International Symposium on Communication Engineering & Computer Science (CECS 2018)

Research on Network Attack Defense Architecture Based on New Energy Plant Station

Jinxiong Zhao[1,a], Xiaodi Xie[2], Xun Zhang[1], Lina Gao[1], Fan Yang[1], Zhiru Li[1], Shulin Li[1], Yong Zhi[1], Bo Zhao[3], Wenjing Li[1]

[1] Electric Power Research Institute, State Grid Gansu Electric Power Company, Lanzhou 730070, China;

[2] Renewable Energy Research Center, China Electric Power Research Institute (CEPRI), Beijing 100192, China;

[3] State Grid Gansu Electric Power Company, Lanzhou 730070, China.

[a]18352449382@163.com

Abstract. An energy revolution with new energy as its fulcrum has become a new development trend, and many network security problems have emerged while new energy is developing rapidly.In this paper, the threat-driven network security methodology is used to analyze and model the threat of new energy field station from the whole of new energy station.Then, take the time and the attack stage as the main line, carries on the double analysis judgment;Finally, establish a complete monitoring system, including the network attacks on the detection, search, exploitation of loopholes, such as recognition, blocking.

Keywords: New energy sources, Threat, Network security, Attack.

1. Introduction

New energy refers to all kinds of energy situation outside traditional energy sources, including wind energy, solar energy, biomass energy, etc., is the trend of future power grid development. Since the third industrial revolution, human society has achieved unprecedented economic and technological development, the accompanying challenge is a series of problems, such as the large consumption of conventional fossil energy, the environmental pollution and shortage of resources, which force people to start looking for clean renewable energy [1-2], namely new energy. Compared with traditional fossil energy sources such as coal, oil and natural gas, new energy sources are generally characterized by less pollution and large reserves. It is of great significance to solve the problems of environmental pollution and shortage of resources in the world [3]. The pressure of resources and environment has brought new challenges to the power system. Using new energy to replace traditional energy to generate electricity will be the trend of the power industry in the future. New energy generation has good development prospect and practical value.

With more and more new energy plant station construction and access network, new energy plant station network security risks are increasingly prominent [4-7]. In the security inspection of the new energy plant in Gansu province in 2016 and 2017, 21 and 16 cases of illegal outreach were detected respectively. This has brought the huge security threat to the safety of the new energy plant station, at the same time, the alarm has sounded for the safety protection from the new energy plant [8-11]. In 2017, according to a letter from the national energy administration on the study of wind power safety, the center carried out a field survey of wind power plants. There are terminal access risk, remote operation risk, network connection, physical safety risk, system ontology security risk and personnel safety management risk, etc. [12-15].

2. IDDIL/ATC Method.

The current network security risk management practice is largely driven by compliance requirements, which makes people have to invest in security control and vulnerability. Risk management involves many aspects, including assets, threats, loopholes , controls, and is assessed on the basis of the likelihood and impact of an accident. Threats can cause damage to information systems through loopholes, while security controls are measures to prevent or mitigate attacks by threat sources. However, because of their commitment to security controls and loopholes, they ignore the most important factor in risk management-the threat. This imbalance is manifested in adhering to the existing safety framework, standards and principles in engineering practice. And emergency response is paid more attention to rather than risk management. Therefore, the threat-driven network security methodology is emerged.

The threat-driven approach is a methodology, a collection of practices and thinking patterns. Its main purpose is to enable the organization to allocate commensurate resources to protect its assets, develop the necessary skills to support these efforts, prevent or mitigate loopholes and attack vectors, and then achieve the purpose of protecting assets.

3. IDDIL/ATC Model.

The concept of threat-driven approach is based on a relationship model between threat, asset and control. This relationship model is shown in figure 1: the target of a threat is assets within an organization that are ubiquitous in one or more components. Threat sources gain access to assets through vulnerabilities in attack vectors and components (holding assets or providing direct access to target assets). Security control acts on components to prevent or mitigate vulnerabilities and attack vectors used by threat sources, thus to achieve the goal of protecting assets. At the same time, this relationship also highlights the significance of the threat perspective in the model.

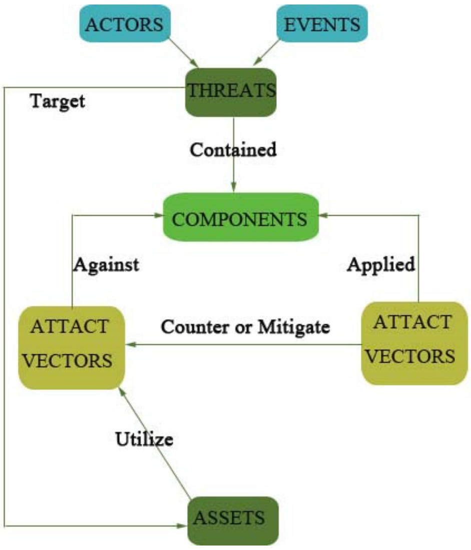

Fig. 1 Relationship model of threat, asset and control

In this relationship, threat sources do not or rarely access target assets directly, and one should acquire target assets involves interacting with other elements of the system and avoiding them at the right moment. Control does not directly affect assets. Instead, control measures must provide security function to recognise threats, attack vectors, and vulnerabilities-the ability to access components of assets. A basic principle is that the control chosen and implemented requires one or more functions to deal with threats and attack vectors. Architects, engineers, and analysts can work together to identify potential weaknesses and assess the effectiveness of control when the model contains threat intelligence. In turn, the security of systems and infrastructure will continue to be upgraded. When threat modeling and analysis are introduced into this model, the areas of possible exposure and their effects are strengthened, which optimizes the selection and implementation of control.

