Research on Security Architecture of Global Energy Internet Standard Support System

Pei Shen^{1,*}, Sining Wang², Nie Ling²

¹Global Energy Interconnection Development and Cooperation Organization, Xicheng District, Beijing, China

²Beijing china-power information technology co.,ltd, Haidian District, Beijing, China

Abstract. The global energy Internet standard support system plays a vital role in global energy interconnection. However, the system brings convenience to the global energy interconnection and introduces new security issues. Due to the diversity of users, the complexity of the environment and the internationalization, there will be more and more malicious network intrusions from outside and inside. The security system of the global energy Internet standard support system faces great challenges. To this end, this paper proposes a security architecture that combines active and passive, establishing a chain of trust between the active security architecture and the passive security architecture, ensuring a new security architecture, a security organization framework, a security policy framework, a security operation framework, and a closed-loop system that integrates the security technology framework. A deep learning algorithm was introduced for network intrusion learning to achieve sustainable management of the information security life cycle. The combination of active and passive security systems and continuous monitoring strategies based on deep learning fully ensure the security of the global energy Internet standard support system.

1 Introduction

In the 20th century, human beings entered the electrical age, and the power system became the infrastructure of human industrial life. With the decline of traditional energy storage and the constant pursuit of environmental protection, the clean energy power generation technology based on solar energy and wind energy has become increasingly mature, and a new energy structure characterized by electric energy as the center and environmental friendliness has gradually formed. Driven by the wave of the Internet, China proposed in 2015 to build a global energy Internet to promote global energy demand in the form of clean energy and green energy. The “Internet + Clean Energy” model will also improve the existing energy network architecture[1].The Global Energy Internet provides an effective solution for the efficient allocation of clean energy resources around the world, ensuring the safety and sustainability of clean energy use [2].

The global energy Internet is dominated by power systems, distributed energy generation replaces fossil energy generation, and uses advanced power electronics and information and communication technologies to develop new routers to realize power networks, transportation networks, heating networks, natural gas networks and information networks. Tight coupling [3] is a global energy allocation platform with strong power transmission capability, wide service range, strong configuration capability, high safety and reliability, open

interaction, green and low carbon. In the construction and development of the global energy Internet industry, it is of vital importance to establish a standard support system for the unified regulation of the global energy Internet. The Global Energy Internet Standard Support System is a systematic project that is an organic combination of informatization in various business and management fields. Compared with the general information communication system, the standard system needs to provide support for the development and internal operation of the global energy Internet standard work, to establish a standard system information system for the global energy Internet unified norm, and establish a sound standardization standardization process as the main goal, and build Open and transparent standard work system to enhance the credibility of standard setting. At the same time, the system needs to meet the needs of technology development, equipment manufacturing, demonstration applications and construction operations of multinational networking.

At present, there is no clear and unified regulation for the standard support system architecture of the global energy Internet. Therefore, it is not necessary to standardize the unified global energy Internet standard system to promote the construction and development of the global energy Internet [4, 5].The architecture of global energy Internet standard support system is huge, involving many fields, in which the safe transmission and storage of system user information has become the focus. Therefore, starting from the design goals and

* Corresponding author: shenpei666@outlook.com

basic principles of the security system, this paper establishes a security architecture that combines active and passive. Meanwhile, a chain of trust is constituted between the active security architecture and the passive security architecture, to ensure that the new security architecture is a closed-loop system with security organization framework, security policy framework, security operation framework and security technology framework. Deep learning algorithms are introduced for network intrusion learning to achieve sustainable management of the information security life cycle. The combination of active and passive security systems and continuous monitoring strategies based on deep learning fully ensure the security of the global energy Internet standard support system. Providing a stable and reliable security system and powerful information technology for the development of global energy Internet standards work is of vital importance for maintaining the safe and smooth operation of the global energy Internet international standard information system.

The primary contributions of this work are as follow:

- The concept of global energy Internet standards is proposed to standardize the interaction of energy information between various countries in the process of global energy Internet construction.

- Initiative and passive safety system architecture are combined to ensure the safe operation of global energy Internet standard system. Initiative active safety system includes border security, application security, data security, host security, network security and terminal security. But for passive safety system, the topological relation is built from three aspects with safety standards, safety management and safety technology.

