(19)

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

(11) N° de publication : **LU504593**

(12) **BREVET D'INVENTION** **B1**

(21) N° de dépôt: LU504593

(22) Date de dépôt: 27/06/2023

(51) Int. Cl.:
H04L 9/40, H04L 12/46, H04L 67/12

(30) Priorité:
11/04/2023 CN 202310382600.8

(43) Date de mise à disposition du public: 09/01/2024

(47) Date de délivrance: 09/01/2024

(73) Titulaire(s):
HUANENG NINGXIA ENERGY CO., LTD. – 750000 Yinchuan City, Ningxia (China), YANCHI ZHONGYING CHUANGNENG NEW ENERGY CO., LTD. – 750001 Yinchuan City, Ningxia (China)

(72) Inventeur(s):
YAN Liang – China, XU Jianguo – China, WANG Guizhong – China, CHEN Xingyu – China, LIU Mingchun – China, GAO Xin – China, MA Liang – China, CAO Naihong – China, JI Xuehai – China, ZHANG Xinyong – China, XI Jianlin – China, YANG Zhenyong – China, WU Hua – China, TONG Yan – China, SHI Zhengpu – China, WANG Lixing – China, ZHAO Junhong – China

(74) Mandataire(s):
IP SHIELD – 1616 Luxembourg (Luxembourg)

(54) **Method for deploying longitudinal encryption and authentication device in electrical power system.**

(57) The invention relates to a method for deploying longitudinal encryption and authentication device in electrical power system, and the method includes the following steps: removing a firewall and adjusting an original network; configuring a first longitudinal encryption and authentication device; accessing the first longitudinal encryption and authentication device between a remote terminal unit and a router; modifying and improving the strategy of the first longitudinal encryption and authentication device; accessing a second longitudinal encryption and authentication device between a power management unit and the router; and installing a third longitudinal encryption and authentication device in the plant. According to the invention, the longitudinal encryption and authentication device creates a virtual private network tunnel to transmit service data and encrypt, so as to ensure the relative security of the power grid.

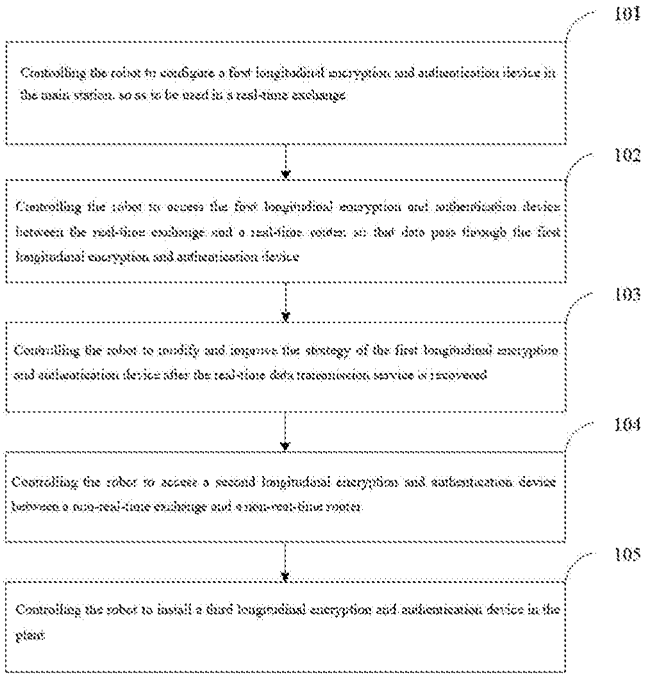
101
Controlling the robot to configure a first longitudinal encryption and authentication device in the main station, so as to be used in a real-time exchange
102
Controlling the robot to access the first longitudinal encryption and authentication device between the real-time exchange and a real-time router so that data pass through the first longitudinal encryption and authentication device
103
Controlling the robot to modify and improve the strategy of the first longitudinal encryption and authentication device after the real-time data transmission service is recovered
104
Controlling the robot to access a second longitudinal encryption and authentication device between a non-real-time exchange and a non-real-time router
105
Controlling the robot to install a third longitudinal encryption and authentication device in the plant

Fig 1

Method for deploying longitudinal encryption and authentication device in electrical power system

Technical field

The invention relates to the technical field of electrical power dispatching automation, in particular to a method for deploying longitudinal encryption and authentication device in electrical power system.

Background technology

Smart grid dispatching control system has a large number of data transmission service scenarios. With the technical progress and service development of power grid, the functions of smart grid dispatching control system are becoming increasingly powerful, and all kinds of applications show the characteristics of complexity and diversification in data communication, specifically, a large amount of data transmission, diverse data acquisition methods, high real-time data interaction, and high safety and reliability requirements for data communication. In order to meet the needs of power grid development, it is urgent to study the data transmission technology of smart grid dispatching control system.

At present, the EMS system of power grid dispatching is protected by firewall; the longitudinal encryption gateway has the security filtering function of firewall, thus it can be used to replace the firewall.

