A Practical Solution to the Information Security Risk Evaluation Problems in Power Systems

Yun Ye, Wei-min Lin, Song Deng and Tao Zhang
China Electric Power Research Institute, Nanjing Branch, Nanjing 211106, PRC China
{yeyun, linweimin, dengsong and zhangtao}@epri.sgcc.com.cn

Abstract - With the rapidly development of computer and network technology, information technology has been widely used in many energy systems, such as power system. Power system is a very important sector and energy industry in China, but it presents more and more weakness in its information systems along with the increasing dependence on information and network system. Information security has threatened the security and steady operation of the power system which means that the grid information security will face great threats and challenges. Therefore, information security risk assessment is vital important for state grid whose electric power information level is very deep. Risk assessment of power system provides the data of current risks and points out the future risks and potential impact of these risks in power system. Therefore, the risk assessment supports very important analysis methods and assessment tools for power system. In currently, grid system is lack of effective information security assessment. In this paper, we carried out an improved theoretical model using analytic hierarchy process (AHP) method based on the current state in power system. Finally, we simplified the situation and evaluate the terminals' risk in details using the data in power system through another simplified model. We can conclude that both of the models are effective in evaluate the assessment risk in power systems.

Index Terms - information security risk assessment, power system, Analytic Hierarchy Process

1. Introduction

Power system plays an important role in energy industry in China and it is also an important component of national infrastructure and core sector of information. Information construction of the power system began in the 1960s, which has been 50 years of history. Over the past 20 years, information technology has developed rapidly and improved continuously, which has driven a wide range of applications of information and network technology in the power system. Thus, information systems have been deep into the field of power systems, which manifested that information systems are becoming the infrastructure for better production, operation and management in all levels of power companies. However, power system increasingly exposed the vulnerability of information systems with the deepening dependence on information systems, making information security of the power system face great threats and challenges. Therefore, the information security and reliable of the power system have become important parts of the construction in power enterprises and effective implementation of information security risk assessment has a vital significance in power system.

Information security risk is the security incidents caused by the man-made or natural threat using system vulnerability and the impact on the organization based on the importance of the damaged information assets [1, 2]. The key elements of risk are asset, threat and vulnerability: asset is anything of value to the organization, including information assets, systems assets, software assets, hardware assets and personnel assets; threat is defined that the potential causes of harmful events which could be bad to the organization or system (threat, system problems or other problems caused by network-based access or physical-based access); vulnerability means that the weaknesses of the asset which could be used by a threat and the technical vulnerabilities include organizational vulnerabilities, design vulnerabilities, and configuration weaknesses) [3]; risk refers to the potential or potential impact of harmful effect caused by threat using of asset vulnerabilities. In addition, the information security risk assessment evaluates the confidentiality, integrity and availability of information system, which also denotes that the determination of quantitative or qualitative value of risk related to resource missing and a recognized threat in computer system and network [4, 5]. Therefore, effective risk assessment could help people fully understand the current and future risks of power system. By analyzing the assessment security threats and the potential impact of these risks, effective measures could be taken in order to determine the security policy, establish the information systems, and make the security risks in the controlled range. Moreover, risk assessment also provides a solid foundation for power system becoming a safe, reliable, economical, green and smart grid. Therefore, the risk assessment is an integral part of analysis methods and assessment tools of power system.

Information security risk assessment is a systematic engineering with scientific theoretical foundation, its reasoning and estimation processes need to follow certain scientific theories and evidence. The involved basic principles and theories include law of large numbers, statistical inference principle and the principle of inertia: (a) the dialectical relationship between necessity and contingency in law of large numbers is used to estimate the probability of risk events and losses sizes; (b) based on limited information of sample, statistical inference is used to infer general principles and characteristics of the security situation and achieve sufficient information and data; (c) analysis of past events to predict risks and losses which may occur in the future in accordance with the principle of inertia. Currently, effectiveness of the information security risk assessment has attracted attention

among nations, and a series of theories, techniques, methods, measures and mechanisms have been presented [1, 6, 7]. More internationally recognized standards of information security risk assessment are: ISO/IEC TR 13335-1 security administration guide [8], AS/NZS 4360 risk management standard [9], BS7799 information security management systems [10]. In addition, risk assessment model is the basis for information security risk assessment. After decades of research and development, there have been many mature security model in information security domain, such as P2DR model, APPDRR model, IS015408 model and Ann company risk assessment model.

