Information system risk assessment for global energy interconnection

Information system risk assessment for global energy interconnection

Xiaodong Chu[1, 3], Weihao Wang[1], Maosen Tang[1], Haoyi Huang[1] and Lei Zhang[2]

[1] School of Electrical Engineering, Shandong University, Jinan, China;
[2] Electric Power Research Institute of State Grid Shandong Electric Power Company, Jinan, China.

[3] E-mail: chuxd@sdu.edu.cn

Abstract. As the largest manmade physical system to be built in the near future, the global energy interconnection (GEI) features close coupling between power systems and information systems. Risks of information systems will have great impacts on the security of the power systems. With a series of risk factors of information systems defined, a risk assessment model for coupled physical-information systems is proposed in this paper. A risk evaluation method is presented. Simulations results of a typical power system and information networks demonstrate the effectiveness of the proposed assessment model and evaluation method.

1. Introduction

The research started in 1970s [1] on information system risk assessment and management is aimed to control increasing system operational complexity and reduce system uncertainty [2]. At the meantime, the development of information system itself introduces new risks [3]. Risk evaluation methods are first used in the software projects in information technology [4] and then extend to other fields [5]. Recent research covers a variety of theories, methods and phenomena in different layers of information technology. But most of them are empirical and qualitative [6], which is difficult to adapt to the increasing uncertainty and ambiguity faced by information systems.

Based on the rational character and ignore the influence of irrational behaviors, information system risk assessment and management are roughly divided into three steps. Firstly identifying the various risk factors of the system and taking appropriate actions to control the risk [7]. Secondly modeling the process of risk management as risk identification, analysis, evaluation, disposal and review [6]. Thirdly establishing the relationship between system process characteristics and uncertainty levels to provide an overall risk profile to develop more specific response decisions [8].

To solve the sustainable development problem of energy, global energy interconnection is proposed. GEI is a highly integrated energy network which takes electric grid as core, and it is compatible with multiple forms of energy to achieve optimal allocation and sustainable development worldwide [9]. Information system plays an important role in realizing the GEI and risk assessment and management are key problems to be solved.

In this paper we make the following contributions. Based on the physical system and information system risk measurement, we present the GEI information system risk quantitative model and evaluation method. Then we propose human attacks, communication quality problems and natural disasters as risk factors of information systems. We conduct simulations based on different information systems to validate our analysis and illustrate the performance of proposed method.

The rest of the paper is as follow: in section 2 modeled the risk measurement in both physical system and information system of GEI, and then in section 3 formulated the risk measurement assessment of GEI. In section 4 simulation results are given and the paper is concluded in section 5.

2. Risk measurement in both physical system and information system

The risk in this paper refers to the probability of causing accidents and the severity of the accidents. The aim of risk assessment is to enable system operators to foresee the possible accidents in a systematic manner and take appropriate safety measures. The use of risk assessment can quantitatively reflect the probability and severity of the accident. Thus it can more comprehensively reflect the impact of the accident on the entire power system.

The information system risk signal which indicates the impact on power system after failure of communication can be stated as

$$R = P_{Event} \bullet S_{Event} \tag{1}$$

where R is the information system risk measurement, P_{Event} is the probability of accident and S_{Event} is the severity of accident.

2.1. Physical system risk measurement

In physical systems, different devices operating in different conditions have different possibilities for accidents and may cause different impacts on power system. The differences between them are difficult to characterize through traditional analysis which only can qualitatively reflect the impacts of accidents. The risk measurement based on uncertainty analysis can make up for this deficiency. Compared to the traditional analysis methods, the main advantage of the risk measurement is its quantitative expression of risk factors. Considering both probability and severity of the accidents, risk measurement can accumulate the risks of all components which composes the whole risk signal of the power system. At the same time, risk signal is time-sensitive and can be accumulated over a certain period of time to provide decision information for system operators.

The definition of the risk signal of power system is the product of probability and severity of the accident that can be stated as

$$R\left(Y_t \middle| E, L\right) = \sum_i P\left(E_i\right) \times P\left(Y_t \middle| E_i, L\right) \times S\left(Y_t\right) \tag{2}$$

where Y_t is specific operational status, E_i is the uncertain accident happens at time t, L is load status of power system, $P(E_i)$ is the probability of E_i occurrence, $P\left(Y_t \middle| E_i, L\right)$ is the status probability distribution of power system after E_i occurrence, $S(Y_t)$ describes severity of accident at status Y_t, $R\left(Y_t \middle| E, L\right)$ is the risk signal.

