Analysis and Evaluation on the Network Security Defense in Power Marketing Industrial Control System

Jiawei Li 1,2, Kehe Wu 1, Bo Zhang 3

1 North China Electric Power University, Beijing, 102206, China
2 State Grid Beijing Electric Power Company, Beijing, 100031, China
3 Global Energy Interconnection Research Institute, Nanjing, 210003, China
LJWsgccBj@163.com

Abstract. With the implementation of the energy Internet, ‘Internet+power’, power IOT, and digital transformation and upgrading strategy, the power marketing system has carried out the massive metering acquisition and load control terminals, which are interactive and open accessed. Also, it has enhanced the coordinated operation and control with core power control systems such as power dispatching, transportation inspection. The current protection is mainly based on traditional passive defense concepts and technologies such as isolation protection, which cannot meet the demand of high reliability, high availability, safe and stable operation in the energy Internet environment. Therefore, it is urgent to establish a new generation of industrial control system for power marketing security protection system, which breaks through technologies in control terminal widely safe access, network safe and reliable interaction, system safe and trusted operation. The proactive defense technology brings new inspiration to the research on the security protection theory of the industrial control system for power marketing, including ontology security immune enhancement and pre-warning detection. Moreover, applying the theory of proactive defense to the field of power marketing security can provide a new way to improve the security protection of power marketing system.

1. Introduction
In recent years, there have been many network attacks for power systems in the world [1]. The frequency and threats of various attacks such as Prefix Hijacking [2] [3], Man-In-The-Middle (MITM) attacks [4], DoS/DDoS [5] [6] [7], Code Injection [8], Advanced Persistent Threat (APT) [9] are increasing rapidly, and the power network security is becoming increasingly severe [10]. China's power industry has always attached great importance to network security and the network security of power marketing system [11] [12]. A defense model of identity authentication and transmission encryption and decryption for power marketing system based on password theory [13] is constructed, which solves the problems of identity authentication and safe transmission of core control data in the process of remote access of meter and acquisition terminals in the power marketing isolation protection private network to the power intranet. However, with the implementation of the energy Internet, "Internet + Power", the Internet of Things and the digital transformation and upgrading strategy of power companies, as well as the development of new businesses such as Power Marketing 2.0, integration of operation and distribution, and "friendly interaction among source, network and load", the industrial control features of power marketing, dispatching, distribution and other power monitoring systems such as the whole network are strengthened. The power grid is changed from "power supply regulation" to the combination of "power..."
supply regulation" and "load regulation", the power marketing system is transformed and upgraded to an industrial control system for power marketing, and remote access and online monitoring control of power marketing terminals such as massive heterogeneous distributed power sources, microgrids, electric vehicles, charging piles, concentrators, smart meters are realized. The innovation and development of industrial control system for power marketing make the existing power marketing security protection system face new technical challenges.

Aiming at the main security problems faced by the new situation of industrial control system for power marketing, this paper focuses on the three core key issues faced by power marketing, namely, the lack of autonomous protection of massive heterogeneous terminals in uncontrolled field environment, the lack of trusted transmission technology of monitoring data network, and the lack of system security monitoring and active early warning capabilities. It provides demand guidance for exploring and constructing an proactive defense system for power marketing industry control with "defense line moving forward, harm suppression and risk early warning".

2. Development Status of Industrial Control System for Power Marketing
The construction of the power marketing system mainly started in the 1980s and 1990s. Since it was initially used for electricity tariff calculation and report processing, it has entered the stage of comprehensive analysis of electricity consumption, management decision-making and load control. The use of power marketing system can accurately meet the strategic requirements for the development strategy of power marketing. At the same time, the power marketing system is not an isolated system. It can not only realize real-time interaction with power users, but also fully combine with banking business, etc. to realize the function of authorized collection, extend the service system and provide more convenient services for customers.

