Risk Assessment of the Global Energy Interconnection System

I. M. Aliev
Chechen State University, Grozny, Russia

Keywords: Information system, risks, energy system, analysis, resources, attacks.

Abstract: As the largest artificial physical system to be built in the near future, the Global Energy Interconnection (GEI) is characterized by a close relationship between energy and information systems. Information system risks will have a major impact on the security of power systems. In this article, with a number of identified risk factors for information systems, a risk assessment model for related physical-information systems is proposed. A risk assessment method is presented.

1 INTRODUCTION

Research started in the 1970s in risk assessment and information systems management aims to control the increasing complexity of system operation and reduce system uncertainty. Meanwhile, the development of the information system itself introduces new risks. Risk assessment methods were originally applied in software projects in the field of information technology, and later were extended to other areas. Recent research covers many theories, methods and phenomena in various layers of information technology. But most of them are empirical and qualitative, and difficult to adapt to the growing uncertainty and ambiguity that information systems face. Based on rationality and ignoring the influence of irrational behavior, risk assessment and management of information systems can be roughly divided into three stages. First, identify the various risk factors of the system and take appropriate risk control measures. Secondly, modeling the risk management process in the form of identifying, analyzing, assessing, eliminating and verifying risks. Third, establishing a relationship between system process properties and levels of uncertainty to obtain a general risk profile to develop more specific response solutions. To solve the problem of sustainable energy development, a global energy connection is proposed. GEI is a highly integrated grid-based energy system compatible with many forms of energy to achieve optimal distribution and global sustainability. The information system plays an important role in the implementation of the GEI, and risk assessment and management are key issues that need to be addressed.

In this article, we make the following contributions. Based on physical system and information system risk measurement, we present a quantitative GEI information system risk model and evaluation method. We then suggest human attacks, communication quality problems, and natural disasters as risk factors for information systems (Egorova, 2013). We performed simulations based on various information systems to validate our analysis and illustrate the effectiveness of the proposed method.

2 MATERIALS AND METHODS

Risk in this article refers to the likelihood of accidents and their severity. The purpose of risk assessment is to enable system operators to systematically predict possible failures and take appropriate safety measures. The use of risk assessment can quantify the likelihood and severity of an accident. As a result, it can more fully reflect the impact of the failure on the entire power system. In physical systems, different devices operating under different conditions have different failure probabilities and can affect the power system in different ways. The differences between them are difficult to characterize using traditional analysis, which can only qualitatively reflect the consequences of accidents. Risk measurement based on uncertainty analysis can compensate for this shortcoming (Ralph, 2011). The main advantage of risk measurement over traditional methods of

Aliev, I.
Risk Assessment of the Global Energy Interconnection System.
DOI: 10.5220/0011556800003524
In *Proceedings of the 1st International Conference on Methods, Models, Technologies for Sustainable Development (MMTGE 2022) - Agroclimatic Projects and Carbon Neutrality*, pages 169-171
ISBN: 978-989-758-608-8

analysis is the quantification of risk factors. Taking into account both the probability and the severity of accidents, the risk measure can accumulate the risks of all components, which constitutes the overall risk signal of the electrical system. At the same time, the risk signal is time sensitive and can accumulate over a period of time to provide system operators with information for decision making. From a risk management perspective, qualitative and quantitative analysis methods are used to systematically analyze the vulnerabilities of information systems and the risk factors they face. Then propose adjusted risk management to minimize negative impacts and economic losses. The measurement of information system risk should contain 4 main factors, including information assets.

System, vulnerability of information resources, threats to information resources and implemented security measures (Egorova, 2015). The vulnerability level represents the severity of the vulnerability of an asset, and the threat level is represented by the object threatened by the threat, the subject of the threat, the frequency of the threat, etc. Based on the risk management model, the measurement of the risk of an information system can quantify the risk signal through the analysis of potential accidents. With the development of information and communication technologies and automatic control technologies, the traditional power system has turned into a complex interactive large system consisting of three parts: a global physical system, a modern information and communication system, and a developed monitoring system. However, the introduction and widespread use of advanced information technologies can also adversely affect the reliability and safety of the electrical system. In this large system, the failure of one component of the information system can affect the entire power system. Therefore, it is important to monitor the information system in real time and ensure fast and accurate delivery of information about the power system to the system operator. In a highly coupled physical information system, risks in both the physical system and the information system can lead to disasters (Porfiriev, 2010).