In China, the information security risk assessment is still in the development stage, so there are some problems, for example, assessment criteria are not standardized and assessment methods are poor maneuverability. To address the problem of risk evaluation in theory in power system, we propose an improved theoretical model. In this paper we analyze the asset risk in power systems, and then present a risk evaluate model. Based on the theoretical model, we simplified the situation to utilize the data in power system to evaluate the risk. We can see that the model is effective in risk evaluation process in power system through the results.

2. Related works

A. Analytic Hierarchy Process(AHP)

The analytic hierarchy process (AHP) is an effective decision analysis combing qualitative analysis with quantitative analysis and a structured technique based on mathematics and psychology. AHP was proposed by Thomas L. Saaty in the 1970s [11] and it has been extensively studied and used around the world in a wide variety of complex decision problems with multi-objective, multi-factor multi-level and multiple standards characteristics, especially in strategic decision-making problems. AHP could provide modeling and digitizing thinking process, which help decision-makers decompose the complex problems into several hierarchies and several factors to compare those elements with each other for evaluating alternative solutions. Each of the hierarchies can be analyzed independently and each of the elements can relate to any aspect of the decision problem. Furthermore, AHP have many advantages including that (a) users could get more correct data without plenty of related data and calculation; (b) establishing a hierarchy structure is a foundation of AHP, and all of the following steps are based on the hierarchy structure; (c) AHP overcome the problem that some indicators are difficult to accurate, which are convenient for taking appropriate measures. Therefore, AHP rather than put forward a correct decision, it helps decision-makers find the best decision which is appropriate for their goal and their understanding of the problem.

B. ISO 17799 Information security management implementation standard

In 2000, the first edition of the standard ISO 17799 is published based on the BS 7799 standard. It consists two parts, the one is about the guide to information security management system, the other is about the normal of information security management. Till 2005, the standard has become the international standard in information security systems.

In ISO 17799:2005, there are 11 areas as follows:

1. Security Policy: to provide the guidance and support for the information security management.
2. Organizing Information Security: to manage the information security in the corporation.
3. Asset Management: to apply the appropriate protection measures to manage the corporation information assert.
4. Human Resources Security: to decrease risk of the man faults, stolen, deceive or abuse of the information facilities.
5. Physical and Environmental Security: to avoid the unauthorized accession, damage or disturbance to the business locale or information.
6. Communications and Operations Management: to ensure the information management devices securely running.
7. Access Control: to manage the accession to the information.
8. Information Systems Acquisition, development and maintenance: to ensure the information system secure.
9. Information Security Incident Management: to manage the secure affaires and emergency measures.
10. Business Continuity Management: to avoid the termination of business affairs and protect the key business process from heavy disasters.
11. Compliance: to avoid any violations of laws, contracts or other security requirements.

Throw the ISO 17799, we can classify the risks of the information system in details. It contains devices' security, information security, system security and security management. In the eye of technology, the system security contains OS security, apps, firewalls, modification of the internet, information audition, information encryption, disaster recovery and secure scanning. By some targeted models, we can analyze the risks of the information scientifically.

C. Theoretical model of the information assets.

1) P2DR model: in the control and guidance of the entire secure strategy, by using the protection tools such as the firewalls and encryptions, and the detection tools such as the vulnerability evaluation and intrusion detection, we can acknowledge and assess the status of the system security. And then we can adjust the status of the security of system. It includes four parts: Policy, Protection, Detection and Response. This structure makes sure of the information system's security.

2) Three or four level risk evaluation model: according to the ISO 17799, we can divide the factors of the risks into 11 parts, 3 levels. There are some relationships between each part, and we can set some parameters to reflect the relationship. Also, this model demonstrates the relationship between each level, and we will get the evaluation results for every part, then deduce to the other levels.

