Power Internet of Things card and infrastructure resources security supervision business model and platform construction under the background of energy Internet

Author 1, Wang Ben, Author 2, Zhao Qing

[1]BEIJING FIBRLINK COMMUNICATIONS CO.,LTD. , Beijing 100070
[2]BEIJING FIBRLINK COMMUNICATIONS CO.,LTD. , Beijing 100070

Abstract. In response to the national call to strengthen the construction of new infrastructure, State Grid Corporation takes the acceleration of new digital infrastructure as an important basis for transformation and upgrading and the realization of strategic objectives. With the surge in the number of power Internet of Things terminals and the demand for data processing, the development of Internet of Things card and infrastructure resource operation business has become the focus of the industry. This paper investigates and clarifies the business background, business positioning and research theory of the business platform, explains the basic framework, basic functions and implementation plan of the platform construction, and analyzes the market status quo and business model of the platform operation. This paper provides theoretical basis and case reference for the new digital infrastructure construction of State Grid Corporation, and has certain theoretical inspiration and practical significance for the construction of mutually beneficial, sharing and co-construction energy Internet ecology.

1 Preface

《Report on the Work of the State Council in 2020》[1] explicitly pointed out that to strengthen the construction of the new infrastructure, including "new digital infrastructure" means on the basis of a new generation of information and communication network, drive that based on digital technology and Internet, need to adapt to the energy Internet construction, construction of supporting enterprise digital transformation, grid intelligence upgrade, ecological integration innovation infrastructure and services. [2] Accelerating the construction of new digital infrastructure is the key to the transformation and upgrading of the power grid to the energy Internet, as well as an important foundation for the State Grid Corporation to achieve its strategic objectives. [3] Therefore, under the strategic promotion of the new infrastructure of the State Grid, it is imperative to build an electric Internet of Things that can cover all links of the power system, promote the extension of the grid perception measurement and control boundary to power supply measurement, customer measurement and supply chain, and comprehensively improve the holographic perception ability of the grid and terminal equipment [2]. With the accelerated construction of 5G, low-power wide area network and other infrastructure, hundreds of millions of new terminal devices will be connected to the power Internet of Things and generate massive data, and the demand for the number of terminal device configurations and data processing capacity is also increasing. This is a major challenge to the current management of terminal devices, the computing and processing capacity of large amounts of data, and the carrying capacity of wireless networks.

2 Business background

In order to continue to accelerate the upgrading and development of the emerging digital industry, the planning layout and top-level design of power basic resource sharing operation will help improve the level of joint construction and sharing. By the end of 2020, State Grid Information Industry Group and 10 network companies in Chongqing, Shanxi, Jilin, Ningxia, Jiangsu, Xinjiang, Sichuan, Shandong, Henan, Anhui have set up Siji Technology Service Co., Ltd. It is expected that State Grid Information Industry Group will set up 22 joint ventures in the national network in 2021. Its main business mainly includes: information and communication network construction and service business; Investment in auxiliary facilities of power infrastructure (poles and towers, channels, optical fibers, substations, etc.), and implementation of multi-station integration and other value-added services; Integration, application, development and value-added services of energy data resources. Thus, it can be seen that Siji Technology Service Co., Ltd. established with 22 provincial companies will become the main force for State Grid Information Industry Group to carry out information communication business and value-added business operation in provincial companies.

* Corresponding author: zwywzhdxj@126.com

On October 12, 2020, China Radio and Television Network Co., Ltd. was formally established, and State Grid Telecommunicature Industry Group invested 10 billion yuan in it, marking the cooperation between State Grid Corporation and China Radio and Television in 5G construction, wireless operation and other aspects. Therefore, in addition to the cooperation with China Unicom, China Mobile and China Telecom, China Radio and Television will become a more reasonable and cost-effective choice for the operation of power Internet of Things business.

According to estimates, at present, about 10,000 charging terminals in Tianjin apply wireless access, and the annual rent is 1.2 million yuan; about 120,000 marketing electricity acquisition terminals, and the annual rent is 7.2 million yuan; and about 3,000 market energy efficiency terminals, and the annual rent is 180,000 yuan. The equipment department's electricity monitoring and high-voltage monitoring terminals are about 4,000 units, with an annual rent of 240,000 yuan; the annual rent of marketing messages and business offices is 4 million yuan; the unified logistics vehicles are about 25,000 units, with an annual rent of 480,000 yuan (mobile operation terminals cannot be counted). The total annual wireless communication operation cost of State Grid Tianjin Company is 13.3 million yuan (the above incomplete caliber statistics). Meanwhile, Jiangsu Electric Power Company has more than 2 million sets of electricity acquisition terminals, and the annual rent is about 60 million yuan. According to the calculation of power supply capacity (based on the analysis of power supply and demand of State Grid in May, State Grid 438.485 billion kWh and Tianjin 6.754 billion kWh), the annual wireless charge of State Grid is 863 million yuan (conservative estimate). With the large-scale construction of power Internet of Things, the number of terminals will grow exponentially, and the annual wireless fee of State Grid is expected to exceed 4 billion yuan in 5 years. Therefore, there is a huge development momentum and potential market in the wireless operation market. Enterprises should plan the development opportunities of "new infrastructure" with advanced consciousness, grasp and connect the development trend and demand in the wireless operation field, formulate scientific plans and schemes, and define the strategic development direction and target positioning of enterprises.[4]

