TAICS

TAICS TR-0017 v1.0:2021

5G專網多接取邊緣運算資安研究報告

Cybersecurity study report for multi-access edge computing in 5G non-public networks

2021/01/07

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

5G 專網多接取邊緣運算資安研究報告

Cybersecurity study report for multi-access edge computing in 5G non-public networks

出版日期: 2021/01/07
終審日期: 2020/12/18

誌謝

本研究報告由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 毛敬豪 所長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 行動通訊資安工作組組長：財團法人資訊工業策進會 徐暐釗 組長

技術編輯：財團法人資訊工業策進會 蔡宜學 博士

此研究報告制定之協會會員參與名單為(以中文名稱順序排列)：

中華電信股份有限公司、安華聯網科技股份有限公司、亞旭電腦股份有限公司、明泰科技股份有限公司、英業達股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人資訊工業策進會、財團法人電信技術中心

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

神達電腦股份有限公司、國家通訊傳播委員會、雲達科技股份有限公司

本研究報告由經濟部技術處支持研究制定。

目錄

前言

本研究報告係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業研究報告。

本研究報告並未建議所有安全事項，使用本研究報告前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本研究報告之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

多接取邊緣運算 (Multi-access Edge Computing, MEC) 是一個兼具運算資源與無線網路的平臺，透過融合雲端運算能力及行動網路的多接取邊緣運算 (MEC) 技術，將運算能力擴展到網路邊緣的位置，以實現 5G 專網低延遲率與高可靠性以及高傳輸速率的服務，同時達成用戶設備 (UE) 的入網身份驗證、移動性和漫遊等功能。深究 MEC 的名稱由來與歐洲電信標準協會 (European Telecommunications Standards Institute, ETSI) 息息相關，初期該名稱的原意是行動邊緣運算 (Mobile Edge Computing, MEC)，後來基於擴大用戶設備 (User Equipment, UE) 的服務範疇考量，才更名為多接取邊緣運算 (Multi-access Edge Computing, MEC)，並透過國際電信標準組織第三代合作夥伴計畫 (The 3rd Generation Partnership Project, 3GPP) 制定相關標準規範 (1)，以提供多種 5G 專網多接取邊緣運算 (MEC) 的佈建型態。

經濟部技術處表示包含日月光、台塑、三軍總醫院、友嘉、台塑與中油等超過 20 家企業已經明確表達建置專網 (non-public networks, NPN) 需求，且台灣行政院層級的「5G 專網專頻」政策規劃於 2021 至 2022 年間分階段釋出 4.8GHz 到 4.9GHz 頻段之專網頻譜執照 (2)。當企業欲建立起 5G 專網環境時，可透過租用電信營運商的 5G 網路達成，但礙於企業的資訊需要保密，故需要將邊緣運算 (Edge Computing, EC) 平台部署於企業網路中。同時為了實現低延遲與高可靠度以及高傳輸速率的垂直領域應用服務，需將 5G 專網多接取邊緣運算與 5G 專網電信業者無線接取網路及核心網路的通訊設備緊密整合，以此所示，多接取邊緣運算是未來部署 5G 企業專網的關鍵。

由於 5G 專網多接取邊緣運算並非部署在電信機房安全等級的環境，因此可能遭受設備實體入侵與傳輸網路入侵等威脅；然而，現有伺服器資訊安全大部分都只討論應用服務本身，缺乏以 5G 通訊技術的觀點來探討邊緣應用伺服器 (Edge Application Server, EAS) 的安全議題，有鑑於 5G 專網多元應用型態於佈建時需要依賴 5G 專網多接取邊緣運算技術，若能夠協助台灣邊緣應用伺服器製造商在開發階段即早發現資安相關問題，可大幅提升產品的國際市場競爭力。

在經濟部技術處「5G+系統暨應用淬鍊計畫」的支持下，資策會資安所團隊「5G 專網多接取邊緣運算資安研究報告」 (以下簡稱本研究報告)，參考「TAICS 企業組網情境與架構研究報告」[1] 與第三代合作夥伴計畫 (The 3rd Generation Partnership

Project, 3GPP) 相關標準規範與研究報告，以及歐洲電信標準協會 (ETSI) 的多接取邊緣運算資安研究報告，提供 5G 專網系統整合商與伺服器製造商以及電信事業了解使用 5G 專網多接取邊緣運算技術 (MEC) 會面臨的威脅與因應之道，並歸納出 5G 專網多接取邊緣運算 (MEC) 的基本網路架構，作為未來制定 5G 專網多接取邊緣運算 (MEC) 相關資安測試規範之依據。