2.2. Information system risk measurement

From a risk management perspective, qualitative and quantitative analytical methods are used to systematically analyse the vulnerability of the information system and the risk factors which they face. Then propose rectified measures against risks to minimize negative impacts and economic losses.

Information system risk measurement should contain 4 basic factors including information assets of the system, vulnerability of the information assets, threats to the information assets and deployed security measures. The level of the vulnerability represents the severity of the asset vulnerability and the level of the threat is represented by the threatened object, the threat subject, the frequency of the threat, and so on. Based on risk management model, information system risk measurement can describe the risk signal quantitatively through analyzing potential accidents.

The severity S of accident can be stated as

$$S = f\left(A, T, F, V\right) \tag{3}$$

where A is the system asset, T is the threat to system, F is the rectification measures and V is the vulnerabilities of system. It should be noted that the variables of assets, threats, measures, and vulnerabilities are not completely independent.

With the development of information and communication technology and automatic control technology, traditional power system has developed into a complex interactive large system composed of three parts: wide-area physical system, modern information communication system and advanced monitoring system. However the introduction and widely application of advanced information technology also has a potential negative impact on the reliability and security of power system. In this large system, if any components in the information system fails, it may affect the whole power system. Therefore it is significant to monitor the information system in real time and ensure that the information of the power system is delivered to the system operator quickly and accurately. In a highly coupled physical-information system, risks in either the physical system or the information system may cause accidents.

The risk factors of information systems can be divided into three aspects, namely, human attacks, communication quality problems, and natural disasters. The corresponding information system models are established in the following.

3. GEI information system risk quantitative assessment

The risks of the GEI information system have increased significantly due to the coupling of physical systems and information systems. Attacks target at GEI information systems can not only harm information systems, but also cause physical system accidents through the boundaries of physical-information systems. Other than human attacks, communication quality problems and natural disasters also bring trouble to GEI.

3.1. Human attacks

To realize high efficiency, self-healing, high reliability and security properties in smart grid, the amount of information that needs to be transmitted and processed will be much larger than the current. Due to the high coupling of physical-information systems, information security is becoming more and more important and human attacks can be dangerous. Information attackers can attack one or more communication nodes in the information network which may lead to the failure of information uploading and transmitting.

In human attacks, important nodes are more likely to be attacked. Attackers are tend to cause as much damage as possible at minimal cost. The probability of each communication node being attacked by human attackers can be expressed as

$$P_{Event}^{i} = \frac{o_i}{\sum_j o_j} \tag{4}$$

where o_i is the importance of communication node i.

3.2. Communication quality problems

With the development of smart grid, communication technology has evolved from PDH (Plesiochronous Digital Hierarchy) to the current SDH (Synchronous Digital Hierarchy). At present, most of power system information in China are communicating in the form of a transmission mode combining SDH optical fibre communication with other communication devices. With the upgrading of the smart grid, the number of communication nodes is increasing. At the same time, the probability of communication equipment failure increases.

The probability of damage to the communication equipment due to communication quality can be considered to obey the Poisson distribution. Let λ_i be the average rate of accidents of the equipment, and the probability of no accidents is:

$$\overline{P}^{i} = \frac{e^{-\lambda_i}(\lambda_i)^0}{0!} = e^{-\lambda_i} \tag{5}$$

In the accident of power communication system:

$$P_{Event}^{i} = \left(1 - e^{-\lambda_i}\right) e^{-\sum_{j \neq i} \lambda_j} \tag{6}$$

Equation (6) represents that the probability of failure of each device is independent of each other and only one device failed in each accident.

3.3. Natural disasters

At present, regional power grids' main transmission lines are made of optical fiber in China. When sudden natural disasters such as hurricanes, floods, earthquakes, or mudslides occur, communication network may be destroyed, causing the communication network's transmission capacity to decline or even paralyze. The probability of natural disaster which lead to damage to all communication facilities in the area occurrence can be obtained from historical data statistics.

3.4. Information system risk quantitative assessment

Power system risk assessment has been focused since 1980s, but most researches are concentrating on the primary system. Nowadays the primary system risk assessment of power system has been systematic studied. There are relatively perfect analysis and evaluation methods, and they have been applied to power grid operation. But in terms of information systems, research on overall system risk assessment is still lacking. And there is still little research on the role of information system risk in the primary system of electricity.