At present, the industrial control system for power marketing mainly includes power load management system, power consumption information collection system, electric vehicle smart charging and switching service system, smart community/smart building management system, 95598 interactive management system, etc. It realizes three core industrial control functions of power consumption business, including data collection, parameter setting and control.
Taking the power consumption information acquisition system of the industrial control system for power marketing as a typical architecture analysis, the industrial control system for power marketing mainly includes the acquisition system master station, communication channel, terminal equipment and the acquisition system Web user end. The main station of the acquisition system also interacts with other business systems such as dispatching, security supervision, transportation inspection, transportation supervision, and development policies to provide data support for these business systems.

Data collection business functions of industrial control system for power marketing: various types of data such as electric energy data and event record data are collected by means of timing automatic collection, manual call and measurement, automatic reporting, etc., and the data are calculated, analyzed and checked for rationality through the data inspection and analysis module. Data collection services include online monitoring, data analysis, Web page information release and other functions.

Parameter setting business functions of industrial control system for power marketing: other business systems such as marketing, security supervision, transportation and inspection can realize batch parameter setting function by collecting batch configuration information issued by the main station of the system; Internal users at the provincial, municipal, county and power supply level access the collection master station through the Web server to realize point-to-point parameter configuration.

Control business functions of industrial control system for power marketing: the acquisition system can control the power, electricity quantity and time period of the acquisition terminal at a fixed value. At the same time, it can remotely control the electric energy meter according to other business system tasks, and perform remote control, power protection, elimination and other operations. The control execution function can also realize orderly electricity consumption management, arrears control management and other businesses.
At present, the network communication channels of industrial control system for power marketing have also been developed in a variety of ways. Various network communication modes such as wireless APN/VPN private networks such as operators GPRS/CDMA/3G/4G, 230MHZ wireless private networks, Beidou private networks and optical fiber private networks have been widely adopted, which makes the channels for data uplink and parameter setting and control data downlink of industrial control system for power marketing more open and further increasing the network security risks.

The terminal equipment layer of industrial control system for power marketing includes three types: acquisition equipment, meter equipment and metering field operation terminal.

Acquisition equipment: In the middle layer of the acquisition system, it includes concentrator and special transformer terminal. Concentrators are generally deployed near the user transformer, and are responsible for collecting and summarizing the electricity consumption information of residential user watt-hour meters under the jurisdiction of the transformer, and uploading the summarized data to the main station. Industrial and commercial users are generally equipped with special transformer terminals, which collect the electricity consumption information of users' electricity meters and realize communication with the main station of the acquisition system. The concentrator does not have control function, and the special transformer terminal has load control function.

Meter equipment: Located at the bottom of the acquisition system, it mainly refers to smart watt-hour meters and multifunctional watt-hour meters. General smart watt-hour meters have the function of fee control, which can be implemented according to the user's payment information and electricity consumption. Fee control functions include local fee control and remote fee control. The local fee control charging and control links are completed locally in the electricity meter, and the remote fee control command is initiated by the main station of the acquisition system. Remote multi-function fee-controlled watt-hour meter generally refers to the watt-hour meter with GPRS remote communication module integrated internally. The watt-hour meter integrates the functions of concentrator and watt-hour meter at the same time, and is generally used for electricity metering equipment for remote users or temporary users. The smart electric energy meter has the function of cost control and belongs to the equipment with control.

Metering site operation terminal: It is a mobile operation equipment for emergency repair and site maintenance of electric energy meters and acquisition equipment. The built-in communication module of metering site operation terminal can directly communicate with the main station, which is connected to the acquisition operation and maintenance module of the acquisition main station system. The network architecture is equivalent to a mobile acquisition terminal. When the link between the electricity meter and the main station fails, the transmission channel between the main station and the electricity meter can be established through the metering field operation terminal, the fault points between the electricity meter, the acquisition terminal and the main station can be checked, the faults can be checked and repaired, and the emergency repair and on-site maintenance of the electricity meter and the acquisition terminal can be realized.

3. Current Research Status of Proactive defense in Industrial Control System for Power Marketing

In the aspect of industrial control system for power marketing security protection, power companies focus on the boundary security of industrial control system for power marketing, supplemented by passive defense research such as terminal security, network security and application security based on the isolation protection of power secondary security network. Therefore, the power marketing key management system is further constructed, and the core sensitive information of the marketing industrial control system is encrypted and decrypted based on the cryptographic technology, thus realizing the cryptographic security protection technical framework of the power marketing system.