In the electrical power system network, the local network of each level of power dispatching company is usually divided into four different areas based on the different types of data services, namely, control area, production area, production management area and management information area; the four areas are named from work area to V area in turn. The control area, production area and production management area have service exchange and transmission with each other, while the management information area basically has no service exchange with the other three areas. Based on this feature, the deployment of safety protection equipment and facilities in power secondary system is usually based on the principle of "layering and zoning, boundary strengthening" and the strategy of "horizontal isolation and longitudinal protection"; the deployment stipulates that the data communication between longitudinal I/II areas (i.e., control area and production area) should be protected by longitudinal encryption equipment.

Summary of the invention

In order to solve the problem of power grid dispatching safety protection, the invention provides a method for deploying longitudinal encryption and authentication device in electrical power system.

The invention provides a method for deploying longitudinal encryption and authentication device in electrical power system, and the longitudinal encryption and authentication device creates a virtual private network tunnel to transmit service data, so as to connect the upper-level and lower-level power dispatching centers; the method comprises the following steps:

S101, configuring a first longitudinal encryption and authentication device in the main station, so as to be used in a real-time exchange, and powering-on;

S102, accessing the first longitudinal encryption and authentication device between the real-time exchange and a real-time router, so that data pass through the first longitudinal encryption and authentication device;

S103, modifying and improving the strategy of the first longitudinal encryption and authentication device after the real-time data transmission service is recovered;

S104, accessing a second longitudinal encryption and authentication device between a non-real-time exchange and a non-real-time router;

S105, installing a third longitudinal encryption and authentication device in the plant.

Wherein, before the first longitudinal encryption and authentication device is powered on, the strategy is configured as full release; the network cable is disconnected during power-on.

Wherein, in S104, if the service operation is not recovered for a long time (30s), the network is disconnected, the real-time exchange is reconnected to the router, and then diagnosis is made.

Wherein, the full release rule in the strategy of the first longitudinal encryption and authentication device is deleted, and then the affected situation of the services is obtained and checked until all services are normal.

Wherein, the link strategy of the second longitudinal encryption and authentication device is configured with reference to the first longitudinal encryption and authentication device; in S105, before the second longitudinal encryption and authentication device is accessed, a heartbeat line is connected first, and then network cables corresponding to other network ports are connected. After the second longitudinal encryption and authentication device is accessed, exchange between master device and standby device is conducted, the network cable of the first longitudinal encryption and authentication device is unplugged, and the second longitudinal encryption and authentication device operates as a master equipment to recover service operation.

Wherein, the real-time exchange is a remote terminal unit (RTU exchange); the non-real-time exchange is a phasor measurement unit (PMU exchange).

Wherein, in step 6, the third longitudinal encryption and authentication device is installed at the front end of the router in the plant.

Wherein, in step 6, the third longitudinal encryption and authentication device is installed at the back end of the router in the plant.

The invention has the beneficial effects that the longitudinal encryption and authentication device creates a virtual private network tunnel to transmit service data, so as to connect the upper-level and lower-level power dispatching centers. The power private network includes two major network systems: power dispatching data network and power data communication network. Wherein, the power dispatching data network consists of routers, exchanges, longitudinal encryption and authentication devices and other equipment. The longitudinal encryption and authentication device is deployed in a single-link port of the exchange to encrypt all service data collected by the exchange, the encrypted data are forwarded to the interconnection port of the router, and then the router forwards the data to the power private network through the designated route, thus realizing the confidentiality and integrity protection of data transmission; besides, the longitudinal encryption device also realizes the conversion function of the application layer communication protocols (IEC-104, DL476-92, etc.) of power private network, so as to realize point-to-point selective protection. According to the requirements of private network management of power system, longitudinal encryption equipment must be deployed in the central station and all substations under its jurisdiction, and corresponding encryption tunnels should be established according to the dispatching relationship in this jurisdiction, so as to realize the encryption transmission of the whole communication link data; usually, each longitudinal encryption device is deployed as a mesh network. By deploying the longitudinal encryption and authentication devices, the application program in the smart grid dispatching control system can realize horizontal cross-regional transmission, and support the data interaction between dispatching centers at all levels, thus meeting the requirements of the smart grid dispatching control system to share data in a wide area in multi-level dispatching control centers, and preventing hackers from invading and improving the security performance.

Description of attached drawings

Fig. 1 is a flowchart of a method for deploying longitudinal encryption and authentication device in electrical power system according to Example 1 of the invention;

Fig. 2 is a schematic diagram of a specific example of the deployment of longitudinal encryption and authentication device in electrical power system of the invention;

Fig. 3 is a schematic diagram of the deployment of the longitudinal encryption and authentication device in electrical power system according to Example 1 of the invention;

Fig. 4 is a schematic diagram of the deployment of the longitudinal encryption and authentication device in electrical power system according to Example 2 of the invention.

Specific embodiments

In the following description, numerous details are set forth to facilitate a thorough understanding of this specification. However, this specification can be implemented in many other ways different from those described here, and those skilled in the art can make similar promotion without violating the connotation of this specification, so this specification is not limited by the specific examples disclosed below.