3 Business location

As the number of power Internet of Things terminals increases rapidly, the demand for wireless network expands, and the scale of co-construction and sharing of power infrastructure resources expands, it will also bring about problems such as poor economy of wireless charges by each network province fighting on its own, lack of unified control, access management and supervision of Internet of Things card and infrastructure resource operation, and lack of security guarantee means. Aiming at the target customers of Siji Technology Service Co., Ltd., State Grid Corporation and various grid provincial companies, this paper carried out the solution research on the security supervision platform of power Internet of Things card and infrastructure resources. Through business integration with operators' operation support systems and business support systems, communication business data can be visible, manageable and controllable, and users can be provided with IOT card status monitoring, traffic monitoring, tariff management, security monitoring, and infrastructure resource management such as poles, towers, channels and lines, and other related operation and maintenance services. On the one hand, users' business needs are uniformly accepted on the platform side and given real-time feedback; on the other hand, users can inquire independently through portals and APIs, etc., and finally achieve unified display of the whole network wireless applications and centralized query, statistical analysis, fault discovery and unified display of provincial business platform data.

4 Research theory

4.1 Theoretical basis of the project

4.1.1 Industry standard theoretical basis

《Guidance on Internet of Things Application of State Grid Corporation of China》

《Opinions on big data application of State Grid Corporation of China》

《The State Grid Corporation of China has fully deployed the construction of ubiquitous power Internet of Things》

《State Grid Ubiquitous Electric Internet of Things Construction Outline》

《We will accelerate the implementation plan for the application of "Internet Plus" marketing services》;

《State Grid Corporation Information Standard System》;

《State Grid Corporation Information Standard Guide》;

《State Grid Corporation of China 95598 customer service business management measures》（State Grid Administration〔2016〕41）;

《Test procedure for condition maintenance of power transmission and transformation equipment》;

《Measures for the Administration of State Grid Information Structure》;

《Code for integrated design of application software of State Grid Corporation of China》;

《Technical specification for the design of power carrier communications》;

《Technical specification for monitoring device of power information acquisition terminal》;

《Technical guidelines for intelligent electricity service system》Q/GDW/Z 518-2010 ;

《Information security technology - Guidance for

information system security level protection rating》GB/T 22240-2008

4.1.2 J2EE-based technical architecture

The security supervision platform of power Internet of Things card and infrastructure resources adopts J2EE based technology architecture to improve the flexibility, scalability, security and concurrent processing capacity of the system. Meanwhile, data interaction with the three major operators is realized through unified data interface. J2EE technology architecture has the following characteristics:

（1）Support for heterogeneous environments

J2EE is capable of developing portable applications deployed in heterogeneous environments. Whether it is a mainframe, a UNIX platform, or a Windows operating system, applications developed based on J2EE are not dependent on any particular operating system, middleware, or hardware. As a result, a properly designed J2EE-based program can be developed once and deployed to a variety of platforms.

（2）scalability

Applications based on the J2EE platform can be deployed on a variety of operating systems. For example, it can be deployed to high-end UNIX and mainframe systems that can support 64 to 256 processors on their own. Vendors in the J2EE space offer broader load balancing strategies that eliminate bottlenecks in the system and allow multiple servers to be deployed together. This deployment can reach thousands of processors, enabling a highly scalable system to meet the needs of future large-scale applications.

（3）Stable availability

The platform must be able to operate 24/7 to meet the needs of the company's customers, and downtime at night for maintenance can cause serious damage. If the shutdown is unexpected, it will cause disastrous consequences. J2EE is highly reliable and can be deployed in a reliable operating environment, thus supporting long-term availability. J2EE can be deployed in a Windows environment, or you can choose a more robust operating system such as Sun Solaris, IBMOS/390, etc. The most robust operating systems can achieve 99.999% availability or just 5 minutes of downtime per year, making them ideal for enterprise systems with high real-time requirements.

4.1.3 Application framework based on MVC

In the application framework of MVC, M refers to the business model, V refers to the user interface, and C is the controller. The purpose of using MVC is to separate the implementation code of M and V, so that the same program can use different forms of expression. Its main characteristics are as follows:

（1）Low coupling

The separation of the view layer from the business layer allows changes to the view layer code without recompiling the model and controller code. Similarly, changes to an applied business process or business rule can only be made to the model layer of MVC. Because the model is separated from the controller and view, it is easy to change the application's data layer and business rules.

（2）High reusability

As technology continues to improve, there are more and more ways to access applications. MVC pattern allows the use of different types of view to access the same server-side code, because multiple views can share a model, it includes any WEB browser (HTTP) or wireless browser (wap), for example, the user can through the computer can also be used by mobile phone to order a sample product, although the different way of ordering, but processing order products is the same way. Since the data returned by the model is not formatted, the same artifacts can be used by different interfaces.

（3）Low life cycle cost

MVC makes developing and maintaining a user interface less technical.

（4）The deployment of fast

Using the MVC pattern reduces development time considerably by allowing the programmer to focus on business logic and the interface programmer to focus on presentation.

（5）High maintainability

Separating the view layer from the business logic layer also makes Web applications easier to maintain and modify.

(6) Advantages software engineering management

Because different layers perform their duties, different applications of each layer have some of the same characteristics, which is conducive to the management of program code through engineering and tool. Controllers also provide the benefit of being able to use them to connect different models and views to fulfill user needs, which in turn can provide a powerful means of building applications. Given some reusable models and views, the controller can select the model to process according to the user's requirements, and then select the view to display the processing results to the user.