- A chain of trust is established between the active and passive security system topology diagrams, for building a master-passive integrated security defense system.

- In the active defense system, the deep learning algorithm is used to learn the intrusion behavior in real time, and the model is used to monitor the real-time system security performance to achieve intelligent early warning.

2 Security architecture objectives and principles

In the process of designing the global energy Internet standard system security system, the existing standard system security system is the mainstay, and according to the future development trend of the global energy Internet, a framework that can be used for future flexible expansion is constructed. This section introduces the basic principles and methodology of the construction in conjunction with the design goals of the standard system security architecture.

2.1 Security Architecture Design Goals

The global energy Internet support system security system level protection is divided into three levels, according to the "State Grid Corporation Smart Grid

Information Security Protection Overall Plan" (State Grid Information [2011] No. 1727) requirements, follow the "partition domain, security access, dynamics The security policy of "awareness and comprehensive protection" is scalable, strengthening the protection of the website according to the continuous improvement of the business system to ensure the safe, reliable and stable operation of the system to the utmost extent. Protection target:

- The identity of the support system user is ensured to be authentic to prevent malicious users and unauthorized users from accessing it.
- The integrity and confidentiality of user transmission and interaction data are guaranteed to prevent the external network users from being eavesdropped and tampered with when accessing the information external network application server.
- The security of the application system for the global energy Internet support structure is guaranteed to prevent unauthorized access to the resources of the system, leakage of sensitive data, and illegal attacks.

2.2 Basic principles of security architecture design

The global energy Internet support system security architecture design follows a certain methodology for selecting the security architecture design and extracting typical features. These methodologies are strictly scrutinized and portable, and we can follow these design rules when designing the system security architecture. The system provides greater scalability and stability.

(1) Coordination principle: The global energy Internet involves many fields, large scale and wide coverage .Therefore, the standard security system needs to be applicable to all relevant areas, coordinate and co-ordinate security issues in the areas involved, and ensure interoperability. The standard safety system designed should be based on the whole and comprehensively consider the various components of the system to form an organic and complete system.

(2) Inheritance principle: The construction of the global energy Internet is not to reinvent the existing system, but to interconnect existing systems to improve system performance. As far as its standard support system is concerned, many key technologies already have mature and complete technical standards, they only need to be improved and upgraded on the basis of the global energy Internet .Therefore, the standard system is inherited and can be compatible with existing technical standards such as smart grid [6].

(3) The principle of scalability: At present, the research on the security architecture of the global energy Internet standard system is in its infancy, and there is still a lot of room for development and development prospects. Therefore, the security system should be an open architecture with scalability. As the advancement of technology and awareness, the security system could be update and expand in a timely manner, to adapt the rapid development of global energy Internet.

3 Active and passive security architecture of the global energy Internet standard system

The global energy Internet standard support system needs to provide important services such as information acquisition, identity authentication, training and learning, and transaction settlement to internal enterprises, relevant institutions and the public through internal and external networks. Since the global energy Internet realizes multi-system interconnection and its scale is much larger than the independent subsystem in the traditional mode, the global energy Internet standard support system is more complicated and the requirements for safety and reliability are more strict than the traditional communication support system. While system business, applications, and various collection terminals are all exposed to various malicious attacks from the Internet or other areas within the global energy Internet. Data of important user identity information, transaction settlement, and facility operation monitoring face higher risks of leakage, destruction, tampering and so on when stored and transmitted.

Based on a comprehensive analysis of the current status and application scenarios of the global energy Internet, this paper proposes an active and passive energy security architecture based on the active and passive security architecture. This architecture connects the active and passive defense systems through a chain of trust, which complement each other and provide security for the global energy Internet standard system.

3.1 Active Security Defense Architecture

In the traditional security architecture, the technical identity authentication, firewall, and access restrictions often used by the defense system are used to construct the security architecture. Due to the complexity and security requirements of the global energy Internet standard system, traditional passive defense technology can no longer meet the needs of the system. Active defense security systems include border security, application security, data security, host security, network security, and terminal security.

