ATLANTIS PRESS
Advances in Computer Science Research, volume 50
4th International Conference on Electrical & Electronics Engineering and Computer Science (ICEEECS 2016)

An Information Security Prevention Model Based on Fuzzy Simulation

Dang Fangfang[a], Yang Ying, Wang Shiwen[b], Mei Lin, Cui Peng, Zhu Lei

Information&Telecommunication Co. of State Grid Henan Electric Power Company, Zhengzhou, 450052, China

[a]email:1365351078@qq.com, [b]email:wangsw8@163.com

Keywords: risk indicator; intelligent acquisition; fuzzy intelligent analysis

Abstract. Due to the appearance of some new characteristics of the electric power industry such as widely interconnection, high intelligent, the open and interactive, energy internet architecture put forward more new requirements of the electric information network security prevention and the information security faced a severe challenge. At present, the method of information security is extensive, management model and prevention system exist some weak links. This paper put forward a new model to guide the overall development of information security work through the quantization of risk indicator and fuzzy intelligent analysis.

Introduction

With the gradually propulsion of information, some information systems such as Office Automation System, Financial Management System, Power Marketing Management System and Production Management System have been widely used in Henan electric power enterprise. Information has played an important role in supporting to establishment of the “three sets of five” system and the operation and management of electric power enterprise. With the development of new techniques such as innovation and breakthrough of “Internet +” model, study on intelligent electric grid and energy internet, gradual promotion of the integration between information and industrialization, the ecological environment of power industry has changed rapidly [1-2]. At present, the information security faces a lot of problems such as extensive management, slack protection system and so on. There were some security vulnerabilities and hidden troubles on electric industrial control equipment, and the application of new techniques and equipment brought risk and challenge to information security, the information security has been facing a serious and complex situation. It has been urgent affairs that innovate information security prevention model, improve the ability of alarming and rapid dealing.

Quantify the Information Security Risk Pointer, Realize Information Security State Intelligent Acquisition

The quantitative evaluation is an important aspect to develop risk assessment. How to utilize the existing information security state pointer to characterize the level of information security comprehensively? How to extract the quantitative evaluation information that can reveal the information security characters and development trend effectively from mass data and conduct a deep processing? How to make information security countermeasures and emergency plans according to the existing information security characters? All above are the key factor to avoid .

Pass by a serious of exploration and practice, this paper innovated the information security risks management model and adopted ISO27001 standard. Brought the concept of information security state pointer into security risk management, qualified the information security state pointer, show them in the information security management system visually and concisely by the method of indicator.

The information security state pointer system as is shown in Figure 1.

