GTI

Security Guidelines for 5G-Enabled Vertical Industries

http://www.gtigroup.org

Security Guidelines for 5G-Enabled Vertical Industries

Version	V1.0
Deliverable Type	□**Procedural Document** ■**Working Document**
Confidential Level	□**Open to GTI Operator Members** □**Open to GTI Partners** ■**Open to Public**
Working Group	**Security**
Task	Security Guidelines for 5G-Enabled Vertical Industries
Source members	CMCC, Huawei, CAICT
Support members	Qualcomm, Datang Mobile, ZTE
Editor	Feng Zhang, Qin QIU, Xiaoguang YU, Yingxin YU, Sijia XU, Hongmei YANG, Weiying PENG
Last Edit Date	14-07-2021
Approval Date	DD-MM-YYYY

Table of Contents

1 Introduction 5

2 Overview of 5G-Enabled Vertical Industries 5

3 Security Solutions of 5G-Enabled Vertical Industries 6

3.1 Smart Grid 6

3.1.1 Industry Introduction 6

3.1.2 Security Requirements 6

3.1.3 Security Solutions 8

3.2 Smart Manufacturing 12

3.2.1 Industry Introduction 12

3.2.2 Security Requirements 13

3.2.3 Security Solutions 14

3.3 Smart Port 18

3.3.1 Industry Introduction 18

3.3.2 Security Requirements 18

3.3.3 Security Solutions 20

4 Security Practices in 5G-Enabled Vertical Industries 23

4.1 Security Solutions 23

4.2 Advantages 27

4.3 Benefits and Promotion Value 27

5 Recommendations 28

1 Introduction

5G, the new telecommunications infrastructure enabling ubiquitous connectivity, in-depth human-machine interaction, and intelligence-driven transformation, has already been applied across various scenarios, ranging from mobile Internet to industrial and energy domains — and its value will be even further emphasized by its use in vertical industries. However, the deep integration of 5G and industries also introduces a range of new security risks and challenges.

This white paper analyzes differentiated cyber security risks and security solutions in the context of such 5G application scenarios as manufacturing, energy, and ports, aiming to guide vertical industries on how to build and deploy appropriate cyber security capabilities, while also improving the security level of 5G applications.

2 Overview of 5G-Enabled Vertical Industries

The fourth global industrial revolution, characterized by digitalization, networking, and intelligence, is now well underway. Amid this exciting new technological revolution, 5G — the core, universally applied technology — has become the development focus of countries across the world. 5G's ability to enable ultra-large bandwidth, ultra-wide connection, and ultra-low latency will drive economic transformation and social progress, while also improving the lives of people around the world. By the end of 2020, 412 operators in 131 countries had invested in 5G in various ways, 140 operators in 59 countries and regions had promoted the commercial use of 5G, and more than 1 million 5G base stations had been built worldwide.

According to the *White Paper on the 5G Application Innovation* released by the 5G Applications Industry Array, thanks to the continuous development and evolution of 5G converged applications, 5G is expected to be put into large-scale commercial use in a dozen fields (such as factories, mines, ports, and power grids), and its application scenarios have already begun to take shape. For example, by deploying the 5G Mobile Edge Computing (MEC) in the smart factory field, converged applications including "5G + machine vision" and "5G + VR/AR-aided assembly" integrate 5G with emerging technologies such as artificial intelligence (AI) at the edge, ensuring that such technology is no longer limited by the processing capability and cost of terminals. Meanwhile, in the smart grid field, 5G enhances power system management capabilities through new service modes such as mobile inspection, video surveillance, and environment monitoring. Here, the differential protection for power distribution networks uses 5G's low latency and high-precision network timing features to accurately locate and isolate power distribution network faults, and quickly enables the switchover to standby lines to shorten power outage times from

hours to seconds.

3 Security Solutions of 5G-Enabled Vertical Industries

3.1 Smart Grid

3.1.1 Industry Introduction

The smart grid refers to power communication using 5G technologies to achieve intelligent, unattended, and secure power production and control. There are two types of wireless communication application scenarios: control and collection. Control scenarios include intelligent distributed power distribution automation, demand response (DR), and distributed energy control, while collection scenarios mainly involve advanced metering and big video applications of smart grids.

The application scenarios of 5G technologies in smart grids are classified into five types.

Type 1: The use of 5G's lower latency and new technologies such as slicing to realize differential protection for grids. Examples include differential protection for power distribution networks of smart grids.

Type 2: The use of 5G's lower latency and new technologies such as slicing and edge computing to guarantee telemetry, remote communication, and remote control for grids. Examples include automated telemetry, remote communication, and remote control for power distribution networks of smart grids.

Type 3: The use of 5G's larger bandwidth and new technologies such as slicing and edge computing to ensure normal services and secure operations of power grids. Examples include unattended inspection of smart grids and emergency grid communication.

Type 4: The use of 5G's larger bandwidth and lower latency, as well as new technologies such as slicing and edge computing, to ensure normal services and secure power grid operations. Examples include smart grid power monitoring unit (PMU) and precise load control.

Type 5: The use of 5G's larger bandwidth and massive connection capabilities, as well as new technologies such as slicing and edge computing, to ensure normal services and secure power grid operations. Examples include advanced smart grid metering.

3.1.2 Security Requirements

(1) Regulatory and customer requirements

As a key infrastructure, power grids are vital to national interests and individual livelihoods. A large-scale electrical accident may cause serious economic losses and personal injuries, affecting millions of people. Consequently, security is a fundamental and paramount requirement in the smart grid field. It is vitally important to strengthen the information security management of the power monitoring system, prevent hackers and malicious code from attacking it, and ensure the secure and stable operations of the power system. The National Development and Reform Commission (NDRC) of China issued the *Regulations for Security Protection of the Power Monitoring System* (Order No. 14 [2014] of NDRC), which stipulates that the security protection of the power monitoring system must comply with the national classified protection system for information security and adhere to the principles of "secure partitioning, dedicated networks, horizontal isolation, and vertical authentication" in order to secure the power monitoring system.

(2) Service security requirements

This section analyzes the main service characteristics and application scenarios of "5G + smart grid", and identifies the following major security risks and requirements facing 5G grids.