The risk factors of information systems can be divided into three aspects, namely: human attacks, communication quality problems and natural disasters. The risks of the GEI information system have increased significantly due to the interconnection of physical systems and information systems. Attacks against GEI information systems can not only damage information systems, but also cause failures of physical systems beyond the physical boundaries of the information systems. In addition to human attacks, communication quality issues and natural disasters also cause problems for the GEI. In order to realize the properties of high efficiency, self-healing, high reliability and security in the smart grid, the amount of information that needs to be transmitted and processed will be much larger than the current one. Due to the high connectivity of physical-information systems, information security is becoming increasingly important, and human attacks can be dangerous. Information intruders can attack one or more communication nodes in an information network, which can lead to a failure to download and transfer information. Human attacks most often target important nodes (Nikoláeva, 2018). Attackers try to inflict as much damage as possible with minimal cost.

3 RESULTS AND DISCUSSION

By evaluating the risk of an information system, it is possible to refine the security status of an information system. Information systems risk assessment is the basis for the optimal distribution of information systems protection tools. Based on the results of the risk assessment, information system security policies and security problem solving strategies can be proposed to control the operation of the information system. At present, the main power lines of China's regional power systems are made of optical fiber. When sudden natural disasters occur, such as hurricanes, floods, earthquakes, or landslides, the communication network may be destroyed, resulting in reduced or even paralyzed communication network capacity. The probability that a natural disaster will damage all communications in the area of the event can be obtained from historical data statistics (Porfiriev, 2010). Power system risk assessment has been focused since the 1980s, but most research is focused on the primary system. Currently, the primary systemic risk assessment of the power system is being systematically studied. There are relatively advanced methods of analysis and evaluation, and they have been applied to the operation of electrical networks. But from the point of view of information systems, studies on the overall risk assessment of the system are still lacking. And there is still little research on the role of information system risk in the primary power supply system.

In accordance with various risk factors, a model of the probability of failure of an information system node is created. From the point of view of the human attack factor, information intruders, as a rule, attack the most important communication nodes. From the

point of view of the problem factor of communication quality, the state of the communication device installed at each node plays an important role in the security of the information system. From the point of view of the factor of natural disasters, natural disasters can lead to the simultaneous failure of several nodes in the region. By evaluating the risk of an information system, it is possible to refine the security status of the information system. IT system risk assessment is the basis for the optimal deployment of IT system security resources. Based on the results of the risk assessment, information system security strategies and security problem solving strategies can be proposed to control the operation of the information system (Taylor, 2012; Avgerou, 2004).

4 CONCLUSIONS

A quantitative risk model for the GEI information system is proposed that evaluates three risk factors: human attacks, communication quality problems and natural disasters. The negative impacts of accidents on power systems are analyzed with the identification of key nodes of the information system. Most of the current work is focused on risk assessment of the power system and information system, respectively. Several studies are devoted to the effects of the connection of a physical-information system. The main contributions of this article are the proposed quantitative risk model and estimation method. The simulation results of a typical test power system and two communication networks confirm the effectiveness of the proposed evaluation model and evaluation method.

REFERENCES

Egorova, M. S., 2013. Russian strategy for the development of ecological construction. *Megapolis management: Scientific-theoretical and analytical journal*, 6(36).

Ralph, F., 2011. *The Green Revolution.* Economic growth without damage to the environment: Alpina Non-fiction Publishing House.

Egorova, M. S., Tsubrovich, Ya. A., 2015. Analysis of the demand for "green" technologies in Russia. *Economic Sciences.*

Porfiriev, B., 2010. *Climate change: risks or development factors Russia in global politics.* http://www.globalaffairs.ru/number/Atmosfera-i-ekonomika-14886.

Nikoláeva, L.B., 2018. *Latin American economy in the face of climate changes. New priorities.*

Taylor, H., Artman, E., Woelfer, J. P., 2012. *Journal of Information Technology*. 27. pp. 17-34.

Avgerou, A., Ciborra, C., Land, F., 2004. *Oxford University Press*. pp. 17-37.