(1) Border security

Boundary security includes two types: the vertical boundary of the information intranet and the horizontal boundary of the information intranet. The dynamic characteristics of the network are monitored from four aspects: network access control, network intrusion detection, border traffic monitoring, logging and auditing. On the one hand, by deploying a firewall, an access control policy is established for data interaction between service systems, and the port level is refined, the access rights between domains are controlled, and the access control granularity is refined to the port level configuration VLAN access control. On the other hand, by deploying an intrusion detection system, mirroring switch boundary traffic, configuring an intrusion detection probe policy, configuring IP and mac binding,

preventing address spoofing, deploying intrusion prevention devices, and monitoring and preventing port intrusion, Trojan backdoor attacks, etc. Attack behavior and analysis and audit of the log. Once the hazard is discovered, it is immediately blocked, alerted, and repaired to ensure the security of the network boundary.

(2) Application security

Application security involves leaking and tampering with information risks and malicious code risks. Security protection is implemented by means of identity authentication, input and output verification, configuration management, session management, and application interaction security. Design user application operation rights and key resource access rights on the server side, application permissions are hierarchically refined according to function modules, application interfaces, and operation buttons. Access to key resources is controlled according to database tables, key records, and data field levels. Roles application administrators and business users are divided according to business functions, refined to the menu level, control the granularity of user rights, provide log record function for permission allocation, administrators and business users perform different permission division. It is forbidden to return to the client the stack trace details including the function name and the number of lines that have problems when debugging the build. Unified return to the client for general error messages. Structured exception handle mechanisms were used to catch exceptions. Exception transaction rollback and compensation mechanisms were set up to provide transactional security rollbacks when exceptions occur.

(3) Data security

Data security requirements enable complete detection and recovery of system management data, authentication information, and important business data to ensure data storage, backup, transmission, and confidentiality. The md5 hash encryption algorithm is used to encrypt and store in the database, the user account and the authentication information are not stored in the client, the data industry data storage integrity is realized through the program logic check and the database constraint condition. The service information is stored in the database. Regularly back up your system data.

(4) Host security

According to the grid information security level protection requirements, host security includes both server security and desktop security. The five aspects of access control, intrusion prevention, vulnerability scanning, resource control, and security auditing are further refined to further enhance the security defense system. Access should be controlled by prohibiting privileged account remote management, non-privileged using in daily operations, approval process for privileged account activation. SSH terminal access mode was used for remote management and maintenance of operating system, and access limitation of network address. Different privileges were set for users to manage the operating system and database to achieve separation of permissions. The access rights of the built-in default accounts for various services should be limited, and business non-essential accounts be disabled. Sensitive

identifiers need be set for system key information, such as configuration parameters and security logs, to control access rights. The system default account is prohibited from using the default initial password. Unused expired accounts should be deleted on a regular basis. For intrusion prevention, deep learning algorithms were used to complement the use of intrusion detection and firewall virus protection in the network boundary. For vulnerability scanning, a vulnerability scanning tool was used to periodically scan the system for security and process the vulnerabilities in a timely manner, which including installing patches, configuring network access control policies, and monitoring data flows of hackers exploiting vulnerabilities. For resource control, disk quotas and other means were used to limit the maximum limit of system resources by individual users. For security auditing, the operating system log auditing function was used for important security events such as user behavior and abnormal access to system resources. The auditor performs log auditing and issues audit reports as needed. In the design process of the safety system, according to the current low overall quality of the staff, it is necessary to strengthen the training of all levels and types of comprehensive talents to meet the needs of the safety system design. In order to promote the effective implementation of the safety of the system, it is necessary to strengthen the training of existing staff members [7-9].

(5) Network security

The security system of this paper abandons the past single-point, isolated protection ideas [10], replaced by three-dimensional, global intelligent protection and control ideas [11-13]. The network device account uniqueness mechanism is used to identify and authenticate the user identity of the user who logs in to the network device. The device management policy is configured to limit the login address of the administrator of the network device. Set the login timeout and account lockout policy[14,15]. The local or remote device management must perform identity authentication. When the login fails, the session termination measures are taken to limit the number of illegal logins. The network login connection times out automatically. When the network device is remotely managed, it is safe. Remote management by SSH and HTTPS to prevent the authentication information from being eavesdropped during network transmission; use the network device system to provide the audit function or deploy the log server to ensure that the administrator's operation is audited; disable the unneeded network port and close the unwanted network service.

