Virtual Private Cloud Based Power-Dispatching Automation System—Architecture and Application

Dongxu Yang, Hua Wei, Yun Zhu, Peijie Li, *Member, IEEE*, and Jian-Cheng Tan, *Senior Member, IEEE*

***Abstract*—This paper presents the framework of a power-dispatching automation system (PDAS) based on a virtual private cloud, which extracts advantages of technologies, such as a virtual private cloud, a virtual private network, an https protocol, etc. Unlike existing on-premise or public cloud hosted PDASs that are vulnerable and may be subject to blackouts due to extreme conditions, such as natural disasters or cyberattacks, the proposed framework operates more safely and securely under those conditions, while at the same time meeting the reliability requirements for power systems as well. This paper presents the theory, architectural design, characteristics, and implementation process of the system, as well as its reliability and cyber security measurements. The annual failure time of the proposed system is reduced from 61.2 to about 0.43 min, about 142 times less than those of existing PDASs. This framework has been implemented in the Lipu power system in China since May 2016. Results show that the proposed system is reliable, safe, and cost-effective, with a bright prospect for future applications.**

***Index Terms*—Cyber security, power-dispatching automation system (PDAS), virtual private cloud (VPC), virtual private network (VPN).**

I. Introduction

THE power-dispatching automation system (PDAS) is the center of a power system. It plays a critical role in monitoring and controlling the electricity production process and is responsible for the overall security and stability of the system. With the expansion of power system scale, the existing PDASs are limited by hardware resources, which are incapable of storing, calculating, and analyzing massive data. On the other hand, due to problems in the construction and deployment of existing PDASs, the construction, operation, and maintenance costs are high, and they are unable to resist the impact of local extreme natural disasters, such as earthquakes and typhoons. For example, in September 2016, typhoon "Morandi" blew away the main and backup PDAS in Xiamen, China, leading to the loss of the entire power-dispatching center and the blackout of a large geographical area.

In recent years, with rapid advancements in cloud computing technology, commercial cloud computing platforms already have a series of advantages, such as low cost, high reliability, reliable disaster recovery, elastic calculation, storage, and network. At present, relevant research works have applied it to power systems. The cloud computing technology is being applied to power systems gradually, which offers elastic computing, flexible data storage, and reliable disaster recovery [1], [2]. It not only solves the problems posed by hardware resource limitations, so as to meet the requirements of future power systems for the speed and accuracy of large-scale computing and the need for processing and analyzing massive data, but it also reduces the cost of building the system. The cloud computing technology is also applied in the simulation and analysis of large-scale power system transients [3], [4], where traditional methods are subject to insufficient computing capacity. An efficient scheduling approach for the charging and discharging of electric vehicles is formulated and presented based on a cloud computing infrastructure [5], which relieves the smart-grid capacity and storage limits. The cloud computing technology is also applied in the data processing and analysis of user side in smart grids, and an architecture designed for data processing is proposed [6], which meets the requirements of smart grids for massive data processing, real-time data analysis, and data sharing. In addition, the application of cloud computing also involves energy efficiency and quality of service (QoS). An adaptive resource scheduler for networked fog centers, which meets the QoS requirements of minimum transmission rates, maximum delays, and jitters [7], is proposed for energy and throughput optimization in cloud computing applications and is tested for energy efficiency. A novel resource allocation principle is proposed to enable an energy-aware service function chaining for software defined network-based networks, and heuristic algorithms are used for different optimization problems to achieve near-optimal solutions with acceptable computing times [8].

Manuscript received October 4, 2017; revised January 30, 2018 and April 28, 2018; accepted June 5, 2018. Date of publication June 29, 2018; date of current version March 1, 2019. This work was supported in part by the National Key Basic Research Program of China (973 program) under Grant 2013CB228205, and in part by the National Natural Science Foundation of China under Grant 51667003. Paper no. TII-17-2156. *(Corresponding author: Hua Wei.)*

D. Yang, H. Wei, Y. Zhu, and P. Li are with the Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University, Nanning 530004, China (e-mail: yangdongxugxu@163.com; weihua@gxu.edu.cn; zhuyun@gxue.net; lipeijie@gxu.edu.cn).

J.-C. Tan is with the College of Electrical Engineering Guangxi University, Nanning 530004, China (e-mail: jctan@gxu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2018.2849005

With the wide application of the cloud computing technology in power systems, security issues are becoming increasingly prominent. A comprehensive discussion on applying the cloud computing technology as the new information infrastructure for next-generation power systems is proposed [9], and some cyber security is considered, including four kinds of cyberattacks. The security of a power cloud platform is analyzed [10], as well as the associated security defense plan. Information-masking technology is used [11] as the security means during data transmission, and its feasibility and effectiveness are validated. An encryption-sharing algorithm is presented to encrypt the data before transmission [12]; this ensures the security of data transmission between the smart grid and the cloud. The architecture of a cloud computing platform is analyzed [13], and its basic functions and security designs are discussed. An overview of existing works that integrate cloud computing in the existing smart grid architecture is presented [14] in order to have a reliable, efficient, and secure energy distribution. Several security technologies in terms of security issues of cloud computing applications are proposed. Besides, a virtual private cloud (VPC) pilot project has been initiated by ISO New England [15]–[17]; this validates its feasibility, economy, and effectiveness.

The above-mentioned research provides a reference for the application of the cloud computing technology in PDASs. In recent years, public cloud-based PDASs (cloud dispatching systems) have been of interest to researchers. However, most of the current research works only put forward the system architecture but do not deeply analyze its security and reliability or build a practical system, with the main concern being that the security and reliability have not been solved effectively.

In response to the above problems, this paper proposes a VPC-based approach for PDAS, which is referred to as “VPC-PDAS,” and analyzes and calculates its safety and reliability. The system utilizes a mainstream tunnel technology to create a virtual network at the open system interconnection (OSI) second layer “data link,” each assigned a unique tunnel ID, safer than the isolation achieved at the third “network” layer. Different virtual networks are completely isolated and cannot communicate with each other directly. This forms a logically isolated network. The tunnel IDs assigned to each of the elastic compute service (ECS) instances are located at different VPCs, which are in different routing planes, and are thus separated from each other [18]. Besides, a virtual private network (VPN) is used as the data transmission channel to ensure data confidentiality and integrity during transmission, thus meeting the security requirements for power system applications. On the other hand, in order to solve the reliability problem, with the strong disaster recovery capability of the cloud computing technology, the proposed system realizes a remote disaster recovery scheme, which can resist local extreme natural disasters and improve its own reliability. Compared with existing PDASs, the annual failure time of the proposed system is reduced from 61.2 to about 0.43 min, while the reliability of the substation system remains the same. This is about 142 times lower than those of existing PDASs. The system has achieved a good operation performance in the power grid of Lipu, Guangxi, China, with a bright prospect for future applications.

The main contributions of this paper are summarized as follows.