(a) Terminal access security

- Authenticate terminals before they access the 5G communication network, as unauthorized access from malicious terminals to networks dedicated to 5G power services may lead to congested network resources, attacks on grid service applications, or even the theft or unauthorized modification of sensitive power system information.
- Take technical measures to encrypt important service data and protect its integrity, thereby preventing sensitive data leakage and the unauthorized modification of power application service data.

(b) 5G pipe security

- Use an independent 5G network, physically isolated from the public network, to prevent attacks from the public network, as grid security is critical to national welfare and the well-being of individuals.
- Implement differentiated slice security isolation for power services with different sensitivities in areas based on their security levels.
- Utilize measures such as security protocols and encryption technologies to secure data in 5G communication pipes, as communications from the radio access network (RAN) to the core network and edge, as well as to the power service system of the master station, is prone to leakage or unauthorized modification,

which may endanger both lives and property.

- Edge computing
  - Perform security management and control on edge nodes. For example, implement security hardening and identity authentication for the MEC platform, MEC management and orchestration (MANO) system, and edge user plane function (UPF), as an operator's core network and grid system may be vulnerable to attackers aiming to penetrate the MEC on certain edge nodes deployed in smart grids.
  - Implement local breakout to prevent power service data from transferring out of the grid campus, as most grid service traffic is of a sensitive nature.

(c) Security management

- Provide a security situational awareness system based on the integrated and unified security management platform to monitor the security status of power terminals in real time, and to generate alarms.
- Enable the security as a service (SECaaS) to protect grid edge applications and terminal security management.
- Provide differentiated security management services for power slices.

3.1.3 Security Solutions

The construction of "5G + smart grid" must adhere to the basic principles of "secure partitioning, dedicated networks, horizontal isolation, and vertical authentication", as specified in the industry regulatory requirements. In compliance with these basic principles, the "5G + smart grid" security system covers cloud, pipe, and device domains. In other words, power services are secured in an end-to-end (E2E) manner from identity authentication for terminal access security, security isolation and encryption for dedicated 5G power pipe networks, and security monitoring and management on the cloud.

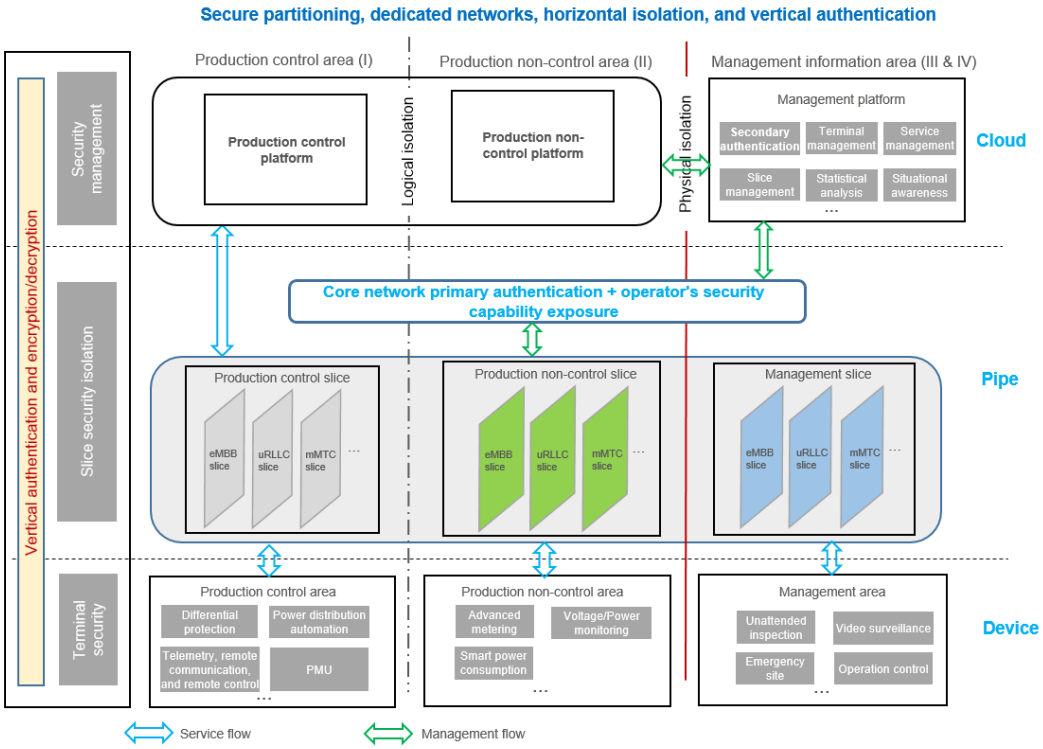

Figure 1 — "5G + smart grid" security framework

Among the basic principles, secure partitioning is designed for power services and devices of different security levels. Pipe security focuses on dedicated networks and horizontal isolation, device security is concerned with vertical authentication and encryption, while cloud security centers on the implementation of security management capabilities such as security detection, response, and recovery. For example, security monitoring and management are implemented for communication pipes and power terminals.

(1) Access security of power application terminals

The access of power application terminals to "5G + smart grid" must meet the vertical authentication requirements. Specifically, terminals are required to pass both the primary authentication on the core networks of telecom operators, and secondary identity authentication based on the importance of the grid system. The following terminal access security solutions are available.

(a) Use the two-way authentication mechanism for power terminals to access the 5G network over the air interface. Select correct slices for terminals based on the Network Slice Selection Assistance Information (NSSAI) to ensure that only authorized terminals can access the specified sliced networks.

(b) Deploy the authentication, authorization, and accounting (AAA) server in the grid and connect it to an operator's core network to perform secondary identity authentication using the identity messages forwarded through core networks on terminals accessing dedicated

power slices.

(c) Configure and enable IP address- and port-based access control. Deploy firewalls, unified threat management (UTM), and intrusion prevention systems (IPSs) to safeguard the master station.

(2) 5G pipe security

The communication pipe network of 5G smart grids includes the RAN, transport network, core network, and MEC edge nodes. This network must meet the security requirements of dedicated networks and horizontal isolation while securing the data of sensitive power services throughout the communication process.

(a) In terms of dedicated networks, completely isolate the 5G network accessed by the grid production area and management information area from the public network, and ensure it is not used together with other services, thereby building a dedicated 5G network (terminal-to-terminal) for the power industry.

(b) In terms of horizontal isolation, use different slice isolation technologies for the RAN, transport network, and core network based on the security levels of power services.

