

5G Virtual Private Networks for Electric Power White Paper: Network Security

2022 March



Preface

5G is now entering diverse industries, including the electric power industry. 5G technologies can be adopted in the electric power industry to quicken the industry's digital and intelligent transformation, which will provide strong support for building a clean, secure, efficient, and low-carbon electric power system. However, before widely applying 5G technologies in the industry, we must address current network security issues. Network security is at the basis of digital transformation and the industry has put forward the security protection principle "secure partitioning, exclusive network use, horizontal isolation, and vertical authentication". To address network security issues and comply with the principle, we need a network security protection system, which can ensure both optimal 5G transmission performance and strong security capabilities.

In April 2021, the 5G Application Industry Array (5GAIA) and 5G Deterministic Networking Alliance (5GDNA) jointly initiated the project for drafting the White Paper for 5G VPP Security. As the project leader, the Power Dispatching and Control Center of China Southern Power Grid has worked with many partners, including electric power enterprises, operators, communications device vendors, terminal chip and module vendors, and network security product and service providers. After thorough discussion on the security issue of the 5G virtual private network for electric power (5GVPP), the parties have drafted this white paper. Approved by 5GAIA and 5GDNA, the parties now would like to jointly release this document to the public.

This white paper is the third of its series, following 5GDN@Smart Grid White Paper: Requirements, Technologies, and Practices (2020) and 5GDN@Smart Grid White Paper II: Building Virtual Private Networks for Electric Power (2021). This white paper expounds the security requirements for and risks in adopting 5G technologies for electric power services, analyzes the security capabilities of 5G networks, and presents a reference security model. It also proposes an available and reliable security solution for 5GVPP, involving security isolation, multi-layer authentication, security protection, and monitoring. In addition, it provides some typical security cases for wide and local area electric power networks, and elaborates on the development trends of 5GVPP.

The materials and information contained in this white paper, including but not limited to text, images, data, points of views, and suggestions are provided solely for informational purposes. Any material or information in this white paper should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject matter. All content provided in this document is protected by copyright laws. Except for content cited from other parties, all copyrights of the aforementioned content and information are reserved by 5G Application Industry Array (5GAIA) and 5G Deterministic Networking Alliance (5GDNA). Without prior written permission, no part of this document may be released, reposted, compiled, transferred, transmitted, sold, or exploited in any form or by any means. When reproducing, distributing, or using any parts of this white paper in any form or by any means, you must cite "Source: 5G Application Industry Array (5GAIA) and 5G Deterministic Networking Alliance (5GDNA)". Any individual or organization involved in the violation of the preceding statements will hold their relevant legal liabilities.

Main Authors

(in no particular order)

- Hong Danke, Tao Wenwei, Cao Yang, Zhang Guoyi, Zhu Hailong, Lin Xubin, and Hu Feifei (from Power Dispatching and Control Center of China Southern Power Grid)
- Kuang Xiaoyun, Chen Liming, and Suo Siliang (from China Southern Power Grid Research Institute)
- Wang Yang, Ding Huixia, Wang Zhihui, Ma Baojuan, Meng Sasuala, and Zhu Sicheng (from China Electric Power Research Institute)
- Chen Bin, Chen Duanyun, Su Suyan, Chen Jinshan, Xia Bingsen, and Li Yuanhao (from China State Grid Fujian Electric Power Co, Ltd.)
- Du Jiadong, Wang Qi, Hou Weibin, and Zhou Jie (from China Academy of Information and Communications Technology)
- Wang Li, Sun Lei and Wang Wei (from Guangzhou Power Supply Bureau of China Southern Power Grid)
- Wang Wenge, Shen Jing, Zhao Yujing, Yang Ying, and Yan Lijing (from China State Grid Henan Electric Power Communication Co., Ltd.)
- Zhou Peng, Chen Xiaoxiao, and Yang Fan (from China State Grid Zhejiang Electric Power Communication Co., Ltd.)
- Yang Peng, Qiu Qing, Zhou Mo, Cui Xusheng, Wu Peizhe, Song Yue, and Wang Rong (from China Mobile)
- Shen Jun, Liu Yatian, Hu Bowen, Bo Mingxia, and Xia Xu (from China Telecom)
- Chen Dan, Wang Changling, Xiao Yu, Jiang Xiaoyan, Fan Yongjie, Zhu Shaobo, Cai Qingyu, Zhao Yuan, and Li Xianda (from China Unicom)
- Yu Xiaoguang, Yu Yingxin, Yang Xiaohua, Hao Jingjing, and Yang Chenjinjian (from Huawei)
- Teng Zhimeng, Feng Yan, and Chen Yongbo (from ZTE);
- Wang Jin and Yuan Yin (from Guangdong Planning and Designing Institute of Telecommunications)
- Zhang Weiqiang, Chen Dingyun, and Zhu Yongxu (from UNISOC)
- Xu Tao (from XJ Group Corporation)
- Hu Yang, Zhang Ying, Gong Liangliang, and Li Yang (from Nanjing NARI Information and Communication Technology Co., Ltd.)

The following personnel also participated in drafting this white paper:

- Liu Gangting, Wang Danhong, and Ren Ruobin (from China Mobile Group Guangdong Co. Ltd.)
- Wei Yingqiang and Sun Baining (from China Mobile Group Fujian Co. Ltd.)
- Jia Qiang (from Beijing Smartchip Microelectronics Technology Co., Ltd.)
- Li Xu'an (from Fibocom Wireless Inc.)
- Ma Lei, Liu Xin, Liu Donglan, Wang Rui, and Zhang Hao (from China State Grid Shandong Electric Power Research Institute)
- Xu Qun, Liu Mingfeng, Li Kun, Meng Jian, and Hou Lu (from China State Grid Qingdao Power Supply Company)
- Zhang Likun, Zeng Shan, and Wang Ruixiang (from Aostar Information Technologies Co., Ltd.)



Introduction

The electric power industry includes power grid enterprises and power generation enterprises. The general requirements for service classification and security control are basically the same., a key infrastructure, is vital to the nation and people's livelihood. As the power grid becomes intelligent, we will see a wide application of 5G network technologies in the industry. These cutting-edge technologies — like network slicing and multi-access edge computing (MEC) — are involved in all electric power service sectors, including electricity generation, transmission, transformation, distribution, and consumption. Leveraging these technologies, we have formed 5G virtual private networks for electric power (5G VPPs), speeding up the power grid's intelligent transformation.