4.2 Key points and difficulties of the project research

4.2.1 Key points of project research

(1) Platform requirement analysis and function confirmation

Accurate function positioning of the platform is the key to effectively solve the pain points of the security management of power Internet of Things card and infrastructure resources. Because there is no precedent for the development of the Internet of Things card operation management platform in the power system, there is no experience to refer to, so the analysis of demand and function is particularly important. This requires a lot of energy in the early stage, communication with operators, network companies and prefectural companies, demand collection and analysis, and the development of reasonable and effective platform demand specifications based on the principles of practicality, efficiency, security

and stability.

（2）Interface development and docking with three major operators

If the components and functional modules of the platform are the skeleton of the platform, then data access is the blood of the platform. The main data of this platform comes from the three major operators' Internet of Things management platforms, such as China Mobile CMIOT, China Telecom CTWING and China Unicom CUIOT platform. Through the customized development of API interface, the type, volume and timeliness of the data requirements of the platform can be satisfied, which plays a decisive role in the realization of the platform functions. Therefore, the early communication with the three major operators, as well as the platform interface development and docking work, is particularly critical. Up to now, through preliminary communication with the three major operations of China Mobile, China Telecom and China Unicom, they all indicate that the data of the management platform of the Internet of Things is open, the demand is customizable, and the cooperation intention is open and welcome.

（3）The platform must be easy to extend

With the gradual development of the wireless operation of the Internet of Things and the gradual advancement of the construction of the electric Internet of Things, the number of Internet of Things cards connected to the platform will increase exponentially, and the new demands of users will also gradually increase with the use of the platform. Operators 5 g technology mature gradually, meanwhile, large-scale construction of the base station 5 g, 5 g network gradually began to be put into use, a smart grid based on 5 g scene will be more widely applied, the platform also to meet the demand of 5 g biopsy operation, form fit the power industry application scenario eMBB (large flow) mobile broadband business operation mode, URLLC) (low latency, high reliable business operation mode, mMTC) (mass machine connected business operation mode. In order to ensure the practicability and economy of the platform development, the platform must be scalable and easy to extend.

4.2.2 Project Research Difficulties

（1）Implementation schedule risk

The whole project implementation is composed of multiple links, each link of complete directly affect the whole progress of the project: the project implementation requires and mobile, unicom, telecom system of three carriers such as interface debugging, interface debugging workload is very big, also requires them to cooperate with the debugging, it is hard to guarantee implementation progress. The implementation progress of the system is out of control, and the risk of failing to complete the construction task as scheduled exists.

Countermeasures:

1）In order to ensure the smooth implementation of the system, reasonable allocation of the construction team is the first condition, must ensure that the construction team is composed of senior leaders of both parties, experienced business experts, technical experts, and ensure that the participants put enough energy into work;

2）Implementation schedule control, and careful analysis and research are needed to determine the reasonable goal, during the period of construction by scientific means such as operational research, network planning technique, review, modification, implementation organization design and project schedule, coordination and supervision, remove interference, to make the system function and system construction in stages goals step by step, finally guaranteeing the construction task deadline;

3）Strengthen the tripartite communication with the pilot units and the three major operators and system manufacturers, and the pilot units promote and coordinate the work of all parties;

4）Strengthen process supervision and acceptance to ensure construction quality.

（2）Risks to the system network environment

The platform needs to exchange data with the three major operators such as China Mobile, China Unicom and China Telecom and deploy it at the headquarters level, so it puts forward high requirements for network resources and network operation and maintenance. When the network interruption and congestion will directly affect the stable operation of the system.

Countermeasures:

1）To fully demonstrate and analyze the network traffic and the expected development, to provide sufficient and scientific width, and effectively provide a strong guarantee on reliability and security in the network construction and planning.

2）Establish a strong operation and maintenance guarantee system to improve the network operation level.

3）The application of distributed and cache mechanism is an effective technique to reduce the pressure of network traffic.

4）The design of the system should provide and consider the temporary working mode of network failure under extreme circumstances, and provide services for the critical business under extreme circumstances, thus reducing the operation risk of the whole system.

（3）System network security risk

Whether the network architecture of the power Internet of Things card and infrastructure resources security supervision platform is designed according to the security architecture and security mechanism is directly related to the security guarantee ability of the network platform. The main security risks of the system host network include the structural risk of the network, the intrusion of the network boundary, the attack of the malicious code such as the virus inside the network, and the illegal use of the network equipment.

Network structural risks mainly include whether the network bandwidth can meet the business requirements, whether the service processing capacity of the network equipment can meet the current and foreseeable business requirements, whether the network segment division is correct, whether the network routing Settings are reasonable, and whether the network equipment is

redundant. Although the system is located in the information network of the power company, the main station of the system will still be attacked by viruses, Trojans and other malicious software, and there will even be internal hacker attacks, which can seriously affect the performance of the system at light, or even paralyze the system at heavy, and also greatly increase the risk of sensitive information leakage. As the backbone facilities of the system master station, the network equipment will seriously threaten the normal operation of the system if it is logged in illegally and modified.

Countermeasures:

1）System network boundary security protection is to formulate the corresponding security measures to standardize and guide the system and other systems through the network data exchange security requirements.

2）The security protection of the interface between the security supervision platform of the power Internet of Things card and infrastructure resources and the operators is mainly realized through the security isolation device to ensure the security of the exchanged data.

5 The platform architecture

The architecture of the power Internet of Things card and infrastructure resources security supervision platform is divided into three layers, as shown in the figure below.