- For the RAN, the exclusive and sharing modes of base stations may be used. The exclusive mode applies to local area networks (LANs) in scenarios such as power stations and substations, while the sharing mode applies to 5G wide area networks (WANs) in scenarios such as power distribution and power transmission. There are three slice isolation methods for the sharing mode that can be flexibly selected based on service isolation requirements: 5G QoS Identifier (5QI), RB reservation, and independent spectrum, listed in ascending order of security isolation levels.
- For the transport network, the following technologies are available: soft isolation based on virtual private networks (VPNs) and quality of service (QoS), channelized sub-interface, and FlexE-based hard isolation, listed in ascending order of isolation effects. Of these, FlexE-based hard isolation provides the best isolation at a reasonable cost. It is recommended that FlexE-based hard isolation be used between the production and management areas to implement horizontal isolation between the areas, and that the VPN + QoS mode be used to realize logical isolation between different services in an area.
- For the core network, either exclusive use or partial sharing of 5G NFs can be used in power services. If there is no need to exclusively use all 5GC NFs with extremely high requirements, it is

recommended that a dedicated edge UPF be deployed to share other 5GC NFs on an operator's network to implement independent isolation of the service plane. On the core network, slices shall be divided using the virtual LAN (VLAN) or virtual extensible LAN (VXLAN) according to service requirements, and hardware or virtual firewalls shall be deployed at the physical or virtual network border to implement access control. Slices shall be physically isolated based on physical deployment to ensure that each slice can obtain relatively independent physical resources.

(c) MEC edge node security

- Isolate the MEC deployed in specific campuses (such as power stations and substations) from the local edge cloud through firewalls.
- Use the Uplink Classifier (ULCL) and firewall trustlist to ensure traffic flows only on local networks and to prevent service data leakage.
- Integrate the MEC with TPM 2.0 to implement secure boot. For scenarios where power applications need to be deployed on the MEC, enable the software installation integrity check on the MEC platform to implement API security capabilities, including two-way authentication for access to APIs and API access traffic control.

(d) Data transmission security

- Integrate 5G power terminals with security chips or modules, and deploy an encryption and authentication gateway at the master station. Establish an IPsec VPN tunnel between the master station and terminals that complies with the Chinese encryption standards to implement IP-layer data encryption and two-way authentication.
- For sensitive power services, enable the service-plane encryption over the air interface during registration of 5G power terminals. Use IPsec or multi-protocol label switching (MPLS) for connection between the UPF and the master station of the power service to prevent data leakage.

(3) Security monitoring and management

(a) Make the grid slice management plane available to grid users, and perform authentication and authorization for all open interfaces. Use the Transport Layer Security (TLS) protocol for encryption and integrity protection of the transmission on the management plane, and enable the Network Slice Management Function (NSMF) to support permission- and domain-based management and prevent unauthorized O&M. In addition, specify roles for different nodes within a process.

(b) Operators open their slice management capabilities as tenants, so that grid users can monitor and manage grid slices via the operator's slice openness platform.

(c) Operators open their capabilities to monitor and handle abnormal terminals. Build a security management center within the grid and connect it to an operator's security openness capabilities to control terminal access, visualize abnormal terminals, and implement independent management of terminals.

3.2 Smart Manufacturing

3.2.1 Industry Introduction

Thanks to 5G's low latency, large bandwidth, and Massive Machine Type Communication (mMTC), the application of 5G in smart manufacturing addresses the following issues resulting from the use of optical fibers and Wi-Fi in manufacturing factories: complex line deployment, high construction and O&M costs, poor stability, and low reliability. In addition, 5G realizes fast and reliable connections between machines, between machines and cloud platforms, and between machines and people in manufacturing factories. The application of 5G greatly improves production efficiency and provides a brand-new solution for secure communication within manufacturing factories.

The application scenarios of 5G technologies in the manufacturing industry are classified into four types.

Type 1: The use of 5G's lower latency and larger bandwidth, as well as new technologies such as network slicing and edge computing, to ensure precise remote control. Examples include remote robot control and remotely controlled robotic arms.

Type 2: The use of 5G's larger bandwidth as well as the low latency and powerful computing capabilities of edge computing, to collect and transmit terminal videos to the cloud for analysis, thereby supporting machine vision, AI-assisted detection, and augmented reality (AR)-assisted troubleshooting and guidance.

Type 3: The use of 5G's massive connection capabilities, to collect and transmit sensor data from the programmable logic controller (PLC) in factories to the cloud for analysis. Another application is the use of 5G's lower latency to implement PLC operations, such as PLC control, PLC collaboration, and PLC cloudification.

Type 4: The use of 5G's lower latency and new technologies such as precise base station locating, edge computing, and network slicing. These can be used to report information to the cloud in real time (such as the location of the object

to be operated on) for analysis and processing. In addition, 5G can realize automatic material delivery, automated guided vehicle (AGV) scheduling, and autonomous driving, and replace wired devices with wireless alternatives.

3.2.2 Security Requirements

The 5G network connects the factory's original unconnected or relatively closed dedicated network to the Internet, which in turn makes industrial control protocols and IT system vulnerabilities more prone to exploitation. Based on regulatory and customer requirements as well as the analysis of preceding scenarios and service characteristics, the application of 5G in the manufacturing industry mainly faces the following security challenges and requirements.

(1) Manufacturing terminal access security

- A large number of dumb terminals do not support 5G communication in various service scenarios. If numerous unauthenticated dumb terminals access the 5G network through customer-premises equipment (CPE), zombie-based denial of service (DoS) attacks and data leakage may occur. Therefore, 5G routing terminals and enterprise Internet of Things (IoT) platforms shall implement identity authentication for dumb terminals accessing the network.
- If unauthorized 5G terminals access the factory's dedicated 5G network using forged identities, fault injection, distributed denial of service (DDoS) attacks, and sensitive service data leakage may occur. As such, the 5G network shall authenticate the identity of 5G terminals accessing the network. For important services, enterprise networks shall perform secondary identity authentication on terminals.
- Location control technology should be used to restrict important service terminals to only the indoor manufacturing network. If terminals are connected to an outdoor illegal network, they may be maliciously controlled, thereby incurring security production risks and terminal data leakage.
- Unauthorized and abnormal terminals accessing the factory's 5G network should be quickly identified and blocked to prevent further losses.

(2) Edge computing

Edge computing nodes are generally located in the manufacturing campus and used to build an E2E 5G network dedicated to smart manufacturing, implementing local management of service data.