Table 1.1 Network requirements of 5G VPP services

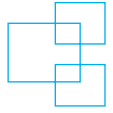
Service Type	Typical Application Scenario	Current Situation	Future Requirement
Basic services	Intelligent distributed power distribution automation, intelligent power distribution network synchronous phasor measurement, power demand response, advanced metering, distributed energy control, charging piles, and emergency communications	The service solutions are mature and available. 1. Connection mode: Centralized master stations + distributed sub-stations 2. Data collection frequency: Low 3. Precision: Low	1. Connection mode: Master stations are moved downwards to process local services. 2. Data collection frequency: High (minute-level) 3. Precision: High (millisecond-level, node-specific)
Extended services	Inspection robots, unmanned aerial vehicle (UAV)-based inspection on power transmission lines, Internet of Things (IoT)-based status monitoring, intelligent customer service centers, warehousing management, and smart home	The service solutions are under rapid development and continuous optimization. Basic data and images can be collected. The bandwidth for a single terminal ranges from 100 kbit/s to 2 Mbit/s. The number of data collection terminals connected to the network is limited.	1. Strong connection capabilities are needed for a large number of connections, as the number of terminals rise along with the development of IoT technologies. 2. A higher bandwidth is required as more high-definition (HD) video applications will be adopted. 3. Convergent data collection is needed for implementing precise industrial production control. 4. More requirements need to be met as AI technologies develop and are being adopted in the industry.
Special scenarios	Smart campuses, smart power plants, in-depth coverage in underground plants, 3D space positioning, visualized O&M, intelligent diagnosis, power source-power network coordination, and decision-making support	The service solutions are in the initial stage.	1. Positioning is urgently needed, especially for underground environments. 2. Massive connections are required as the number of IoT devices, like sensors, grows exponentially. 3. Network entity collaboration, intelligent diagnosis, and decision-making support based on AI and big data technologies are needed.

The 5G VPP solution provides highly reliable security isolation for services in different power grid sectors, addressing the preceding requirements. Leveraging new technologies like software-defined networking (SDN), network functions virtualization (NFV), and service-based architecture (SBA), this solution isolates physical and virtual resources at different layers.

However, 5G VPP is still in its infancy and its security system needs to be improved. For example, the security isolation solution for network slices needs to be refined, as do the scenarios and processes of secondary authentication for terminals. In addition, as new services like energy big data and comprehensive energy services emerge, the ecosystem and service environment are becoming more complex, and data is shared more frequently. All these require changes to the network security architecture for electric power services, and bring huge challenges to service and data security. As such, the industry must urgently improve the 5G VPP security protection solution and integrate it with the electric power service security protection system, so as to guarantee communication security for smart grid services.

This white paper analyzes the security requirements on 5G VPP from the technical perspective, presents a reference model and architecture, and offers an available and reliable 5G VPP security solution, as well as some typical application cases.

02 Security Requirements and Risks upon 5G VPP



This chapter analyzes the security requirements for and risks in using 5G VPP for electric power services.

2.1 Security Requirements of Electric Power Services

According to regulations, the electric power service monitoring system must comply with the principle "secure partitioning, exclusive network use, horizontal isolation, and vertical authentication". To this end, this white paper classifies electric power services into three types — basic, advanced, and maximal security services — based on their security requirements.

Basic security services refer to common Internet services, like instant messaging and staff training. These services have low security requirements, and can be accessed through Internet channels.

Advanced security services are in the management information security area. These services involve electric power production management and office automation, and require frequent interactions between the personnel and the computers running production or management systems, like the power dispatching operation management and asset management systems. The advanced security service data needs to pass through the wireless virtual private network and firewall to the information intranet, and then through the secure access platform to the service master station.

Maximal security services are involved in electric power generation and dispatching, including real-time control and information collection services, like the automatic security control and tele-meter reading systems. These services require high-level security protection. As in advanced security services, the service data needs to go through the wireless virtual private network and firewall to the information intranet, but then needs to access the service master station through the secure access area (containing the forward and reverse isolation devices, front-end processor, and secure access gateway).

2.2 Security Risks upon 5G VPP

Currently, Limited by the maturity of the 5G power industry chain, the 5G power virtual private network has certain security risks., in terms of terminals and modules. There are only a few vendors producing applicable terminals and modules, which are expensive but have insufficient forms and poor service adaptation capabilities. All these factors hinder these terminals and modules from being widely applied for electric power services. Meanwhile, in terms of 5G network applications, the servers running electric power services will generate, process, and store a large amount of users' sensitive information, including their personal identity information and privacy information. If the service systems have weak security protection such as in user identity security protection as well as data integrity and confidentiality protection, user data may be obtained by hackers, which will endanger users' interests and cause severe social impact. In addition, in some complex service scenarios, 5G networks may be interfered by electromagnetic waves.

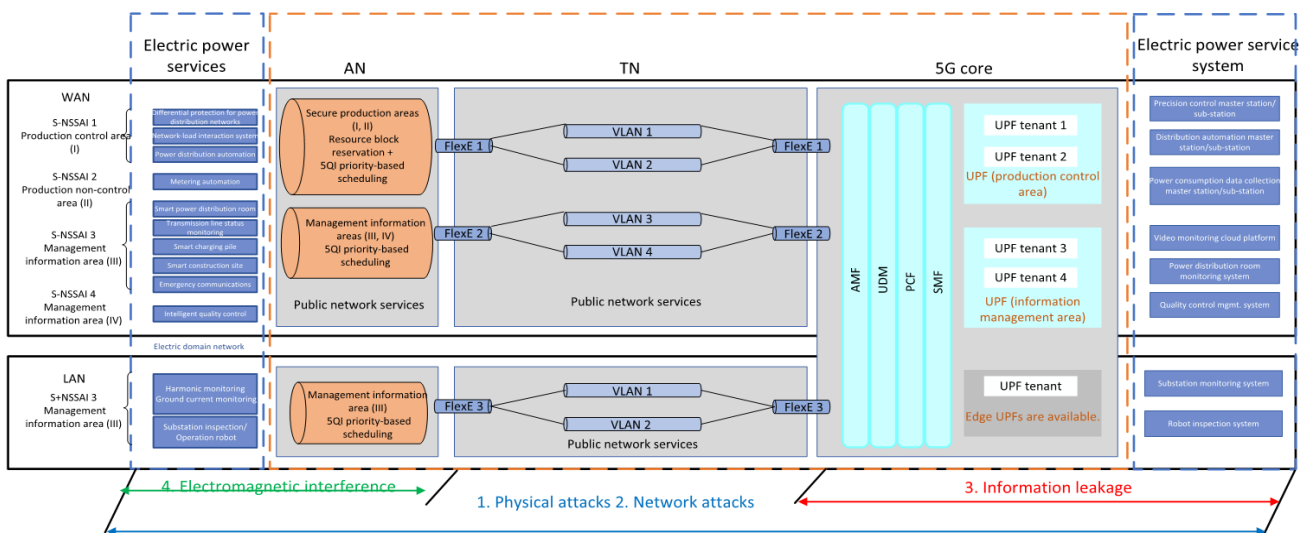
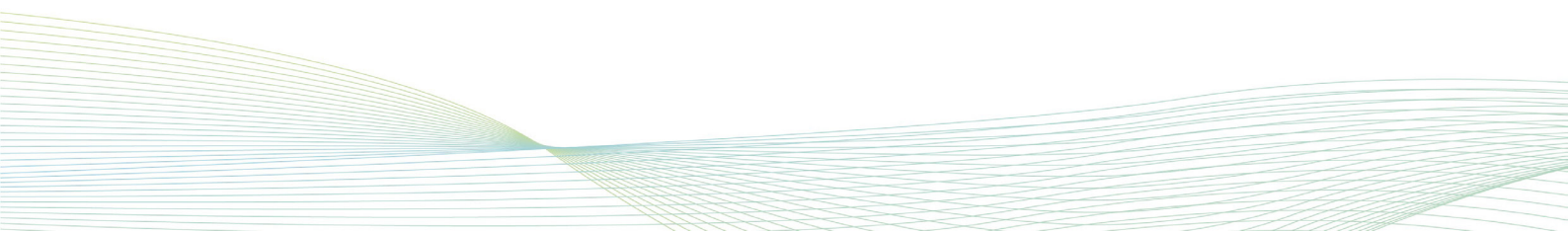