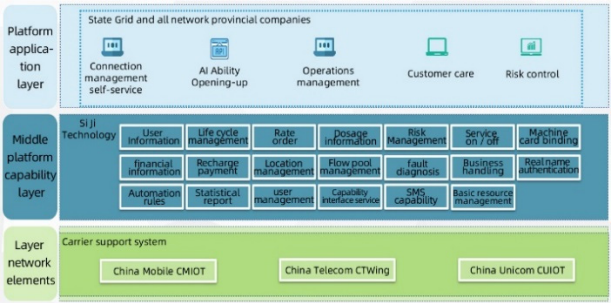

Figure 1. Architecture diagram of the security supervision platform for power Internet of Things card and infrastructure resources1

5.1 Layer network elements

Electric power network card and infrastructure resources security regulatory platform main data and service support from three carriers iot management platform, CTWing CMIOT such as China mobile, China telecom, China unicom CUIOT platform, mainly for its Internet card implementation: total life cycle management, connection, diagnostic ability, risk control and prevention and treatment management, open interfaces, and other functions.

5.2 Ability to middle layer

The platform capability is managed by Sciki Technology for the power Internet of Things card and infrastructure resources, which is mainly divided into 10 categories and 23 subcategories. The specific classification is shown below.

Information overview: mainly includes card information management, communication services, flow pool management and other subclasses;

Life cycle management: it mainly includes card information statistics and management in multiple cycles, such as test period, inventory period, pending activation period, activation period, shutdown period, pre-closing account period and closing account period.

Intelligent services: mainly include terminal management, intelligent diagnosis, automation rules and other subcategories;

Risk prevention and control: mainly includes risk analysis, prevention and control measures and other subcategories;

Fee management: mainly includes enterprise fee, group fee, single card fee, fee opening and other subcategories;

Accounting management: mainly includes corporate bills, single card bills, balance query and other subcategories;

Statistical analysis: mainly includes single card usage statistical analysis, group usage statistical analysis, enterprise usage statistical analysis and other sub categories;

System configuration: mainly includes group setting function;

Basic resource management: It mainly includes a panoramic overview of basic resources such as poles and towers, channels and optical cables, and subcategories such as resource management;

Extended capabilities class: mainly contains API integration capabilities.

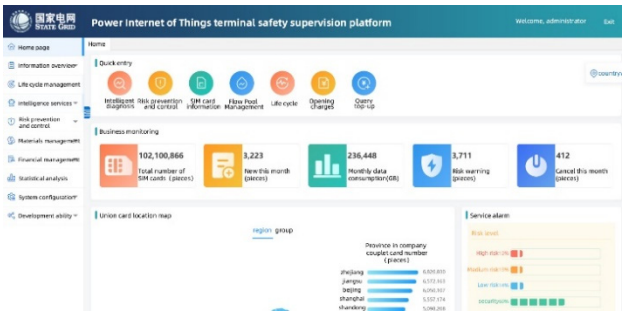

Figure 2 Interface Diagram of Safety Supervision Platform of Electric Internet of Things Terminal

5.3 Platform application layer

The application layer of the platform mainly refers to the relevant value-added services that the platform can provide to China Net, provincial network companies and exclusive industries, such as self-service of connection management, API capability opening, operation management, customer guarantee, risk control and other functions, so as to meet the needs of customers for independent management to a certain extent.

6 Platform features

6.1 Self-service management class functions

Card information management: query the basic information of Internet of Things card, such as card number, ICCID, account opening date, network type, card status, real-time consumption, cycle consumption, etc. Inquire and edit the device information bound by the Internet of Things card, such as device type, device name, device code, unit of ownership, etc., and support the batch import and export of relevant information;

Communication service: it mainly refers to the on-off and off-off of communication service, which supports the on-off and off-off functions of card level, grouping level, region level, device type and other dimensions that can be customized;

Fee management: check the subscription of enterprise, group, Internet of Things card and other dimensions, and can order or change the subscription according to the needs of users.

Accounting management: conduct enterprise history bill query, real-time bill query, list display of bill items, real-time query of single card history bill information and single card detailed list on the platform, which is convenient for users to check accounts.

6.2 Intelligent management class functions

Lifecycle management is specifically divided as shown in Table 1 below.

Table 1 Life cycle of power Internet of Things card and security supervision platform of infrastructure resources

THE LIFE CYCLE	PERIODIC STATE
The test period	Free to provide users with test flow, test SMS (specific test package selected by the user shall prevail), used for the normal and connectivity test of the user's equipment, the data and SMS beyond the free part will be calculated at the normal rate. The SIM card in the testable period provides a cycle choice of 1-9 months, and will automatically enter the next life cycle state after expiration. Users can also manually switch the life cycle state
The inventory period	The behavior of the SIM card in the inventory state is similar to that in the defunct state. It is used for long-term storage after the normal function test is completed. If the card is to be used normally, the management platform must change the card state to the active state; During the pending activation period, the SIM card only turns off the billing function, and the communication function is normal. The automatic activation principle of the first call bill is followed, which means it will be automatically activated when Internet surfing or SMS occurs
To activate period	The SIM card to be activated only turns off the billing function and the communication function is normal. The SIM card to be activated automatically will be activated when Internet surfing or SMS occurs according to the principle of automatic activation of the first call bill. During the activation period, the SIM card is used normally in accordance with the predetermined package charges
The activation period	Activation period SIM card is normal use SIM card, according to the predetermined package rates for use; Downtime: the SIM card will stop automatically after overdue payment for a period of time, or the user can initiatively change the shutdown status to shutdown
Outage period	The SIM card will stop automatically after overdue payment for a period of time, or the user can initiatively change the stop status to stop
Advance cancel account period	After three months of shutdown (the time can be configured), the pre-closed account will automatically enter the pre-closed account state, and the pre-closed account SIM card will be in the inactive state
Account closing period	After the expiration of the reservation period, the SIM card for the pre-cancellation account is cleared of data and number collection, and completely erased from the network

（2）Flow pool management: for the opened flow pool or flow sharing pool, users can manage SIM cards by themselves, flexibly add and exit the SIM cards in the pool, set the dosage threshold of the SIM cards in the pool, carry out automatic monitoring and management, and support the corresponding operation to take effect the next day and the next month.