3. An Improved Theoretical Model for the Risks Evaluation Process in Power Systems

A. The process of the terminals' risk evaluation in power systems

The traditional process of the risk evaluation contains six parts: assets' evaluation, vulnerabilities and risk analysis, evaluation measures development, decision making, communication and modification. However, in the Power Systems, we focus the risk mostly on the evaluation itself, such as vulnerability evaluation. So, we simplify the process to three parts as follows:

1) Assets evaluation:

Assets are the key parts in the whole evaluation process. It can be in the various forms in the real world, such as the hardware, software, files, coding, servers and even the power system company image. There are three characteristics for assets, confidentiality, integrity and availability.

2) Threats evaluation:

Threats are the possibilities of the damage to the power systems' assets. The threats maybe come from the direct or indirect attacks such as information leakage and unauthorized accession. Also, they may be come from some accident events. There are two characteristics for threats, likelihood and impact.

3) Vulnerabilities evaluation:

Vulnerability is relative to assets. Vulnerability itself will not do any damage to assets, however, it can cause the damage to assert. Usually, we can classify the vulnerability by its origin and cause.

4) Comprehensive evaluation

Throw the three stages above, we can do assets evaluation work for specific assert. Using appropriate models, we not only can do the theoretical analysis, but also the quantitative analysis.

B. A theoretical model for the Power Systems

Based on the ISO 17799, we can divide the power networks into 11 parts as follows [8, 12]:

T_0 : Security Policy (SP in short);

T_1 : Organizing Information Security (OIS in short);

T_2 : Asset Management (AM in short);

T_3 : Human Resources Security (HRS in short);

T_4 : Physical and Environmental Security (PES in short);

T_5 : Communications and Operations Management (COM in short);

T_6 : Access Control (AC in short);

T_7 : Information Systems Acquisition, Development and Maintenance (ISADM in short);

T_8 : Information Security Incident Management (ISIM in short);

T_9 : Business Continuity Management (BCM in short);

T_{10} : Compliance (C in short);

T_0 *to* T_{10} are the first level of the model, cover the whole areas of the ISO 17799. Also, we can see that the between each other, there are some relationships. For example, the PES and AM, both are assets. The PES can cause some changes to the AM. There are some similar relationships between AC and HRS, ISADM and BCM, SP and OIS and so on. In order to capture the relationships, we employ the matrix M to reflect the quantitative value between each other. For example, $m_{1,4}$ stands for the relationship between OIS and PES.

$$M = \begin{bmatrix} m_{0,0}, m_{0,1}, \cdots, m_{0,10} \\ \vdots \cdots\cdots\cdots\cdots \vdots \\ m_{i,0}, \cdots, m_{i,j}, \cdots m_{0,10} \\ \vdots \cdots\cdots\cdots\cdots \vdots \\ m_{10,0}, m_{10,1}, \cdots, m_{10,10} \end{bmatrix}$$

In each area, there is a set of parts that describe the area in details. Take PES for example. In physical and Environmental Security, there are at least three parts to describe it. Secure areas, devices' security and normal control. We can denote the three parts as follows ($T_{i,j}$):

$T_{4,0}$: Secure areas;

$T_{4,1}$: Devices' security;

$T_{4,2}$: Normal control;

This can be the second level of this model. Similarly, there are some relationships between each other of this level, we denote it as follows:

$$M_i = \begin{bmatrix} m_{0,0}^{(i)}, m_{0,1}^{(i)}, \cdots, m_{0,n}^{(i)} \\ \vdots \cdots\cdots\cdots\cdots \vdots \\ m_{i,0}^{(i)}, \cdots, m_{i,j}^{(i)}, \cdots m_{i,n}^{(i)} \\ \vdots \cdots\cdots\cdots\cdots \vdots \\ m_{n,0}^{(i)}, m_{n,1}^{(i)}, \cdots, m_{n,n}^{(i)} \end{bmatrix}$$

In the detailed parts, there are still some tips to describe the second level. For example, in Devices' security, there are switches, computers and mobiles and so on. So we can describe the level in details, just like this ($T_{i,j,k}$):

$T_{4,1,0}$: Computers;

$T_{4,1,1}$: Switches;

And so on.