Terms used in one or more example (s) of this specification are for the purpose of describing specific examples only and is not intended to limit one or more example (s) of this specification. The singular forms "a" and "the" used in one or more example (s) of this specification and the appended claims are also intended to include the plural forms, unless the context clearly indicates other meaning. It should also be understood that the terms "and/or" used in one or more example (s) of this specification refer to and include any or all possible combinations of one or more associated listed item (s).

It should be understood that although the terms first, second, etc. may be used to describe various information in one or more example (s) of this specification, these information should not be limited to these terms. These terms are only used to distinguish the same type of information from each other. For example, without departing from the scope of one or more example (s) of this specification, first can also be called second, and similarly, second can also be called first. Depending on the context, the word "if" as used herein can be interpreted as "in case that" or "when" or "in response to a determination".

In the electrical power system network, the local network of each level of power dispatching company is usually divided into four different areas based on the different types of data services, namely, control area, production area, production management area and management information area; the four areas are named from work area to V area in turn. The control area, production area and production management area have service exchange and transmission with each other, while the management information area basically has no service exchange with the other three areas. Based on this feature, the deployment of safety protection equipment and facilities in power secondary system is usually based on the principle of "layering and zoning, boundary strengthening" and the strategy of "horizontal isolation and longitudinal protection"; the deployment stipulates that the data communication between longitudinal I/II areas (i.e., control area and production area) should be protected by longitudinal encryption equipment.

Longitudinal encryption, as the name implies, generally means that the superior power dispatching center is connected with the subordinate power dispatching center, and then the longitudinal encryption and authentication device creates a vpn tunnel to transmit real-time and non-real-time service data; once the service data are encrypted (there are two commonly used algorithms at present, rsa and sm2), hackers cannot crack the message even if they get it, because the encryption and decryption public keys and the private keys at both ends of the tunnel are in one-to-one correspondence, thus ensuring the relative security of the power grid. Therefore, the actual physical object corresponding to longitudinal encryption is the longitudinal encryption and authentication device, and the longitudinal encryption and authentication device is generally used in power plants, photovoltaic power plants and wind farms.

In the description of the invention, a method for deploying longitudinal encryption and authentication device in electrical power system is provided. The power grid dispatching system is protected by firewall; the longitudinal encryption gateway has the security filtering function of firewall, thus the firewall shall be closed first before deployment and then replaced by the longitudinal encryption and authentication device.

Fig. 1 shows a flow chart of a method for deploying longitudinal encryption and authentication device in electrical power system according to examples of this specification, and the method includes:

101, configuring a first longitudinal encryption and authentication device in the main station, so as to be used in a real-time exchange, and powering-on;

102, accessing the first longitudinal encryption and authentication device between the real-time exchange and a real-time router, so that data pass through the first longitudinal encryption and authentication device;

103, modifying and improving the strategy of the first longitudinal encryption and authentication device after the real-time data transmission service is recovered;

104, accessing a second longitudinal encryption and authentication device between a non-real-time exchange and a non-real-time router;

105, installing a third longitudinal encryption and authentication device in the plant.

Specifically:

The first longitudinal encryption and authentication device needs to be configured offline, and the strategy should be set as full release first; the first longitudinal encryption and authentication device configured offline is powered on, with the network cable not connected at this time; the first longitudinal encryption and authentication device is accessed between the RTU exchange and the real-time router, and the connection between the PMU exchange and the non-real-time router is disconnected, so as to ensure that the data pass through the first longitudinal encryption and authentication device.

The recovery situation of the network service (generally, the recovery time is 30s) is observed. If the network service is not recovered for a long time, the first longitudinal encryption and authentication device is disconnected from the network, the RTU exchange is reconnected to the router, and then diagnosis is made. If the network service is recovered, the operation of the service is observed for a period of time, and then the following steps are conducted after it is stable.

All the passed links are checked in the first longitudinal encryption and authentication device, and the strategy of the first longitudinal encryption and authentication device is modified and improved according to the link conditions; the full release rule in the strategy of the first longitudinal encryption and authentication device is deleted, the services are observed and then subjected to checking and debugging until all services are normal.

The configuration of the first longitudinal encryption and authentication device is imported into the second longitudinal encryption and authentication device; the second longitudinal encryption and authentication device is installed and powered on, then the heartbeat line is connected first, and then the network cables corresponding to other network ports are connected; the eth0 port network cable of the first longitudinal encryption and authentication device is unplugged (connected back after 5s), at this time, the master equipment and standby equipment are exchanged, and Gigabit B will operate as the master equipment.

Exchange between master equipment and standby equipment may cause interruption of some services, so the recovery and operation of the services need to be observed after the exchange master equipment and standby equipment. If the services are not recovered for a long time after exchange (generally 30s), the second longitudinal encryption and authentication device is disconnected from the network, and then the reasons are checked; if the the services are recovered, more exchange operations are made to ensure absolute normality.