In this paper, the IDDIL/ATC method is applied to the new energy plant, and the threats to the key assets in the new energy plant are analyzed in detail showed in Fig. 2. There are two main objectives of threat analysis: first, to understand clearly and thoroughly the assets owned, the threats and attacks faced by them, and to make relevant decisions based on risk level and risk management practice; The second is to identify deficiencies in the selection, implementation and evaluation of security controls at the application, system, infrastructure and enterprise levels.

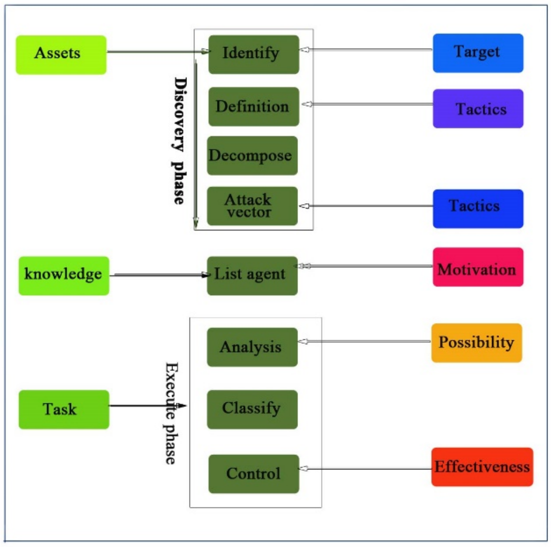

Fig. 2 IDDIL/ATC Model

IDDIL/ATC methodology divides it into two working stages: IDDIL is the discovery phase and ATC is the implementation phase. In this article, we focus on the discovery phase. The IDDIL stage includes 5 items: Recognition assets, there are two main types of assets, 1) the system business is very important to the data, components and functions, that is, business assets; 2) the data, components and functions arouse the particular interest of the attacker, namely, the security asset. These two assets are not always the same, we can identify the system's assets through business context input, asset identification also includes obtaining threat intelligence of the other party, recording the type of asset in the system and environment and indicating its location; Defined attack surface, after completing the asset recognition, the components and elements in the application system are identified from the macro level, which record the communication between the system and even provide some way to access the assets. The attack surface can help define the system trust boundaries and control the scope of responsibility, and to determine whether a work is out of range. The data flow diagrams generated at this stage (or any type equivalent to a chart) can best present the environment in which the system is located; Decomposed the system, use the information collected in the first two steps to decompose the application system into hierarchical views. Technologies such as equipment, interfaces, libraries, protocols, functions, and API need to be covered, and the effectiveness of security controls within the scope of work is subsequently reviewed; Identified attack vectors, the attack path is recorded by recording the attack surface, the decomposed system, and the main use cases. Capture components and functional ranges included in these paths, including existing security controls and services; List threat sources and attack agents: identify who wants to attack the system, and why they want to attack it.The characteristics to be understood include attack motivation, skill level, resources and targets to be analyzed, and then listed separately. Think about the different types of attack sources, because the current threat intelligence is important for this step.

4. Summary

Based on the present situation of safety protection of new energy plant, this paper introduces IDDIL/ATC methodology by constructing the safety threat and evaluation model. The security of network attack scene and power unit acquisition terminal is analyzed and studied. On this basis, fundamentally, it solves the main risks of terminal access, remote operation and maintenance, network connection, physical security risk, system ontology security risk and personnel security management.

References

[1]. Marta Meleddu, Manuela Pulina. Public spending on renewable energy in Italian regions. Renewable Energy. Vol. 115 (2018), p. 1086-1098.

[2]. Kyle Forinash. Renewable energy. Physics and the Environment. Vol. 6 (2017), p. 1-29.

[3]. Mike Sharpe. The Science and Politics of Global Warming. Challenge. Vol. 60 (2017), p. 490-492.

[4]. D. R. B. Miller. A survey SCADA of and critical infrastructure incidents. in Proceedings of the 1st annual conference on research in information technology, ACM, 2012.

[5]. J. H. Guan J., J. Graham. A digraph model for risk identification and management in SCADA systems, 2011 IEEE international conference on intelligence and security informatics (ISI), IEEE CP., 2011, pp. 150-155.

[6]. H. J. A. Nicholson, S. Webber, S. Dyer, T. Patel, SCADA security in the light of cyber-warfare, Comput Secur., vol. 31, no. 4, pp. 418-436, 2012.

[7]. M. F. Z. Tudor, What went wrong? A study of actual industrial cyber security incidents, Industrial Control Systems Joint Working Group (ICSJWG) spring conference, 2010.

[8]. H. Morgan, Cyber security risk management in the SCADA critical infrastructure environment, Eng Manag J, vol. 25, no. 2, pp. 38-45, 2013.

[9]. T. Sommestad, G. N. Ericsson, and J. Nordlander. SCADA system cyber security 2014, Power Energy Soc. Gen. Meet. 2010 IEEE, pp. 1-8, 2010.

[10]. L. Kohnfelder and P. Garg. Threats to Our Products, 2016.

[11]. T. and M. M. M. Ucedavélez. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons: Hobekin, 2015.

[12]. Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, A review of cyber security risk assessment methods for SCADA systems, Comput. Secur., vol. 56, no. Supplement C, pp. 1-27, 2016.

[13]. K. S. J. Aagedal, D. Braber, T. Dimitrakos, B. Gran, D. Raptis. Model-based risk assessment to improve enterprise security, in Proceedings of the sixth international enterprise distributed object computing conference, 2002, pp. 51 – 62.

[14]. I. S. B. Karabacak. ISRAM: information security risk analysis method, Comput Secur., vol. 24, no. 2, pp. 147-159, 2005.

[15]. R. M. R. Coles. Operationalizing IT risk management, Comput Secur., vol. 22, no. 6, pp. 487-493, 2203.