（3）Automatic rules: Automatic rules help users to realize automatic monitoring and operation of the card. Users can set the rules. When the IoT card meets a certain rule, the operation specified by users will be automatically executed. Have card condition monitoring can be set up

monitoring rules (activation, downtime, abnormal shutdown state), communication class monitor (text messages, an abnormal links), dosage of real-time monitoring (package dosage, dosage of flow pool, single card usage, dosage of grouping, unit consumption and so on multi-dimensional monitoring), dosage of historical monitoring (day, week, month and year history dosage monitoring).

（4）Intelligent diagnosis: fault diagnosis is carried out from the following five aspects. Service order, confirm whether SIM card GPRS service is enabled; Card status, confirm whether the SIM card is in shutdown state; Network connection: detect the SIM card's online status within a cycle (1 week /1 month /3 months) and evaluate whether the device can be connected to the wireless network; When the terminal is started, confirm whether the terminal equipment is in the starting state; The communication status checks whether the device has or has previously had a successful session to assess whether the device can interact with the client server.

（5）Data analysis: provide real-time and statistical consumption from a multi-dimensional perspective, help provincial companies to grasp the trend of consumption, and then provide guidance for the development of business operations. It can realize multi-dimensional statistical analysis of real-time consumption and historical usage statistics of single card, real-time consumption and historical usage statistics of flow pool, implementation consumption and historical usage statistics of package, real-time consumption and historical usage statistics of use unit, etc.

6.3 Risk prevention and control functions

（1）Real-name authentication: the enterprise-level real-name authentication requires the provision of business license and other information, as well as the user and responsible person information, so as to prevent the SIM card from being used in illegal ways and unable to make judgment and accountability, and support the user and responsible person change.

（2）Machine card binding: support SIM card to IMEI (International Mobile Device Identity Code) and UDID (Unique Device Identity Code) for unique binding, unbinding and re-binding. When the machine card is separated, SMS or email will be sent to inform the relevant user or responsible person to confirm the maintenance operation or abnormal operation. If it is abnormal operation, it will stop automatically. If it is for maintenance operation, but it causes shutdown, it can apply for restart operation. Support machine card binding history tracking, machine card separation daily statistics and analysis.

（3）Regional restrictions: set the SIM card with province, city, county, or even base station as the unit of regional control authority. When the SIM card is found to leave the restricted area, it will be shut down immediately or restricted to use, so as to ensure the safe use of the card. Support zone limit change application for card, as well as restart application.

（4）Speed limit: Support to set the daily, weekly or monthly usage limit of a single SIM card or flow pool, etc. If the SIM card flow is abnormal and exceeds the normal usage, the card can be limited or shut down. Support card speed limit resume application, as well as resume application.

6.4 Expand the capabilities category

（1）Terminal management: monitor whether terminal equipment is in abnormal state through SIM card state monitoring. If abnormal state is found, notify relevant user or responsible person through SMS or email, timely maintain the equipment and restore the normal working state of the equipment.

（2）API integration: due to the data and functional service needs of the platform, it integrates the interface of the Internet of Things management platform of the three major operators upward to meet the requirements of data acquisition and functional realization of the platform. Open query and handling capability interfaces to State Grid Corporation, provincial network companies and user units, and can be customized according to user needs.

7 Platform architecture

7.1 The overall architecture

The operation management platform adopts the multi-layer technology architecture based on J2EE to improve the flexibility, scalability, security and concurrent processing ability of the system. At the same time, it realizes the data interaction with the three major operators through the unified data interface.

The multi-layer operation management platform adopts component technology to separate the interface control, business logic and data processing, and realize the loose coupling within the system, so as to respond flexibly and quickly to the demands of business changes on the system. Technically, it is divided into the presentation layer, application layer, public component layer, support layer and data layer. It interacts with the three major operators through external interfaces, and realizes system functions through the service relationships among system components at all levels. The specific content is shown in the figure below.

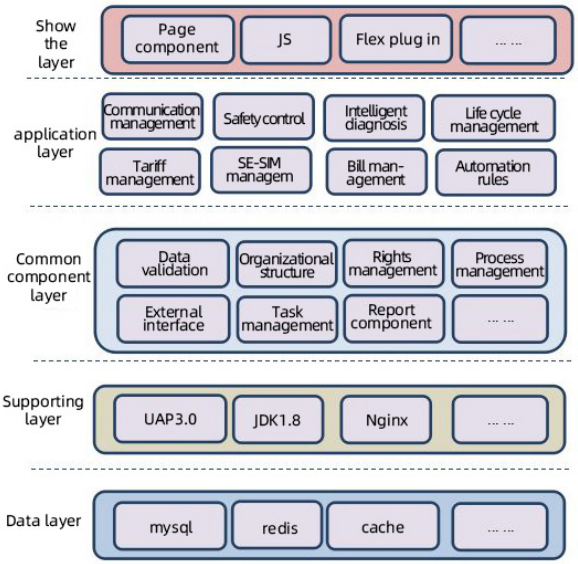

Fig. 3 Infrastructure architecture of the security supervision platform for power Internet of Things cards and infrastructure resources

Presentation layer: the front and rear end separation technology is adopted. Specifically, it is realized through Java EE technology system and MVC application framework, which is composed of interface controller component, interface operation component, Flex component, JSP webpage component and service agent unit. The display of the interface is completed by Flex component and JSP web component; the specific operation on the web page is completed by the interface operation component calling the specific service of the business logic layer through the service proxy unit; the interface controller component is responsible for calling different interface operation components, Flex component and JSP web component uniformly. To some needs the interface special display effect business, can establish the special FLASH processing.

