks, satellite communication, and multiple network protocols coexist, making the power communication network more complicated. As a result, there are risks of illegal eavesdropping, tampering, and destruction in the process of information transmission of wireless communication technology and smart sensor technology, and the network boundary becomes blurred. Besides, due to business development needs and geographical restrictions, some power terminals use wireless networks to connect to higher-level systems, which further increases the exposure of network attacks.

(3) It is difficult to protect massive heterogeneous terminals on-site. Smart grids have a larger number of heterogeneous intelligent interactive terminals, more ubiquitous network security protection boundaries, and more flexible and diverse business security access requirements. Power terminals have the risk of information leakage, illegal access, and control. Power grid attack defense and other aspects have raised higher challenges.
Due to historical reasons and technical constraints, the core equipment and systems of China's energy and power system still use a large number of foreign products. These products and systems have found defects in communication protocols, built-in operating systems, and security protections, which can lead to remote illegal operations and even malicious. In addition to the destruction of the controlled production facilities, several artificially set backdoor passwords and other deeper serious hidden dangers were also discovered and verified.

3. Energy and Information Flow perspective energy Internet security risk indicator system

From the perspective of energy flow and information flow, Energy Internet uses its friendly mutual assistance and coordinated and optimized interaction mode to accurately control the market and civil electricity loads and energy storage resources, and greatly improve the safe operation of the power grid and the ability to respond to large grid failures. Effectively support the development of distributed power sources, contribute to the rational allocation and consumption of distributed power sources, improve the utilization efficiency of grid assets on a large scale, and further promote the iterative development of new industries. Therefore, the research and application of the Energy Internet are of great significance to energy development. Given this, the introduction of energy flow-information flow deep coupling Energy Internet security risk indicator system risk indicators is very important. The indicator system architecture is shown in Figure 2.

3.1. Energy Internet risk indicators from the perspective of energy flow

The safety risk assessment index system model of converged Energy Internet "Source-Grid-Load-Storage" coordination scenario use the power supply side composed of a large-scale power plant and a variety of small distributed power sources, the power grid side with the transmission and distribution network as the main body, and the load side of the industrial load, commercial load, and living load, as well as the energy storage side that uses energy storage devices as the main energy storage equipment, constitute the target object. From the perspective of Energy Flow of the Energy Internet, construct a comprehensive security risk indicator framework for the integrated Energy Internet scenario through the security risks contained in various energy production, transmission, consumption, and storage.

3.1.1. Analysis of indicators at the source

Regarding the operation of power plants and the use of distributed power, based on the level of energy flow, the various factors caused by power generation and distributed power generation are evaluated from fuel management, equipment operation, power load forecasting, stable energy supply, and new energy access capabilities. Such safety risks, for example, the risk of fuel management in the production and operation of power plants is huge, which is usually analyzed in terms of fuel loss and storage period. The fuel will inevitably produce a large amount of loss during the combustion process. Effective reduction of fuel loss is essential to increase the fuel consumption rate of thermal equipment and reduce the energy loss of power plants. The safe operation of power generation equipment is the most critical stage of the entire source-end production capacity, and various problems are prone to occur in the normal operation of power equipment. Therefore, ensuring the safe operation of power equipment plays a significant role in the source-end safe energy supply and improves equipment management. The capacity and efficiency of generating units are coordinated with the total installed capacity and demand-side capacity and energy consumption to effectively ensure the safe and stable operation of power generation equipment. Power load forecasting is an important task in the production and operation process of power plants. Safety risks are often caused by deviations in power load forecasting. It is closely related to production arrangements, maintenance, fuel procurement, and other related production stages, it needs to be evaluated in terms of load forecasting methods, accuracy, and timeliness.

Also, the distributed power supply mode effectively meets the energy needs of a variety of special occasions, provides diversified functional forms, and makes up for the shortcomings of the large power grid in terms of power supply stability. However, distributed power supply relies on surrounding users to a large extent, so it is necessary to consider its safe and stable energy supply and new energy access
capabilities. The coordination of large-scale power grids and distributed power equipment has greatly improved the reliability of power supply and energy supply. Once a natural disaster causes the grid to collapse, distributed power sources can effectively ensure the continued stability of power consumption on the user side to a certain extent. Based on this, the reliable operation of the distributed power supply can effectively evaluate its user experience on the side of surrounding users.