The invention will be described in detail with reference to the attached drawings:

Referring to Fig. 2, it is a schematic diagram of deployment of longitudinal encryption and authentication device in electrical power system in the main station (i.e., the superior power plant) of the invention.

In some specific examples of the invention, two communication gateways are first provided in the main station, and then an exchange is respectively accessed (one is a real-time exchange, and the other is a non-real-time exchange), and a longitudinal encryption and authentication device is deployed between the exchange and the router to replace the security protection function of the original firewall. The data signal is sent to the exchange through the communication gateway, and the signal of the exchange is encrypted by the longitudinal encryption and authentication device and transmitted to the power plant dispatching data network through the router.

Example 1:

Referring to Fig. 3, it is a schematic diagram of deployment of longitudinal encryption and authentication device in electrical power system in the plant (i.e., the subordinate power plant) of the invention.

In some specific examples of the invention, data are sent from the power plant dispatching network, sent by the router to the longitudinal encryption and authentication device for decryption, and then output to the communication gateway in the plant through the exchange to finish receiving the information of superior power plant.

When there is no device in the network, the forwarding paths of receiving and sending messages are inconsistent because the exchange is enabled. In this case, if the standard packet filtering firewall is placed between the router and the exchange, all messages will be discarded, specifically, the request message and the response message sent by the communication gateway cannot reach the same firewall, so they will be discarded as illegal communication. Based on the principle of address borrowing, the longitudinal encryption and authentication device establishes a main tunnel with the remote node device to solve the above problems; the longitudinal encryption and authentication device can support multiple VLANs. Multi-service communication is ensured, with less devices used to be convenient for centralized management.

Example 2:

Referring to Fig. 4, it is a schematic diagram of another deployment of longitudinal encryption and authentication device in electrical power system in the plant (i.e., the subordinate power plant) of the invention.

In some specific examples of the invention, the network environment of the dispatching data network in the main station remains unchanged, as shown in Figure 2. However, in the dispatching data network in the plant, there is no router but only one exchange and two communication gateways, and the longitudinal encryption and authentication device in the plant is deployed between the exchange and the communication gateway. The layout method is flexible and can be applied to various complex environments.

It should be noted that for the sake of simple description, all the aforementioned method examples are expressed as a series of action combinations, but those skilled in the art should know that examples of this specification are not limited by the sequence of described actions, because some steps may be performed in other sequences or simultaneously according to examples of this specification. Besides, those skilled in the art should also know that the examples described in the specification are all preferred examples, and the actions and modules involved are not necessarily necessary for the examples in this specification.

In the above examples, the description of each example has its own emphasis. For the parts not detailed in one example, please refer to the relevant descriptions of other examples.

The preferred examples of this specification disclosed above are only used to help explain this specification. Alternative examples do not describe all the details in detail, and also do not limit the invention to the specific examples described. Obviously, many modifications and changes can be made according to the contents of the examples in this specification. These examples are selected and described in detail in this specification in order to better explain the principles and practical applications of the examples in this specification, so that those skilled in the art can better understand and make use of this specification. This specification is limited only by the claims and their full scope and equivalents.

CLAIMS

1. A method for deploying longitudinal encryption and authentication device in electrical power system comprises the following steps:

controlling the robot to configure a first longitudinal encryption and authentication device in the main station, so as to be used in a real-time exchange;

controlling the robot to access the first longitudinal encryption and authentication device between the real-time exchange and a real-time router, so that data pass through the first longitudinal encryption and authentication device;

controlling the robot to modify and improve the strategy of the first longitudinal encryption and authentication device after the real-time data transmission service is recovered;

controlling the robot to access a second longitudinal encryption and authentication device between a non-real-time exchange and a non-real-time router;

controlling the robot to install a third longitudinal encryption and authentication device in the plant;

wherein, the longitudinal encryption and authentication device creates a virtual private network tunnel to transmit service data, so as to connect the upper-level and lower-level power dispatching centers.

2. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 1, wherein the strategy of the first longitudinal encryption and authentication device is configured as release before powering-up.

3. The method for deploying longitudinal encryption and authentication devices in power system according to claim 1, wherein the link strategy of the second longitudinal encryption and authentication device is configured with reference to the first longitudinal encryption and authentication device.

4. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 1, wherein if the service operation is not recovered after a set time, the network is disconnected, the real-time exchange is reconnected to the router, and then diagnosis is made.

5. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 4, wherein the full release rule in the strategy of the first

longitudinal encryption and authentication device is deleted, and then the affected situation of the services is obtained and checked until all services are normal.

6. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 1, wherein before the second longitudinal encryption and authentication device is accessed, a heartbeat line is connected, and network cables corresponding to other network ports are connected.

7. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 6, wherein after the second longitudinal encryption and authentication device is accessed, the network cable of the first longitudinal encryption and authentication device is unplugged, and the second longitudinal encryption and authentication device operates as a master equipment to recover service operation.

8. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 1, wherein the real-time exchange is a remote terminal unit; the non-real-time exchange is a phasor measurement unit.

9. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 1, wherein the third longitudinal encryption and authentication device is installed at the front end of the router in the plant.