Figure 2.1 Risks and threats faced by 5G VPP

As shown in Figure 2.1, when 5G VPP is used for electric power services, it faces four types of risks: physical attacks, network attacks, information leakage, and electromagnetic interference. Table 2-1 elaborates on these types of risks:

Type	Example
<p>Physical attacks</p>	<ul style="list-style-type: none"> Physical attacks on the information system infrastructure: This will affect physical system running, and cause equipment damage and even system breakdown. For example, if physical attacks are implemented together with network attacks, electric power outages may occur across the country. Physical damage to MEC and UPF equipment: Attackers may physically destroy MEC and UPF equipment or access these devices without authorization, which may damage other equipment or interrupt communications.
<p>Network attacks</p>	<ul style="list-style-type: none"> Network intrusion and computer virus infection: If the network is intruded or infected by a computer virus (like worms), the information system of the power grid may be faulty. Identity spoofing: Attackers may forge authorized user accounts to access the network. Tampering of user data Unauthorized access: Resources in a slice may be accessed by unauthorized users from other slices, which may cause faults and errors in the slice, and affect proper slice operations. Distributed denial of service (DDoS) Device version damages: Version files (including software version files (.set) and patch files (.pkg)) and firmware files may be tampered with or damaged during the E2E process covering version release, onsite installation, and upgrade. Therefore, the version files must be digitally signed before being released. During file transfer and version installation/upgrade, the files can be verified based on digital signatures to ensure their validity, integrity, and security.
<p>Information leakage</p>	<ul style="list-style-type: none"> Data leakage: The core network database faces many risks, involving SQL injection, default accounts and passwords, database platform vulnerabilities, abuses of rights, and privilege escalation. All these may be exploited to access and obtain data. User privacy information leakage: User privacy information in 5G networks includes user identities, the mobility mode, location information, and data usage mode. Attackers may use various methods to obtain such privacy information.
<p>Electromagnetic interference</p>	<ul style="list-style-type: none"> Interference on wireless operating frequency bands: Attackers may use wireless radio transmitters to cause interference on wireless channels, causing communication interruption. As a result, service terminals will become "blind" and unable to control.

Table 2.1 Security risks and example threats for 5G VPP



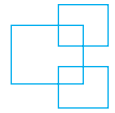
2.3 Security Requirements on 5G VPP

In terms of the three electric power service security levels, 5G VPP risks, and 5G communication technology features, this white paper puts forward the following security requirements for using 5G VPP for electric power services.

No.	Security Risk	Security Requirement	Security Mode		
			Basic	Advanced	Maximal
1	Physical attacks	Monitoring + abnormality response	<ul style="list-style-type: none"> • Provide security monitoring for electric power equipment. • Develop security management policies. • Scan for vulnerabilities and update system patches in a timely manner. 	<ul style="list-style-type: none"> • Provide all-round and around-the-clock security monitoring for all involved equipment and devices. • Develop security management policies. • Scan for vulnerabilities and update system patches in a timely manner. 	<ul style="list-style-type: none"> • Provide all-round and around-the-clock security monitoring for all involved equipment and devices. • Develop security management policies. • Scan for vulnerabilities and update system patches in a timely manner.
2	Network attacks	Isolation + encryption + authentication	Implement logical isolation, and adopt dedicated security encryption algorithms, primary authentication of 5G networks, slice access authentication, and network exception monitoring.	Implement physical isolation or strong logical isolation, and adopt dedicated security encryption algorithms, dedicated encryption and authentication	Implement physical isolation, and adopt dedicated security encryption algorithms, dedicated encryption and authentication devices, multi-layer authentication, and 5G smart grid terminals with enhanced authentication.
3	Information	Encryption + authentication	Adopt dedicated security encryption algorithms, primary authentication of 5G networks, and slice access authentication.	Adopt dedicated security encryption algorithms, dedicated encryption and authentication devices, and multi-layer authentication.	Adopt dedicated security encryption algorithms, dedicated encryption and authentication devices, multi-layer authentication, and 5G smart grid terminals with enhanced authentication.
4	Information	Encryption + authentication	Adopt dedicated security encryption algorithms, primary authentication of 5G networks, and slice access authentication.	Adopt dedicated security encryption algorithms, dedicated encryption and authentication devices, and multi-layer authentication.	Adopt dedicated security encryption algorithms, dedicated encryption and authentication devices, multi-layer authentication, and 5G smart grid terminals with enhanced authentication.

Table 2-2 Security requirements on using 5G VPP for electric power services

03 Reference Security Model and Architecture



This section describes the reference security model and architecture of 5G VPP from the aspects of isolation, authentication, security monitoring, and response to meet the requirements of basic, advanced, and maximal security services.

3.1 Security Model for 5G-Enabled Electric Power Services

The following figure illustrates the reference security model of 5G VPP, showing the requirements of services at different security levels on isolation, encryption, authentication, monitoring, and response.