(6) Terminal security

In the global energy Internet standard system, terminals are distributed all over the world, causing great security risks, such as information leakage, illegal access, terminal tampering, terminal illegal control, etc., these hidden dangers will cause immeasurable Loss. In view of the business characteristics of the global energy Internet standard system, the following measures are taken: the internal office computer mac and IP address are bound to the switch port; the internal network office computer is all installed with the national network table

management terminal; the internal network office computer is all equipped with Rising antivirus Software; access to the terminal is restricted by the firewall. Terminal security is not only critical within the system, but the outflow of power data at the national strategic level poses significant risks.

3.2 Passive Security Defense System Architecture

On the basis of the active security defense system, combined with the passive defense system to supplement it makes the system more secure. The passive defense system includes three aspects: security standard, security management, and security technology. The defense against known attacks is designed by designing defense rules in advance. The overall framework is shown in Fig.1.

Fig. 1. Global Energy Internet Standard Support System Security Architecture

(1) Safety standards

The main responsibility of the safety standard is to specify the administrative policies and technical standards for corporate confidence and security, to provide security standards for system clients, and related activities need to be carried out under security standards. The system security standards include: Cloud Alliance CSA Cloud Security Guide, ISO27000 Information Security Management System, and Information System Security Level Protection. Network administrators or CIOs perform network security maintenance based on security standards. The implementation of security standards is usually based on authorization. Without proper authorization, information cannot be given, not accessed, not allowed to be referenced, and no resources can be used. Safety standards guide the organic integration of information security management with business and processes, and clarify the direction and strategy of information security construction. According to the nature of the authorization, security standards are

divided into identity-based security standards, rule-based security standards, and role-based security standards.

(2) Security management

Security management includes three aspects: security audit, operation and maintenance control, and compliance review. The rationality review is mainly the decision-making level and the management's review of the system use compliance of the executive level. There is a clear responsibility to define that all enterprise information security-related activities need to be carried out under the clear definition of responsibility. Operation and maintenance control is mainly to monitor the state of the system, monitor the state of the learning system at all times, and increase the monitoring strategy of the model to improve the security defense coefficient. Audit security manages, counts, and analyzes daily behaviors and obtains security assessments of current status.

(3) Security technology

The security technology architecture provides technical support for enterprise information security management, and is mainly divided into data protection, unified security policy, and virtual security to provide technical protection. Prevent corporate confidential information disclosure, infrastructure attack intrusion, IT access control, security management, and compliance auditing. The main innovative technologies adopted in this paper include: network intrusion detection based on deep learning algorithm, active and passive security management system, and trust chain technology for establishing active and passive security management system, which enhances the security and scalability of the system.

3.3 Global Energy Internet Active and Passive Security System Model Architecture

In response to the specificity and high safety factor requirements of the global energy Internet standard system, combined with the national grid for network information security guidelines. This paper constructs an architecture combining active security defense system and passive security defense system. The two complement each other through the trust chain to provide security for the global energy Internet standard system. The model structure of the active and passive security system of the global energy Internet standard system is shown in Fig. 2.

4 Analysis of the active and passive security architecture of the global energy Internet standard system

The active and passive security architecture of the global energy Internet standard system has the following characteristics: active and passive integration, intelligence, and three-dimensionality, providing multi-dimensional security for global users.

Fig. 2. Active passive defense systems

(1) Active-passive combination

The architecture of this paper has the combination of active and passive. The security problem of the global energy Internet standard system is more complicated. It can't just stay at the level of passive defense. The security architecture should be proactive, forward-looking and prevent security problems. On the basis of passive defense, the system is maintained by active protection.

(2) Intelligent

On the basis of the active and passive architecture, the deep learning algorithm is used to monitor the system traffic, illegal intrusion, illegal tampering and other issues in real time, and learn its behavior, confirm its illegal record and join the system blacklist. As time goes by, the internal conditions of the system are continuously learned, and the stability and defense functions of the model are getting stronger and stronger.