10. The method for deploying longitudinal encryption and authentication device in electrical power system according to claim 1, wherein the third longitudinal encryption and authentication device is installed at the back end of the router in the plant.

REVENDICATIONS

1. Une méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinal dans un réseau électrique comprend les étapes suivantes :

commander le robot pour configurer un premier dispositif longitudinal de cryptage et d'authentification dans la station principale, de manière à ce qu'il soit utilisé dans un échange en temps réel ;

commander au robot l'accès au premier dispositif longitudinal de cryptage et d'authentification entre l'échange en temps réel et un routeur en temps réel, de sorte que les données passent par le premier dispositif longitudinal de cryptage et d'authentification ;

commander au robot de modifier et d'améliorer la stratégie du premier dispositif longitudinal de cryptage et d'authentification après que le service de transmission de données en temps réel a été rétabli ;

commander au robot l'accès à un deuxième dispositif longitudinal de cryptage et d'authentification entre un échange en temps non réel et un routeur en temps non réel ;

commander le robot pour installer un troisième dispositif longitudinal de cryptage et d'authentification dans l'usine ;

le dispositif de cryptage et d'authentification longitudinal crée un tunnel de réseau privé virtuel pour transmettre les données de service, de manière à relier les centres de répartition de l'énergie de niveau supérieur et de niveau inférieur.

2. Méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinal dans un système électrique selon la revendication 1, dans laquelle la stratégie du premier dispositif de cryptage et d'authentification longitudinal est configurée comme une libération avant la mise sous tension.

3. Méthode de déploiement de dispositifs de cryptage et d'authentification longitudinaux dans un système électrique selon la revendication 1, dans laquelle la stratégie de liaison du second dispositif de cryptage et d'authentification longitudinal est configurée en référence au premier dispositif de cryptage et d'authentification longitudinal.

4. Méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinale dans un réseau électrique selon la revendication 1, dans laquelle, si l'opération de service n'est pas rétablie après un certain temps, le réseau est déconnecté, l'échange en temps réel est reconnecté

au routeur, puis un diagnostic est effectué.

5. Méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinal dans un réseau électrique selon la revendication 4, dans laquelle la règle de libération complète dans la stratégie du premier dispositif de cryptage et d'authentification longitudinal est supprimée, puis la situation affectée des services est obtenue et vérifiée jusqu'à ce que tous les services soient normaux.

6. Méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinal dans un réseau électrique selon la revendication 1, dans laquelle, avant d'accéder au deuxième dispositif de cryptage et d'authentification longitudinal, une ligne de battement de cœur est connectée, et les câbles de réseau correspondant à d'autres ports de réseau sont connectés.

7. Méthode de déploiement d'un dispositif longitudinal de cryptage et d'authentification dans un système électrique selon la revendication 6, dans laquelle, après l'accès au deuxième dispositif longitudinal de cryptage et d'authentification, le câble réseau du premier dispositif longitudinal de cryptage et d'authentification est débranché et le deuxième dispositif longitudinal de cryptage et d'authentification fonctionne en tant qu'équipement maître pour rétablir le fonctionnement du service.

8. Méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinal dans un système électrique selon la revendication 1, dans laquelle l'échange en temps réel est une unité terminale distante ; l'échange en temps non réel est une unité de mesure de phasage.

9. Méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinal dans un réseau électrique selon la revendication 1, dans laquelle le troisième dispositif de cryptage et d'authentification longitudinal est installé à l'extrémité avant du routeur dans l'installation.

10. Méthode de déploiement d'un dispositif de cryptage et d'authentification longitudinal dans un réseau électrique selon la revendication 1, dans laquelle le troisième dispositif de cryptage et d'authentification longitudinal est installé à l'extrémité arrière du routeur dans l'installation.