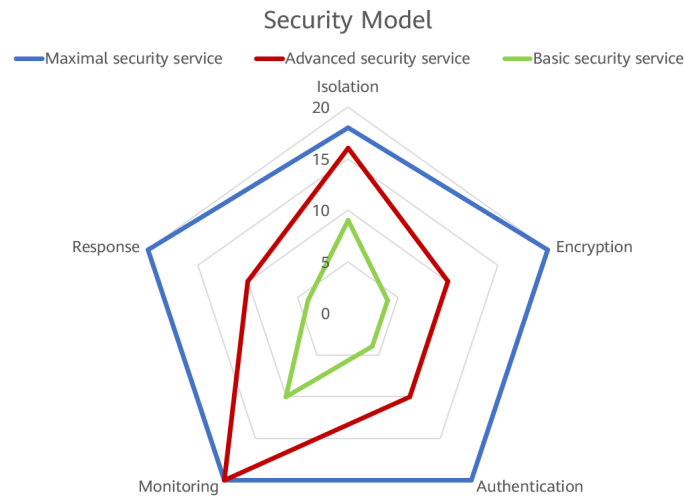


Figure 3-1 Reference security model of 5G VPP

Isolation, both hard and soft isolation, is the division of RAN resources (including base station processing resources and radio spectrum resources), TN resources, and CN resources based on different slicing solutions.

a. Hard isolation

Hard isolation is close to physical isolation, for example, isolating production control services from production management services. In this type of isolation, independent spectrums are used and resource blocks (RBs) are reserved on the RAN to provide different radio resources. On the TN, transmission devices are used to carry control-plane and user-plane data, and FlexE-based hard slicing is supported. On the CN, electric power services use the exclusive edge UPF and independent control-plane function units. Terminals are allowed to access the self-owned service platform in a site through secure access zones.

b. Soft isolation

Soft isolation, by contrast, is close to logical isolation. For example, regions are classified into different types based on service requirements and isolated from other types using S-NSSAIs. On the RAN, reserved RBs are shared by certain services and scheduled based on 5G Quality Identifier (5QI) priorities. On the TN, VPN technologies are supported. On the CN, electric power services can use the UPF or certain control-plane NFs exclusively, or share the UPF and all control-plane NFs with other services to meet various security isolation requirements. Based on whether the VPN encryption technology is used on the TN and whether dedicated NFs are used on the CN, soft isolation is classified into strong logical isolation and common logical isolation.

Encryption means encrypting terminal data storage and data transmission during communication.

Authentication is performed on terminal identities and accesses to terminal data and the system.

Monitoring is used in 5G network security to identify sudden attacks.

Response means the generation of alarms and handling of detected attacks, including the detection and handling of security vulnerabilities that may compromise products or solutions and the handling of physical attacks and electromagnetic interference.

3.1.1 Security Model for Basic Security Services

Basic security services transmit data and authenticate identities on the Internet or VPNs. The network must be able to detect attacks from the Internet and provide security protection that meets service requirements.

3.1.2 Security Model for Advanced Security Services

Advanced security services can be connected to the Internet and can perform strong logical isolation, which is close to physical isolation, and the necessary authentication, encryption, and access control to prevent attacks from the Internet and ensure reliable access to the service system. Among the advanced security services, the security protection of the video content analysis service is highlighted.

3.1.3 Security Model for Maximal Security Services

Maximal security services require encrypted transmission and identity authentication on the dedicated communication network for electric power and are physically isolated from services of other security levels on the communication network. Devices and networks with low-level security protection capabilities used in the same service must be interconnected with those with high-level security protection capabilities through the necessary security isolation. Maximal security services require the 5G network to provide high-performance monitoring capabilities to support real-time and intensive accesses, and demand response and recovery capabilities in the case of network faults and intrusions.

3.2 Overall Reference Security Architecture

Before further developing the smart grid, 5G VPP should comply with four general security principles: security zoning, dedicated networks, horizontal isolation, and vertical authentication. Its security architecture covers the three layers of cloud, pipe, and device and involves device security, pipe security, platform security, and security management.

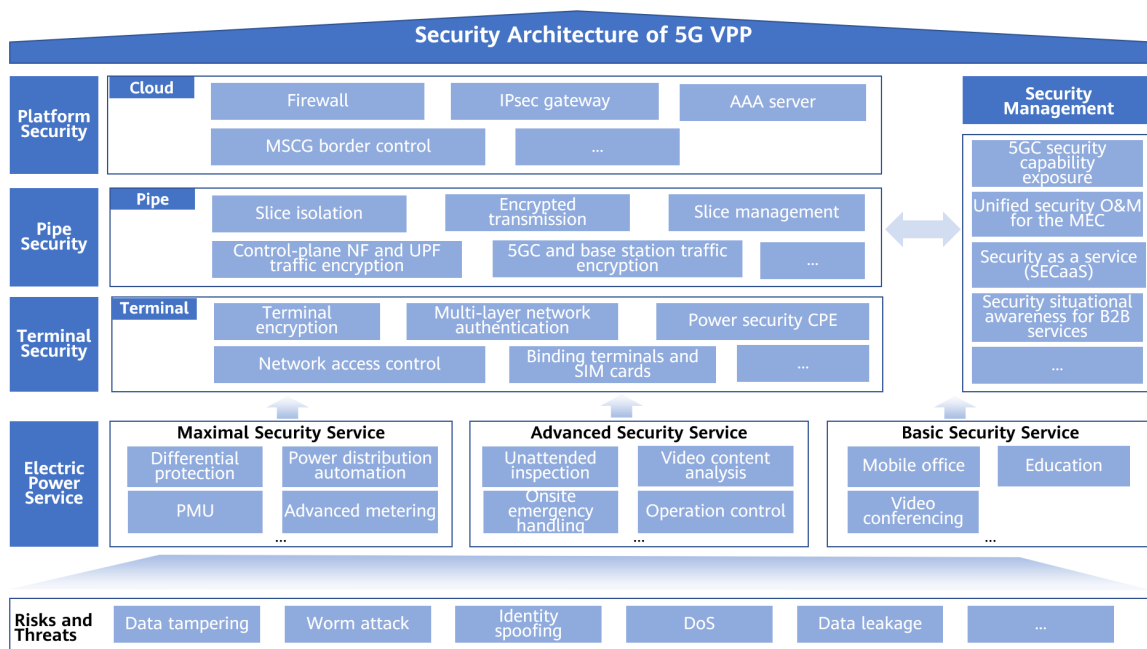
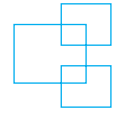


Figure 3-2 5G Overall reference security architecture

This architecture focuses on building security protection capabilities at the terminal, pipe, and platform layers and strengthening the security management capabilities of 5G VPP to meet security requirements of different levels.

