Discussion on the Security Mechanism of Energy Internet in 5G network

Hao Yao1*, Qi-ge Ye1, Xiao-ling Yan1 and Zong-shun Tang1
1Guangzhou Electric Power Design Institute Co., Ltd, Guangzhou, China
*E-mail: 13632269600@163.com,

Abstract. With the coming of 5G network, it is possible for energy Internet to achieve high bandwidth and low delay interconnection. At the same time, it also brings new security problems. The core elements of 5G - virtualization, cloud migration, network slicing, Internet of Things, 5G gateway and even related software development may become security vulnerabilities. Aiming at the possible security problems in the application of 5G in the energy Internet, including the overall security architecture, industry security subdivision, Internet of Things security operation and maintenance, and the application of new security mechanisms, this paper expounds the relevant concepts and threats. This paper puts forward that in security architecture, we should make full use of security mechanisms such as logical isolation and access control to achieve in-depth defense; in industry segmentation, we should have customized security capability response for different application scenarios of different industries; in the security operation and maintenance of the Internet of Things, we should aim at the complex network environment and topology of mass terminals. In the new security mechanism, it should be combined with large data analysis and AI intelligent processing to enhance the ability of security early warning. Finally, combined with the application scenario of the energy internet, this paper proposes a comprehensive solution to the energy Internet Security in the 5G.

1. Introduction
The energy Internet is the product of the deep integration of energy and the Internet. Its purpose is to realize the internetization of energy, promote the marketization and efficient allocation of energy, so as to eliminate environmental pollution and realize the goal of harmonious development. The internetization of the energy network inevitably requires the energy Internet to possess the most fundamental characteristic of the Internet: openness. This openness is not only reflected in the open interconnection of various types of energy, the open peer-to-peer access of various devices and systems, and the open participation of various participants and end users, but also in the energy markets and trading platforms in different regions, open data and standards, etc.

In June 2019, the ministry of industry and information technology officially issued 5G licenses, marking the beginning of the commercial phase of 5G. 5G will deliver a leap in network performance with a new network architecture that provides bandwidth of more than 10Gbps, millisecond latency, and ultra-high density connectivity. ITU defines three scenarios for 5G: enhanced mobile bandwidth (eMBB), ultra-reliable low-delay communication (uRLLC), and large-scale machine-like communication (mMTC) [1].

The combination of 5G and energy Internet enables the energy Internet to provide technical support for the realization of energy physical equipment sharing, distributed edge computing scheduling and other application scenarios.
2. Application of 5G technology in energy Internet

“4G changes lives, 5G changes society.” 5G will not only bring ultra-high bandwidth, ultra-low latency and ultra-large scale user experience to the energy Internet, but also have a wealth of vertical industry applications to meet the needs of different users.

For the energy Internet, the application scenarios of 5G technology are mainly embodied in the two categories of device control and data collection. Among them, the control class includes distributed distribution automation and user-side conformance to demand response. Distributed energy regulation; Collection business mainly includes advanced measurement business. [2]

| business types | typical scene | Characteristics right now | future trend |
|----------------|---------------|--------------------------|--------------|
| Control type service | Intelligent distributed automation, Demand side response of power load distributed energy resource | Connected mode: Master Station/ substation mode, Y connection | Connected mode: Distributed point-to-ground connections, Master Station/ substation mode, Local proximity control |
| | | Time delay requirement: second | Time delay requirement: millisecond |
| Acquisition type service | Advanced Metering Infrastructure, Smart grid video applications (robot for inspection, Uav patrol, Video surveillance in distribution rooms, Construction site monitoring) | Collection frequency: month, day, hour | Collection frequency: Minutes, Near real-time |
| | | Collection contents: Basic Data, image | Collection contents: high-definition video (HD video) |
| | | Collection scope: primary equipment, Measuring terminal | Collection scope: Secondary equipment, Internet of Things |

5g network section, the application of open two innovation function, will change the traditional energy industry business operations and operation mode, can better in the ubiquitous access, safe and reliable, tube can be controlled, etc, to develop innovative, intensification of business application, promote energy from the extensive management to fine, implement clean energy substitution and electricity core strategic ground, for the energy industry users to create customized service industry private network, can better serve the needs of the business differentiation, further enhance the capacity for independent control of the enterprise to its business and operational efficiency.