1) This paper presents the problems of existing PDASs and proposes a new architecture of a PDAS based on a VPC. Besides, the performance of the proposed system compared with that of existing ones is calculated and analyzed in detail, including its security and reliability.
2) This paper discusses how a power system can benefit from the VPC-based PDAS architecture, develops specific cloud-enabled power applications, which aim to demonstrate how to develop PDAS applications on a state-of-the-art cloud platform, and demonstrates the advantages of the developed system as well. Finally, the proposed system has been applied to the actual industry.

The remainder of this paper is organized as follows: Section II describes the main technologies. The new architecture of a PDAS based on a VPC, including its design and features, is proposed in Section III, Section IV calculates and analyzes the performance of the existing and proposed systems. Section V describes the implementation and advantages of the proposed system in detail and applies it to an actual power system. Last, Section VI concludes the paper.

II. Virtual Technology

A. Virtual Private Cloud

By using the overlay technology [19] and Vxlan protocol [20], a VPC is constructed and isolated at the OSI second layer, the data link, with separated virtualized networks and independent tunnel identifications. Different VPCs cannot communicate with each other directly, thereby achieving network isolation between different VPCs. Tunnel encapsulation technology is used to encapsulate the IP packets from the ECS so that information at the data-link layer will not leak to the network layer; isolation is achieved between different ECSs at the data-link layer [18]. These technologies enable the VPC to defend itself against any cyberattacks, such as ARP spoofing, broadcast storm, host scanning, and so on, leading to a safer and isolated virtualized network environment.

Compared with a public cloud, a VPC provides virtual switches and routers so that users can create a virtual network through planning network segments, IP addresses, routing tables, and gateways and isolate the newly created VPC from the Internet. The VPC security is ensured by setting up an ECS security group, a relational database service (RDS) access white list, and other security policies.

With rapid advancements in the cloud computing technology, and a strong demand for network security, it is evident that the VPC is booming—Amazon VPC online was made available in 2009, Default VPC was launched in 2013, and ClassicLink utilizing the Amazon VPC cloud was officially launched in October 2014 [21].

B. Virtual Private Network

The VPN is a kind of technology that establishes dedicated data communication networks in public networks. Tunnel and encryption technologies are used to provide a secure and reliable communication between users so that dedicated communication lines are not required in order to transmit user-specific information securely. By using logically isolated network channels, information can be exchanged and shared via various networks over large geographical regions at low cost [22]. Compared with other communication technologies, such as resilient public IP, channel, Net, and load balancer. VPNs have the advantages of tunneling and encrypting, which ensure data confidentiality and integrity during the transmission process.

Different VPNs use different technologies, such as the second-layer tunnel protocol, the third-layer security protocol IPSec, the secure socket layer SSL, and the multiprotocol label switching. By investigating various types of VPNs, it is found that IPSecVPN has strong identity authentication and tunnel authentication mechanisms, as well as providing strong data integrity and confidentiality protection. Therefore, the IPSecVPN is utilized in this paper to establish data transmission channels between the master station and substations. In addition, the SSLVPN enables rigorous unique identity authentications of connected devices and users, and it is suitable for browser/server-based applications. Thus, the SSLVPN is adopted as a user access channel to the VPC-PDAS. Moreover, users can manage and control the network access easily and can also expand and reconstruct. Presently, it is the preferred technology for enterprises to achieve secure interconnections between internal and external networks and is used widely in practice.

III. VPC-PDAS Framework Design

A. Framework of the system

Considering the deficiencies in security, reliability, and economy of existing PDASs and cloud-dispatching systems, the framework of the VPC-PDAS is proposed in this paper and applied to an actual power system. The framework of the system is shown in Fig. 1.

The functions of the PDAS as services are deployed in the VPC. Communication between substations and the VPC-PDAS is achieved through the IPSecVPN, and the information exchange between the service requester and the service provider is via the SSLVPN. This framework meets the security protection requirements of the power system.

B. Features of the framework

Generally, the PDAS can be divided into three parts, namely, the master station system, the transmission system, and the substation system. Compared with existing PDASs and cloud-dispatching systems, the VPC-PDAS proposed in this paper has the following innovative features.

Master system: Compared with the existing master system, a VPC is used in this paper to avoid the purchase of hardware devices, such as servers, storage, router, and so on; it does not require a room to install these hardware devices, and it does not need special maintenance. Besides, the calculation, storage, and network resources can be elastically expanded and disaster recovery is easily realizable, thus solving the problems, such as high cost of construction, operation, and maintenance of the existing PDAS, and the issue that it cannot withstand local extreme natural disasters. These methods improve the economy and reliability of the system. On the other hand, besides the cloud-dispatching master system, the VPC also supports user-set gateway, routing, IP, and so on. Users can create an isolated and virtualized network, which can prevent cyberattacks, such as hackers, viruses, and malicious codes, and meet the power system's security requirements.

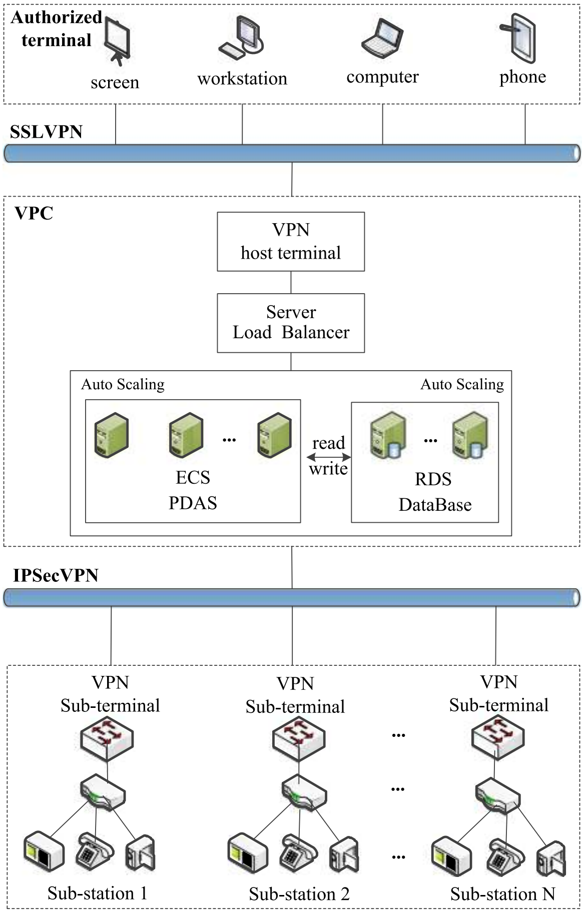


Fig. 1. Framework of the proposed system.

Transmission channel: VPN host terminals are deployed in a VPC, and VPN subterminals are set up at each substation so that an IPSecVPN tunnel can be created as a data transmission channel between the VPC-PDAS and each substation. This not only reduces the cost of construction but also safeguards the integrity and confidentiality while dispatching data during the process of transmission.

IV. Performance Analysis of VPC-PDAS

A. Security Analysis

The PDAS, as part of a power system's direct production system, monitors and controls the overall power system in real time and is the core business system where the security defense system is armed to protect. Information security mainly includes data security and cyber security.