- Terminal security:** Terminals can integrate customized security modules and support asymmetric encryption based on Chinese cryptographic algorithms, implementing terminal identity authentication through the master station and protecting packet integrity. For important terminals, zero-trust access control approaches such as two-way authentication and data encryption are supported. In addition, for certain key services, security policies, like IMSI-IMEI or DNN-S-NSSAI binding, can be applied.
- Pipe security:** Slice isolation and customization can be combined to formulate slice policies that adapt to electric power services of different security levels and to ensure private network security.
- Platform security:** Different security access areas are established for electric power services, and AAA servers are deployed for secondary authentication, to prevent attacks from malicious terminals or third-party applications.
- Security management:** Carriers have applied 5G network security capabilities in the electric power industry. With these capabilities, they can centrally monitor terminals, slices, MEC devices, the exclusive UPF, and security protection devices, achieving uninterrupted and comprehensive security situational awareness, in 5G Electric Power Virtual Private Network.

04 Reference Security Solutions



5G VPP should meet basic protection policy requirements: security zoning, dedicated networks, horizontal isolation, and vertical authentication. Based on these requirements, this section describes multiple security capability combinations and reference security solutions on the device, pipe, and cloud sides for different security levels of electric power services.

4.1 E2E Network Security Isolation

According to the requirements of electric power services, different isolation modes are needed for different security zones or for different services in the same security zone. For example, for maximal security services, the isolation should reach or be close to the physical isolation; for advanced security services, the isolation should be close to physical isolation or strong logical isolation; and for basic security services, common logical isolation is enough. Therefore, different isolation methods need to be adopted in the access, transport, and core networks for 5G VPP to implement flexible horizontal isolation.

4.1.1 Security Isolation for Access Networks

In 5G access network security isolation, resources are scheduled mainly using 5QI priorities and RB reservation. RB reservation is an important feature that distinguishes 5G from 4G.

Based on the isolation requirements of different electric power services, the following three isolation modes can be used:

Full resource sharing: All radio resources are shared. No network slice directly participates in resource scheduling. Instead, their resources are scheduled by a common scheduler.

Partially exclusive resources: Radio resources are generally scheduled based on 5QI priorities, and RBs are reserved for dedicated network slice services.

Fully exclusive resources: The access network uses independent hardware and spectrum resources for maximal security. However, this mode may increase network construction costs.

4.1.2 Security Isolation for Transport Networks

Services on the transport network (between the access and core networks) can be isolated using network slicing. The forwarding planes of different network slices are isolated from each other, and the isolation level depends on the slicing technologies adopted by the forwarding planes. Hard slicing and soft slicing are available for the isolation.

Hard slicing: is used for physical hard pipes at Layer 1 or the optical layer. Examples for this type of slicing are FlexE slicing, OTN slicing, and WDM slicing.

Soft slicing: is based on statistical multiplexing and used at Layer 2 or above. It covers SR/MPLS-TP tunneling, SR/MPLS-TP pseudo wire emulation, and VPN/VLAN-based virtualization.

In actual situations, hard slicing and soft slicing can both be used. Hard slicing meets requirements like service isolation security and low network latency, and soft slicing improves bandwidth utilization through multiplexing.

4.1.3 Security Isolation for Core Networks

There are also three resource scheduling modes available for 5G core network security isolation and you can select them based on electric power service types.

Full resource sharing: This mode is the same as the best-effort mode for 2G/3G/4G networks with one transmission path. It is applicable to common consumer services of public networks and has no special requirements for security isolation.

Partially exclusive resources: A few network functions are exclusively used while the others are shared. This mode balances security and costs and is applicable to advanced and maximal security services.

Fully exclusive resources: In this mode, a complete dedicated core network for electric power is constructed. This mode can ensure maximal security protection but with the highest construction and operating costs. It is applicable to special services that require ultra-high security isolation.

In actual networking, isolation modes of the access, transport, and core networks must be selected based on the service security levels and isolation requirements. For example, for applications with high requirements on security isolation, RB reservation and FlexE-based hard pipe isolation must be performed for the access and transport networks, respectively; and the core network should either adopt the partially exclusive mode to exclusively occupy the user plane UPF or the fully exclusive mode to exclusively occupy the user plane UPF and control plane AMF and SMF. For applications with low requirements on security isolation, the access network either adopts the full sharing mode or performs resource scheduling based on 5QI priorities, the transport network uses VPN channels for soft isolation, and the core network adopts the full sharing mode to share the edge UPF.

4.2 Multi-Layer Authentication System for Vertical Authentication

According to the requirements of electric power services, technical measures like authentication, encryption, and access control need to be taken to secure data transmission. On 4G networks, only APN names and passwords can be used to authenticate service access requests. Once authentication information is disclosed, electric power networks can be accessed by unauthorized users. As such, 5G VPP requires vertical authentication measures, like terminal access authentication and secondary authentication, to ensure the validity of terminals accessing the master station.

In 5G VPP, the multi-layer authentication system was proposed based on the 3GPP 5G authentication system. It uses the standard three-layer authentication and additionally provides authentication on the electric power side. This prevents attackers from using unauthorized IMSIs or IMEIs to access the power system or slice and initiating network attacks on the master station of power services.

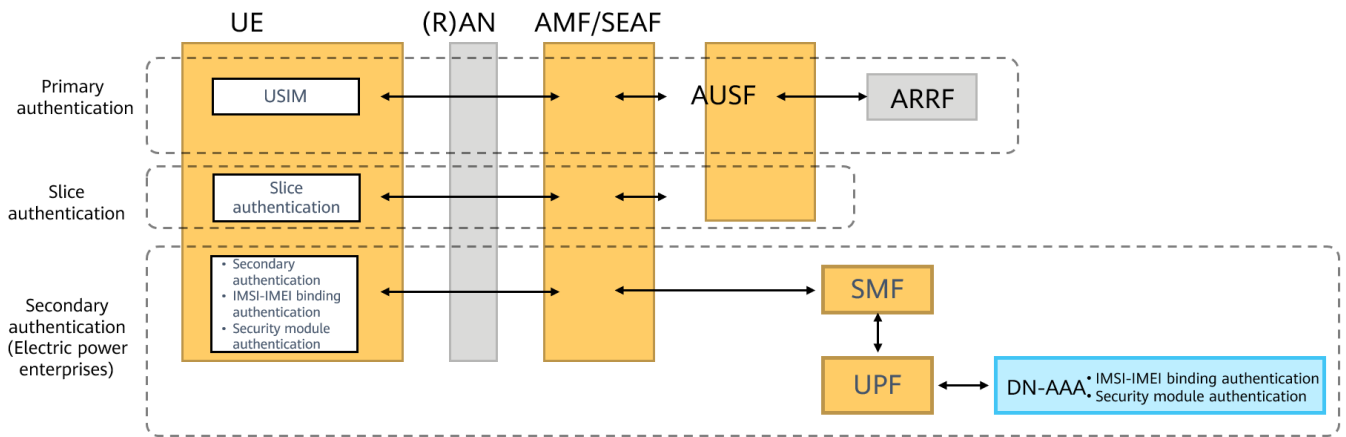


Figure 4.1 Multi-layer authentication

Multi-layer authentication includes:

IMSI-IMEI binding: The core network performs IMSI-IMEI binding authentication. If a UE's IMSI and IMEI do not match, the UE cannot access the network.