- Due to the deep coupling of operator and factory resources on edge computing nodes, attackers may exploit the vulnerabilities of edge factory applications to attack an operator's core network or penetrate

into enterprise intranets through the operator's management plane. Therefore, identity authentication and isolation measures are required to prevent mutual penetration between enterprise applications and operators' edge NFs.

- The 5G NFs and MEC platform on edge computing nodes depend on remote O&M and management. Proper measures, such as identity and permission management, edge computing hardening, and vulnerability scanning, must be taken to prevent attacks on the MEC through the operator's management plane.
- In the manufacturing industry, multiple interfaces on edge computing nodes connect to an operator's 5GC. Therefore, malicious operations or attacks must be prevented from transferring service data out of the campus.

(3) Data leakage

- Sensitive information may be leaked if service data is transferred out of the manufacturing campus. The system should be able to detect if service data leaves the campus, quickly block the outbound port through measures such as security operations, and support quick recovery.
- Sensitive service data and user privacy data must be encrypted in E2E mode across trusted domains to prevent data leakage.

(4) Network slicing

- Incomplete slice isolation may lead to service data leakage.
- Various 5G services with different security requirements are involved in manufacturing factories. Differentiated security isolation and stable slice resources shall be provided. For services with high security requirements such as PLC and machine vision, slices shall be isolated in E2E mode, with other slices not affecting resources.
- If terminals bypass the authentication and authorization of the core network, such unauthorized access to slices may cause service data leakage and slice-based attacks to the factory's private network.
- Inappropriate slice permission management or vulnerabilities such as privilege escalation may lead to the unavailability of slice resources and affect normal production activities.

3.2.3 Security Solutions

To address the security risks and requirements of applying new 5G technologies to the manufacturing industry, effective solutions shall be provided to implement identity authentication and to control terminals that access the network. This will ensure that manufacturing service data is not transferred out of the campus and dispel possible concerns by industry customers and telecom

operators about the security of edge computing, as well as monitor and handle the security status of the dedicated 5G manufacturing network in real time. In this way, it is possible to ensure the stability of the 5G network and prevent manufacturing industry users from suffering major economic losses.

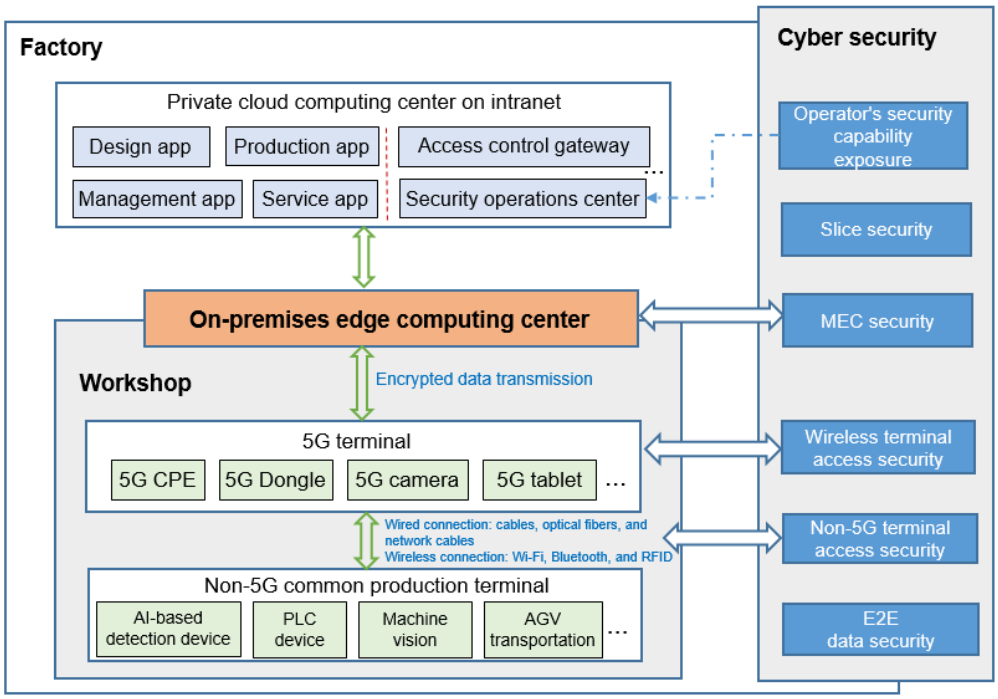

Figure 2 — Overall security architecture of smart manufacturing

Security solutions for the 5G manufacturing industry shall clearly define the security responsibility boundaries of operators and industry users to ensure service data is not transferred out of the production campus, secure sensitive business information, and guarantee the stable and sustainable production of key services. The overall security can be ensured from the following aspects: terminal access to the dedicated 5G production network, edge computing node security, security isolation for slices, and E2E data security protection.

(1) Terminal access security

The "5G + smart factory" scenario involves 5G terminals and numerous existing factory terminals that do not have 5G capabilities. The security and reliability of all these terminals accessing the dedicated 5G manufacturing network shall be taken into account.

(a) Deploy the AAA system on the factory's internal IT network, ensuring that all terminals are authenticated by the system and subject to secondary identity authentication before accessing the factory's IT system.

(b) For important production terminals, enterprises can bind SIM cards through the operator's Unified Data Management (UDM) or use its own AAA system to implement terminal-SIM card binding authentication. This can protect SIM cards from being omitted or illegally inserted or

removed, while also preventing unauthorized terminals from intruding into the factory's dedicated 5G network.

(c) For manufacturing industry users with requirements on the network access location, use the Unified Policy Control Function (UPCF) or AAA server to implement location binding policies for SIM cards of specified terminals in batches. This prevents terminals from accessing illegal external networks after leaving the campus.

(d) For services with data confidentiality requirements, enable user-plane encryption and integrity protection over the air interface.

(e) If unauthorized terminals access the dedicated 5G network, utilize the security operation services provided by operators to promptly bring the unauthorized terminals offline or block them through the AAA server.