The corresponding relation matrix $M_{i,j}$ can be denoted as follows:

$$M_{i,j} = \begin{bmatrix} m_{0,0}^{(i,j)}, m_{0,1}^{(i,j)}, \cdots, m_{0,n}^{(i,j)} \\ \vdots \cdots\cdots\cdots\cdots \vdots \\ m_{i,0}^{(i,j)}, \cdots, m_{i,j}^{(i,j)}, \cdots m_{i,n}^{(i,j)} \\ \vdots \cdots\cdots\cdots\cdots \vdots \\ m_{n,0}^{(i,j)}, m_{n,1}^{(i,j)}, \cdots, m_{n,n}^{(i,j)} \end{bmatrix}$$

In order to avoid the subjective judgment of the importance of each part, we import the weight for every description part of each level. Take the first level for example, we set the weight to each area as follows:

$$W = \{w_0, w_1, \cdots, w_{10}\}, \quad \sum w_i = 1$$

Similarly, we can set the weight to the other levels. We denote it as follows:

The second level: $W_i = \{w_{i,0}, w_{i,1}, \cdots, w_{i,n}\}, \ \sum_j w_{ij} = 1$

The third level: $W_{i,j} = \{w_{i,j,0}, w_{i,j,1}, \cdots, w_{i,j,n}\}, \ \sum_k w_{ijk} = 1$

In order to minus the subjective judgment, we imply the rule below to decide the importance of each part in the power system. The rule consists of seven parts: consistency, availability, adaptability, feasibility, integrity, validity and creditability. Each part we give a mark to evaluate the importance, denoted as 0 or 1. Then sum up the whole marks to get the real score. We grade it into five sets: less than 2 is not acceptable, more than 1 and less than 4 is not safe, more than 3 and less than 6 is acceptable, 6 is safe and 7 is very good. The set can be depicted as follows:

$$V = \{v_0, v_1, \cdots, v_4\}$$

In the eye of statistics, there is a ratio of element in each level that belongs to the element in set V. Therefore, we can get a matrix to depict the relationship as follows:

$$P_{i,j} = \begin{bmatrix} p_{0,0}^{(i,j)}, p_{0,1}^{(i,j)}, \cdots, p_{0,4}^{(i,j)} \\ \vdots \cdots\cdots\cdots\cdots \vdots \\ p_{n,0}^{(i,j)}, p_{n,1}^{(i,j)}, \cdots, p_{n,n}^{(i,j)} \end{bmatrix}$$

The process can be depicted as the picture below:

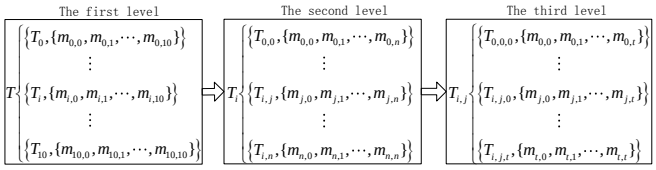

Figure 1 demonstrate of the level structure

The sequence of the computation for the three levels can be depicted as the picture below:

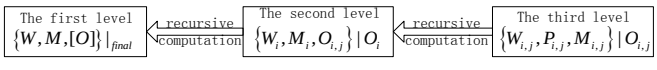

Figure 2 the sequence of the computation

Base on the model above, we can do the judgment as follows:

In the third level, $O_{i,j} = W_{i,j} \bullet P_{i,j} \bullet M_{i,j}$;

In the second level, $O_i = W_i \bullet M_i \bullet [O_{i,j}]$

In the first level, $O = W \bullet M \bullet [O_i]$

After the whole process, we can get the output of the evaluation numerical value. Through comparing the set V, we can evaluate the system whether it's safe or not. Compared with the others' previous methods, we point out that in the third level; there are still some relationships between each other, $T_{4,1,0}$ and $T_{4,1,1}$ for example. The risks of the Switches will directly inflect the Computers and other terminals, and will pass the possibility of risk to the other levels' elements. Thus, we adopt the matrix $M_{i,j}$ to denote the relationships. We do the computation from the last level to the first level, and then the final output will reflect all the relationships in each level, thus minimize the subjective judgment in the whole evaluation process.