Secondary authentication: Based on 3GPP's secondary authentication architecture and standard protocols, secondary authentication is performed between a terminal and the DN-AAA server. If the secondary authentication fails, the terminal is not allowed to access electric power services.

Security module authentication: Terminals are each integrated with a security module that support Chinese cryptographic algorithms. They implement bidirectional identity authentication at the network layer and then set up IPsec VPN tunnels with the central security gateway for data transmission.

In actual applications, the security isolation mode needs to be appropriately selected based on the service security level and vertical's authentication requirements. Particularly after the multi-layer authentication system was introduced for 5G VPP, service data encryption and identity authentication can be flexibly used based on requirements. Compared with the traditional bidirectional identity authentication and channel encryption through hardware security modules, this multi-layer authentication system significantly simplifies the authentication process.

4.3 Security Applications Under Cloud-Edge Synergy, Providing Security Protection and Monitoring

For cloud-edge synergy-based security applications, MEC security protection and security situational awareness must be used in 5G VPP based on 5G security capability exposure, and the security authentication mode of "5G + blockchain" should be explored for certain services.

4.3.1 MEC Security Protection Based on Infrastructure and App Services

The MEC platform of electric power involves the UPF (in the trusted domain) and MEP+third-party apps (in the untrusted domain). MEC security can be enhanced through one of the following methods:

Deploy virtual security components like virtual firewalls to block invalid access requests from edge apps. Implement access control and data transmission security mechanisms, such as confidentiality protection, integrity protection, and replay attack prevention, between apps and the MEC platform as required. With port scanning, disable unnecessary ports and services of the MEC platform, and use vulnerability scanning to identify vulnerable services and ports and harden them.

Provide app lifecycle security protection. Isolate resources used by apps and provide integrity protection, confidentiality protection, and access control for app images and image repositories. In addition, provide security protection for apps, including identity security, image security, and intrusion detection.

4.3.2 5G Network Security Situational Awareness

By deploying the network security situational awareness system, electric power enterprises integrate the built-in security probes of user-side security devices and the operator's security capability exposure platform, deliver security policies, and report security device information. This accelerates E2E 5G network threat detection and provides security management capabilities before, during, and after attacks, providing quick response to security incidents and ensuring effective network security planning, construction, and operations.

4.3.3 Security Authentication for "5G + Blockchain"

The MEC site for electric power is dedicated to the edge user plane and managed by the central control plane. It is a key node for electric power enterprises and operators to build a consortium blockchain in the future. In addition, the MEC site's distributed deployment and computing capabilities match the decentralization of blockchains.

Therefore, on the basis of 5G system authentication and data encryption, technologies like 5G capability exposure and MEC can be used together with blockchains for 5G VPP, especially with the consortium blockchain of power enterprises and operators. In this way, the anti-tamper capability and security reliability of cross-domain information can be enhanced in scenarios like trusted access of power distribution terminals, local communication group member management for differential protection of power distribution networks, demand-side response, network and load interaction, virtual power plants, and electric power market trading.

4.4 Encrypted Data Transmission

5G CPEs and security modules that comply with Chinese cryptographic algorithms are used together to establish IPsec VPN tunnels. This enables encrypted data transmission on the 5G VPP and provides access authentication and communication encryption for terminals. For dispatching centers, power plants, and substations — whose data is highly sensitive and requires special protection — dedicated vertical encryption authentication devices or encryption authentication gateways as well as relevant facilities that have been tested and certified by state-designated departments should be provided to implement bidirectional identity authentication, data encryption, and access control. The encryption and authentication gateways should offer all the functions of encryption and authentication devices and be capable of processing data communication application layer protocols and messages in power systems.

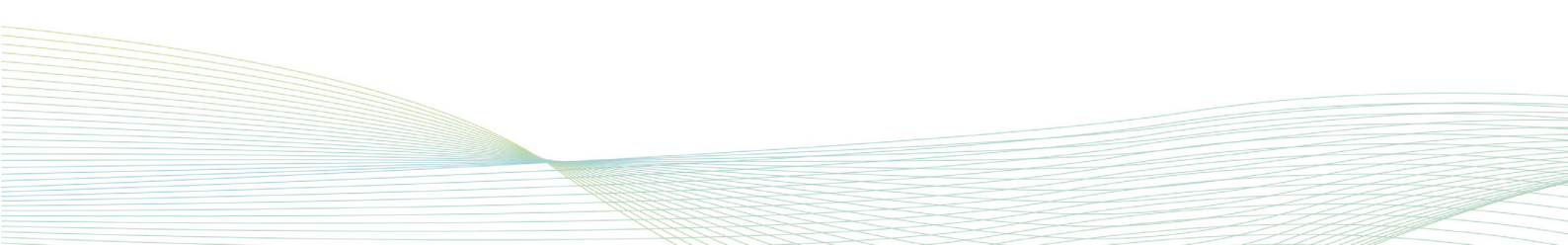
On a 5G network, user communication data must first be sent to the UPF before it is forwarded to the destination. This forms a transmission tunnel from the terminals, to the base stations, and then to the UPF. Through this tunnel, user data will be kept away from the public network, ensuring the data's security.

On the signaling plane of a 5G VPP, built-in or external IPsec VPN tunnels must be established for non-service interfaces (including N2, N3, and N4 interfaces) to provide encryption and ensure the integrity of data transmitted on the signaling plane. An authentication mechanism should also be provided between interfaces to prevent attackers from spoofing NFs to launch signaling attacks on the 5G VPP.

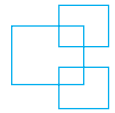
For data security, multiple technologies are adopted, such as data classification, sensitive data encryption, and traffic monitoring. These guarantees data security during data storage, processing, and exchange against data leakage and ransomware attack risks.