1. 適用範圍

本研究報告的有效範圍將涵蓋 5G 專網多接取邊緣運算 (Multi-access Edge Computing, MEC) 之架構探討以及資安的研究分析。本研究報告之 5G 專網架構將以第三代合作夥伴計畫 (3GPP) 標準規範與研究報告為主，並參考歐洲電信標準協會 (ETSI) 的多接取邊緣運算資安研究報告，探討 5G 專網多接取邊緣運算的資安風險。適用範圍包括圖 1「多接取邊緣運算平台架構」與圖 2「獨立佈建多接取邊緣運算網路架構」的紅色線框部分以及圖 3「與公網整合多接取邊緣運算網路架構」的紅色線框部分。當存取網路 (Access Network, AN) 採用 5G 基地臺集中單元與分散單元分離時，5G 基地臺集中單元 (gNB-CU) 將會邊緣運算 (Edge Computing) 整合共同部屬於 5G 多接取邊緣運算 (MEC) 的平台上 (圖 2 與圖 3 中紅色虛線框部分)。

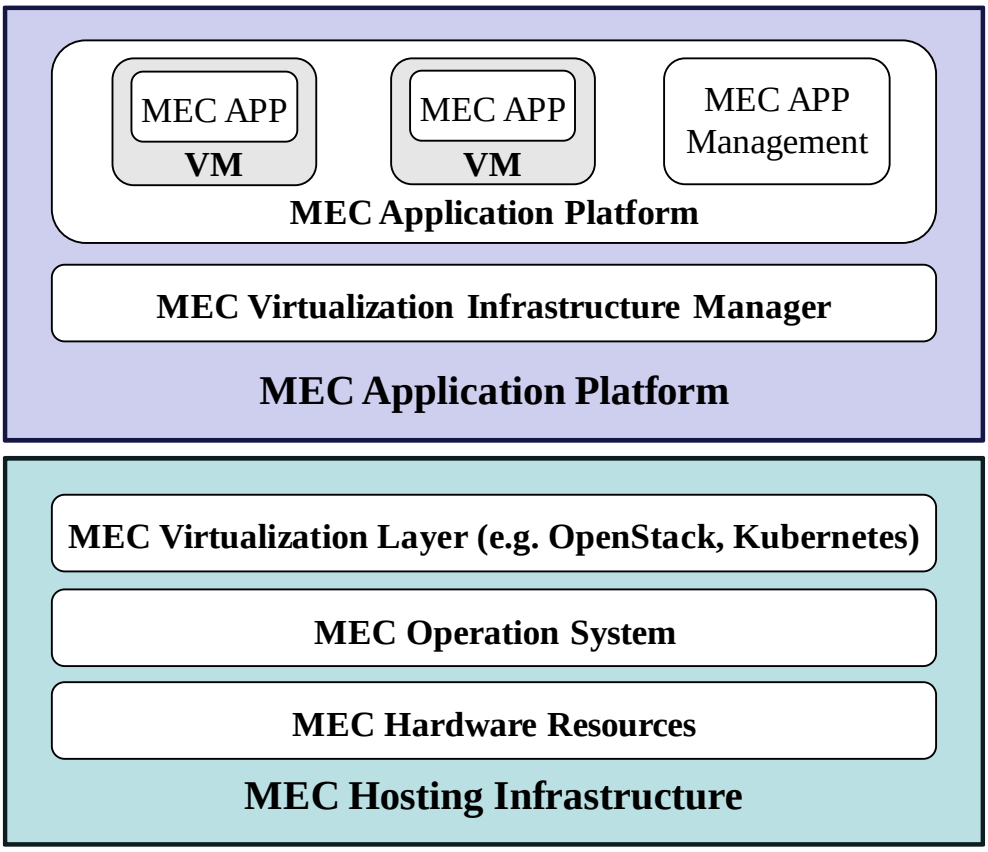


圖 1 多接取邊緣運算平台架構

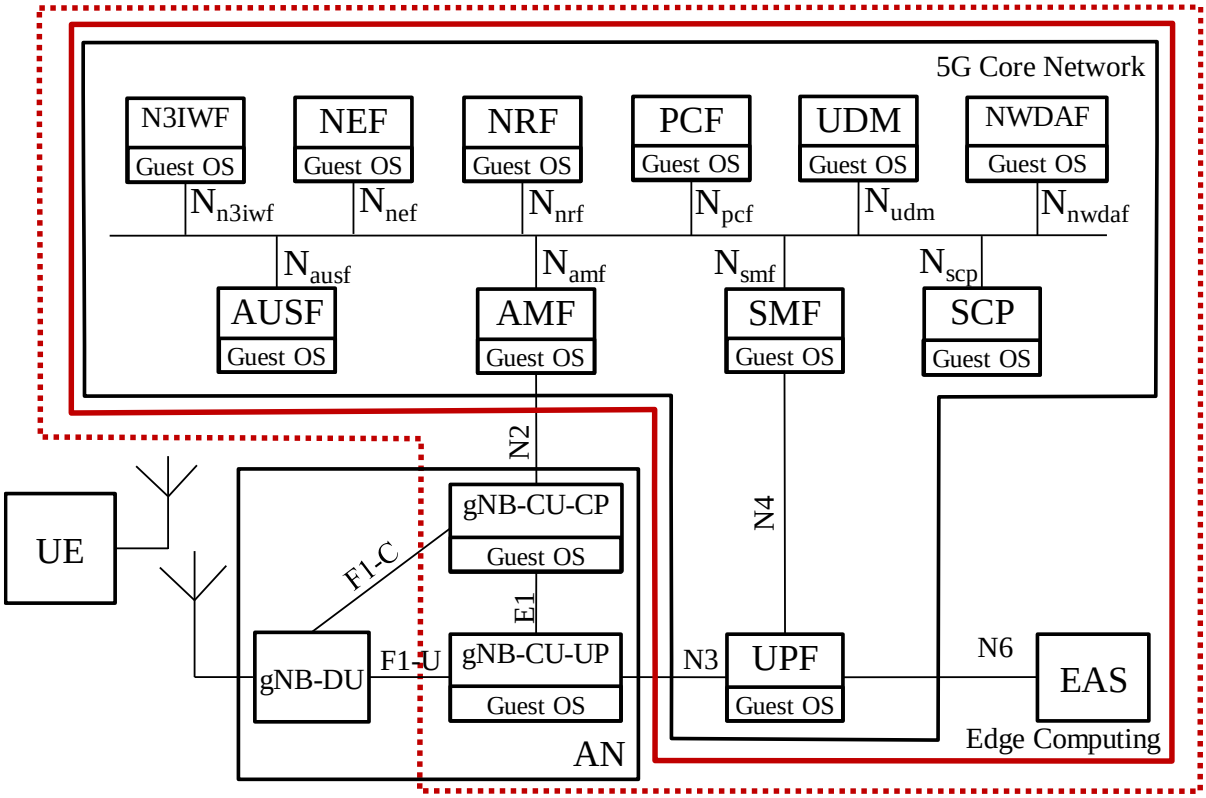


圖 2 獨立佈建多接取邊緣運算網路架構

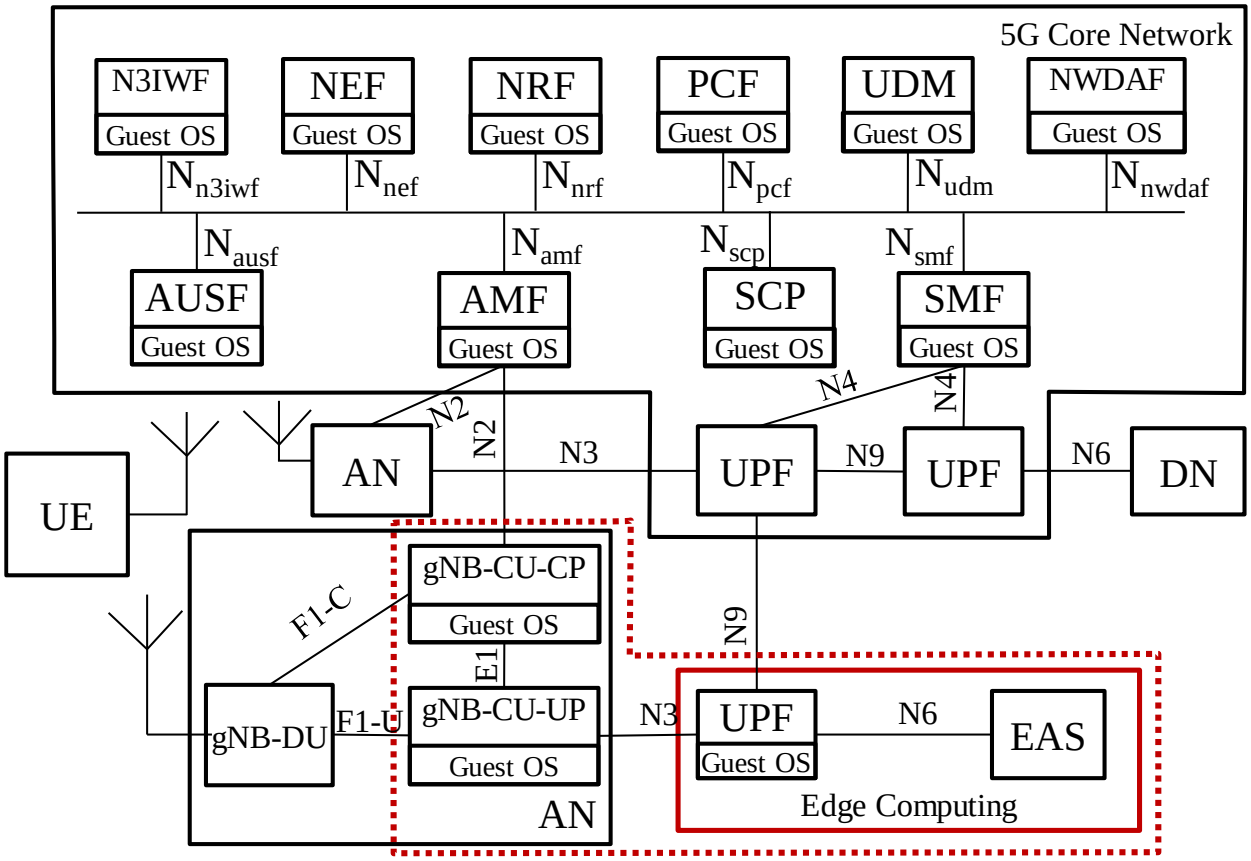


圖 3 與公網整合多接取邊緣運算網路架構

2. 引用標準

以下引用標準係本研究報告必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

[1] TAICS TR-0011 企業組網情境與架構研究報告, 2019

[2] 3GPP TR 23.748-040 Study on enhancement of support for Edge Computing in 5G Core network (5GC) (Release 17)