(2) Edge computing security

(a) Networking security

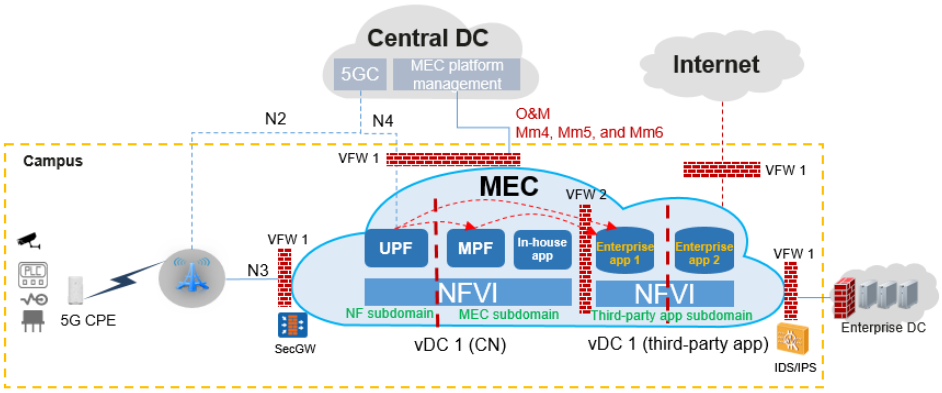

Figure 3 — Edge node security networking

- Security domain division: If enterprise applications are deployed on edge computing nodes, divide the MEC into the internal operator security domain, enterprise application security domain, and the MEC external security domain, among which the operator security domain can be further divided into the UPF subdomain and MEC subdomain (MPF and in-house applications).
- Security domain isolation: Physically isolate computing resources between different security domains using vDC technology, and inter-domain data communication using firewalls. Isolate security subdomains by firewalls based on actual risks and requirements.
- Plane isolation: In MEC networking, physically isolate the management, signaling, service, and storage planes or logically isolate them using VLANs.

(b) Edge security as a service

- Set security access zones based on the actual risks faced by MEC resources and deploy security protection devices as required to protect the self-owned resources of MEC nodes and user edge cloud service applications from any external attacks.
- Provide edge security as a service to customers as required to prevent security attacks from outside the MEC. In addition, ensure that operators and customers are able to detect edge computing security vulnerabilities and situations in real time, as well as monitor and audit the risks of service data from leaving the campus.

(3) Service data protection

(a) Local management of service traffic: Implement local offloading of service traffic for production terminals by binding the Data Network Name (DNN) of the edge UPF or E2E slicing.

(b) Encrypted transmission of service traffic: If service traffic between production terminals and enterprise applications is transmitted across zones without stringent security measures, encrypt transmission channels using IPsec or Layer 2 VPNs (L2VPNs).

(c) Monitoring of data leaving the campus: Use the firewall deep packet inspection (DPI) to monitor the traffic service type and traffic over the N9 interface, check whether the outbound traffic contains service data, and report alarms to the security operations center.

(4) Slice security

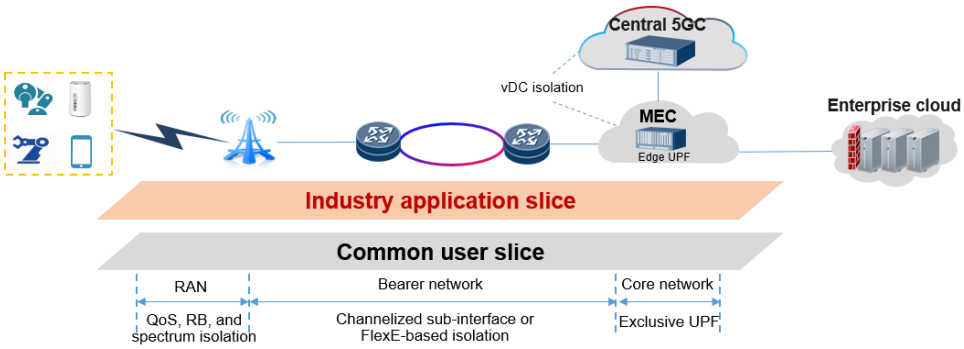

Figure 4 — Slice security in the manufacturing industry

(a) Provide exclusive 5G B2B slices with high security isolation for services requiring high security and reliability, such as machine vision, remote support, and 5G PLC. These services are isolated from common services to ensure the stability and reliability of network resources required by these services and to prevent data leakage.

(b) Independently deploy vDCs and host aggregates for slices requiring high security and isolation and implement physical isolation, while using

independent vDCs and shared host aggregates with logical isolation for common slices.

3.3 Smart Port

3.3.1 Industry Introduction

Smart ports are demanding in terms of ensuring low latency, large bandwidth, and high reliability. This means the communications system of automated ports must be able to efficiently and reliably transmit control data and multi-channel video data across special, large-scale equipment. However, legacy communication modes (for example, optical fiber and Wi-Fi) have drawbacks such as high construction and O&M costs, poor stability, and low reliability. Against this backdrop, 5G is introduced to empower smart ports through low latency, large bandwidth and capacity, and high reliability, as well as provide dedicated port network solutions and E2E application components backed by 5G virtual dedicated access.

The application scenarios of 5G technologies in the smart port industry are classified into four types.

Type 1: The use of 5G's lower latency and new technologies such as slicing and edge computing, to implement the real-time remote control of port equipment.

Type 2: The use of 5G's larger bandwidth and new technologies such as network slicing and edge computing, to shoot HD videos and transmit them back to the service platform, for the purposes of video surveillance in ports and video-aided remote control of equipment such as gantry cranes and bridge cranes.

Type 3: The use of 5G's lower latency and new technologies such as network slicing and edge computing to meet the high requirements of remote control, autonomous driving of AGVs, and automated tally at yards.

Type 4: The use of 5G's larger bandwidth and lower latency, as well as new technologies such as network slicing and edge computing, to meet the requirements of video surveillance in ports, AI operation identification, and intelligent inspection using drones and robots.

3.3.2 Security Requirements

Based on the service characteristics, the port industry mainly includes the following 5G security requirements.

(1) Terminal access security

(a) To prevent unauthorized terminals from accessing the port's dedicated 5G network, which may lead to service data theft and even attacks on

the port's internal IT system, the port's 5G network must implement identity authentication and control all terminals that access the network.

(b) For key Ultra-Reliable Low-Latency Communication (uRLLC) services such as autonomous driving and remote control, DDoS attacks launched by unauthorized terminals may severely affect network reliability and latency, or even paralyze port communication services. Therefore, both edge computing and the air interface must be capable of defending against DDoS attacks.