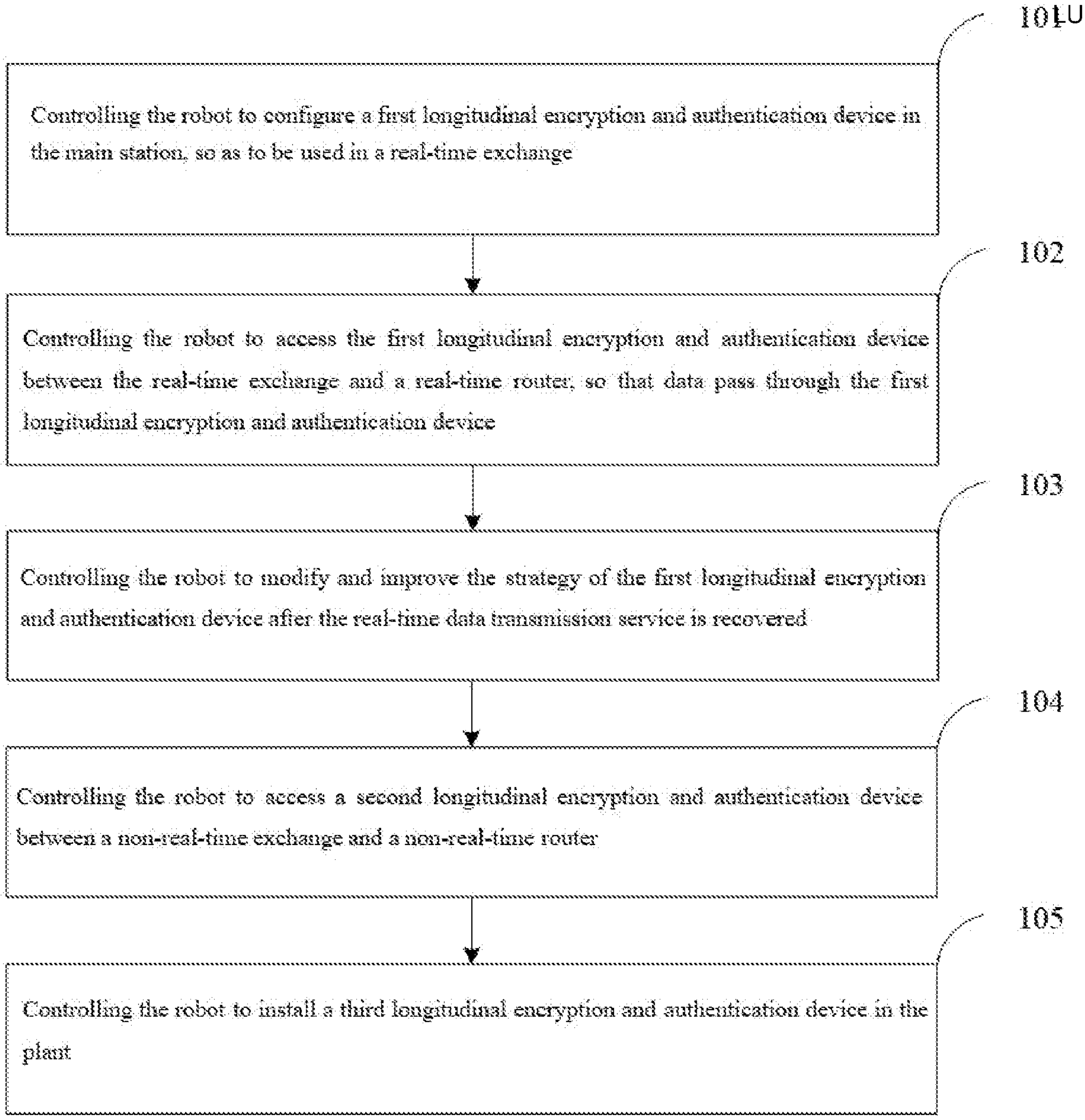
101
Controlling the robot to configure a first longitudinal encryption and authentication device in the main station, so as to be used in a real-time exchange
102
Controlling the robot to access the first longitudinal encryption and authentication device between the real-time exchange and a real-time router, so that data pass through the first longitudinal encryption and authentication device
103
Controlling the robot to modify and improve the strategy of the first longitudinal encryption and authentication device after the real-time data transmission service is recovered
104
Controlling the robot to access a second longitudinal encryption and authentication device between a non-real-time exchange and a non-real-time router
105
Controlling the robot to install a third longitudinal encryption and authentication device in the plant