3.1 Network security protection of industrial control system for power marketing

Its core protection goal is to prevent the inside of the border from being attacked from the outside, and it is also used to prevent malicious internal personnel from carrying out attacks across the border or
external personnel from entering the internal network through open interfaces and hidden channels. In the early stage of the occurrence of security events, the attack hazards can be found through the analysis of security logs and intrusion detection events. After the occurrence of security events, intrusion event records can be provided for audit tracking. For this reason, power companies divide the network boundary of industrial control system for power marketing into information intranet and third party boundary, information intranet boundary, information intranet horizontal domain security boundary, information intranet vertical security boundary, etc.

Table 1: Security Protection Measures for Network Boundary of Industrial Control System in Power Marketing

| Boundary Type                        | Boundary Description                                                                 | Security Protection Technology                          |
|--------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------|
| Information Intranet and Third Party Boundary | The boundary between the information intranet, the wireless private network and the operator's virtual private network. | 1. Hardware Firewall or Software Firewall  
2. Virtual Firewall Technology  
3. Access Control Technology between VLANs |
| Information internal and external network boundary | The boundary between information intranet and information extranet. | -                                                      |
| Security Boundary between Horizontal Domains of Information Intranet | The communication network boundary between security domains. | -                                                      |
| Vertical Security Boundary of Information Intranet | The vertical security boundary of the information intranet includes the network boundary between the headquarters and the companies in each network province, and the network boundary between the companies in each network province and the companies in the city. | -                                                      |

3.2 Security protection of industrial control terminal in power marketing

In addition to the protection measures such as anti-theft and anti-damage, the industrial control terminal equipment for power marketing also adopts a security module to ensure the security of the communication data interface in the system. At present, power companies have taken different security protection measures for three different types of power marketing industrial control terminal equipment, such as acquisition equipment, meter equipment and metering site operation terminals.

The acquisition equipment is located in the middle layer of the acquisition system, as shown in Table 3-2. The security measures adopted mainly include: 1) Embedding security modules supporting SM1, SM2 and SM3 algorithms on the acquisition terminal equipment; 2) The authentication mechanism of digital certificate is adopted; 3) Encryption protection is carried out from the transport layer and the application layer respectively; 4) Transport layer encryption realizes identity authentication, key negotiation and data encryption transmission, while the application layer encryption ensures the data integrity protection and authority control.

Table 2: Security Protection of Acquisition Terminal

| Terminal Form   | Security Requirements | Compliance | Implementation Methods and Measures                                                                 |
|----------------|-----------------------|------------|-----------------------------------------------------------------------------------------------------|
| Acquisition equipment | - Identity Authentication | Compliance | Digital certificates are issued for each terminal, and identity authentication is carried out between the security module supporting SM1, SM2 and SM3 algorithms and the dedicated isolation gateway of the master station. |
|                | - Data Security       | Compliance | The embedded security module is used to encrypt and protect the data from the transport layer and the application layer respectively, thus realizing the functions of data integrity guarantee and authority control. |
The meter equipment is at the bottom of the acquisition system, as shown in Table 3-3, and the security measures adopted mainly include: 1) embedding a security module supporting SM1 algorithm on the meter equipment; 2) adopting challenge response mode for identity authentication; 3) encrypting and protecting key instructions such as recharge, control and parameter setting from the application layer.

| Terminal Form | Security Requirements | Compliance | Implementation Methods and Measures |
|---------------|-----------------------|------------|-------------------------------------|
| Meter equipment | • Identity Authentication | Compliance | • Through embedded security module supporting SM1 algorithm, identity authentication is carried out by challenge response. |
|               | • Data Security        | Compliance | • The embedded security module is used to encrypt and protect the data from the transport layer and the application layer respectively, thus realizing the functions of data integrity guarantee and authority control. |