(2) Network slicing

(a) Access slice authentication

If unauthorized terminals access dedicated port slices using forged identities, multiple risks such as service losses, personnel injuries, and information leakage may occur. Therefore, slice authentication and secondary authentication capabilities must be provided for terminal access.

(b) Service slice isolation

Key remote control services, such as gantry cranes and unmanned container trucks, must be securely isolated from other service slices. Congested network resources may affect services demanding low latency. Slice resources shall be strictly controlled and communication and data shall be isolated to prevent data leakage and unauthorized access between slices.

(3) Edge computing

(a) Platform security

The MEC, where port applications are deeply coupled with operators' edge NFs, is vulnerable to attackers aiming to penetrate an operator's core network through the port's internal IT system. Therefore, the following security protection measures are required for edge nodes:

- Ensure the security of routing links between the MEC and an operator's core network and between the MEC and the port's IT system.
- Deploy firewalls between the MEC and the external operator network and between the MEC and the port's IT network.
- Secure the MEC platform and applications installed thereon using measures such as platform security hardening, app signature verification, API two-way authentication, and traffic control.

(b) Management security

Improper O&M on the MEC management plane or attacks on the NFs of

operators' edge computing nodes through the management plane may cause the port's 5G network to be unstable or even paralyzed, threatening normal services and personnel safety. Therefore, operators shall use security protocols such as TLS and SSH2 to manage the MEC infrastructure resources and platform and periodically perform security vulnerability scanning and hardening.

(c) Data leakage prevention

Take measures such as DNN binding, slicing, and ULCL to implement the local management of port service data, preventing sensitive service data leakage and port service losses.

(4) Data leakage prevention

(a) Encrypted transmission of sensitive data

Protect Enhanced Mobile Broadband (eMBB) services such as video surveillance and HD video backhaul against data theft and leakage. Enhance terminal identity validity control and encrypt communication links for sensitive services to secure user-plane data transmission.

(b) Protection for service data from leaving the campus

Prevent service data from being leaked via the MEC. Take protection measures in terms of the 5G networking architecture, service data monitoring, and security auditing to mitigate risks of service data leakage.

3.3.3 Security Solutions

To address the security risks and requirements of applying 5G technologies to port scenarios, proper security solutions are required to build a dedicated 5G data network for local traffic offloading, ensure E2E data transmission security, and implement differentiated service-level agreements (SLAs) based on service priorities.

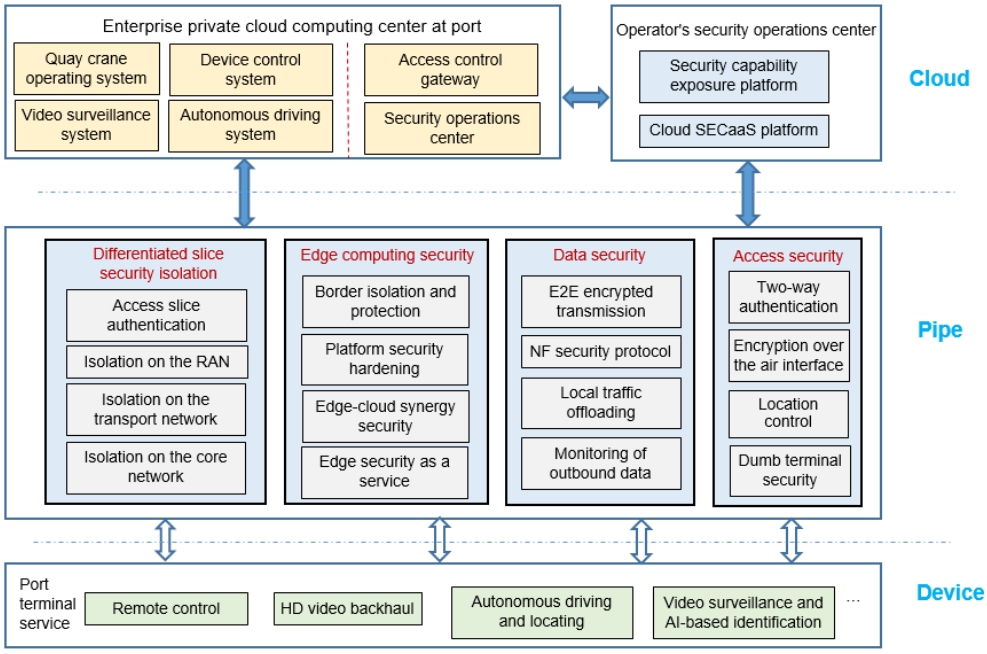

Figure 5 — Smart port security framework

The overall port security framework is considered from multiple dimensions including secure terminal access, data security protection, edge computing security, slice security, and networking security.

(1) Terminal access security

(a) Enable the 5G Authentication and Key Agreement (AKA) and signaling-plane encryption for port terminals accessing the 5G network. For sensitive services such as gantry cranes and AGVs, enable the service-plane encryption over the air interface during registration.

(b) Deploy a demilitarized zone (DMZ) and an AAA server on the port intranet to verify terminal-card binding and to perform secondary identity authentication for terminals accessing the port's dedicated 5G network.

(c) Connect terminals such as tower cranes to the CPE through physical network cables or strong Wi-Fi authentication, and configure the MAC address or IP address trustlist on the CPE.

(d) For mobile 5G terminals of Type 3 and Type 4 port services, set the tracking area code (TAC) via the Access and Mobility Management Function (AMF) to bind terminals and cells to restrict the location range of terminals accessing the port's 5G network.

(e) Use the security operations center to detect abnormal terminal behavior, generate alarms, and monitor and block access of abnormal terminals.

(2) Slice security

(a) Bind the Single NSSAI (S-NSSAI) of port service slices, international mobile subscriber identity (IMSI), and tracking area identity (TAI) to

restrict authorized terminals to specified service slices only within a certain location range.

(b) Physically isolate port services and public network services. Implement differentiated slices for port services with different security requirements. For example, use slices with high security levels for sensitive services such as remote control, video surveillance, and AI-based identification.

(3) MEC security

(a) Border isolation and protection

Deploy the MEC in an independent equipment room in the port campus. Isolate the MEC site from operators' 5GC and the port enterprise intranet through firewalls. If enterprise applications are hosted on the MEC node, isolate the UPF and Multi-access Edge Platform (MEP) in the operator's trusted domain from port enterprise edge applications through firewalls, and use Virtual Private Cloud (VPC) provided by the MEC to isolate resources between applications.