Fig 1

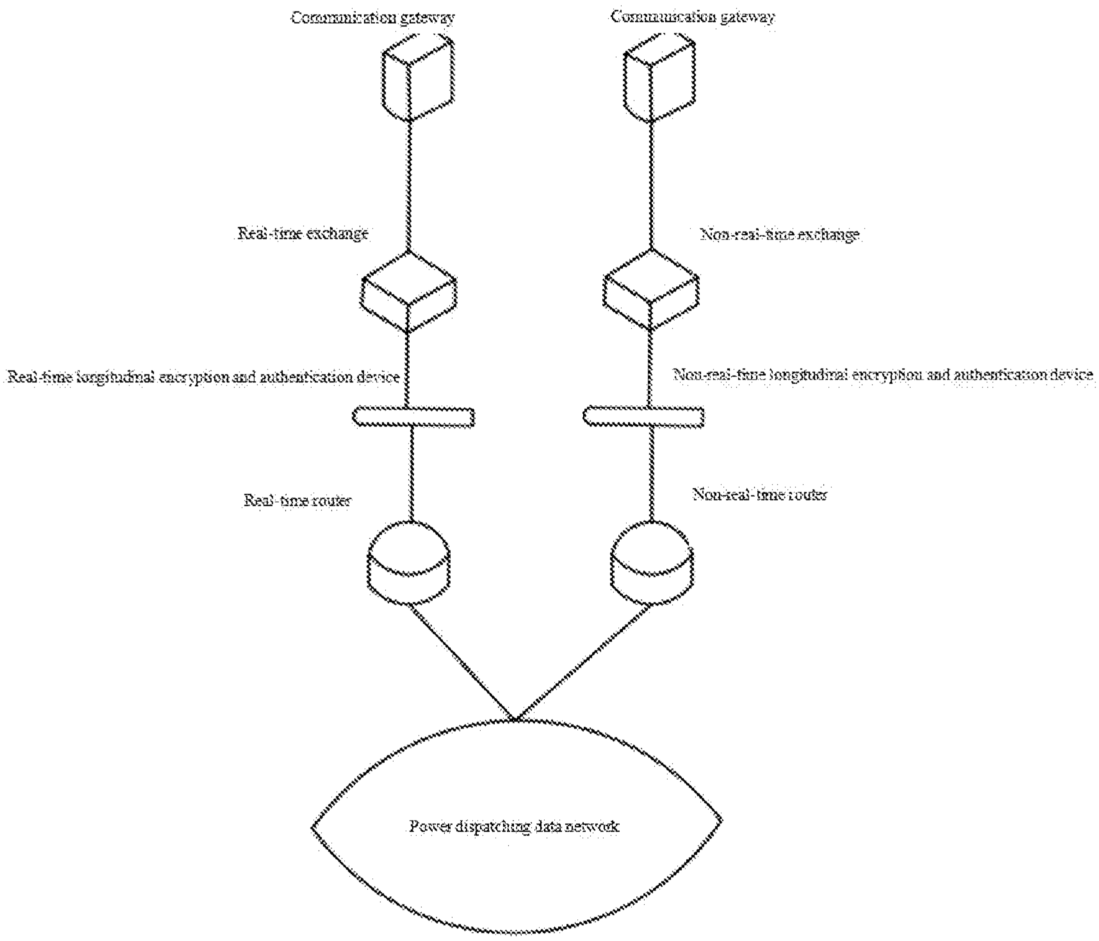
Communication gateway
Communication gateway
Real-time exchange
Non-real-time exchange
Real-time longitudinal encryption and authentication device
Non-real-time longitudinal encryption and authentication device
Real-time router
Non-real-time router
Power dispatching data network

Fig 2

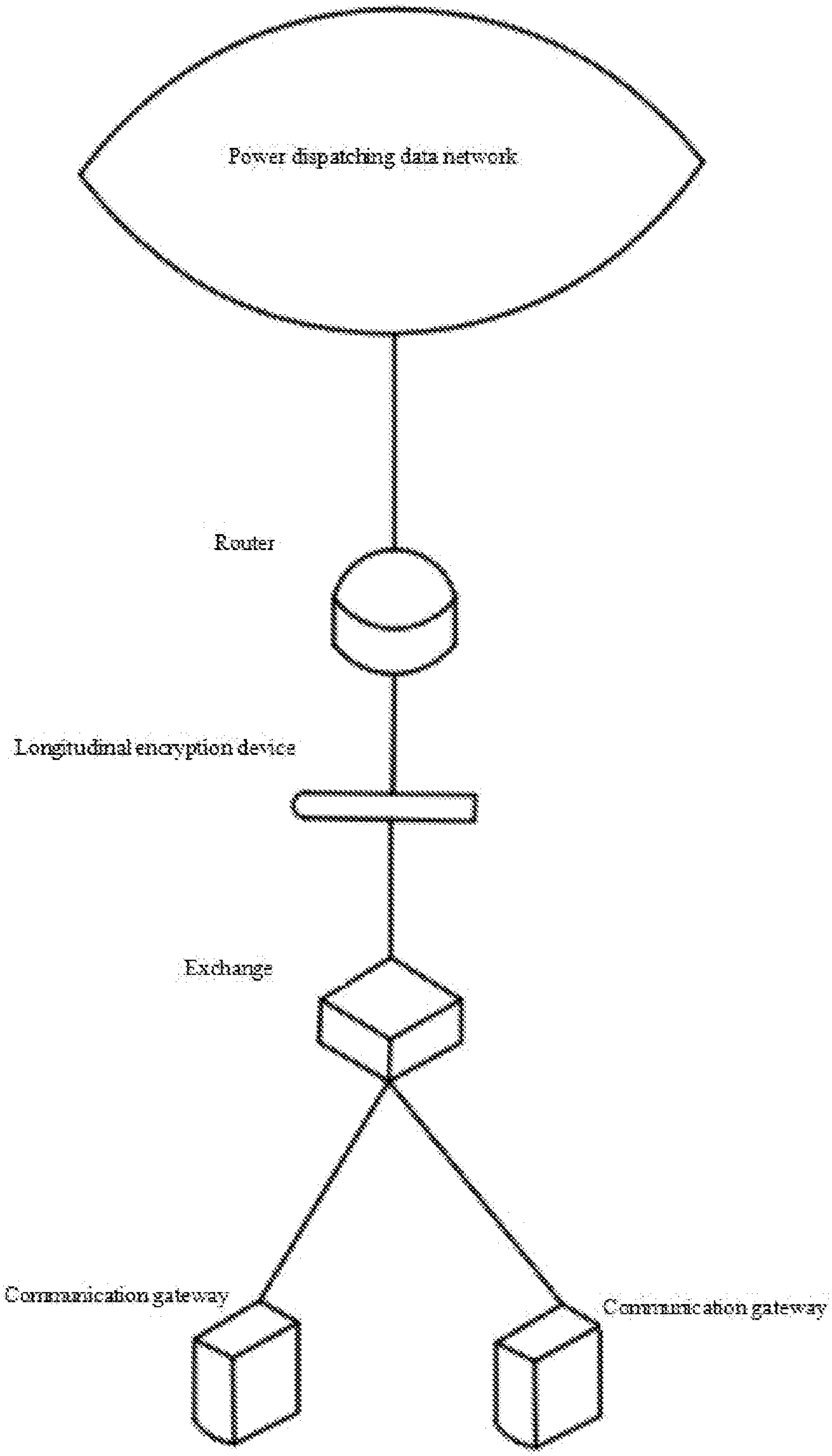
Power dispatching data network
Router
Longitudinal encryption device
Exchange
Communication gateway
Communication gateway