3.1.2. Analysis of indicators on the power grid
In the context of large-scale interconnection and interconnection of power networks and the increased operating voltage of power systems, the power supply capacity of the power grid has been greatly improved. At the same time, the risks arising from the operation of the power grid are also increasing. The safe and stable operation of the power grid has become a new requirement for the risk tolerance of the power grid. By identifying the risks that the grid may face from the aspects of grid resilience, grid operation loss, and grid operation margin, the corresponding index set is listed. For example, power grid resilience mainly focuses on the defense and recovery capabilities of the power grid, to fully, quickly, and accurately sense the operating situation of the power grid, thereby enhancing the power grid’s ability to respond to disturbances and disasters. Grid operation loss refers to a series of safety accidents that have caused the power grid after a security risk event has occurred, including evaluation indicators such as grid cascading failures, grid load loss, and power grid equipment losses. The operation loss risk of the power grid often reflects the direct security risks caused by the power grid during operation. Another example is the grid operating margin. Under normal working conditions, various operating data of the grid are within a certain amplitude range. However, when the voltage limit, grid overload, and three-phase load imbalance occur, it is safe to deviate from the set data range. Incidents will threaten the normal operation of the power grid.
### Energy Flow-Information Flow Perspective Energy Internet Security Risk Index System

#### Energy Flow

| Source | Power plant |
|--------|-------------|
|        | Distributed Power |

| Power grid | Transmission grid |
|------------|-------------------|
|            | Distribution grid |

| Storage and load | Industrial, commercial, living load |
|------------------|-------------------------------------|
|                   | Energy storage system |

#### Information Flow

| Completeness | System design |
|--------------|--------------|
|              | Circuit configuration |

| Availability | Information service |
|--------------|----------------------|
|              | System running |

| Controllability | Information content |
|-----------------|----------------------|
|                 | Information dissemination |

| Reliability | Information content |
|-------------|----------------------|
|             | Information dissemination |

| Confidentiality | Storing data |
|-----------------|-------------|
|                 | Transfer data |

#### Grid structure level

- Inter-station communication rate of medium voltage line
- Average score of medium voltage line

#### Grid operation margin

- Voltage limit
- Grid overload
- Three-phase load unbalance

#### Power grid

- Voltage limit
- Grid overload
- Three-phase load unbalance

#### System tamper-proof

- Data tamper-proof
- Security Protocol
- Transmission process
- Storage structure
- Random accessibility
- Multi-faceted

#### System running

- Time for normal system operation
- System full load operation time

#### System security to home ratio

- Line intact rate
- Equipment intact rate

#### Energy flow and information flow deeply coupled energy internet security risk index system.

![Diagram of Energy Flow-Information Flow Perspective Energy Internet Security Risk Index System](image)

Figure 2. Energy Flow-Information Flow Deeply Coupled Energy Internet Security Risk Index System
Therefore, the power grid operation safety margin effectively reflects the load-bearing capacity and the ability to resist security risks during the operation of the power grid. Besides, the application of grid distribution automation and the level of grid structure can also reflect the safe state of grid operation.

3.1.3. Analysis of indicators at the load and storage terminals

The load end is the energy use side of the Energy Internet, which mainly focuses on the safety and convenience of industrial, commercial, and living energy. The load supply capacity has thus become a test user for the Energy Internet’s "Source-Grid-Load-Storage" synergy, safe, and stable energy supply the most effective method. By quantifying the “N-1” pass rate, voltage collapse rate, and load verification degree of the power grid, it is easy to obtain the stability of power consumption at the load end in a certain period.

Energy storage is an important link in the Energy Internet coordination scenario. For a long time, energy storage technology has plagued the steady development of the power system. However, through the development of "Source-Storage" coordination, "Grid-Storage" interaction, and "Load-Storage" integration, the application of energy storage technology in the power system is becoming more and more widespread. Based on this, the access capability of the energy storage system has become an important object worthy of attention at the energy storage end, including the line, equipment integrity rate, system safety to the household ratio, and power fiber to the household ratio is an effective quantitative indicator of system access capability. Energy storage is a key supporting technology for building the Energy Internet, and an important means to ensure stable operation of the power grid, optimize energy transmission, absorb clean energy, and improve power quality.

3.2. Energy Internet risk indicators from the perspective of information flow

In the process of building the Energy Internet, the supporting role of informatization is indispensable. The extremely open environment brought about by informatization provides ordinary users with a very convenient and very effective interactive mode of information transmission and reception. Openness is bound to have a negative impact on the construction of the Energy Internet. Malicious man-made attacks and malware attacks are more diversified and convenient in an open and interactive information environment. Malicious individuals can achieve attacks on the Energy Internet through a variety of specific channels. The security situation of the Energy Internet information environment is very severe. At the same time, the interconnection of the Energy Internet has been upgraded for the extensiveness of the Energy Network interaction process. However, this has greatly expanded the scope of malicious attacks and the threat level has increased sharply. Based on this, it is imperative to ensure information security in the construction of the Energy Internet, and building an Energy Internet information security risk evaluation index system is a key step for information security.