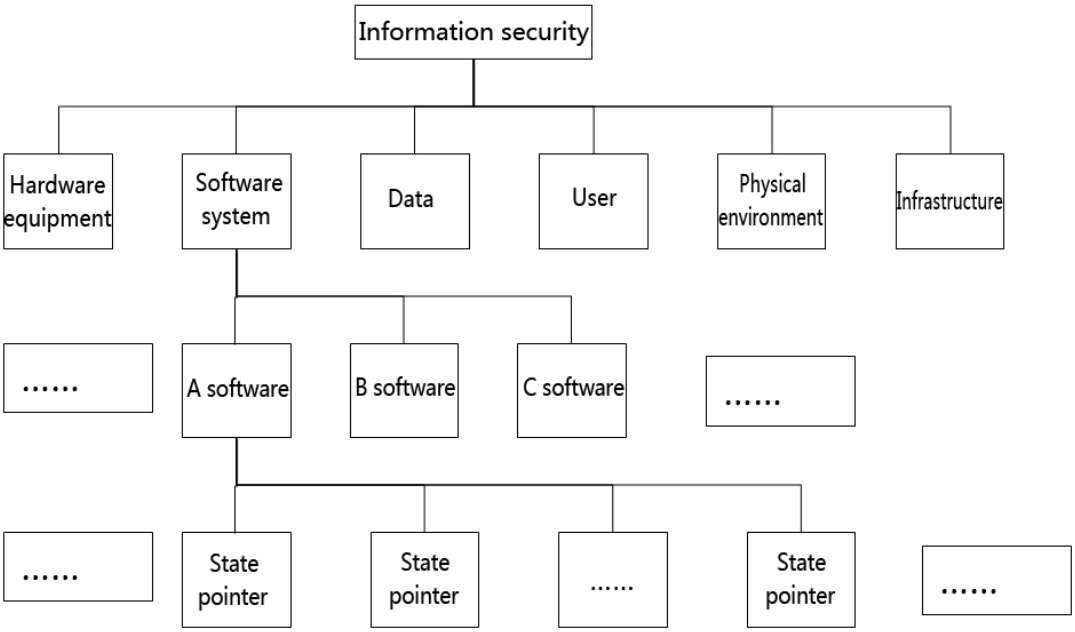

Figure 1. The information security state pointer system

The information security state pointer system is composed of three grade indicators. The second grade risk factors can be divided into 6 aspects(hardware equipment, software system, data, users, physical environment, infrastructure).The third grade risk factors can be divided into 54 aspects. According to these kinds of risk factors, formulate abnormal state pointer standard. Each state pointer can be divided into 4 state grades(A-B-C-D) based on the influence degree of risk factors. Corresponding to qualification value, prepare for the subsequent intelligent analysis and cluster. State pointer conducts intelligent acquisition from “log and event”, “user and asset” and “network traffic” directly.

Fuzzy Intelligent Analysis, Output Visual Information Security Grade, Guide the Development of Information Security Work

On the basis of the above risk pointer qualification information intelligent adopt, the information security fuzzy simulation system conducts three-layer fuzzy intelligent operation. Between these layers, utilize Markov Chain to realize logical link. The first layer operation is intelligent transformation, the second layer is intelligent analysis, the third layer is intelligent cluster[3-4]. Rating all the risk factors, through data extraction, conversion and handling, complete the treatment of massive data and construction of data warehouse, and then, complete risk indicator intelligent (fuzzy simulation) evaluation depend on the integrated basic information [5-6].

After get the risk indicator grade of hardware equipment, software system, data, users, physical environment and infrastructure, conduct the judgment depending on the principles in Table 1.

On this basis, establish risk factor qualification model and each sub-factor calculation method. After qualification calculation, get the risk grade of each production unit. I grade(red highest risk), II grade(orange high risk), III grade(yellow moderate risk), IV grade(blue low risk). Display these grade and guide the concrete security work. As is shown in Table 2.

Conclusion

This paper constructed the electric power enterprise information security classified model, on this basis, developed the information security state pointer assessment standard. At the same time, adopted fuzzy clustering theory, developed a series of algorithms which was used to display the information security classified indicators and provide information security early waning. All above provided the foundation of information risk pre-discovery and promotion of information security prevention ability.

Table 1. Risk grade judge principles

Six risk sub-indicators	Principle
Hardware equipment risk sub-indicator Software system risk sub-indicator Data risk sub-indicator User risk sub-indicator Physical environment risk sub-indicator Infrastructure risk sub-indicator	If there are three or more risk indicators are not only the same but also the highest grade(except I and IV), then the information security risk indicator can be upgrade.
	In other cases, information security risk indicator is determined by the highest grade of all the sub-indicators.

Table 2. Risk grade grid

Risk Grade	Colour
I grade(red highest risk)	
II grade(orange high risk)	
III grade(yellow moderate risk)	
IV grade(blue low risk)	

References

[1]Yin Zhi-qing. The Analysis and Practice of Electric Power Enterprise Network Security Construction[J]. Power Information, 2009.

[2]Hassan A. Yousef; Mohamed Hamdy. Observer-based Adaptive Fuzzy Control for a Class of Nonlinear Time-delay Systems [J].International Journal of Automation and Computing , 2013.

[3]Jie Zhang. A New Fuzzy Simulation for Fuzzy Systems [C] . Proceedings of the Sixth International Conference on Information and Management Sciences , 2007.

[4]Application of Improved Fuzzy Immune PID Controller to Bending Control System [J]. Journal of Iron and Steel Research(International) , 2011.

[5]Haijun Wang. Research on network information security model and system construction [C]. Proceedings of the 2015 3rd International Conference on Information Technology and Career Education(ICITCE 2015) ,2015.

[6] Gengshen Yu; Qian Guo. Risk-based information security audit applied research in the power industry [C]. Proceedings of 2015 Joint International Mechanical, Electronic and Information Technology Conference(JIMET 2015) ,2015.