4. A Practical Solution for the Terminals' Risks Evaluation in Power Systems

In the previous sector, we presented a theoretical model for the risk evaluation. In this part, we will simplify the situation, that is to say, we only consider the risk of terminals in power systems, just like the figure below:

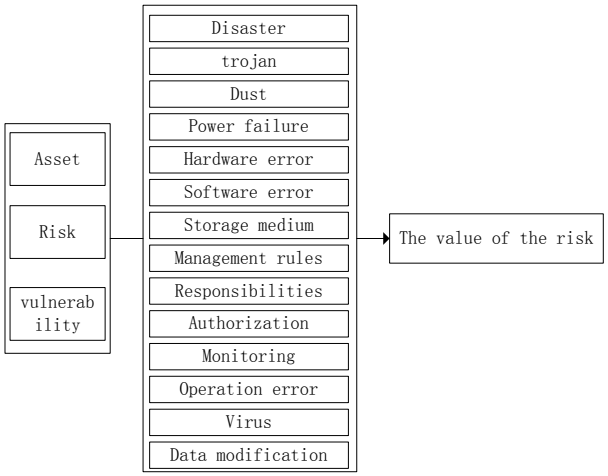

Figure 3 demonstration of the simplified risk evaluation process

A. The risk evaluation concerns in power system

Firstly, we will capture the whole security concerns in power systems. Risk evaluation in power systems should cover four areas: the network in power systems, application systems, business processes and management rules.

The network in power systems including: the network bandwidth in power systems, communication protocols, key devices such as switches and routers, geographical distribution and network management. The asset of the internet including interface to the bank, DMIS, SCADA/EMS hierarchy and horizontal edge and ADSL or VPN et al.

System software including: the OS, database, middle-ware and so on. The application including: WWW, Email, DNS,

FTP, Proxy and so on. The Business system including: SCADA/EMS, electric metering system, load control system, distribution automation, transformer substation automation, atmosphere connection system, electricity marketing system and production management system and so on. Safety facilities including: fire wall, anti-virus system, IDS, PKI and so on. Security management including: safety management organization, safety rules and system maintenance management. Specifically, the secure leader group, password, management rules in machine room, data backups and so on.

B. A pracitcal solution to the risk evaluation problem in power systems.

There are too many concerns of risk evaluation in the power systems, so we eliminate to a simplified model, that is to say the terminals in the system.

In this part, we employ the simplified model in [13, 14] to evaluate the risk in quantitative value. According to the information security inspect job, we get the respective numerical values for each element. Take the secrecy into consideration; we shuffled the values and the devices to hide the privacy. The table of the concerns is as follows:

Table 1: the quantitative value of the asset in power systems

the second level	the third level	the fourth level	the matrix of the evaluation				
the enviromantal risk(0.1)	physical risk(0.4)	natural disater(0.1)	0	0.2	0.2	0.3	0.3
		electromagnetic interference(0.1)	0.1	0.1	0.2	0.2	0.4
		dust(0.3)	0	0	0	0.5	0.5
		franklinism(0.2)	0.1	0.1	0.2	0.2	0.4
		power failure(0.1)	0	0.1	0.1	0.2	0.6
		humidity/temperature(0.2)	0.1	0.1	0.1	0.2	0.5
	technical error(0.6)	hardware error(0.3)	0	0.1	0.1	0.2	0.6
		software error(0.5)	0	0	0.2	0.2	0.6
		storage medium(0.2)	0	0.1	0.1	0.2	0.6
the human factors(0.9)	physical flaws(0.2)	management rules(0.3)	0	0.1	0.1	0.2	0.6
		responsibilities(0.1)	0	0.1	0.1	0.3	0.5
		authorization(0.3)	0	0.1	0.2	0.2	0.5
		modification(0.3)	0	0.1	0.2	0.2	0.5
	human errors(0.6)	operation error(0.7)	0	0.1	0.1	0.1	0.7
		maintenance error(0.3)	0	0.1	0.1	0.2	0.6
	human intention(0.2)	virus(0.1)	0	0.1	0.1	0.2	0.6
		trojan(0.1)	0	0.1	0.1	0.2	0.6
		worms(0.1)	0	0.1	0.1	0.3	0.5
		unauthorization(0.4)	0	0.1	0.1	0.1	0.7
		data modify(0.2)	0	0.1	0.1	0.2	0.6
		steal(0.1)	0	0.1	0.2	0.3	0.4
			very low	low	middle	high	very high