Application layer: The application layer is to realize specific business applications, reorganize data sources of data layer from the perspective of business users, and provide them to the presentation layer for use.

Public component layer: the public component layer is built on the Java platform, and provides the common service interface components required by the operation and management platform with the help of the middleware and the interface services of the third-party service providers. Through the service layer, the logic needed can be rationalized, through the coordination of models, specific application services, and workflows.

Support layer: The support layer is composed of UAP3.0 platform, JDK1.8, NGINX and other components to support the business layer and the public component layer.

Data layer: The data layer is composed of data mapping layer and data source. The data mapping layer completes the access encapsulation of data source and makes the design and implementation of the business logic layer more focused on the functions of the system itself. At the same time, the existence of the data mapping layer shielded the dependence of the business logic layer on the underlying data storage form, so that the application system can adapt to various types of databases. Data sources mainly include: database, memory data, message queue and so on.

7.2 Physical framework

The operation management platform is deployed in the way of "one-level deployment and multi-level application" by the headquarters. The platform is deployed in the platform service provider, and the role personnel such as State Grid, province, city and county can access the platform application. The specific deployment architecture is shown in Figure 4 below.

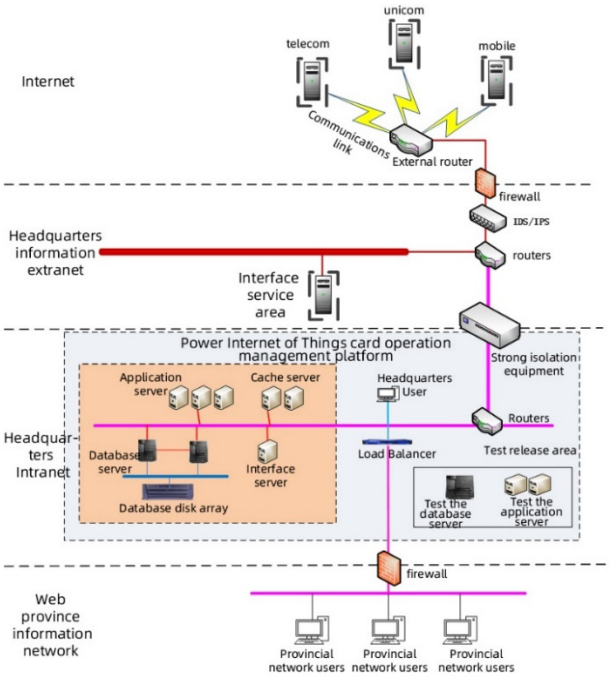

Fig. 4 Physical framework of the security supervision platform for the power Internet of Things card and infrastructure resources

7.3 Safety framing

7.3.1 Architecture design

System security shall follow the company's overall information security strategy, and the security protection intensity shall meet the company's internal network security protection standard; Safety protection pays attention to operation safety to avoid the spread of safety risks.

System security needs to be managed from network protection, user authentication and authority management, data storage, computer room environment and management system.

(1). Network security

The operation management platform runs in the company's information Intranet and needs to rely on the company's unified security protection system and measures. The access to mobile terminals and videos

should follow relevant State Grid security regulations.

(2). Application security

Application security protection from identity authentication, authorization, input and output verification, configuration management, session management, code security, encryption technology, parameter operation, exception management, audit and log, residual information protection, data storage confidentiality, data storage integrity, backup and recovery of application data and other aspects of security protection.

(3). Data security

Business data is the basis of the normal operation of the system, and the confidentiality, integrity and availability of business data in transmission, processing and storage must be ensured.

1）Key sensitive data should be achieved: login authentication, strict authorization, transmission encryption, real-time data backup;

2）Authentication must adopt strong authentication, such as digital certificate, one-time password, etc.

3）Adopt strict authorization management to protect data and programs from arbitrary tampering by unauthorized users;

4）When data is no longer needed, it should be safely deleted, destroyed or disposed of. It should not be arbitrarily placed because the data is outdated;

5）It can detect whether the integrity of business data is damaged in the process of processing, transmission and storage.

(4). System security

System security mainly refers to the security of the platform, including operating system, middleware, database system security. Choose relatively secure operating systems, middleware and database systems, and prohibit default and weak passwords; The system files are effectively protected to prevent tampering and replacement.

Install the network virus prevention server on the system network, install the network virus prevention software on the internal network server, install the anti-virus software on the single computer environment, and regularly update the virus library.

(5). Physical security

The physical operation environment involved in the operation management platform mainly includes application server, load balancer, etc. The requirements for the computer room environment generally follow the standards of the State Grid Corporation on the computer room construction.

(6). Terminal security

Terminal security protection requires that the identity of the logged in user is real, to ensure the safety of the website terminal data transmission to the server: to ensure the confidentiality, integrity and non-repudiation of the data. Depending on the user type, login authentication is performed in a variety of ways: user name, password, and digital certificate authentication. Registered users can be divided into two categories according to security requirements: business personnel and system administrators. This is shown in the following table.