The metering site operation terminal is connected to the acquisition operation and maintenance module of the acquisition master station system. The network architecture is equivalent to a mobile acquisition terminal. Its security protection measures are implemented with reference to the acquisition terminal. As shown in Table 17, the adopted security measures mainly include: 1) Embedding security modules supporting SM1, SM2 and SM3 algorithms on the metering site operation terminal equipment; 2) Adopting the identity authentication mechanism of digital certificate mode; 3) Encrypting and protecting from the transport layer and the application layer respectively; 4) Encrypting in the transport layer to carry out identity authentication, key negotiation and data encryption transmission, encrypting in the application layer to ensure data integrity, and solving the problem of authority control at the same time.

| Terminal Form | Security Requirements | Compliance | Implementation Methods and Measures |
|---------------|-----------------------|------------|-------------------------------------|
| Metering site operation terminal | • Identity Authentication | Compliance | • Digital certificates are issued for each terminal, and identity authentication is carried out between the security module supporting SM1, SM2 and SM3 algorithms and the dedicated isolation gateway of the master station. |
|               | • Data Security        | Compliance | • The embedded security module is used to encrypt and protect the data from the transport layer and the application layer respectively, thus realizing the functions of data integrity guarantee and authority control. |

3.3 The safety protection for power marketing industrial control system
The application of safety protection mainly refers to the protection for power marketing industrial control system itself, the system and the users’ interface, data interface among systems, and the data interface inside of the system.

The goal for the safety protection of power marketing industrial control system is to guarantee the security of the system and the transmitted data while interacting with other systems by taking safety measures, such as ID identification and access control. In addition to that, audit measures can identify the intrusion attempts before the occurrence of the security incidents or conduct audit trail after such incidents take place.

The main technological approaches adopted by the power marketing industrial control system mainly consist of the ID identification mechanism, user privilege and access control, application security audit, residual information protection, data storage security, anti-denial, software fault tolerance, resource control, backup and recovery of application data.

After the occurrence of blackout caused by network attack for overseas major power network security incidents including Ukraine, power enterprises put the active defense requirement of the No.14th order
released by National Development and Reform Commission (NDRC) and carry out the optimized scheme of safety protection of the electricity information collection system for power marketing. Safety access of power marketing has been added to the network structure, deploying the power marketing industrial control system to the special safety access, which is loaded to the internal information network, realizing the logic insulation from the other parts through firewall. The collection terminal for electricity information will be accessed to special safe area through the mobile customized APN network and communicate with the main station.

Network boundary communication intrusion detection for power marketing industrial control system has been proposed by the power enterprises on the basis of this, requesting the information flowing to the internal and external third-party network boundary mirrored to the intrusion detection system for the detection of service data flow. The following points are focused on: to customize the intrusion detection strategy, for instance, identifying the service type and port number to be monitored to customize the intrusion detection rule according to the source and destination address to be detected; to customize the instantaneous alarm strategy for the intrusion detection of major events. Bottom line is to monitor the below attacks, port scan, powerful attack, trojan backdoor attack, service-denial attack, buffer overflow attack, IP debris attack and network worm attack. In case of attacks have been detected, the intrusion detection system shall keep record for the IP of attack source, type, purpose and time and shall provide timely alarm information while severe intrusions happen. The scholars and research institutions in China carry out the technological study based on this requirement and propose to apply multiple technologies, including physical integration of information, layered monitoring, machine learning and abnormal detection, to the intrusion detection and prevention of the network security in the power system, improving the accuracy of the attack detection, enhancing the detection capability for customization and novel attacks. Among which, the mainstream technologies consist of the abnormal detection method based on behavior features and such method based on the decision-making tree, analysis on main components and ant colony optimization mechanism. However, related research achievements for the above technologies applied to the power marketing industrial control system have not yet realized.

