The Training Base Construction of Network Security of Power Monitoring System

Xinxin Song[1*], Shitao Wang[1], Jixiang Zhao[1], Chunhong Shan[2]

[1] *State Grid of China Technology College, Jinan, Shandong, 250000, China*
[2] *State Grid Dalian Electric Power Supply Company, Dalian, 116000, China*
[*]*Corresponding author's e-mail: 81781559@qq.com*

Abstract.
The training base of network security of power monitoring system covers an area of 592 square meters with 114 training stations. It supports horizontal interconnection and vertical connection with the existing training rooms of the State Grid of China Technology College (SGTC), such as dispatching master station, intelligent substation, power plant, distribution automation system and new energy station. It can build a full scene practical attack and defense drill base, which basically includes five actual power business scenarios: generation, transmission, transformation, distribution and utilization. The trainees can conduct practical exercises in a 1:1 real environment. The training base has become the first comprehensive demonstration project with 1:1 combination of experimental environment and operation environment of power monitoring system in the power industry, filling the gap in the construction of training base in this field.

Keywords: *the training base; network security of power monitoring system; actual power business scenarios; 1:1 real environment*

1 INTRODUCTION

In recent years, network security incidents occur frequently and the situation is extremely severe [1]. Countries all over the world generally attach great importance to the development and security of cyberspace [2]. SGTC built a network security training room in 2015 in order to further deepen the construction of network security talent team of power monitoring system of State Grid Corporation of China (SGCC) [3]. In 2017, SGTC upgraded the software and hardware equipment of the training room to establish a network security expert echelon in power industry [4]. In 2019, SGTC was the first to deploy the network security simulation training platform based on Virtual Technology in China [5]. It can improve the training mechanism of compound talent team and the practical confrontation and security protection skills of network security teams of power enterprises [6]. Over the past five years, SGTC has invested nearly 20 million yuan to create a training support and simulation verification environment with the characteristics of "multi field, full scene and wide integration", so as to provide a solid guarantee for the construction of network security professional team.

2 INFRASTRUCTURE CONSTRUCTION OF TRANING BASE

The training base of network security of power monitoring system covers an area of 592 square meters, as shown in Figure 1. The training room I has 18 training stations, the training room II has 24 training stations, the training room III has 16 training stations, The training room IV has 56 training stations. The training base is equipped with 16 sets of network security operation equipment, those are provided by Nari. Each set includes Longitudinal encryption device, forward physical isolation, reversetype physical isolation, monitoring device I, monitoring device III, switches and workstations, as shown in Figure 2.

© The Author(s) 2023
B. Fox et al. (Eds.): IC-ICAIE 2022, AHCS 9, pp. 1555-1560, 2023.
https://doi.org/10.2991/978-94-6463-040-4_234

Fig.1 The training base of network security of power monitoring system

Fig.2 The network security operation equipments

3 THE NETWORK SECURITY SIMULATION TRAINING PLATFORM

The training base was the first to deploy the network security simulation training platform based on Virtual Technology in China. The training platform is one of the special key work of internet of things in Power System (IOTIPS) for SGCC. And it is also the core content of the self expansion project approved by the Internet Department of SGCC. The training platform realizes the functions of course training, virtual laboratory, examination center and talent evaluation. The function module of the virtual laboratory deeply simulates the vertical encryption device, forward and reverse isolation equipment, monitoring device, switch and router through virtualization technology, and supports the practical exercise of virtual and real combination with the existing equipment in the network security training room.

3.1 *Course training*

The function module of course training has the functions of class management, online class and so on. The training contents include power monitoring penetration technology and power safety protection technology. Lectures are presented in the form of documents, videos, etc. Distance online training and education can be expanded in the future.

Fig.3 Course training

3.2 *Virtual laboratory*

The function module of virtual laboratory provides shooting range and tools. It simulates the power special network security equipment and general equipment through virtualization technology. It supports the interconnection between virtual equipment with real equipment. The students can build dynamic virtual environment arbitrarily in the virtualization scenario including dispatching master station, intelligent substation, power plant, distribution automation system and new energy station.