(b) Edge security as a service

If only the UPF traffic distribution mode is used on edge computing nodes, then only firewalls on the MEC need to be deployed; these will be remotely managed through the network management system (NMS) by operators. If applications are hosted on the MEC node, operators can provide edge security as a service based on user requirements.

- Telecom operators shall set security access zones based on the actual risks faced by MEC resources and deploy security protection devices as required, such as firewalls, web application firewalls (WAFs), and IPSs. This will protect the self-owned resources of MEC nodes and enterprise edge cloud applications from any external attacks.
- Edge-cloud synergy security: Operators can build a unified cloud security operations center for the 5G network to provide edge threat intelligence analysis, security situational awareness, security MANO, and emergency responses to security incidents.
- Based on the enterprise users' requirements, provide edge security as a service, such as host vulnerability scanning, antivirus, and bastion host, to help users detect and defend against external MEC security attacks and threats, and detect security vulnerabilities and situations on edge nodes in real time.

(4) Data leakage prevention

(a) Encrypted data transmission

- Enable signaling-plane encryption over the air interface for port terminals to access the 5G network, and user-plane encryption over the air interface for sensitive service terminals during SIM card registration.
- Enable the IPsec VPN tunnel between the port 5G CPE and MEC gateway and between the MEC gateway and the port enterprise intranet as required to implement E2E service data encryption.
- Use security protocols between NFs on the E2E 5G network. For example, use Datagram Transport Layer Security (DTLS) between the port base station and the core network, and TLS or the Secure File Transfer Protocol (SFTP) between the edge node and the core network.

(b) Protection and detection of data leaving the campus

- Use the DNN binding and E2E slicing solutions to build a dedicated 5G channel for port services to implement offloading of port service data on the local level.
- Use measures such as the traffic probe and outbound traffic volume monitoring to detect potential risks of service data leaving the campus in real time and generate alarms.

4 Security Practices in 5G-Enabled Vertical Industries

4.1 Security Solutions

Using a smart factory in Guangdong that uses the on-premises MEC as an example, this section illustrates an advantageous solution based on the factory's assessed security risks. The 5G security solution can secure terminal access, ensure data security, and defend against external attacks, as shown below.

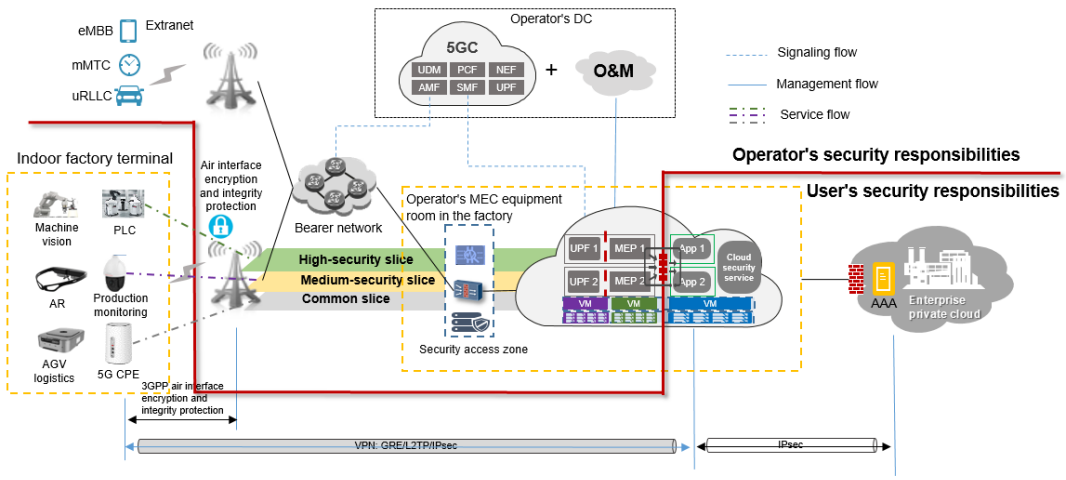

Figure 6 — Security solution of a smart factory

In line with the security requirements discovered from the device-pipe-edge-cloud analysis of the factory's working scenarios and security risks, the security solution covers the following areas: 5G terminal access security, tamper-proof 5G pipe encryption, protection against edge computing attacks, secure data processing on campus, and cloud security management and O&M. Detailed requirements of the solution are as follows.

(1) Terminal access security

(a) Independent validity authentication for terminal identities: Use the "device-SIM card binding + secondary authentication" scheme to enable the factory to independently authenticate terminal identities. This can prevent non-specified terminals from accessing the indoor dedicated manufacturing network and avoid unauthorized terminal identities caused by malicious insertion and removal of SIM cards.

- Deploy an AAA server on the factory's internal IT network, and import the identity authentication information such as the international mobile equipment identities (IMEIs) and IMSIs of authorized terminals. Then, implement direct secure VPN connections via the AAA agent and the Session Management Function (SMF) on a telecom operator's core network.
- When a terminal registers with the network, it sends its identity information including the IMSI and IMEI to the factory's AAA server through the core network SMF for secondary identity authentication. The AAA server uses the combination of the IMEI and IMSI as the unique identity information of the terminal and compares the information with that imported before.

(b) Network access location control: Bind terminals (with SIM cards) to NR Cell Global Identifiers (NCGIs) using the UPCF so that specified terminals can access only the indoor dedicated manufacturing network but not the outdoor network.

- Add user numbers and the list of cells available for user access to the UPCF through the Business Operations Support System (BOSS). When a user accesses the 5G network, the SMF sends the user's location information (such as NCGI) to the UPCF. The UPCF checks whether the location is within the allowed range, and then decides to allow or deny the access as appropriate.

(2) Campus edge computing security

(a) Solution 1: Divide the MEC into trusted zones and isolate the zones to implement hierarchical isolation and protection from outside in.

- Trusted zone division: As shown in the MEC node in the overall framework, divide the edge MEC into the operator security domain (including UPF subdomain, MPF subdomain, and in-house applications) and factory application security domain (including virtual machines and applications for machine vision and AI-based detection; subdomains to be set up based on security levels).
- Communication security isolation: Externally, deploy border firewalls on the MEC to defend against external attacks and configure typical security policies to ensure all external access to the MEC (including from 5GC, O&M systems, terminals, and factory intranet) is filtered by the firewalls. Internally, divide security domains using (virtual) firewalls based on trusted zones to isolate operator and factory domains. In addition, isolate resources between security domains using vDC, and isolate communication by firewalls. Isolate security subdomains in each trusted zone by firewalls based on customer requirements.