According to different risk factors, the information system node failure probability model is established. In terms of human attack factor, information attackers tend to attack most important communication nodes. In terms of communication quality problem factor, the status of communication device installed at each node plays an important role in the security of information system. In terms of natural disaster factor, disasters may cause multiple nodes in a region to fail at the same time. Thus it is assumed that the probability of regional damage to the device is $1/n$ (n indicates the number of regions) for modelling convenience. The flow chart (Figure 1) is as follows:

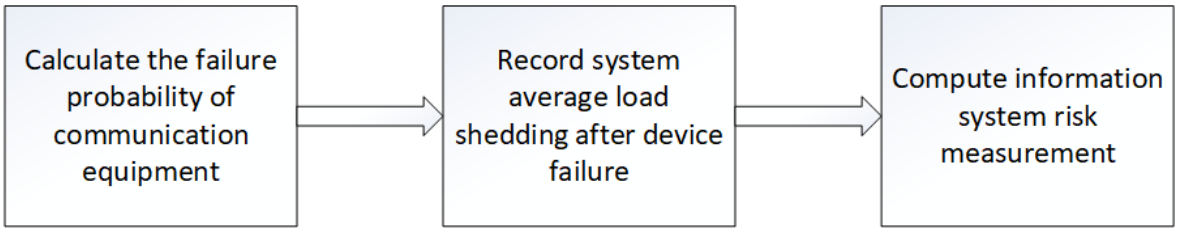

Figure 1. Information system risk assessment flow chart.

Through information system risk assessment, the status of information system security can be clarified. Information system risk assessment is the basis for optimal allocation of information system defence resources. According to the risk assessment results, information system security strategies and security problem solutions can be proposed to guide the operation of the information system.

4. GEI information system risk quantitative assessment

4.1. Natural disasters

Our simulations are based on the New England power system representing the physical side of GEI and two communication networks shown in figure 2 representing the information side of GEI.

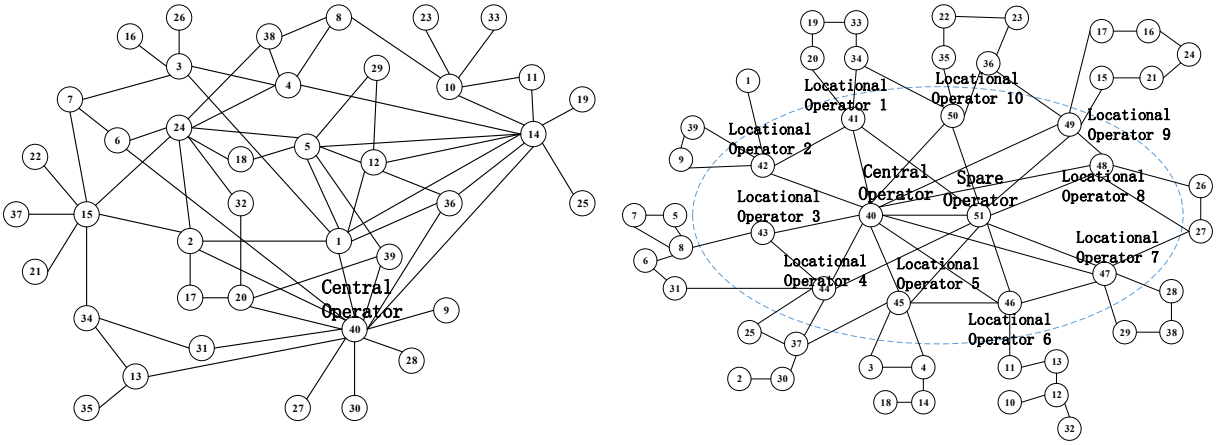

Figure 2. Random communication network and binary communication network.

4.2. Severity of accidents

Figure 3 shows the average load shedding after the failure of each communication node in two communication networks. In the random communication network, the failures of the communication nodes 3, 14, 16, 21 lead to mass load shedding. The original power system is split into two areas but the operator doesn't know it due to the failure of node 3 and 16. Then the subsequent scheduling decision may lead to chain failures. As for the binary communication network, the failures of nodes 15, 16, 21, 49 lead to mass load shedding and the amount of load shedding is obviously larger than in the random communication network. The comparison between two simulation results shows that different communication networks have different impact on the severity of accidents and the binary network is more vulnerable than random network.