Table 2 Safety protection types of power Internet of Things card and infrastructure resources safety supervision platform

USER TYPE	MAIN BUSINESS	PROTECTIVE MEASURES
Business person	Business management, business parameter configuration, data statistics, etc	Safety reinforcement of the terminal; Install anti-virus software to prevent virus from harming the terminal; Install terminal safety check software to ensure the health of the access terminal; Encrypt transmission of key and sensitive information; Access to the Internet is strictly prohibited when conducting business in the information Intranet; Conduct security audits of business operations.
System administrator	System management, system parameter configuration, log management, system maintenance, etc	Install anti-virus software to prevent virus from harming the terminal; Install terminal safety check software to ensure the health of the access terminal; Install the safe communication module and establish the safe communication channel; Install the host behavior control system, based on the mandatory operation control (MRC) technology, to provide multi-level website security access protection, from the terminal behavior process to ensure the safe access to the website; Access to the Internet is strictly prohibited when conducting business in the information Intranet; Conduct a security audit of the operation.

(7). Border security

The border security protection includes the security protection of the third party boundary of the information extranet, the third party boundary of the information internal and external network, the boundary of the information internal network of the headquarters and the provincial (municipal) company. The details are shown in the following table.

Table 3 Border security measures of the security supervision platform for the power Internet of Things card and infrastructure resources

THE BORDER	DESCRIBE	CONTROL MEASURES
Information extranet third party boundary	And the Internet	Deploy two firewalls (Internet boundary firewall and information extranet boundary firewall) to effectively block security threats from the Internet; Intrusion detection system and vulnerability scanning system are used to detect and filter illegal access and attacks from the Internet. Deploy the external network security access platform to conduct user identity authentication and website business access control
Information Intranet Third Party Boundaries	Boundaries with other business systems on the Intranet	Access control is carried out by firewall
Information Intranet Boundaries	The boundary between the Web server and the database	Deploy isolation device to ensure that the information outer network does not directly connect to the information inner network; The logic strong isolation device is used to realize the safe interaction of information. According to the "General Project Security Protection Plan of SG186" of State Grid Corporation of China, the access control of third-party business is carried out by firewall.
Headquarters and network province	The boundary between the provincial Intranet and the headquarters Intranet	Access control is carried out by firewall

(8). The safety management

The operation management platform needs to interact with other business systems in terms of data and interface. There are risks of security risk proliferation and amplification at all levels such as network, system, data and application, and new security vulnerabilities are formed. Therefore, security assessment should be carried out before access, and only after security reinforcement is allowed to formally put into operation.

The system should avoid the access and link of any unit, personnel and system without security assessment or formal permission, especially the emergency and temporary access should be monitored, and the high-risk access mode should be avoided to lead to the system security accident. Developers, operation and maintenance personnel should formulate working norms and working procedures for system operation, and monitor and audit the operation that violates the norms and working procedures, so as to reduce man-made safety accidents.

7.3.2 Policy support

The security architecture design complies with the "State Grid Corporation Network and Information System Security Management Measures", which mainly involves the following clauses:

（1） Article 22. The admittance work for information security archival filing shall be strengthened. All levels of units to consolidate the information security record access results, strengthen the collection terminal security record, strict information assets security record as a necessary condition for access to the network.

In compliance with this provision, Internet data access to the power information Intranet needs to be filed with the communication administration department.

（2） Article 23 Requirements for Security Management of New Businesses such as Weibo and WeChat Article 4 Units at all levels shall control the number of special lines for the third-party special lines of the internal network to access the company's information network. For new businesses that really need third-party access, they shall choose a safe access mode and strengthen the implementation of border security protection measures.

In accordance with the provisions of this article, the section of boundary security in the security architecture design has made detailed explanation on the security protection of the third party boundary of the information extranet, the boundary of the information extranet, the boundary of the headquarters and the boundary of the network province.

（3） Article 24 Access security management requirements Article 1 Strengthen the centralized administration of Internet access and Internet exports, make full use of the company's power communication links, and strictly control, merge, unify and monitor the Internet exports of the subordinate units with the provincial units and the three local disaster recovery centers as the main body.

In accordance with the provisions of this article, the channel designed in the physical architecture is to reuse the existing power communication network, and security measures are set according to the power system security protection requirements.

（4） Article 29 the network security technology requirements 6 To strengthen the security of information inside and outside the net line, for Banks and other external units of the Internet, dedicated to deploy strong logic isolation measures, set up the access control policy, monitoring and auditing of the contents, allow only the specified, trusted network, and users can exchange data.

In compliance with this provision, the boundary

security information in the design of the security architecture has been included in the design of the internal and external network boundary logical strong isolation devices

7.4 Project Implementation Steps

The whole project was carried out in the following steps: platform functional demand investigation, overall technical plan formulation, software platform functional research and development, platform interface development, platform deployment and testing.

（1）Research on platform functional requirements

Conduct in-depth investigation on the functional requirements of the operation management platform, clarify the functional requirements of each module, and form the "Platform Functional Requirements Manual".

（2）Formulate the overall technical plan

According to the preliminary investigation and demand documents, the detailed design, functional design and definition of the system were carried out, and the formulation and planning of technical schemes were carried out.

（3）Software platform development

According to the requirement specification and technical scheme, carry out the research and development of each function module of the system, start the specific programming work, respectively realize the function of each module, so as to achieve the function, performance, interface, interface and other aspects of the target system requirements.

（4）Platform Interface Development

Develop the platform interface according to the data docking requirements between the platform and the operator.

（5）Platform deployment and testing

With the support of various hardware and software, the platform's various functions are tested to verify the integrity and availability of the platform's functions. The main contents of testing include functional testing, data integrity testing, user interface testing, performance testing, security and control testing, system configuration testing and so on.