1) Data Security: In order to ensure data security, VPN tunnels are adopted for user access and data transmission, which is safer, saves construction costs, and reduces the maintenance workload.

IPSecVPN tunnels are established between the VPC and each substation to achieve end-to-end connections. The strong identity and tunnel authentication mechanism uses the unique identity of a substation and the encryption of data to ensure the integrity and confidentiality of the dispatching data during the transmission process.

In addition, a multitier application deployment mode is adopted that uses the RDS and ECS to deploy the database and the PDAS, respectively. The RDS is a stable, reliable, elastic online database. Compared with building a database at the server, the RDS has many advantages, such as disaster recovery, backup, monitoring, migration, and so on, which not only reduces the burden of the ECS, making the system more smoothly, but also monitors and manages the database conveniently by only accessing the Internet. Through the RDS, users can backup data manually anywhere and at any time, and can also set up a backup strategy to achieve automatic data backup. The RDS supports disaster recovery in two ways: one at a different city in the same region and the other at a different city in a different region. Data can be recovered within two years [23]. This reduces the workload of operating and maintaining the database and improves the security and reliability of the system significantly. At the same time, it supports payment on-demand, achieves elastic expansion according to business needs, and can also intercept structured query language (SQL) injection and violence crack, with a strong cyber protection capability. There are more obvious advantages of using the RDS than installing a database in a local computer room or installing a database on an ECS.

2) Cyber Security: Considering the aspect of cyber security, a VPC is adopted in the system, which isolates the network at the second layer by using the overlay technology [19] and Vxlan protocol [20] so that physical and virtual networks are separated completely to achieve the same effect as traditional virtual local area networks. Each virtual network has a unique tunnel identification; different VPCs cannot communicate with each other directly, which results in logically isolated networks. Besides, the ECS IP in a VPC is encapsulated to ensure no exposure to the public; this differs from the public cloud. Users can plan and manage the range of IP addresses, network segments, routing tables, and gateways to form a self-controlled network. By adopting the above measures, users can create an isolated virtual cyber environment, with internal IPs only for improved security and isolation from the Internet. To improve the security of the system further, distributed denial of service is used to protect against a large volume of traffic attacks. Besides, the web application Firewall is used to prevent SQL injection, cross-site scripting, common web-server plug-in vulnerabilities, Trojan horse, and other common attacks, thus protecting the safety of the website in this application.

For computers, mobile phones, and other network terminals to access the VPC-PDAS, the SSLVPN technology is used to certify the unique identity of these devices and users. This authentication method is unique and cannot be copied or stolen, thus preventing any unauthenticated devices or users from accessing the VPC-PDAS. Moreover, other methods, such as setting up an ECS security group, an RDS access white list, and other access policies, are used to block the e-mail and web services. These measures provide the VPC-PDAS with a network barrier, thereby improving the security of the system to some extent. At the same time, a security certificate from the certification authority institution is adopted to prove the use of the server, and the transmission protocol is upgraded and improved. As an https protocol sends content in a clear text, it does not provide data encryption in any way. If an attacker intercepts the transmitted message, it can be easily understood. Therefore, the http protocol is replaced with an https protocol in this paper, which encrypts and authenticates the dispatching data before transmission, to avoid using plain text during data transmission [24], [25].

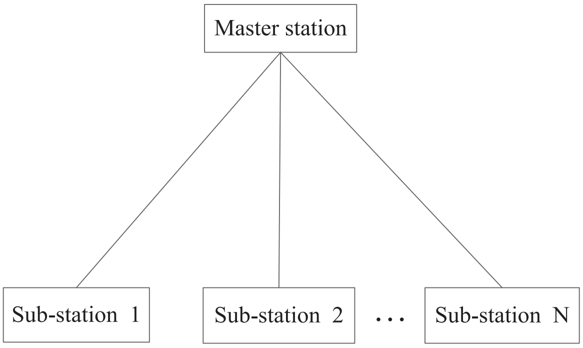


Fig. 2. Information transmission system diagram of the existing PDAS.

In summary, the VPC-PDAS meets the security requirements of a power system with high security requirements.

B. Reliability Analysis

In this paper, the information transmission system and the master station system are improved. Therefore, the reliability of the information transmission system and the master station system is analyzed and compared under the premise of the same reliability of the substation system.

1) Reliability Comparison of Information Transmission System: The existing information transmission system of a PDAS consists of the master station communication devices, the substation communication devices, and the fiber channel equipment. The architecture of communication between the master station and substations is shown in Fig. 2.

The proposed VPC-PDAS consists of the VPN host terminal, VPN subterminals, and VPN channels. A network structure is adopted, which is shown in Fig. 3.

For convenience, we assume that the information transmission system associated with the existing PDAS is “point-to-point” connected, and that the proposed VPC-PDAS has simplified networked connections, as shown in Fig. 4.

Assuming that the availability (for a component) of each channel is α, the reliability (for a system) of the “point-to-point” structure can be estimated as follows:

$$Y_1 = \alpha. \tag{1}$$

For the networked structure, the state enumeration method [26] is used for reliability analysis in this paper. Assuming that the availability of each channel is α, and the network contains

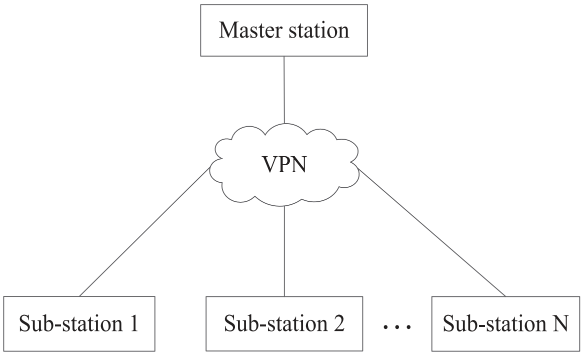


Fig. 3. Information transmission system diagram of the proposed VPC-PDAS.

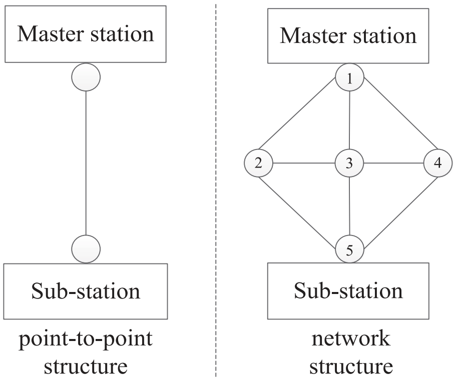


Fig. 4. Simplified diagram of information transmission systems.

five nodes and eight channels, the relationship between these nodes can be represented by the following matrix:

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{2}$$

where "0" represents a no-communication path between two nodes, and "1" represents a communication path between two nodes.

If a node and its associated row/column elements are all zero, there are no data transmission channels between the master station and the remaining nodes or the substation and the remaining nodes, resulting in an "information island," which is unable to transmit data. Assuming the master station is node 1 and the substation is node 5, there are the following three cases of no data transmission between these two nodes.