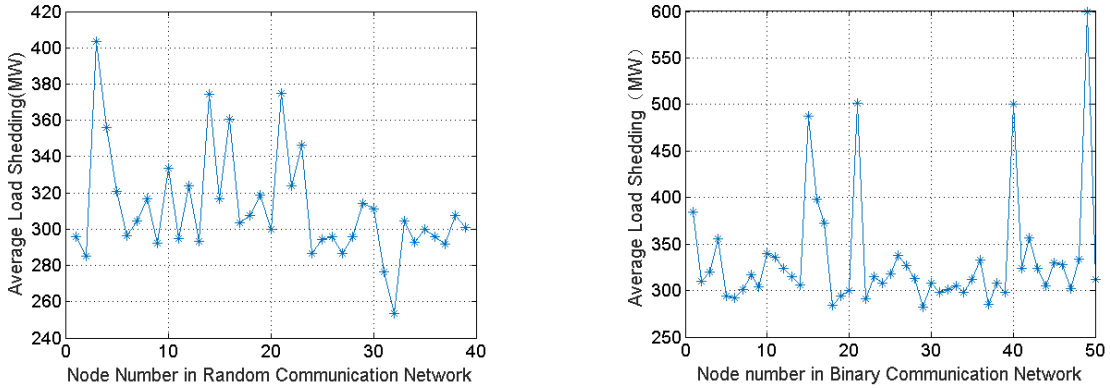

Figure 3. Average load shedding in different communication networks.

4.3. Possibility of accidents

For different risk factors, the calculation formulas for probability are different. Figure 4 shows the possibility of node failure caused by human attacks and communication problems in two communication networks.

In the random network, central nodes such as node 1, 2, 5, 14 and 24 are of great importance, so they are more likely to be attacked by human attackers. The communication nodes working in harsh conditions such as node 17, 25, 26, 29 and 34 are considered to face more communication quality problems. Binary network is somewhat alike to random network. Locational operation nodes which are of great importance are more vulnerable in human attacks. Communication quality problems are

more likely to happen at communication nodes working in harsh conditions. The simulation results show that the important communication nodes need to be more careful about human attacks and communication nodes working in harsh conditions require more maintenance.

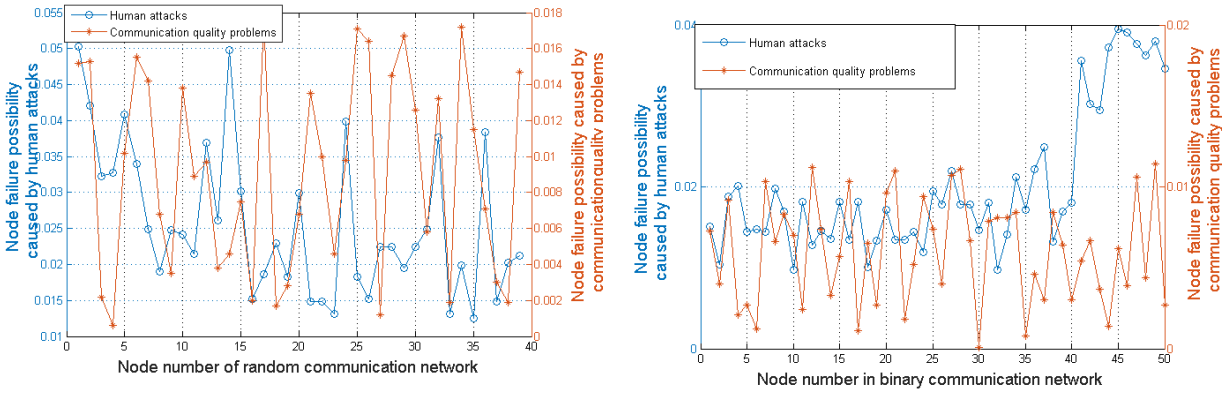

Figure 4. Possibility of node failure in two communication networks.

4.4. Risk measurement

Figure 5 shows the risk measurement after the failure caused by human attacks and communication quality problems in the random communication network and binary communication network.

In random network, the risk of node 14 failure is obviously larger than other nodes' risks under human attacks. In the meanwhile, nodes' risks brought by communication quality problems are randomly distributed. It is similar to the binary network. The locational operation nodes (41-50) are of higher human attack risk than normal nodes and the risks brought by communication quality problems are randomly distributed. This is because that human attackers are tend to attack the most vulnerable node in the information network while communication quality problems are caused by harsh conditions and lack of maintenance.