4.5 Security Incident Response

The 5G VPP provides services for smart grids over 5G. A smart grid generally has diversified services and application systems with high confidentiality, integrity, availability, and reliability requirements, and 5G involves multiple new technologies, participants, and complex systems. To ensure electric power services run securely and reliably and to prevent cyber security incidents, the 5G VPP must provide efficient security incident response capabilities. These capabilities, together with the joint collaboration and efforts of all parties, help effectively address security challenges facing 5G-powered smart grids. To overcome these challenges, electric power enterprises can work with industry partners — like operators, suppliers, industry associations, and standards organizations — to build an ecosystem that will help them fully leverage external technical forces to prevent, monitor, and handle security incidents. The specific process may include the following operations:

- Establishing a security incident response process and mechanism.
 - Scanning for and receiving cyber security incidents and vulnerability reports from inside and outside an enterprise.
 - Confirming the existence of an incident or vulnerability and determining its severity and impact scope.
 - Determining the root cause and the optimal solution to suppress or eliminate the impact.
 - Monitoring the progress of implementing the incident or vulnerability solution.
 - Monitoring electromagnetic interference and physical damage and providing countermeasures.
- 

05 Security Applications of the 5G VPP



5.1 5G VPP on a WAN

A 5G WAN VPP has been constructed based on the top-level architecture of the 5G VPP and 5G SA slice network in a power supply area. This "5G + smart grid" demonstration area covers 51 service scenarios throughout power generation, transmission, distribution, transformation, consumption, and integration.

So far, production control services, including online substation equipment monitoring, distribution automation, distribution network differential protection, and Phasor Measurement Units (PMUs), have been implemented in the demonstration area. Currently, management information services, like online transmission line status monitoring, video analysis, robot inspection, and intelligent power distribution rooms, are in trial use. The demonstration area has successfully provided an innovative operation mode for security application of the 5G VPP on the WAN.

1. Reliable security isolation: Based on the 5G VPP's top-level architecture, RBs are reserved on the wireless network's air interfaces, FlexE-based hard pipes are configured on the transmission network, and electric power-dedicated slices, UPF devices, and MEC devices are provided on the core network. The solution isolates services of electric power companies and other public and industry users and enables 5G slices carrying production control services to provide E2E isolation, a step up from logical isolation on 4G networks, fully meeting security requirements for bearing electric power services.

2. Stable ultra-low latency and precise timing: The 5G network, featuring ultra-low latency and precise timing, meets the requirements for differential protection and synchronous phasor measurement. According to the test results from the demonstration area, the average latency of differential protection on the distribution network is in milliseconds on the WAN, the maximum latency affected by delay variation and the sampling amplitude errors of differential protection are greatly reduced, and the PMU-based timing precision is significantly improved, fully meeting the requirements for bearing electric power services.

3. Comprehensive service security monitoring and situational awareness: Based on carriers' open network capabilities, a 5G network management platform has been built to centrally manage 5G services, network slice performance, and electric power terminals. In diverse 5G application scenarios and complex network architectures, the platform enables flexible network management and control, network channel management, and massive terminal monitoring, reducing the complexity of network O&M and ensuring electric power 5G applications run efficiently, securely, and reliably.

5.2 5G VPP on a LAN

A 5G LAN VPP has been deployed in a thermal power plant and a converter station, where 5G network coverage is provided through co-construction and sharing to improve intelligent O&M and management.

The 5G VPP in the thermal power plant uses three types of 5G network slices — URLLC, mMTC, and eMBB — supporting the application of 5G in various service scenarios, like large industrial system control, video analysis, sensor access, personnel security management and control, intelligent inspection, device O&M diagnosis, and security emergency. The 5G network is also integrated into other service fields of the thermal power plant, including the Intelligent Control System (ICS) for power generation and the Intelligent Management System (IMS). The following describes the security application modes applied to the power plant's 5G VPN to enable services to go networked, information-based, digital, and intelligent.

1. High-quality coverage: Five indoor and outdoor 5G macro base stations as well as 37 5G micro base stations have been deployed to build a plant-level self-organizing 5G network that will provide high-quality 5G signal coverage in the 0.28 km² power plant. The network provides a 350 Mbit/s downlink rate and 160 Mbit/s uplink rate, ensures less than 15 ms two-way delay, supports a connection density of 107/km², and delivers an over 10 Gbit/s data processing capability.

2. Secure and controllable network security: The 5G network URLLC slicing technology is used on the production control network. On top of this, a series of technical measures, like isolated network operation, secure access zones, MEC, security isolation, log audit, situational awareness, and traffic monitoring, are adopted to ensure network security and control.



3. Integrated service application: 5G is integrated into the Distributed Control System (DCS) of the thermal power plant to build a demonstration intelligent thermal power plant with full 5G coverage and 5G service applications. This helps the thermal power plant implement preliminary global awareness, status warning, multi-station collaboration, domain-specific optimization, precise control, and comprehensive efficiency improvement.

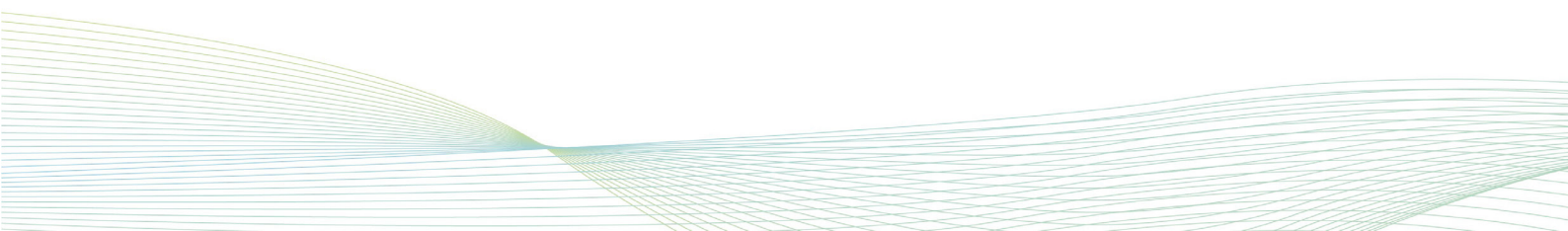
The 5G VPP in the converter station — which is a campus private network — mainly serves terminals that require basic or advanced security, like onsite operation control terminals, movement monitoring devices, individual operation terminals, intelligent inspection robots, fire control robots, and electric power drones. The following details the security application modes used on the 5G campus private network to ensure secure access and application of converter station services.