The computation is as follows:

$$M_{11} = (0.1,0.1,0.3,0.2,0.1,0.2)\times\begin{bmatrix}0 & 0.2 & 0.2 & 0.3 & 0.3\\ 0.1 & 0.1 & 0.2 & 0.2 & 0.4\\ 0 & 0 & 0 & 0.5 & 0.5\\ 0.1 & 0.1 & 0.2 & 0.2 & 0.4\\ 0 & 0.1 & 0.1 & 0.2 & 0.6\\ 0.1 & 0.1 & 0.1 & 0.2 & 0.5\end{bmatrix}$$

$$= (0.0500 \quad 0.0800 \quad 0.1100 \quad 0.3000 \quad 0.4600)$$

$$M_{12} = (0.3,0.5,0.2)\times\begin{bmatrix}0 & 0.1 & 0.1 & 0.2 & 0.6\\ 0 & 0 & 0.2 & 0.2 & 0.6\\ 0 & 0.1 & 0.1 & 0.2 & 0.6\end{bmatrix}$$

$$= (0 \quad 0.0500 \quad 0.1500 \quad 0.2000 \quad 0.6000)$$

$$M_{21} = (0.3,0.1,0.3,0.3)\times\begin{bmatrix}0 & 0.1 & 0.1 & 0.2 & 0.6\\ 0 & 0.1 & 0.1 & 0.3 & 0.5\\ 0 & 0.1 & 0.2 & 0.2 & 0.5\\ 0 & 0.1 & 0.2 & 0.2 & 0.5\end{bmatrix}$$

$$= (0 \quad 0.1000 \quad 0.1600 \quad 0.2100 \quad 0.5300)$$

$$M_{22} = (0.7,0.3)\times\begin{bmatrix}0 & 0.1 & 0.1 & 0.1 & 0.7\\ 0 & 0.1 & 0.1 & 0.2 & 0.6\end{bmatrix}$$

$$= (0 \quad 0.1000 \quad 0.1000 \quad 0.1300 \quad 0.6700)$$

$$M_{23} = (0.1,0.1,0.1,0.4,0.2,0.1)\times\begin{bmatrix}0 & 0.1 & 0.1 & 0.2 & 0.6\\ 0 & 0.1 & 0.1 & 0.2 & 0.6\\ 0 & 0.1 & 0.1 & 0.3 & 0.5\\ 0 & 0.1 & 0.1 & 0.1 & 0.7\\ 0 & 0.1 & 0.1 & 0.2 & 0.6\\ 0 & 0.1 & 0.2 & 0.3 & 0.4\end{bmatrix}$$

$$= (0 \quad 0.1000 \quad 0.1100 \quad 0.1800 \quad 0.6100)$$

$$M_1 = (0.4,0.6)\times\begin{bmatrix}0.0500 & 0.0800 & 0.1100 & 0.3000 & 0.4600\\ 0 & 0.0500 & 0.1500 & 0.2000 & 0.6000\end{bmatrix}$$

$$= (0.0200 \quad 0.0620 \quad 0.1340 \quad 0.2400 \quad 0.5440)$$

$$M_2 = (0.2,0.6,0.2)\times\begin{bmatrix}0 & 0.1000 & 0.1600 & 0.2100 & 0.5300\\ 0 & 0.1000 & 0.1000 & 0.1300 & 0.6700\\ 0 & 0.1000 & 0.1100 & 0.1800 & 0.6100\end{bmatrix}$$