Case 1: The master station (node 1) forms an "information island"

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & * & 0 & * \\ 0 & * & 0 & * & * \\ 0 & 0 & * & 0 & * \\ 0 & * & * & * & 0 \end{bmatrix}$$

or

Case 2: The substation (node 5) forms an "information island"

$$\begin{bmatrix} 0 & * & * & * & 0 \\ * & 0 & * & 0 & 0 \\ * & * & 0 & * & 0 \\ * & 0 & * & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

or

Case 3: The "information island" consists of both the master station (node 1) and the substation (node 5)

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & * & 0 & 0 \\ 0 & * & 0 & * & 0 \\ 0 & 0 & * & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{3}$$

where $*$ can be zero or one. Assuming that the probability of the master station or substation forming an "information island" is U_i, i is the number of "information islands."

For the first and second cases in matrix (3), the probability that an island will be formed by the master station or substation is estimated as follows:

$$U_1 = U_2 = (1-\alpha)^3[C_5^0\alpha^5 + C_5^1\alpha^4(1-\alpha) + C_5^2\alpha^3(1-\alpha)^2 + (C_5^3 - 1)\alpha^2(1-\alpha)^3 + (C_5^4 - 2)\alpha(1-\alpha)^4]. \tag{4}$$

For the third case, that is, the probability of the master station and substation forming an island simultaneously is estimated as follows:

$$U_3 = (1-\alpha)^6[C_2^0\alpha^2 + C_2^1\alpha(1-\alpha) + C_2^2(1-\alpha)^2]. \tag{5}$$

Therefore, the reliability for data transmission between the master station and the substation is estimated as follows:

$$Y_2 = 1 - \sum_{i=1}^{l} U_i \tag{6}$$

where $\sum U_i = U_1 + U_2 + U_3$ represents the value of information islands.

Thus, the reliability difference between the existing PDAS and the proposed VPC-PDAS is estimated as follows:

$$\Delta Y = Y_2 - Y_1. \tag{7}$$

Equation (7) shows that $\Delta Y > 0$, when $0 < \alpha < 1$. In other words, the reliability of a network structure is always higher than that of the "point-to-point" structure, under the condition that the reliability of a single channel remains the same in all case studies.

The average annual availability of repairable components is

$$\alpha = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{\mu}{\lambda + \mu} \tag{8}$$

where λ is the failure rate (number of failures/year), μ is the repair rate (number of repairs/year), MTBF is the mean time between failure, and MTTR is the mean time to repair. λ and μ

TABLE I
MTBF AND MTTR OF CHANNELS

Item	MTBF(h)	MTTR(h)
Fiber channel	100000	12
VPN channel	160000	10

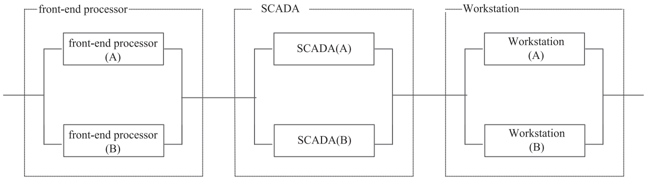


Fig. 5. Master station system reliability diagram of the existing PDAS.

can be estimated by (8760 h/year)

$$\lambda = \frac{8760}{\text{MTBF}} \tag{9}$$

$$\mu = \frac{8760}{\text{MTTR}}. \tag{10}$$

Fiber channels are adopted in the Lipu power system, Guangxi, China, and a VPN channel is adopted in the proposed system. The MTBF and MTTR of the fiber and VPN channels are given in Table I [27].

The failure rate λ_{TE} and the repair rate μ_{TE} of each channel in the existing information transmission system and the failure rate λ_{TV} and the repair rate μ_{TV} of each channel in the VPC-PDAS can be obtained by substituting the data in Table I into (9) and (10), respectively. According to (1)–(7), compared with the "point-to-point" structure, the reliability of the network structure is improved from 99.988% to 99.999%, and the annual failure time is reduced from 1.05 to 0.09 h.

2) Reliability Comparison of the Master Station System: The reliability of the master station system is related to the availability of the equipment, which can be analyzed by the full probability formula. The existing PDAS consists of a front-end machine, a SCADA server, and a workstation; the three sections are connected in series. Each section consists of two machines connected in parallel; the redundancy is achieved to ensure reliability. The reliability block diagram of the existing PDAS master station system is shown in Fig. 5.

The proposed VPC-PDAS consists of an ECS, an RDS, and a workstation; the three sections are connected in series. The computer cluster mechanism used for the ECS and the RDS is able to withstand $m-1$ servers under abnormal conditions, provided all m servers are connected in parallel. The master station system reliability diagram of the proposed VPC-PDAS is shown in Fig. 6.

For two parallel-connected repairable components, the failure rate and the repair rate can be estimated as follows:

$$\lambda = \lambda_1\lambda_2\left(\frac{8760}{\mu_1} + \frac{8760}{\mu_2}\right) \tag{11}$$

$$\mu = \mu_1 + \mu_2. \tag{12}$$

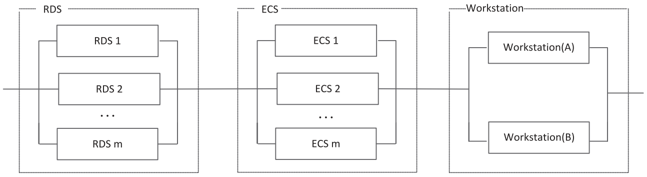


Fig. 6. Master station system reliability diagram of the proposed VPC-PDAS.

TABLE II
MTBF AND MTTR OF THE EQUIPMENT IN THE MASTER STATION

Item	MTBF(h)	MTTR(h)
front-end machine	42000	12
SCADA server	42000	12
workstation	15480	16
ECS	120000	8
RDS	120000	8

TABLE III
COMPARISON OF THE MASTER STATION SYSTEM RELIABILITY BETWEEN THE EXISTING PDAS AND THE PROPOSED VPC-PDAS

Item	Existing PDAS	Proposed VPC-PDAS
architecture	resource localization	resource network
disaster recovery	main and preparation	cluster
Withstanding outage	One unit	$m-1$
Manner of switching	physical	virtual
Speed of switching	second	millisecond
reliability	98.93265%	99.07284%

For n repairable components in series, the failure rate and the repair rate can be estimated as follows:

$$\lambda = \sum_{i=1}^{n} \lambda_i \tag{13}$$

$$\mu = \frac{\sum_{i=1}^{n} \lambda_i}{\sum_{i=1}^{n} \frac{\lambda_i}{\mu_i}}. \tag{14}$$

The existing PDAS consists of a front-end machine, a SCADA server, and a workstation, and the proposed VPC-PDAS consists of ECSs, RDSs, and workstations. The MTBF and MTTR of these devices are given in Table II [28].