1. Flexible and reliable service access: Generally, systems that support converter station services and terminals are deployed in the station or the provincial power company. Using the flexible traffic steering, forwarding, and offloading capabilities of the MEC, the systems support flexible access to various services and terminals. Through the MEC, service data with basic security requirements is distributed to the public network and finally enters the Internet area of the electric power company. As for the service system with advanced security requirements, there are two cases:

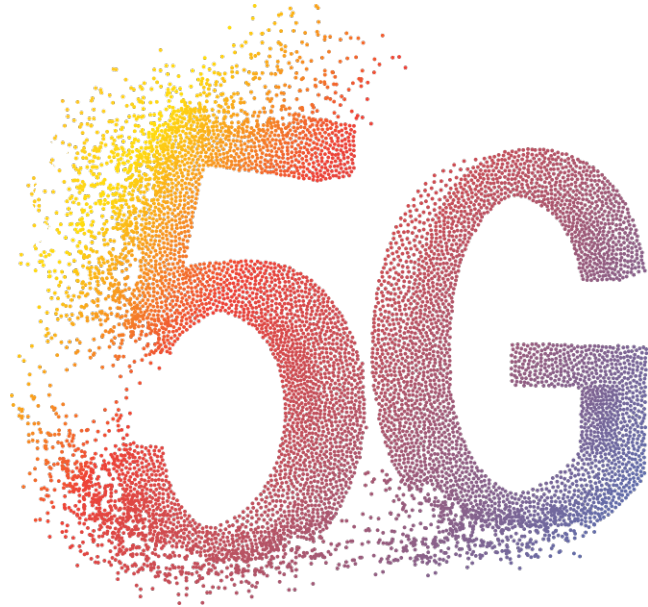
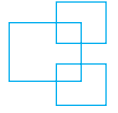
- When the system is deployed in the provincial electric power company, the MEC distributes terminal data and then transmits the data to the provincial electric power company through the electric power communication network to connect to relevant systems.
- When the system is deployed at the converter station, the MEC unloads terminal data locally and then sends the data to the server in the station, and distributes service data and forwards it to security protection devices, like security access gateways, before it is finally transmitted to the management information area.

2. Secure data isolation assurance: A dedicated 5G base station and MEC are deployed in the converter station for electric power services and work with the 5G LAN VPP to keep electric power service data within the campus, achieving high security isolation. At the same time, IMSI-IMEI binding, secondary authentication, and security module authentication are used to secure data transmission between various operating terminals and services.

3. High-performance service application experience: The 5G campus private network supports flexible frame structure configuration on the wireless side to enable uplink/downlink rate configuration, improving network QoS. During annual maintenance of the converter station in the last two years, 5G bandwidth is used to enable real-time data transmission for onsite operation control services and security devices like cameras. This helps implement real-time security control over multiple working surfaces and a large number of operators, significantly improving the efficiency of management and control. According to test results from the station, the average unidirectional latency is ultra-low when terminal data is offloaded by the MEC and then sent to the server, and the mobile video transmission quality and the audio and video interaction among terminals like robots and drones are significantly improved.



06 Summary and Outlook



5G is one of the drivers for a new round of technological revolution and industry transformation around the globe. For the electric power industry, "5G + digital grid" is urgently needed for its digitalization and building a new electric power system, which will greatly reduce carbon dioxide emissions.

As the requirements of the electric power industry change, we need to constantly improve the security capabilities of network slicing, so as to provide reliable and secure network services for the electric power industry, facilitating the construction and large-scale application of "5G + digital grid", and helping with the industry's digitalization and new electric power system.

In terms of technology, as 5G technologies evolve, service requirements change, and attack and defense technologies develop, we also need to continuously improve and enhance our security assurance methods in the RAN, TN, and CN sectors for network slices, to refine 5G VPP secure, independent, and controllable. In addition, the security capabilities of 5G network slicing become more and more intelligent. They will be more flexible and can be combined as required, so vertical industries can select security capabilities and management methods based on their own service requirements.

As for applications, the 5G industry chain will continue to work to assist the electric power industry's digital transformation. The 5G community will roll out a batch of innovative applications and innovation demonstration centers of 5G application security. All involved parties will work together more to address 5G security risks and advance the development of 5G security international standards, establish a global industry consensus and an international 5G security evaluation and certification system based on the consensus, and promote mutual trust and recognition. By doing this, we will gain more confidence and impetus for 5G security development.

Appendix A: Abbreviations

5GC:	5G Core
5GDNA:	5G Deterministic Network Association
AMF:	Access and Mobility Management Function
AUSF:	Authentication Server Function
DTU:	Data Transfer Unit
NSSF:	Network Slice Selection Function
PCF:	Policy Control Function
PMU:	Phasor Measurement Unit
RB:	Resource Block
SMF:	Session Management Function
UDM:	Unified Data Management
UPF:	User Plane Function

Appendix B: References

1. 5G Deterministic Networking Alliance (5GDNA). 5GDN@Smart Grid White Paper II: Building Virtual Private Networks for Electric Power
2. 3GPP TS 23.501 System Architecture for the 5G System
3. 3GPP TS 29.531 Network Slice Selection Services
4. National Energy Administration (NEA) of China. General Scheme of Security Protection for Electric Power Monitoring System
5. 5GDNA. 5GDN@Smart Grid White Paper: Requirements, Technologies, and Practices
6. 5G Applications Industry Array (5G AIA). 5G Industry Virtual Private Network Architecture Whitepaper
7. China Mobile. 5G Industry Private Network Technology White Paper
8. China Telecom. 5G Customized Network Product Guide
9. China Unicom. 5G Industry Private Network White Paper
10. State Grid Corporation of China, China Telecom, and Huawei. 5G Network Slicing Enabling the Smart Grid
11. China Southern Power Grid, China Mobile, and Huawei. 5G for Smart Power Grid Application White Paper
12. China Academy of Information and Communications Technology (CAICT) IMT-2020(5G) Promotion Group. 5G Security Report

Copyright Notice

The materials and information contained in this white paper, including but not limited to text, images, data, points of views, and suggestions are provided solely for informational purposes. Any material or information in this white paper should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject matter. All content provided in this document is protected by copyright laws. Except for content cited from other parties, all copyrights of the aforementioned content and information are reserved by 5G Application Industry Array (5G AIA) and 5G Deterministic Networking Alliance (5GDNA). Without prior written permission, no part of this document may be released, reposted, compiled, transferred, transmitted, sold, or exploited in any form or by any means. When reproducing, distributing, or using any parts of this white paper in any form or by any means, you must cite "Source: 5G Application Industry Array (5G AIA) and 5G Deterministic Networking Alliance (5GDNA)". Any individual or organization involved in the violation of the preceding statements will hold their relevant legal liabilities.