(3) Stereoscopic

The architecture of the system is maintained in multiple directions. The level of information security is divided into: physical security, network security, system security, application security, and management security. The relationship between these several security levels and the three dimensions is shown in Table 1.

Table 1. Dimension function list

	Technical Dimension	Policy Dimension	Guarantee Dimension
Physical Security			√
Internet Security	√	√	
System Security	√	√	√
Application Security		√	√
Administrative Security			√

Table 1 from the functional point of view at all levels of security, three dimensions complement each other, synergy, and organic combination, forming a three-dimensional global energy Internet standard system security architecture. System security is not a static process, it is not a static state. Security is not an absolute security, it is relative. Therefore, the model needs a time characteristic to ensure information security.

The security technology dimension is a static process. He provides five security services through eight security mechanisms. These five security services play a role at the same time in each time period, and there is no interruption at any moment. The security strategy itself is a dimension based on the time model. The six bad ones circulate over time and show a spiraling upward trend. Through the cycle of these six links, the strategy dimension continues to expand. The security assurance dimension is the management foundation of the power grid. From the perspective of time characteristics, the security assurance dimension is a dynamic dimension, and it shows the same upward trend as the strategy dimension. It can be seen that in the process of continuous evolution of time, the three dimensions are constantly developing in their own dimensions, forming a three-dimensional protection system to fully guarantee the security of the global energy Internet standard system.

5 Conclusion

Based on the design goals and basic principles of the global energy Internet standard support system security architecture, this paper proposes a security architecture that combines active and passive technologies, establishes a chain of trust between the active security architecture and the passive security architecture to ensure new security. The architecture integrates the security organization framework, the security policy framework, the security operation framework and the security technology framework into a closed-loop system, the deep learning algorithm is introduced for network intrusion learning to achieve sustainable management and control of the information security life cycle. The security architecture proposed in this paper is reasonable and complete, and it has strong operability. It can adapt to the needs of the development of global energy Internet standard support system under the environment of information security attack and defense. The research results of this paper provide a certain theoretical support for the construction of the global energy Internet standard support system security system, and provide security guarantee and effective guidance for promoting the development and promotion of global energy standards work and construction and development work.

Acknowledgments

This work is supported by State Grid Technology Research Project "Research on Key Technologies of global energy interconnection International Standards Organization Mechanism and Resource Library (521104180012)".

References

1. M. Wei, X. Zhou, Y. Shang, W. Sheng, Power Grid Technology, **39**(2015)
2. Pf. Zeng, Y. Liang, Y. Wang, L. Zhu, Smart Grid. **4 09** (2016)
3. B. Li, Q. Wu, J. Zhang, Ss. Chen, B. Pei, Electric Power Information and Communication Technology, **15-03**(2017)
4. Yb. Cha, T. Zhang, Z. Huang, et al, Science in China, **44-6**(2014)
5. Cy. Dong, Jh. Zhao, Fz. Wen, et al, Power System Automation, **38-15**(2014)
6. J. Zhang, B. Li, Cb. Dai, Power Grid Technology, **41-07**(2017)
7. Hp. Hu, Zg. Huang, Lh. Pang et al, Computer Engineering and Science, **11-14**(2004)
8. Qy. Men, Information and Computer (Theoretical Edition), **12-10**(2010)
9. M. Bozorgi, L.K. Saul, S and G. M. Voelker, In Proc. of 16th Int. Conf. on Knowledge discovery and data mining, **16-14**(2010)
10. D. Wang et al, Power System Automation, **02**(2016)
11. Xb. Zhang, Telecommunications Engineering Technology and Standardization, **27-6**(2014)
12. PALANIAPPAN S, RABIAH A, MARIANA Y, Journal of Information Security and Application, **18**(2013)
13. REBOLLO O, MELLADO D, FERNANDEZ-MEDINA E, et al, Information and Software Technology, **58**(2015)
14. Bx. Liu, P. Xu, Ys. Xu, Computer Engineering and Applications, **8-17** (2001)
15. PALANIAPPAN S, RABIAH A, Journal of Information Security and Application, **18**(2013)