Let $m = 30$ $m = 30$. The failure rate λ_{ME} and the repair rate μ_{ME} of the existing PDAS master system and the failure rate λ_{MV} and the repair rate μ_{MV} of the master station of the VPC-PDAS can be obtained by substituting the data in Table II into (9)–(14). According to (1)–(7), compared with the existing PDAS master station, the reliability of the master station of the VPC-PDAS is improved from 98.93265% to 99.07284%, and the annual failure time is reduced from 93.4999 to 81.2192 h.

The master station system reliability comparison between the existing PDAS and the proposed VPC-PDAS is given in Table III.

3) Reliability Comparison of the PDAS: The reliability evaluation of a power system is usually a limiting state probability problem, which can be solved by using Markov equations.

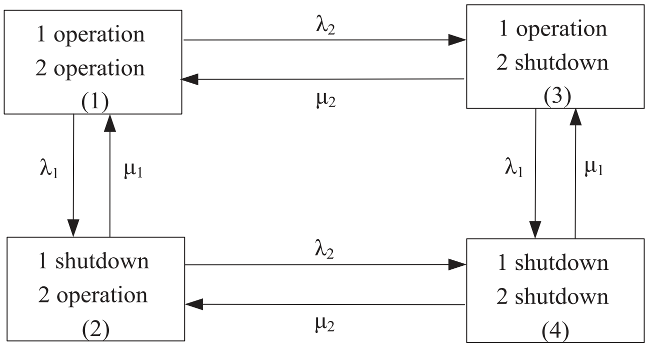


Fig. 7. State-space diagram of two repairable components.

According to the Markov method, for a repairable two-component system, the four states of the two components and their transfer relationship are shown in Fig. 7.

According to the state-space diagram, the following transfer matrix can be established:

$$A=\begin{bmatrix} -(\lambda_1+\lambda_2) & \lambda_1 & \lambda_2 & 0 \\ \mu_1 & -(\mu_1+\lambda_2) & 0 & \lambda_2 \\ \mu_2 & 0 & -(\mu_2+\lambda_1) & \lambda_1 \\ 0 & \mu_2 & \mu_1 & -(\mu_1+\mu_2) \end{bmatrix}. \tag{15}$$

According to the approximation principle of a Markov process, the following equation can be established:

$$PA = 0 \tag{16}$$

where P is the limiting state probability and A is the transfer rate matrix. The following equation can be obtained by the transpose of (16):

$$\begin{bmatrix} -(\lambda_1+\lambda_2) & \mu_1 & \mu_2 & 0 \\ \lambda_1 & -(\mu_1+\lambda_2) & 0 & \mu_2 \\ \lambda_2 & 0 & -(\mu_2+\lambda_1) & \mu_1 \\ 0 & \lambda_2 & \lambda_1 & -(\mu_1+\mu_2) \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ P_3 \\ P_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{17}$$

Since the sum of the probabilities of all states of the system is 1, the following formula is obtained:

$$[P_1 + P_2 + P_3 + P_4] = 1.0. \tag{18}$$

According to (17) and (18), the following formula is obtained by adopting a linear algebraic algorithm:

$$P_4 = \frac{\lambda_1\lambda_2}{(\mu_1+\lambda_1)(\mu_2+\lambda_2)}. \tag{19}$$

The overall structure of the existing PDAS is shown in Fig. 8.

According to the idea of a district and using the Markov method under the premise of not considering the availability of the substation system, the reliability of the existing PDAS can be estimated as follows:

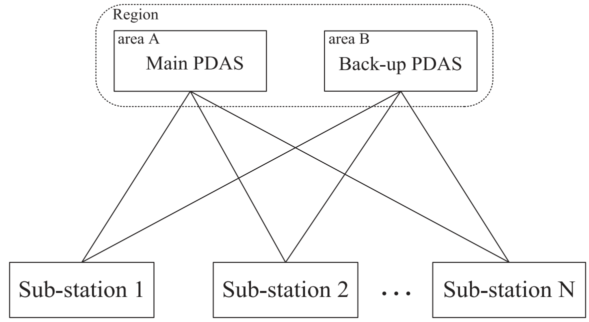


Fig. 8. Overall structure of the existing PDAS.

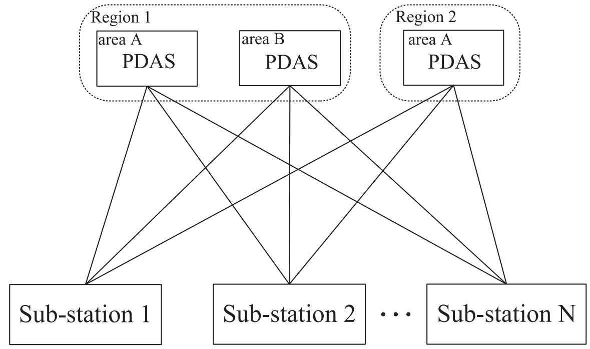


Fig. 9. Overall structure of the proposed VPC-PDAS.

$$Y_3 = 1 - P_4 = 1 - \frac{\lambda_1\lambda_2}{(\mu_1+\lambda_1)(\mu_2+\lambda_2)} \tag{20}$$

where $\lambda_1 = \lambda_2 = \lambda_{\mathrm{TE}} + \lambda_{\mathrm{ME}}$ and

$$\mu_1 = \mu_2 = \frac{(\lambda_{\mathrm{TE}} + \lambda_{\mathrm{ME}})\mu_{\mathrm{TE}}\mu_{\mathrm{ME}}}{\lambda_{\mathrm{TE}}\mu_{\mathrm{ME}} + \lambda_{\mathrm{ME}}\mu_{\mathrm{TE}}}.$$

According to (20), Y_3 can be obtained as follows:

$$\begin{aligned} Y_3 &= 1 - P_4 \\ &= 99.9883556\%. \end{aligned} \tag{21}$$

In order to improve the reliability of the system, consider the factors of disaster recovery system. The system is backup in different regions. The overall structure of the VPC-PDAS is shown in Fig. 9.

Similarly, the reliability of the VPC-PDAS can be obtained as follows:

$$Y_4 = 99.9999992\%. \tag{22}$$

Knowing 8760 h/year, the annual failure time (in minutes) of the existing PDAS can be estimated as follows:

$$\begin{aligned} h_1 &= (1 - Y_3) \times 8760 \times 60 \\ &= 61.2. \end{aligned} \tag{23}$$

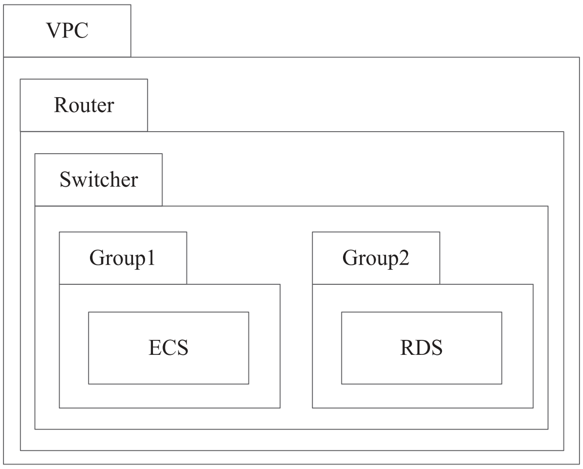


Fig. 10. Network diagram of the master station system of the VPC-PDAS.