$$= (0 \quad 0.1000 \quad 0.1140 \quad 0.1560 \quad 0.6300)$$

$$M = (0.1,0.9)\times\begin{bmatrix}0.0200 & 0.0620 & 0.1340 & 0.2400 & 0.5440\\ 0 & 0.1000 & 0.1140 & 0.1560 & 0.6300\end{bmatrix}$$

$$= (0.0020 \quad 0.0962 \quad 0.1160 \quad 0.1644 \quad 0.6214)$$

M is the evaluation number of the terminals in power systems. We adopt the similar quantitative value, $\{1,2,3,4,5\}$,then we can get the weighted value:

$$(0.0020 \quad 0.0962 \quad 0.1160 \quad 0.1644 \quad 0.6214)*(1,2,3,4,5)' = 4.307$$

We can see that the value is very close to 5, so it represents very dangerous.

5. Conclusions

In this paper, we discussed the main concerns of the risk evaluation in power systems. And then we presented an improved theoretical model for the evaluation problem. In this model, we should consider the relationships between each element. In order to capture the whole evaluation process, we simplified the model. We assume that the relation between each other in every level is irrelevant, that is to say, the relationship matrix $P_{i,j}$ is a unit matrix. Then we adopt another simplified model to compute the evaluation value using the data in power system. The result is obvious correct after comparing to the real data. In the future, we should consider the active risk evaluation model and application in the power

system, since the devices are not always stable in the system. After the devices' add in or remove away, what will be the safety status in real time? It is our future research interest.

Acknowledgment

This work is supported by: (1) the State Grid Corporation project: Key Technologies for Power System Security and Stability Defense Considering the Risk of Communication and Information Systems, (2) the EPRI project: safe protection technologies of the whole of data, information and control for industrial control systems and the technologies of vulnerability discovery model and theories.

References

[1] T.R. Peltier, "Information security risk analysis". 2005: CRC press.

[2] H.F. Tipton and M. Krause, "Information security management handbook". 2003: CRC Press.

[3] K.-J. Farn, S.-K. Lin and A.R.-W. Fung, "A study on information security management system evaluation—assets, threat and vulnerability". Computer Standards & Interfaces, 2004. 26(6): p. 501-513.

[4] D.-g. FENG, Y. ZHANG and Y.-q. ZHANG, "Beijing 100039, China; 2. Institute of Software of Chinese Academy of Sciences, Beijing 100080, China); Survey of information security risk assessment". Journal of China Institute of Communications, 2004. 7.

[5] B. Blakley, E. McDermott and D. Geer. "Information security is information risk management". in Proceedings of the 2001 workshop on New security paradigms. 2001. ACM.

[6] N.I.o. Standards and Technology, "National Institute of Standards and Technology Special Publication". 1988: The Institute.

[7] S.A. Butler. "Security attribute evaluation method: a cost-benefit approach". in Proceedings of the 24th international conference on Software engineering. 2002. ACM.

[8] "ISO/IEC. ISO/IEC TR 13335". http://www.bsi-global.com/en/Shop/Publication.

[9] D. Jones and C. Smith, "The development of a model for testing and evaluation of security equipment within Australian Standard/New Zealand Standard AS/NZS 4360: 2004-Risk Management". 2005.

[10] M. Kenning, "Security management standard—iso 17799/bs 7799". BT Technology Journal, 2001. 19(3): p. 132-136.

[11] T.L. Saaty, "Analytic hierarchy process". Encyclopedia of Biostatistics, 2005.

[12] Zhu yan, yang yongtian, et al. "research on information security evaluation model based on hierarchy structure", Computer Engineering and Applications

[13] Liao hui, Ling jie, "Design and implementation of network terminal security assessment index system.", Vol. 27, No.2, June 2010

[14] Liao hui, Lingjie, "Research on network terminal security assessment index system", 961-964, 2010,31(5)

[15] Li Wenyuan. Risk assessment of power system: model, methods, and applications. New York, USA:John Wiley& Sons, 2005:108-164.