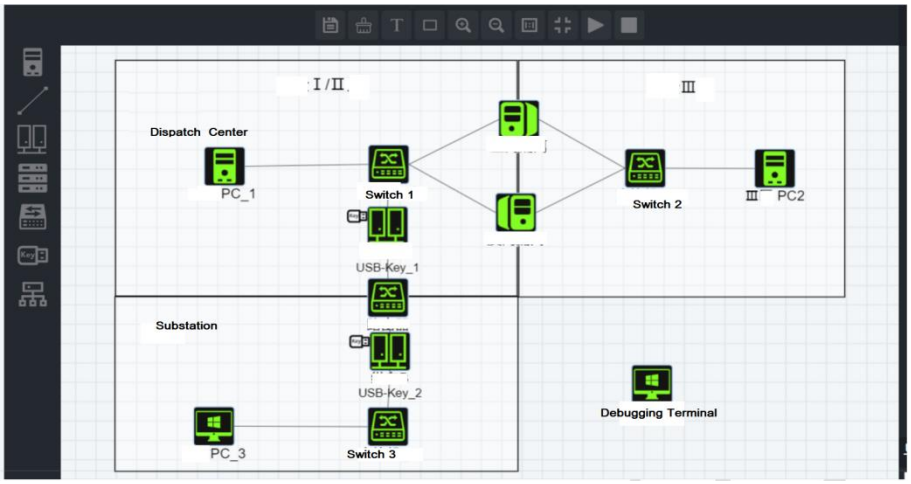

Fig.4 Virtual laboratory

3.3 *Examination center*

The function module of the examination center can realize the exam-question-management. It can randomly select questions and form test papers freely, support the automatic and manual marking functions, and can easily and friendly build test papers in different test sites and carry out diversified examinations.

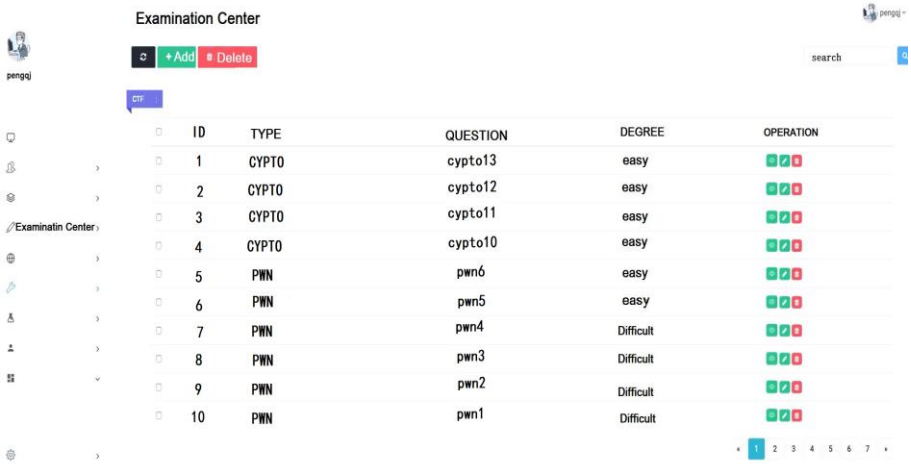

Fig.5 Examination center

3.4 *Talent evaluation*

The function module of the talent evaluation can view the learning progress of the selected course, including the total number of chapters of the course, the number of chapters learned and completed, the number of practical training completed, etc. At the same time, it supports the information overview of individual user examination, including assessment results, ranking, answer analysis, etc. It supports the data analysis of test results, including the total number of examinations, the number of completed examinations, the highest score of the examination, the passing rate of the examination, the list of examination records, etc. Combined with the results of data analysis, we can objectively and scientifically evaluate the breadth and depth of students' current skills, so as to provide a basis for talent selection and post placement in the future.