The annual failure time (in minutes) of the VPC-PDAS can be estimated as follows:

$$\begin{aligned} h_2 &= (1 - Y_4) \times 8760 \times 60 \\ &= 0.43. \end{aligned} \tag{24}$$

In conclusion, compared with the existing PDAS, the proposed VPC-PDAS can reduce the system failure time from 61.2 to about 0.43 min, assuming that substation systems have the same reliability, which is a reduction about 142 times.

V. Implementation of the VPC-PDAS

A. Master Station System

Considering the operating costs, network stability, and business requirements, synthetically, the Ali Cloud in China is used in this paper; the configuration of the ECS is a Windows Server 2016 R2 Standard with 4-core 16G ROM, and the RDS is configured as a Microsoft SQL Server 2008 R2 with 4-core 8G ROM and 100G storage.

The design of the master station system mainly involves network planning, multilayer application deployment, server load balancing, auto scaling (AS), and disaster recovery.

1) Network Planning: It is necessary to plan the network before designing the master station system. The customized route is realized by creating an IP address in the VPC, and a virtual switcher is created in the virtual router. Besides, two security groups are built in the virtual switchers to deploy the ECS and the RDS, respectively. The network diagram of the master station system of the proposed VPC-PDAS is shown in Fig. 10.

2) Multilayer Application Deployment: In order to improve the system security further, the ECS and the RDS are divided into different subnets. By using the security group settings, users can access the VPC-PDAS through the VPN only, but they cannot access the database, which is accessed only through the internal network. The security of the system is improved further by adopting the multitier application deployment mechanism.

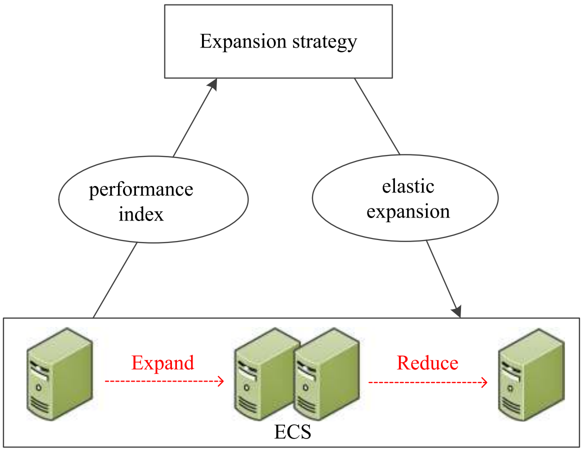


Fig. 11. Diagram of the AS.

3) Server Load Balancer (SLB): To improve the system's external service capabilities, an SLB is used in the master station system design, which adopts weighted-polling traffic-dispatching algorithms to achieve the distribution of traffic to different ECSs automatically, according to the custom weight for the ECS. The SLB has the ability to eliminate the failure of single points so as to improve the availability and reduce the cost of the system.

4) Auto Scaling: In this paper, AS is adopted. Through setting up the AS, an ECS instance is created and released seamlessly. Based on the cloud monitoring performance indicators, such as the CPU and memory usage, it expands the system availability horizontally. It is combined with the SLB and the RDS so that the IP of an ECS can be added to or removed from the SLB and the RDS white list automatically [29]. The CPU usage of ECSs is monitored mainly in this system. When it exceeds 75%, an ECS is added automatically; when it is less than 30%, the ECS is moved out automatically. Moreover, an unhealthy ECS is replaced automatically through a healthy check mechanism, which ensures that the system is available. The diagram of the AS is shown in Fig. 11.

5) Disaster Recovery: The PDAS is deployed in different physical areas of the same region, isolated from each other to achieve the available area redundancy and system backup. When an outage impacts an area, it switches to another available area automatically. In order to improve the reliability of the system further, for example, to avoid total outage at one region because of extreme natural disasters, such as earthquakes and typhoons, the same PDAS structure is deployed at another geographical region; switching between the two regions is achieved automatically to enhance the reliability of the system.

The architecture of the proposed VPC-PDAS master station system is shown in Fig. 12.

B. Information Transmission System

In this paper, a VPN that takes into account the advantages of tunnel and encryption technologies is used as the information transmission channel to transport data between the master station system and the substation systems. VPN tunnels are

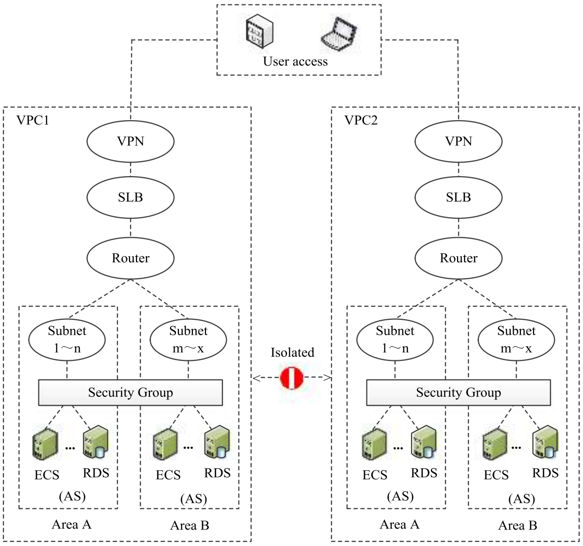


Fig. 12. Architecture of the master station system of the proposed VPC-PDAS.

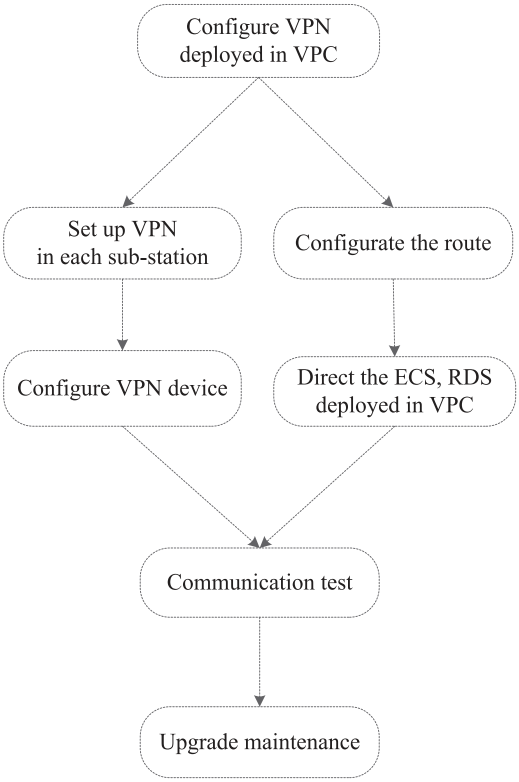

Configure VPN deployed in VPC
Set up VPN in each sub-station
Configurate the route
Configure VPN device
Direct the ECS, RDS deployed in VPC
Communication test
Upgrade maintenance

Fig. 13. Flow diagram of building a VPN.

different from existing self-built dedicated lines. The specific steps to build the VPN are shown in Fig. 13.