(1) Completeness: Traditional network information security integrity is mainly manifested in the hardware system, software system, and data level. For the hardware system, its system design, circuit structure, and input and output can effectively evaluate the completeness of hardware system applications in traditional networks. The software system is applied to the hardware system, and the evaluation of the system's anti-tampering, user application, and system vulnerability detection is of great significance to the integrity of the software system. The application of software and hardware systems will correspondingly generate a large amount of data. To ensure that the integrity of the data is not damaged, the evaluation of risk indicators such as data tamper resistance, security protocols, transmission processes, and data storage structures is very important.

(2) Availability: The availability of information services and the availability of system operation are important manifestations of the security and availability of traditional network information. Information services have four important indicators: random accessibility, multi-fistedness, authorization effectiveness, and business flow control. The ratio of system normal time to system full load time effectively reflects the full-time efficiency of system operation in the Energy Internet, and the evaluation of system equilibrium and system connectivity effectively reflects the difference in system operation and the network nodes in the system Interactive ability.
3) Controllability: The controllability of traditional network information security is mainly manifested in the controllability of information content and the controllability of the information dissemination process. The information content also includes information health management and control, information release authority management, and information supervision efficiency in traditional networks, and the three of them will effectively control the information content. Besides, the breadth and effectiveness of information dissemination as well as the power of management and control to a large extent reflect the security risk management and control methods in the entire cycle of information from generation to dissemination to reception in traditional networks.

4) Reliability: The reliability of traditional network information security is reflected by the survivability of network nodes and the survivability of the network environment. Aiming at the survivability of network nodes, the effectiveness of nodes and lines can be used to comprehensively evaluate traditional Energy Internet nodes. As for the survivability of the network environment, the network topology plays a vital role. In addition, the internal environmental factors of the network and the external environmental level will greatly affect the survivability of the network environment.

5) Confidentiality: In the process of continuous construction of information network security architecture, it is particularly important to keep the information confidential. In the process of information interaction, it is easy to cause information management errors and lead to the leakage of information and data. Therefore, it is particularly important to store data, transmit data, and control the file system. Index elements such as storage media, human factors, data theft methods, and identity authentication all pose certain threats to the confidentiality of data storage and transmission. In addition, indicators such as virus software and level protection can effectively evaluate the confidentiality of the file system. Compared with the single authorization mode of general network users, user authorization based on information security will take more consideration of user privacy and changes in the network environment in the authorization mode to realize the confidentiality of information in traditional networks.

4. Conclusion
Energy Internet is the network architecture that integrates a high degree of automation and digitalization [7]. Based on the consideration of energy and information flow security risk factors, this paper traces on and improves the construction principles and methods of the conventional indicator system, and proposes the evaluation index system for the security risks of energy and information flow scientifically and effectively analyzing the problems faced in the process of building the Energy Internet, which can largely avoid the security risks that exists in the process of Energy Internet information interaction and the deep coupling of Energy and Information Flow. The invisible hazards and risks are the most direct and basic product of the third industrial revolution [8], the detection and protection of Energy Internet security threats will be further improved, and the construction of security risk indicators will also tend to be perfect.

Acknowledgments
We would like to express our sincere gratitude to everyone who helped in this research work. This project is supported by National key Research and Development Plan Project Funding.(2020 YFE0200600) and National Natural Science Foundation of China.(NO.61872343).

References
[1] Hu H.J., Sun F.N., Wang Y.S. (2017) Research on Energy Internet Information Security Architecture.J. Communication World., 17:31-32.
[2] An N.Y., Xu Z.B., Zhou F. (2016) Application of Trusted Computing Technology in the Information Security of Global Energy Internet.J. Electric Power Information and Communication Technology., 014: 84-88.
[3] Xu L.Y. (2020) Research on key technologies of network security risk assessment.J. Wireless Internet Technology., 017: 25-26.
[4] Yang J.C., Luo J.B., Kang L.H., et al.(2017) Comprehensive energy services under the framework of the regional Energy Internet. J. Shanghai Energy Conservation., 003: 137-146.

[5] Dong W., Li Y.G. (2020) Analysis of the impact of smart grid cyber attacks based on complex networks. J. Information Network Security., 001: 52-60.

[6] B. Zhou, Y. Sun, N. K. Mahato, X. Xu, H. Yang and G. Gong. (2020) Optimization Control Strategy of Electricity Information Acquisition System Based on Edge-Cloud Computing Collaboration. In: 2020 5th Asia Conference on Power and Electrical Engineering. Chengdu. pp. 54-59.

[7] Q. Li, Z. Liu, Y. Chen, G. Gong, S. Yang and N. K. Mahato. (2019) Energy Data Security and Multi-Source Coordination Mechanism Based on Blockchain, In: 2019 IEEE Sustainable Power and Energy Conference. Beijing. pp. 1979-1983.

[8] Yu J.X., Shen H.J. (2017) Research on the protection architecture of Energy Internet information security threats. J. Science and Technology Plaza., 07: 99-102.