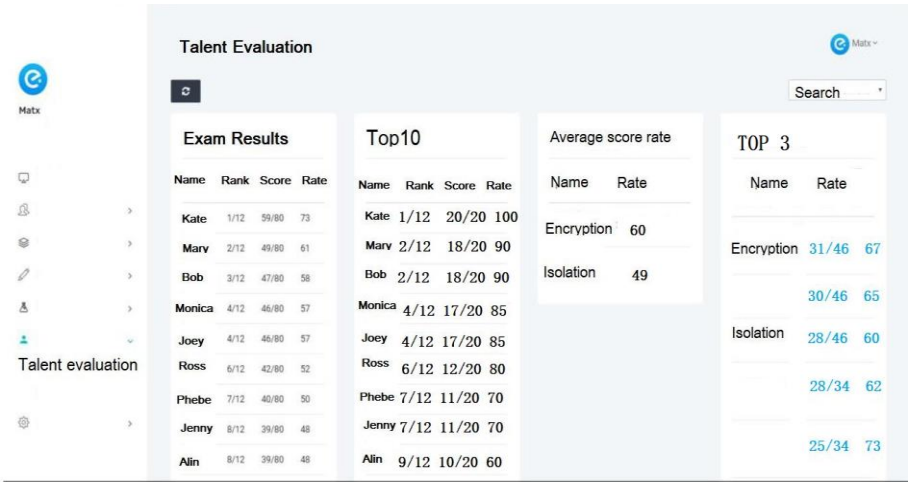

Fig.6 Talent evaluation

4 THE NETWORK SECURITY MANAGEMENT PLATFORM

The network security management platform has advanced and practical functions such as real-time monitoring, early warning and alarm, positioning and traceability, audit analysis, closed-loop control and so on, as shown in Figure 7. It can comprehensively monitor the security behavior of host operating system, database, trusted reinforcement, network equipment, traffic monitoring device, malicious code, general security protection equipment and special power security equipment. It applies technologies such as big data, machine learning, knowledge map, rule engine and automatic arrangement to improve the ability of network security monitoring, early warning and analysis comprehensively. The deployment of the network security management platform is conducive to improving the daily operation and maintenance and security control ability of the power monitoring network system of SGCC.

Fig.7 Network Security Management Platform

5 THE ATTACK AND DEFENSE TRAINING PLATFORM

The training base has the function of red vs blue Laboratory of SGCC. The attack and defense training platform was deployed in the training base, as shown in Figure 8. The platform supports various training methods and competition modes, such as individual drill, red vs blue, AWD competition. It can fully test and improve the safety protection level of power monitoring system of all security teams of SGCC.

Fig.8 Attack and Defense Training Platform

6 TRAINING SYSTEM

The network security training system of power monitoring system is constructed relying on the training base. The training system integrates theoretical basis, skill training, simulation exercise, management assessment and full scene reproduction. The training system designs and develops training programs, course systems, network courseware, test question bank and other training resources for different training objects. Since the training base was put into operation in 2015, it has undertaken 24 training courses for highly skilled talents of State Grid Corporation and 16 centralized training courses for new employees of State Grid Corporation, with a total of 36 training units and more than 6000 trainees, as shown in Figure 9.

Fig.9 Skill Training

7 CONCLUSION

At present, the training base has the ability to undertake industry-level professional competitions. In 2017, the network security skills competition of SGCC was held successfully here. Over 162 contestants from 27 provincial companies participated the competition. The leaders of the company fully affirmed and highly recognized the facility environment and management level of the training base. The training mode of combining learning with practice effectively improves the professional level of participants, provides a solid guarantee for the selection of red vs blue members of SGCC, establishes a echelon of network security experts in the power industry, and improves the practical confrontation and security protection skills of the network security team.

REFERENCES

[1] Ayyarao TSLV, Kiran I R. A Two-Stage Kalman Fiter for Cyber-Attack Detection in Automatic Generation Control System. Journal of Modern Power Systems and Clean Energy[2021-02-02].

[2] Khalaf M, Youssef A, EL-saadany E. (2019) Joint deteciton and mitigation of false data injection attacks in AGC system. IEEE Transaction on Smart Grid,10(5):4985-4995.

[3] Tan R, Nguyen H H, Eddy Y f. (2017) Modeling and mitegating impact of false data injection attacks on automaitic generation control. IEEE Transaction on Smart Grid, 12(7):1609-1624.

[4] Yuan, G.L., Wang, B.Y. (2019) Economic Optimization Scheduling of Virtual Power Plants with Electric Vehicles. Acta Energiae Solaris Sinica., 40:2395-2404.

[5] Zhang, W., Li, H.B., Dong, X.W. (2021) Research on Flexible Auxiliary Service Bidding Strategy of Virtual Power Plant. Electric Power Science and Engineering., 37:48-56.

[6] Xu, F.Y., Xue, A.C., Chang, N.C. (2021) Research Status AND Prospect of Cyber Attack and Defense on Automatic Generation Control in Power System.,45(3):3-14.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.