(b) Solution 2: Operators set up security access zones on the MEC nodes, deploy security protection devices as required, and utilize security operations centers to provide edge cloud SECaaS for the factory. This can alleviate the factory's security concerns about edge computing nodes.

- Set up security access zones: Deploy firewalls, IPSs, WAFs, security access gateways, flow probe (without collecting service traffic), bastion hosts, and log servers in security access zones to protect the MEC assets from external or internal attacks.
- Provide cloud security services to safeguard services: Utilize operators' security operations centers to provide on-demand cloud security services to the factory such as virtual log auditing, host vulnerability scanning, and intrusion detection, to safeguard edge cloud services.
- Ensure security and transparency: Send the security incident logs and device operation logs of edge security access zones to the factory's log audit server, making the edge security measures visualized while also addressing the factory's concerns about the MEC O&M and data leaving the campus.

(3) Slice security

(a) Slice isolation

Solution: Provide differentiated slice isolation solutions based on service security levels.

The following table shows the slice isolation solutions for the RAN,

transport network, and core network with different service security levels.

Location	Low-Security Service	Medium-Security Service	High-Security Service
RAN	QoS priority guarantee	High-priority QoS + RB reservation over the radio air interface	Dedicated base station or cell with exclusive carriers
Transport network	VPN isolation + QoS isolation and scheduling	FlexE interface isolation + VPN isolation	FlexE interface + FlexE cross-connect
Core network	Shared use of B2B core network of the public network	Exclusive use of logical resources of SMF and UPF	Dedicated use of physical resources of SMF and UPF

- Provide exclusive 5G B2B slices with high security isolation for services requiring high security and ultra-high reliability, such as machine vision and 5G PLC. Isolate such services from common services to ensure stable and reliable network resources such as ultra-low latency required by services and prevent data leakage.
- Provide exclusive 5G B2B slices with medium security isolation for services with security requirements, such as AR-assisted remote support and AGV-based intelligent logistics, to meet required security isolation and resource usage priorities.
- Operators' core networks can be used for services without special requirements, such as AR-enabled visit and video-based production monitoring. The RAN and transport network use QoS priority guarantee and only need to ensure that data does not leave the campus.

(4) Factory service data security

(a) Encrypted transmission of service data

Solution: Provide E2E encryption to secure service data.

- For important services that hold sensitive data, use IPsec to encrypt service data over the N3 interface between terminals and the MEC as well as service data over the N6 interface between the MEC and enterprise data centers (DCs) based on cross-security domain risks.

- In scenarios where the edge UPF interworks with the central UPF, implement IPsec encryption on the user plane based on the SecGW. If enterprises' local traffic does not need to flow to the central UPF, use the traffic distribution policy delivered by the SMF for rule matching to implement local traffic distribution based on DNN + location and prevent service data from leaving the campus.
- Use IPsec to encrypt signaling over the N4 interface, starting from the UPF-connected SecGW to the provider edge (PE), with the key being managed by operators.
- Use MPLS VPNs or IPsec to protect the signaling for secondary authentication as it contains the terminal identity authentication information.

(b) Monitoring to ensure service data does not leave the campus

Solution: Use the firewall DPI to identify service types of the traffic and monitor whether the outbound traffic contains service data. If it does, generate alarms or report to security operations centers.

4.2 Advantages

The manufacturing industry user applications and operator NFs need to be deployed together on the MEC, and are deeply coupled. As such, it is challenging to build mutual trust between users and operators on edge nodes. In this regard, the security solution outlined above has the following advantages:

(1) In terms of terminal access security, it provides independent terminal access validity control and terminal location locking control. Only enterprise-allowed terminals in specified indoor areas can access the 5G network. This prevents unauthorized terminals with forged identities from accessing the network, causing data leakage, and affecting services.

(2) As for edge computing, local traffic offloading prevents data from leaving the campus and therefore ensures data security. Edge security access zones help implement isolation and protection between operator NFs and enterprise applications on edge nodes and meet the zero-trust security requirements at the edge.

(3) The SECaaS capability and security detection for outbound data enable operators and users to detect the security status of edge computing nodes without data disclosure, which eliminates security concerns of both factory customers and telecom operators.

4.3 Benefits and Promotion Value

(1) Benefits

Cyber security is a critically important and complex issue facing the manufacturing industry during its transition from the closed network to the open 5G network.

Industry users are concerned about the risks of original network data leakage and intrusion into internal IT systems. As such, security showcases and industry benchmarks are required to promote 5G technologies in the manufacturing industry. The 5G security solution outlined above is based on the research on E2E security solutions for 5G smart factories and is applicable to the entire manufacturing industry.

This will go some way to address security concerns of industry users, and thereby lay a solid foundation for the larger-scale application of 5G across industry.

(2) Promotion value

This case provides an E2E security solution covering terminal access, 5G pipe, edge computing, and slice security, and builds a complete set of cyber security architecture and solution suggestions applicable to smart factory scenarios.

It is the industry's first to implement the E2E security solution that combines the device-pipe-edge-cloud architecture in smart factories. Moreover, its feasibility is fully verified in multiple scenarios within 5G LANs dedicated to smart manufacturing, including machine vision, PLC, indoor locating, indoor logistics, and remote maintenance, eliminating security concerns of industry customers and operators.

In short, this security solution forms the basis for security standards in the manufacturing industry and will further promote the larger-scale rollout of 5G in manufacturing factories.

5 Recommendations

As a revolutionary technology, 5G will accelerate digital transformation in vertical industries such as manufacturing and energy. Safeguarding 5G networks requires joint efforts from operators, businesses, and device vendors to build a security ecosystem.

Throughout the lifecycle of a 5G network, from construction and deployment to operation, the requirements of each vertical industry's security guidelines on industry systems should be followed. A comprehensive and differentiated 5G industry security capability model should be created, industry-oriented 5G security capability sets provided, and baselines for assessment established.

Furthermore, it is important to keep up with industrial security challenges, and ensure the secure construction, operation, and management of 5G networks,

so that the integration of 5G into industry will continue to deliver value.