In addition, users with different identities are assigned different rights; this is achieved by setting the access control policy so that users with different rights can only access the corresponding permitted resources. This improves the system management capability and further enhances the security of the system at the same time.

C. System Implementation

The implementation of the PDAS mainly includes system development, service hosting, and service monitoring.

1) System Development: The SOA is implemented in the system using XML web service mainly. The system is composed of a number of services, and the function of each module in the system is defined as an independent service, made available through the web service interface to clients upon being called for. Overall, the system can be treated as a service to provide a general interface to the client. Therefore, services can be regarded as system components. The overall system uses ASP.NET framework and is based on the C# and JavaScript languages.

2) Service Hosting: Internet information service (IIS) is used to host each service. Compared with self-hosting and windows process activation service hosting, the IIS has dynamic scalability, higher availability, and other advantages. It can reclaim a service process and shut down idling services automatically; this ensures that the deployed service is always made available when the ECS is updated or restarted. The IIS is used to host services, which improves the system availability to a certain extent.

3) Service Monitoring: The services deployed on the ECS are monitored. This includes monitoring the service's current response state, request error, and response time. When an abnormal condition is captured, information, such as the types of fault and the occurrence time, is sent to the relevant staff via message or e-mail and also displayed on the home page of the PDAS with updated time and color; this also improves the system reliability to a certain extent.

D. System Advantages

Compared with the existing PDAS, the proposed system has the following advantages.

1) No Space Construction: There is no need to build rooms to install physical servers, storage, routers, switches, and other equipment, and there is no need for hardware maintenance. Compared with the existing PDAS, the cost of construction is much lower, and the space to construct is almost zero.

2) Resources Are Extended Dynamically: System resources, such as CPU, memory, bandwidth, disk capacity, etc., can be expanded dynamically and can respond in real time, when required, as the power system expands continuously.

3) Seamless Switching Between Main and Backup Systems: Data between the main and backup systems are synchronized in real time and support multiple systems on the same screen, which displays the working states of the main and backup systems at the same time, so that the switching between main and backup systems can be achieved seamlessly; this further improves the security of the system.

4) More Secure and Reliable: The application of the VPC can prevent hackers, viruses, and malicious code attacks, and remote disaster recovery can be achieved easily, which solves the problem of the inability of the existing PDAS to withstand local extreme disasters.

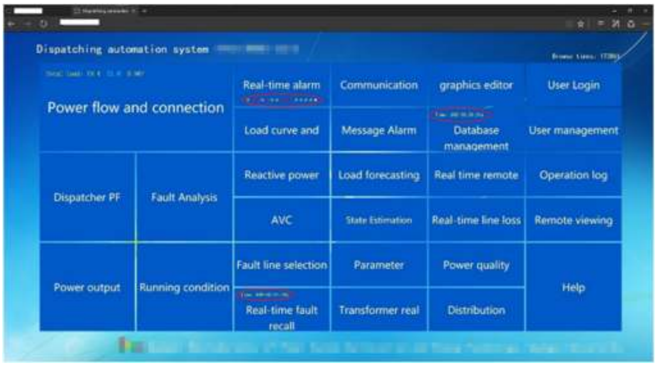


Fig. 14. Home page of the system.

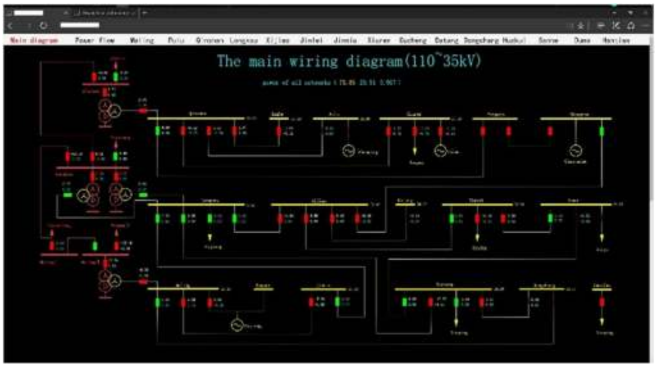


Fig. 15. System operates on a workstation.

E. Operation Effect

The proposed VPC-PDAS architecture design meets the security requirements of power systems by using an array of technical measures, such as VPC, VPN, and so on. Unlike the traditional way that pushes the virtual standard desktop interface to the user's terminal, the PDAS uses the SOA, loosely coupled between subsystems. Users do not need to download or install any plug-ins; this reduces the hardware resource requirements. The system is able to run on standard workstations, as well as on computers or mobile phones and other intelligent terminals where a browser is installed. Extended user equipment and the ability to operate across various platforms facilitate decision-making and coordinated dispatching across different locations.

The proposed framework is applied to the Lipu power system. The metro style is applied to the system home page, as shown in Fig. 14, giving users a clean, open, lightweight, fast, and dynamic feeling and reducing the user's visual fatigue. At the same time, the home page also shows the running time and the running state of each station, which is convenient to use for users.

The dispatching system is able to operate over various platforms and is expandable according to the size of the client screen. Vector-based page design, touch screen or mouse click open or close the circuit breakers in the single line diagram displayed, and zoom in and out facilitate calculation and analysis. Fig. 15 shows a system single line diagram on a workstation, and Fig. 16 shows the zoomed-in interface on a smartphone.

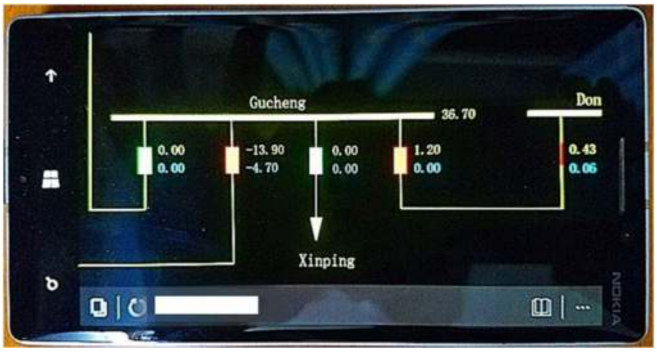


Fig. 16. System operates on a mobile phone.

VI. Conclusion

The framework of a PDAS based on a VPC is proposed in this paper. The proposed VPC-PDAS fully utilizes the VPC, VPN, https protocol and service monitoring technologies. It is capable of a safer, securer, and more reliable operation than existing PDASs and public cloud based PDASs. The VPC-PDAS is not vulnerable to cyberattacks and is capable of continued operation even under conditions of extreme natural disasters. Besides, an SOA is adopted in the system, which is loosely coupled, easy to expand, and cross-platform enabled. Compared with the existing PDAS, the annual failure time of the system is reduced from 61.2 to about 0.43 min, which is 142 times lower than that of the existing PDAS. The framework has been in operation in the Lipu power system, China since May 2016. It is proven to be reliable, safe, and cost-effective, with a bright prospect for future applications.