4. The difference analysis on the active defense research of power marketing industrial control system

The current safety protection system of power marketing is to protect from the network attacks in a way of closed passive defense through the ID identification and insulation protection technology, which is weaker in the security protection capability for the power marketing terminal, network and system. Once attacked by the network, only harmful response, forensics after the attack and disaster recovery can be done. Under the new circumstances, such system cannot suffice the high level real-time, high-level reliable and high-level service continuous protective demands for the power marketing industrial control system and is not able to deal with the horizontal and vertical transmission of network safety threats of such system. It is imperative to convert the recovery protection, such as the aftershock passive response, to the passively active protection including advance warning and transfer. Network safety protection is a dynamic process. The new loophole will keep rising and the novel attacking methods will never stop changing, so, the technologies and capabilities to deal with the network attacks for the power marketing industrial control system are evolving. The misuse detection and static protective strategies for the current system are difficult to tackle the complicated and versatile network attacks effectively, not to speak of the novel network attacks, customized 0-Day loophole attacks and the advanced continuous attacks against the power marketing system. In terms of the information security, the following technical problems for the safety protection of the power marketing industrial control system are still existing.

4.1 The lack of the behavior control technology after access of mass heterogeneous power marketing industrial control terminal

Different from the whole network for the power dispatching and the closed specified environment for the devices, heterogeneous smart terminals, such as numerous smart meters, charging piles and new energy, have been intensively accessed to the power marketing system. The accessing approaches are
diversified and the environments are uncontrollable, which make it easy to be used and controlled maliciously. In addition to that, the risk for the access of illegal terminals and attacks caused by the utilization of the legal terminals make it easy to carry out the network attack for the power grid. Despite the current safety protection method based on password solves the legal identification for the terminal, it cannot measure and dynamically evaluate the credibility of the computing environment and behavior for the terminal of the system. The dependable computing and safe access technology have been put forward by relevant scholars, however, restricted by the complicated reform technology for the terminal, the high occupancy of resource and difficult maintenance, they are not suitable for the safe access of the power marketing industrial control terminal. Hence, the trusted secure access platform for power mobile operational terminals and mobile work terminals has been deployed by the power enterprises, but it does not perfectly deal with the terminal behavior control issues as the safety risks raised by the terminals to the internal network of power are still existing.

4.2 The lack of the defensive technologies for the attacks of the power marketing industrial control network transmission

There are so many service centers for the power marketing system. The monitoring and control cover the residents, designed variable users, new energy fields and electrical vehicle users. The mode has been shifted from the “vertical and closed” to the “horizontal and open”, three forms covering the single data acquisition, “acquisition+ centralized control” and “acquisition + centralized control+ regional autonomy”, which constantly improving the active defense requirement for the network monitoring information transmission. The mixture of uncontrollable environment, devices and users makes the data transmission easy to be tampered, endangering the safety of power grid. The “Longitudinal encryption” scheme proposed in the secondary system safety protection stipulation is not applicable to the service environment with multiple service centers and wide distribution area. Besides, the current encryption and decryption transmission scheme based on password of the power marketing industrial control system is restricted by the transmission efficiency and the complicated key management technology, which cannot be comprehensively applied to the system. It can only protect the transmission with the critical control order, making the protection of the tremendous data collected and the safety for the transmission for user data harder to be ensured. Furthermore, the malicious data tampering, injection attacks and harm evaluation under the power marketing high-level measurement system have been studied by domestic and overseas scholars in the previous years, however, the research achievements on the harmful prevention and inhibited technologies are barely seen.

4.3 The transmission to the power grid caused by the physical integration of information of the power marketing industrial control system.

The innovation and development for new services, such as the comprehensive energy service, smart energy service, source network storage collaborative service, new energy cloud, integration of multiple stations and virtual power plant, have closely coupled with the core control system of the power grid including the load control and cost control of power marketing, transmitting the network risks further to the grid itself. The high reliability of the power marketing industrial control system requires the active warning of the attack risks and avoid the occurrence of the harm caused by the network attack. At present, the abnormal detection methods, such as AI and deep learning, have been adopted by the industry to sound the alarm for the detection of intrusion. Certain achievements have been made, the detection of the attack behaviors is limited to the network layer, though. In the case of the invisible network attacks and enhanced customization, without going deeper to the industrial control system service logic, service behavior and other characteristics of abnormal detection, it still cannot solve the problem of service logic attack identification and the discovery for power marketing industrial control system. The unknown attack defense technique of the mimicry defense redundancy voting has provided references for the study in this paper. Despite that the abnormal detection technologies against the attack behaviors are confined by the attack features, the advance warning is difficult to be realized due to the high rate of missing report. However, the high certainty of the service behaviors of the power marketing
industrial control system can establish the base line for the normal behaviors, which can make the feasibility of the abnormal detection for the system itself and the risk warning technology higher, greatly inspiring the implementation of the active warning for the risks in the paper.