Fig 3

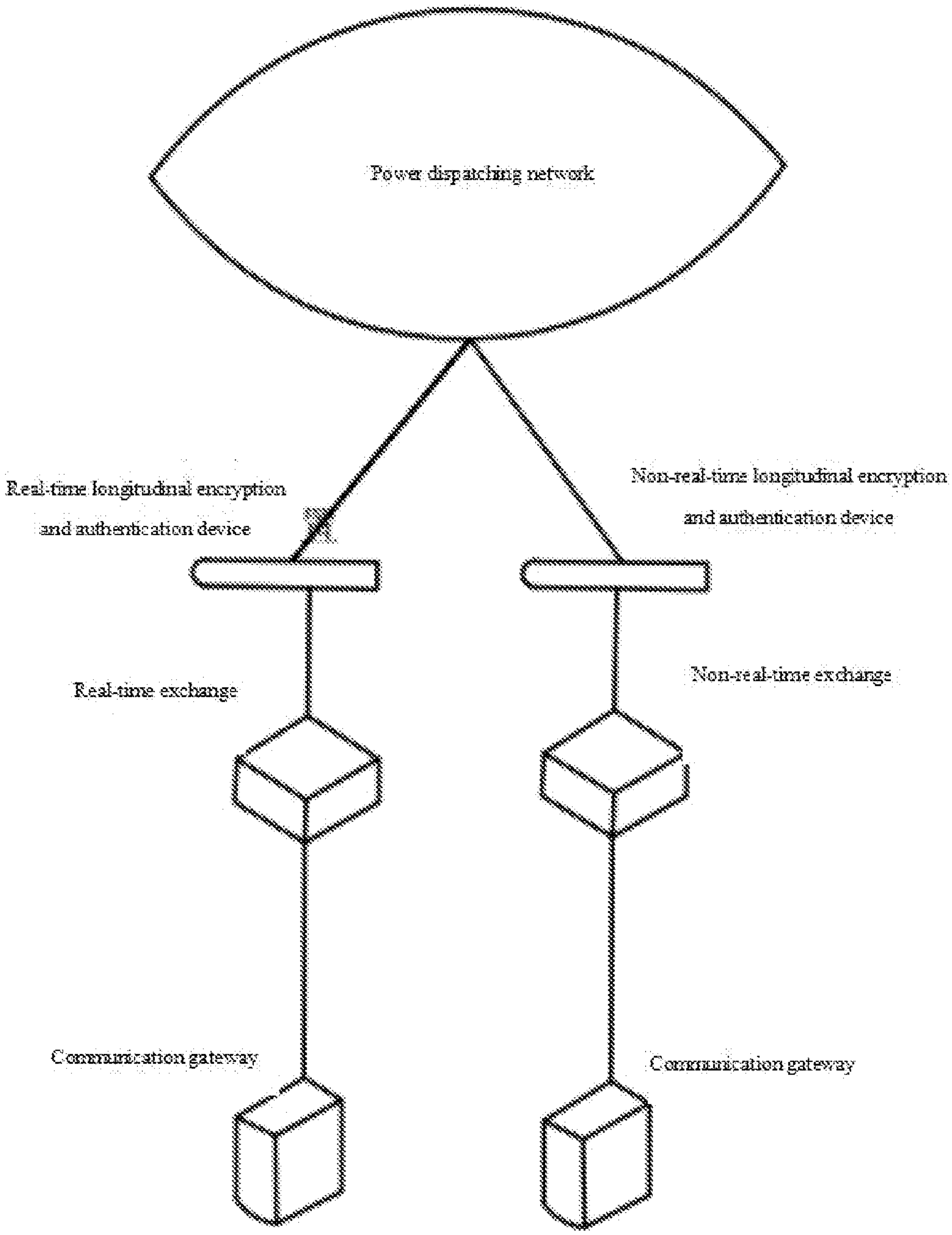
Power dispatching network
Real-time longitudinal encryption and authentication device
Non-real-time longitudinal encryption and authentication device
Real-time exchange
Non-real-time exchange
Communication gateway
Communication gateway

Fig 4