8.Business model

8.1 Business model

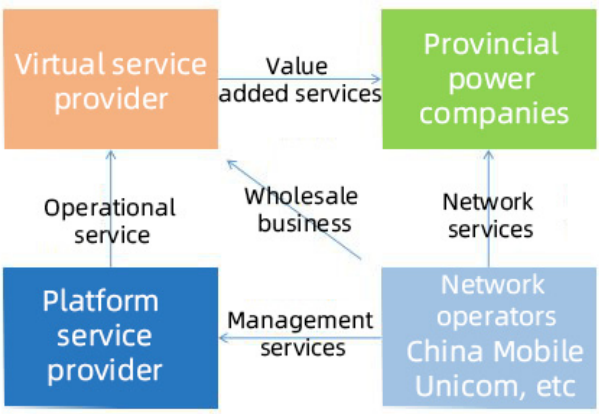

Figure 5 Business model of power Internet of Things card and infrastructure resources security supervision platform

Considering the need for multi-party cooperation in the business operation of the Internet of Things card, it is necessary to integrate all kinds of resources, technologies and talents advantages of card merchants, operators and terminal equipment manufacturers inside and outside the system, give full play to the company's overall management ability, market promotion and communication network operation ability, and jointly build a harmonious operation ecological environment with all parties.

As a certificate service provider, the platform service provider provides card vendors with key issuing, filling and certificate certification services of the Internet of Things cards. The Internet of Things cards used in various professional scenes of State Grid Corporation need to carry out key-related services through our company.

The platform service provider, as the management service provider of the Internet of Things card, applies the operation and security management platform to provide users with relevant operation and maintenance services of the Internet of Things card, such as status monitoring, traffic monitoring, charge management, security monitoring, etc., and centralized control and display of the Internet of Things card of each network province.

Through the unified operation of the national network, the virtual operation service provider provides more economical, more suitable and more secure wireless traffic operation service of the Internet of Things for power users.

As the provider of network channels and network traffic, the three major operators, on the one hand, should ensure the security of the wireless network channels, on the other hand, they should provide our company with network traffic wholesale, as well as the transfer of relevant data such as the status, traffic and charges of the Internet of Things card.

As the terminal equipment provider for the construction of the electric Internet of Things, the terminal equipment manufacturers should, on the one hand, ensure the security of the equipment itself, do a good job of binding the Internet of Things cards and devices, and carry out cooperation for the future application of embedded Internet of Things cards on devices.

8.2 The business model

8.2.1 To sell CARDS

Carry out mobile resale business cooperation with the three major operators, sign framework cooperation agreement or business contract, in order to obtain the telecom virtual operator qualification, become a telecom virtual operator. At the same time, define the energy Internet of Things card of the power system, customize the storage of the corresponding keys and data in the power system, and store the SIM card data of the three major operators, and sell and promote the Internet of Things card within the scope of the State Grid.

8.2.2 Traffic resale business

Combined with the regional conditions of the companies in each province, the company selects the operator resources with good wireless network quality, excellent service and high economic benefits, and provides customized tariff packages close to various application scenarios such as use and purchase, electric vehicles and distribution network, so as to provide more economical, safer and better operation services for the companies in each province.

8.2.3 Operational business

The Internet of Things card and infrastructure resources safety supervision platform is built on the principle of "who owns the assets, who operates and maintains", and is divided according to the main body of the assets to distinguish the operation and maintenance interface. Through business integration with operator operation support system and business support system, communication business data can be seen, managed and controllable. It provides unified display of wireless applications of the whole network for all provincial companies and realizes centralized query and statistical analysis of data of business platforms in each province, including functions such as traffic, charge management, IP address management, fault discovery and unified display. The security service platform provides the corresponding encryption and decryption ability and signature verification ability, as well as the corresponding secret key management, card authentication and other basic services. The final realization of real-time perception, instant access, agile response.

8.3 Conclusion

This paper takes the Internet of Things card and infrastructure resources safety supervision platform for power as the research object, and discusses the business model and platform construction of the Internet of Things card and infrastructure resources safety supervision under the background of energy Internet. The main research conclusions are as follows: ① power network card and infrastructure resources need to follow the national safety regulation platform construction and SGC strategic target, both need to meet the national difference development trend direction, and need to meet the requirement of the current social and economic development, the platform construction as a key support to the economic transformation. ② In the critical period of current social development and reform, business model innovation has been promoted to a more important position. As one of the innovation capabilities of enterprises, business model innovation should constantly focus on and promote the development of innovation capabilities, and take greater driving force reform as the new growth point of enterprise and business development. ③ New digital infrastructure is the core content of the new national infrastructure development strategy, and it is a strong driving force to lead China's scientific and technological innovation and development to the forefront of the world. Under the background of energy Internet, the security supervision platform of power Internet of Things card and infrastructure resources centers on the actual needs of State Grid Corporation, and provides valuable experience for State Grid Corporation to carry out wireless operation business and stride forward to energy Internet through customized services.

reference

1. National People's Congress, 2020 Government Work Report of the State Council[R]，2020.
2. Cui Jing, New Digital Infrastructure: Empowering a Beautiful China[J]，North China electric power，2020（6）:78-80.
3. Hui Xu, Juli Digital New Infrastructure[J]，Electrical appliance industry，2020（9）:48.
4. Electronic Information Institute of CCID Think Tank, "new infrastructure" ignites a new engine of industrial power[J]，Chinese industry and informationization，2020（3）:68-76.