3. Information security risks of energy Internet

The security risks of energy Internet infrastructure are mainly from rogue data injection, data tampering and interruption. Secondly, all kinds of metering data, such as users' electricity data and user identity information that form assets, are attacked by the network and are leaked or tampered with. The openness and inter-connectivity of the energy Internet make possible security vulnerabilities in data collection, data transmission, user authentication and other aspects, which makes it more difficult to protect information security.

In 2019, the state grid corporation of China launched a plan to build the ubiquitous Internet of things. In the construction of ubiquitous Internet of things, more and more intelligent electronic devices with information processing capacity will be deployed in large quantities, providing more opportunities for network attacks. If this kind of attack based on micro network is frequent enough, and there is no strong blocking measures after being breached, it will inevitably cause a chain effect on the security of
the whole network. At the same time, mass interconnection will inevitably enable terminals of different types and protocols to have the ability to interconnect with each other. Therefore, it will cause greater impact on the dedicated communication network and the single communication protocol, making the network more widely exposed. For industrial control network of all kinds of viruses, such as stuxnet virus, ransom-ware wannacry, these viruses through phishing emails, usb sticks and other intrusion into the isolated industrial control network, can also cause great damage. The information interaction of energy Internet is bound to be accompanied by the increase of information risk. In order to cope with the information security risks of the energy Internet, 5G network will establish a security control system from the three levels of end, pipe and cloud. The terminal refers to the intelligent distributed distribution automation terminal, concentrator and other different access terminals. The tube refers to the base station, transmission carrier, core network and other networks, which provide slicing services for the energy Internet. Cloud refers to the Network implementation method based on Network Functions Virtualization (NFV) and Software Defined Networking (SDN), which provides the energy Internet industry with an open and convenient terminal business management and control capability. Security system should be established. According to the relevant requirements of the industry and the country, the cloud layer should be isolated by means of security zone and network gate. As the focus of security control, terminal and tube are mainly used to further improve security by virtue of the unified authentication framework provided by 5G, multi-level network slice security management, flexible secondary authentication, key capability and security capability opening and other new attributes [2].

4. Discussion on energy Internet information security

4.1. Overall security architecture

According to the concept of defense in depth, perfect security architecture is the basic direction of network deployment design and security mechanism construction. The 5G security architecture should be based on the core security functions of the early eMBB scenarios and extended to support the mMTC and uRLLC scenarios, and build an extensible and choreographer intelligent 5G security architecture for business, so as to realize the rapid deployment of differentiated security capabilities and open security capabilities.

The 5G system is a continuation of the 4G system, which meets the security requirements including the two-way authentication between users and the network, the integrity of information and the confidentiality of user data. In addition, the 5G system also includes some security properties that were not adopted in the old system, such as the non-repudiation of service request information. In order to meet differentiated service needs, 5G should utilize new technologies such as network function virtualization (NFV) and software-defined network (SDN) to realize the virtualization of network resources and the centralization of network management. With the introduction of this technology, the network presents a structure of combining centralized control with virtual distributed subsidence. The control interface is still concentrated in the core network. In order to reduce the processing delay and return cost of the user side, the descending situation is distributed according to the needs of the business characteristics, so as to get closer to the user area and improve the user perception.

From the perspective of different functions, the 5G network security deployment architecture is divided into access security domain, core security domain, business security domain and management security domain [3].

Access to the security domain focuses on ensuring the availability of user authentication function and protecting user data and signaling; The core security domain needs to be connected with internal and external business platforms, so intrusion detection, attack defense, data protection and other work should be done well. At the same time, the centralized controller and the north-south interface should be protected for the cloud-based and software-based characteristics of the domain. Business security domain includes capability open platform, self-support platform and third-party business platform, etc. Therefore, it is necessary to protect against network side attacks and abuse of business, as well as network attacks by platform and application. Management security domain mainly includes operation
system, whose protection strategy is similar to platform protection. Software and hardware such as virus protection and vulnerability scanning are deployed in various platforms of this domain, and relevant operations are authenticated, authorized and audited.