References

[1] B. Bitzer, "Cloud-based smart grid monitoring and controlling system," in *Proc. 50th Int. Univ. Power Eng. Conf.*, 2015, pp. 1–5.

[2] B. Bitzer and E. S. Gebretsadik, "Cloud computing framework for smart grid applications," in *Proc. 48th Int. Univ. Power Eng. Conf.*, 2013, pp. 1–5.

[3] G. Leijiao, W. Shouxiang, and G. Xianjun, "Framework design of cloud computing technology application in power system transient simulation," in *Proc. IEEE PES Asia-Pacific Power Energy Eng. Conf.*, 2014, pp. 1–6.

[4] C. Xu, F. Zhao, Z. Wang, X. Lin, S. He, and C. Shao, "Design of cloud computing architecture for power system analysis," in *Proc. IEEE Int. Conf. IEEE Region 10*, 2013, pp. 1–4.

[5] D. A. Chekired and L. Khoukhi, "Smart grid solution for charging and discharging services based on cloud computing scheduling," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3312–3321, Dec. 2017.

[6] Y.-Y. Sun, J.-J. Yuan, and M.-Y. Zhai, "Cloud-based data analysis of user side in smart grid," in *Proc. 2nd Int. Conf. Open Big Data*, 2016, pp. 39–44.

[7] M. Shojafar, N. Cordeschi, and E. Baccarelli, "Energy-efficient adaptive resource management for real-time vehicular cloud services," *IEEE Trans. Cloud Comput.*, vol. PP, no. 99, p. 1, Apr. 2016.

[8] M. M. Tajiki *et al.*, "Joint energy efficient and QoS-aware path allocation and VNF placement for service function chaining," arXiv 2017, arXiv: 1710.0261.

[9] F. Luo *et al.*, "Cloud-based information infrastructure for next-generation power grid: Conception, architecture, and applications," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1896–1912, Jul. 2016.

[10] G. Tan *et al.*, "A safety design of electric cloud computing platform," in *Proc. 4th Int. Conf. Comput. Inform. Sci.*," 2012, pp. 868–871.

[11] S. Xin, Q. Guo, J. Wang, C. Chen, H. Sun, and B. Zhang, "Information masking theory for data protection in future cloud-based energy management," *IEEE Trans. Smart Grid*, vol. PP, no. 99, p. 1, 2017.

[12] S. Baktir, "Privacy preserving smart grid management in the cloud," in *Proc. Int. Conf. IT Convergence Security*, 2014, pp. 1–4.

[13] X. Xiaoping and Y. Junhu, "Research on cloud computing security platform," in *Proc. Fourth Int. Conf. Comput. Inform. Sci.*, 2012, pp. 799–802.

[14] S. Bera, S. Misra, and J. J. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, May 2015.

[15] F. Ma, X. Luo, and E. Litvinov, "Cloud computing for power system simulations at ISO New England—Experiences and challenges," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2596–2603, Nov. 2016.

[16] E. Litvinov *et al.*, "Cloud-based next-generation IT paradigm for the operations of future power systems," in *Proc. Power Syst. Comput. Conf.*, 2016, pp. 1–7.

[17] F. Ma, X. Luo, Q. Zhang, and E. Litvinov, "Cloud computing: An innovative IT paradigm to facilitate power system operations," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, 2015, pp. 1–5.

[18] Aliyun, Virtual Private Cloud, 2014.

[19] C. C. Lamb and G. L. Heileman, "Overlay architectures enabling cloud computing for multi-level security environments services," in *Proc. IEEE Eighth World Congr. Serv.*, 2012, pp. 116–124.

[20] M. Mahalingam *et al.*, "Virtual eXtensible local area network (VXLAN): A framework for overlaying virtualized layer 2 networks over layer 3 networks," Document IETF RFC 7348, Aug. 2014.

[21] Amazon, What is Amazon VPC, 2014.

[22] S. Jahan, Md. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for virtual private networks," in *Proc. Int. Conf. Netw., Syst. Security*, 2017, pp. 39–44.

[23] Aliyun, RDS for SQL Serve, 2014.

[24] O. Yevsieieva and S. M. Helalat, "Analysis of the impact of the slow HTTP DOS and DDOS attacks on the cloud environment," in *Proc. 4th Int. Sci.-Practical Conf. Problems Infocommun. Sci. Technol.*, 2017, pp. 1–5.

[25] The difference between HTTP and HTTPS. [Online]. Available: https://www.cnblogs.com/wqhwe/p/5407468.html

[26] W. Li, "Risk assessment of power systems: Models, methods, and applications," *Interfaces*, vol. 36, no. 2, pp. 179–180, 2014.

[27] S. Verbrugge *et al.*, "General availability model for multilayer transport networks," in *Proc. 5th Int. Workshop Des. Reliable Commun. Netw.*, 2005, pp. 16–19.

[28] Aliyun, Help and Documents, 2014.

[29] Aliyun, Auto Scaling, 2014.

Dongxu Yang received the B.S. degree in power engineering from Guangxi University, Nanning, China, in 2015. He is currently working toward the Master's degree at the Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University.

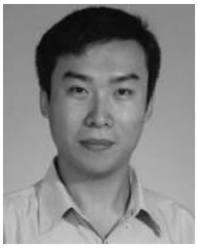
His research interest includes power system optimization.

Hua Wei received the B.S. and M.S. degrees in power engineering from Guangxi University, Nanning, China, in 1981 and 1987, respectively, and the Ph.D. degree in power engineering from Hiroshima University, Japan, in 2002.

He is currently a Professor with Guangxi University. He is also the Director of the Institute of Power System Optimization, Guangxi University. His research interests include power system operation and planning, particularly in the application of optimization theory and methods to power systems.

Yun Zhu received the B.S. and Ph.D. degrees in power engineering from Guangxi University, Nanning, China, in 1997 and 2012, respectively.

He is currently a Teacher with the Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University. His research interests include power system optimization.



Peijie Li (M'15) received the B.E. and Ph.D. degrees in electrical engineering from Guangxi University, Nanning, China, in 2006 and 2012, respectively.

From 2015 to 2016, he was with Argonne National Laboratory, Lemont, IL, USA, as a Visiting Scholar. He is currently an Associate Professor with Guangxi University. His research interests include optimal power flow, small-signal stability, and security-constrained economic dispatch and restoration.

Jian-Cheng Tan (M'96–SM'09) received the B.Sc. degree in electrical engineering from Huazhong University of Science and Technology (HUST), Wuhan, China, in 1985, the M.Sc. degree in electrical engineering from Guangxi University, Nanning,China, in 1988, and the Ph.D. degree in electrical engineering from the University of Manchester Institute of Technology, Manchester, U.K., in 1999.

She is currently a Professor with Guangxi University, China.

Dr. Tan is a Member of the IEC TC 57 Working Group 10. She is involved in several CIGRE and IEEE Power System Relaying Committee working groups.