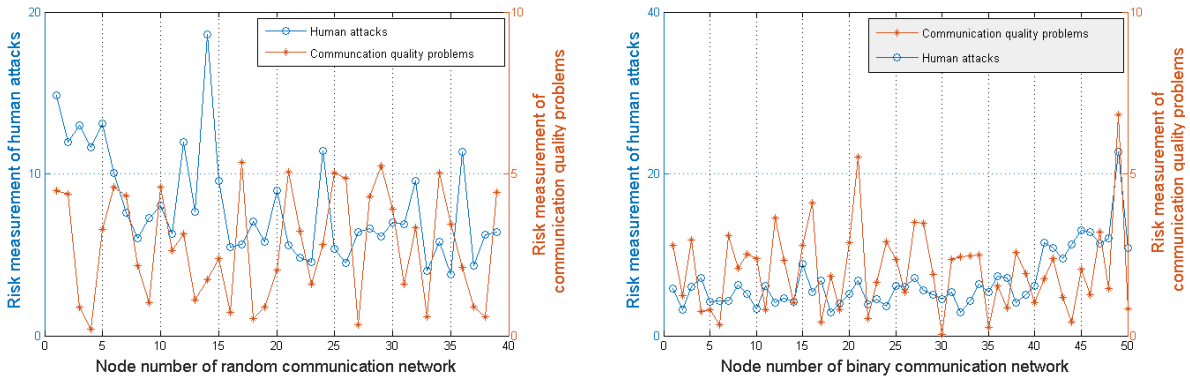

Figure 5. Risk measurement in two communication networks.

Risk measurements after natural disasters in two networks are shown in figure 6. Due to the variety of natural disasters and the different frequency of occurrence of various natural disasters, the possibility of natural disasters occurrence is assumed to be 1/10 (communication system is divided into 10 regions). Figure 6 shows the risk measurement of natural disasters in the random communication network and binary communication network.

The risk measurements of region 4 and 5 in binary communication network are greater than the risk measurements in random network. The reason is that central operator node communicates with normal

nodes through locational operation nodes in binary network. The communication links in binary network are less than in random network, so it is more vulnerable in natural disasters.

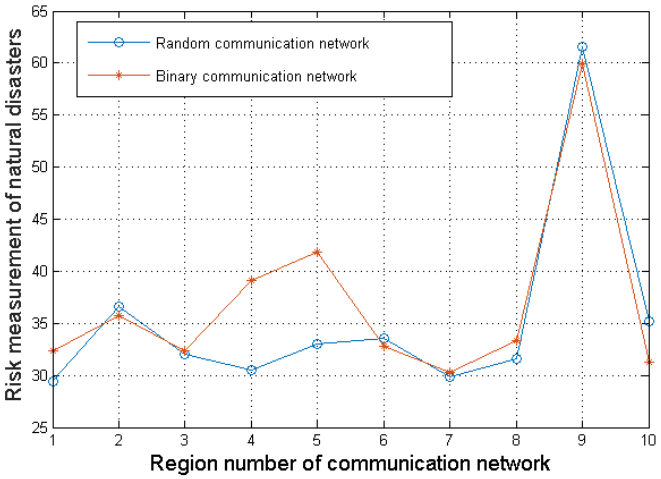

Figure 6. Natural disasters risk measurement in two communication networks.

The above simulation results illustrate risks caused by different factors of information networks. We calculate the amount of average load shedding to represent the severity of accidents. Combined with the probability of risk factors, the risks of different factors can be evaluated quantitatively, which provides an overall risk profile to develop more specific responsive operational decisions.

5. Conclusions

The quantitative risk model for the GEI information system is proposed evaluating three risk factors, i.e., human attacks, communication quality problems and natural disasters. The negative impacts of accidents on the power systems are analysed with the key nodes in the information system identified. Most current works concentrate on power system and information system risk assessment respectively. Few studies are on the coupling effects of physical-information system. The main contributions of this paper are the proposed risk quantitative model and evaluation method. Simulation results of a typical test power system and two communication networks verify the effectiveness of the proposed assessment model and evaluation method.

Acknowledgment

This work was financially supported by Science and Technology Project of State Grid Corporation of China (SGSDDK00KJJS1600061).

References

[1] Boehm B 1973 *Datamation* **19** 49-57
[2] Hanseth O and Claudio C 2007 *Edward Elgar Publishing* 1-6
[3] Keil M, Tiwana A and Bush A 2002 *Information Systems Journal* **12** 103-119
[4] Alter S and Ginzberg M 1978 *Sloan Management Review* (*pre-1986*) **20** p 23
[5] Öbrand L 2015 *Umeå Universitet* 8-23
[6] Bannerman P L 2008 *Journal of Systems and Software* **81** 2118-33
[7] Tesch D, Kloppenborg T J and Frolick M N 2007 *Journal of computer information systems* **47** 61-69
[8] Taylor H, Artman E and Woelfer J P 2012 *Journal of Information Technology* **27** 17-34
[9] Avgerou A, Ciborra C and Land F 2004 *Oxford University Press* 17-37