As the industrial application of 5G network, the energy Internet should be connected to the security domain and the management security domain, so as to improve the security control ability of the users in the industry. The energy Internet has a large number of metering terminals and automatic control terminals. The user authentication control, emergency response management and chip selection of these access terminals must be "self-controlled". The security management of the management domain involves the construction of the user's own control system, which requires us to strictly implement the security management measures and the business system "simultaneously designed, simultaneously implemented and simultaneously put into operation" in the construction of various management systems, so as to strengthen the security from the user side.

Table 2. Security control of 5G Communication and the demands of Energy Internet.

| 5G Security Management | Safety management features | the demands of Energy Internet |
|------------------------|---------------------------|--------------------------------|
| Access Security Sector | improve the usability of user authentication function; protecting Signaling and user data | The user authentication control and emergency response management chip selection of metering terminal automatic control terminal must be controlled autonomously |
| Core Security Sector   | Connect internal and external business platforms, Intrusion Detection, Data Protection, attack defense | Access network as required by operators, take control measures, and configure firewalls and other equipment |
| Business Security Sector| Including Tripartite business platform, own platform; We should not only prevent the network side from attacking the business, but also prevent the platform and application from attacking the network | Improve their control ability to prevent two-way invasion |
| Management Security Sector | It mainly includes operation system, whose protection strategy is similar to platform protection | Strengthen the safety performance of self-built business system, and achieve the principle of three synchronization |

4.2. Energy industry security

For 5G network security maintenance, operators can open up network security capabilities to application developers in vertical industries, allowing third parties to upgrade the security level for specific services. In this way, new businesses can be deployed quickly and flexibly to meet user needs. 5G network slice integrates network virtualization technology, which provides basic security capabilities, including security authorization, privacy protection and transmission encryption. Based on the flexible approach of virtualization technology, 5G network slicing can customize security capabilities for different security needs in different industries. Common slices of Shared infrastructure, with basic security capabilities such as user authorization, data encryption, and security isolation, provide basic security for most applications.

The application of energy Internet is different from that of ordinary industrial users. Because it is related to the safe and stable operation and control of power grid, higher security is required.
Operators, through slicing technology, need to provide customized security services on top of basic security capabilities. These customized security services, on the one hand, serve the isolation of energy Internet data from other industry data; on the other hand, they also need to ensure the high requirement of real-time energy data. Therefore, 5G slicing technology should be combined with the edge computing capacity of energy Internet access devices. While ensuring security, edge computing capacity should be strengthened, data transmission volume should be reduced, and the exposed surface should be reduced, so as to improve the ability to withstand risks.

4.3. Ubiquitous Internet of things operations
The "three high and two low" features and advantages of 5G communication are highly complementary to the features and demands of the power system. The ITU defines three scenarios of 5G: enhanced mobile bandwidth (eMBB), ultra-reliable low-delay communication (uRLLC), and large-scale machine communication (mMTC). For the ubiquitous power Internet of things, 5G communication will be widely used in the five aspects of the Internet of everything, precise control, mass measurement, broadband communication, and efficient computing [4] [5].

Table 3. The corresponding relationship between the characteristics of 5G communication and the demand of energy Internet.

| Features of 5G communication | Energy Internet demand |
|------------------------------|------------------------|
| A high rate                  | Control business, real-time data transmission |
| High capacity                | A large number of video inspection, ubiquitous in the Internet of things business |
| High reliability             | Line protection and other high reliability services |
| Low latency                  | Control business |
| Low energy consumption       | The continuous transmission capability of the Internet of things |

"Ubiquitous" is the basic feature of ubiquitous power Internet of things, which is embodied in the ubiquitous and ubiquitous, as well as the "Internet of everything" between anyone and anything. This kind of "ubiquitous" brings the most direct impact is that the energy Internet has become the unity of terminal variety, inclusive access and complex structure. In order to ensure the security of a large number of Internet of things terminals, it is necessary to limit the connection to the minimum range and only configure the necessary functions. [6] When security events occur, the connection is within the operator's control, so as to block attacks from other Internet of things terminals. At the same time, strictly distinguish between local edge computing information and submitted information, in the protection of local computing power at the same time, the maximum protection of the main information security, establish emergency response mechanism, to identify the business risks, log data, billing data, reduce the security implications of the Internet of things terminal, ensure the security of the terminal will not become the breach of the main attack.