Many safety inspections have been organized by the power network security Red team of State Grid Corporation of China (SGCC) for the risks mentioned above and discovered that the internal network can be accessed through the fake self-service payment terminal. Meanwhile, many offensive and defensive drills have exposed that illegal personnel can forge the marketing industrial control terminal access to the information network and conduct illegal operation without being found in a timely manner, posing a serious threat for the power marketing industrial control system and the security of the information system. Many network security incidents and the actual verification demonstrate that the power marketing industrial control system security protection technology still has shortcomings, which makes the active defense technology pressing.

5. Conclusion
The current status analysis on the active defense system and the key technologies for the safety protection of the power marketing industrial control system show that such studies conducted by both domestic and overseas scholars are still at preliminary stages. The development demands for mega-marketing under the energy internet environment cannot be sufficed without a systematic protection framework. It is imperative to establish an active defense system for the power marketing industrial control system. As a conclusion, in terms of the active defense for the system, it is necessary to surmount the technical difficulties of defending against new attack under the condition of service continuity of industrial control system. The active defense technology and method of power marketing industrial control system covering terminal, network and system shall be put forward to set up the three-dimensional and comprehensive security defense frontline for the system.

ACKNOWLEDGMENTS
This work is Supported by the science and technology project of State Grid Corporation of China: "Research on Security Defense Technology for closed-source power industrial control system ".

References
[1] Zhang Huanguo, Han wenbao, et al. Survey on cyberspace security [J]. SCIENTIA SINICA Informationis, 2016, 46(02): 125-164.
[2] Liu xin, Zhu Peidong, Peng yuxing. Internet Registry Mechanism for Preventing Prefix Hijacks [J]. Journal of Softwar, 2009, 20(03): 620-629.
[3] Khare V, Ju Q, Zhang B. Concurrent Prefix Hijacks: Occurrence and Impacts [C]. In Proceedings of the IMC 2012. 2012: 29.
[4] Desmedt Y. Man-in-the-middle attack [C]. In Encyclopedia of cryptography and security. 2011: 759.
[5] Mirkovic J, Reiherr P. A taxonomy of DDoS attacks and DDoS defense mechanisms [J]. ACM SIGCOMM Computer Communication Review. 2004, 34(2): 39.
[6] Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms to counter the DoS and DDoS problems [J]. ACM Computing Surveys. 2007, 39 (1).
[7] Glenn M. A summary of DoS/DDoS prevention, monitoring and mitigation techniques in a service provider environment [J]. SANS Institute. 2003: 34.
[8] Riley R, Jiang X, Xu D. An architectural approach to preventing and mitigating DDoS attacks [J]. IEEE Transactions on Dependable and Secure Computing. 2010, 7 (4): 35.
[9] Daly M K. Advanced persistent threat [J]. Usenix, Nov. 2009, 4.
[10] Ni Zhen. Research on Key Technologies of security risk analysis and prediction for power industrial control network [D]. Nanjing University of Technology, 2018.
[11] Lu Jiaying. Security risks faced by China's basic power grid from the perspective of Ukraine power grid attack [J]. China Information Security, 2019(11): 97-99.
[12] Hu yan, Dong mingchui, Han yingduo. Consideration of information security for electric power industry[J]. Automation of Electric Power Systems, 2002(07):1-4.

[13] Yan Renning. Research and Implementation of power marketing mobile security protection platform based on virtual terminal[D]. North China Electric Power University (Beijing), 2019.