4.4. The use of new security mechanisms
The data information of energy Internet is carried by 5G network, and the data processing and storage are scattered in the industry user center, access terminal local and operator. The types of data are complex and diverse, with various characteristics. Traditional, data feature-based security methods can be difficult to find abnormal data. Therefore, the new security solution should be able to use mechanisms such as AI and big data analysis to predict and warn security factors in advance through historical data comparison and real-time situation analysis [7] [8].

By making use of the massive measurement and broadband communication performance of 5G network, the collection of equipment configuration information, equipment log information, network traffic information and equipment status information of various types of monitoring systems can be realized, and the standard data disposal and unified modeling can be realized (integration of graph model library) [9]. Through big data analysis, the network security risks of the monitoring system can
be identified online, the network security monitoring data can be comprehensively analyzed, and the cross-regional interconnection, illegal network access and illegal access of mobile media can be analyzed, so as to comprehensively improve the network security risk prevention and control ability of the monitoring system [10].

On the basis of massive data, this paper studies the network security big data analysis technology of power monitoring system. Based on the big data analysis tools and manual verification, this paper realizes the new network security analysis model/algorithm, and comprehensively improves the data network security level of energy Internet.

5. Conclusion

Energy Internet converts all kinds of energy into electricity and realizes the sharing of energy and information through power grid and power communication network. As one of the key technologies to realize energy Internet, 5G communication technology has a direct impact on the construction progress and investment of energy Internet in terms of information security, real-time performance and reliability. This paper puts forward that in security architecture, we should make full use of security mechanisms such as logical isolation and access control to achieve in-depth defense; in industry segmentation, we should have customized security capability response for different application scenarios of different industries; in the security operation and maintenance of the Internet of Things, we should aim at the complex network environment and topology of mass terminals. In the new security mechanism, it should be combined with large data analysis and AI intelligent processing to enhance the ability of security early warning. Finally, combined with the application scenario of the energy internet, this paper proposes a comprehensive solution to the energy Internet Security in the 5G. This paper mainly expounds some challenges faced by energy Internet from the aspect of information security, and makes some prospects, hoping to provide references for energy Internet researchers to study 5G communication technology and its application.

References

[1] Wang Qingming. Research on the transmission network scheme in the era of 5G [J]. World of digital communications, 2008, 11(1) : 1-9.

[2] China southern power grid co., LTD. 5g smart grid paper. https://www.sohu.com/a/239583030_744463

[3] Gao feng, ma zheng, zhang manjun, et al. Discussion on security deployment of 5G network [J]. Post and telecommunications design technology, 2019(4) : 45-48.

[4] Wang yi, Chen qixin, zhang ning, feng cheng, teng fei, sun mingyang, kang chongqing. Application analysis and research prospect of integration of 5G communication and pan-electric Internet of things [J]. Power grid technology, 203, 43(5) : 1575-1585.

[5] GUO H J, LIU G M, LIU T. Construction and evolution of 5G bearer network [J]. Digital Technology and Application, 2020,38(12):29-31.

[6] TONG Wei, YANG Shukuan. Research on the Technology Scheme of 5G Network Co-construction and Sharing under SA Mode [J]. Information and Communications Technology, 2020(12):213-215.

[7] Zhao Junfeng, Li Fang. Innovation and Industrial Development of 5G+ Vertical Industry Bearing Technology [J]. Communications World, 2020(33):36-38.

[8] LI Fang, ZHAO Junfeng, LI Zhenwen. Analysis of 5G Bearing Network Slicing Technology and Application Scheme [J]. Communications World, 2020(32):36-38.

[9] SONG Chuang-xing, XIONG Jun, WANG Si-yao. Discussion on Technology Selection Strategy of 5G Bearing Network [J]. Information Technology and Information Technology, 2020(11):158-161.

[10] ZHUANG W L. Research on the technology of railway 5G private network bearer network [J]. China Railway, 2020(11):46-49.