[3] 3GPP TR 23.758-h00 Study on application architecture for enabling Edge Applications (Release 17)

[4] 3GPP TR 23.734-g20 Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services (Release 16)

[5] 3GPP TR 23.700-07-040 Study on enhanced support of non-public networks (Release 17)

[6] 3GPP TR 33.819-g10 Study on security enhancements of 5G System (5GS) for vertical and Local Area Network (LAN) services (Release 16)

3. 用語及定義

下列用語及定義適用於本研究報告。

3.1 第三代合作夥伴計畫 (The 3rd Generation Partnership Project , 3GPP)

是一個成立於 1998 年 12 月的標準化機構，該機構設立的原初目的在推廣以全球行動通訊系統 (Global System for Mobile communications, GSM) 規格為基礎的國際行動通訊 2000 (International Mobile Telecommunication-2000, IMT-2000) 技術規範，並持續制定符合國際行動通訊升級版 (IMT-A)及國際行動通訊 2020 (MT-2020) 的 4G 與 5G 無線通訊標準，以持續升級既有的國際通用技術標準規格。目前其成員包括歐洲電信標準化協會 (European Telecommunications Standards Institute, ETSI)、日本無線電產業與商務協會 (Association of Radio Industries and Business, ARIB)、日本電信技術委員會 (Telecommunication Technology Committee, TTC)、中國通訊標準化協會 (China Communications Standards Association, CCSA)、北美通訊產業解決方案聯盟 (Alliance for Telecommunications Industry Solutions, ATIS)、韓國電信技術協會 (Telecommunication Technical Assembly, TTA)，以及印度電信標準發展協會 (Telecommunications Standards Development Society, India, TSDSI) 都簽署加入這個合作性協議中。

3.2 邊緣應用伺服器 (Edge Application Server, EAS)

定義於 3GPP TR 23.748 [2] 之第 3.1 小節中，使電信事業可以透過核心網路 (5GC) 選擇一個用戶設備 (UE) 鄰近位置的用戶平面功能 (UPF)，再將用戶設備的資料透過 N6 接口導流至邊緣應用伺服器 (EAS)，以實現視訊分析、健康醫療或企業服務等不同類型的低延遲 5G 應用服務。

3.3 多接取邊緣運算 (Multi-access Edge Computing, MEC)

一種與行動核心網路整合的分散式邊緣運算技術，讓內容服務或應用服務供應商能夠透過行動網路邊緣之處，適時分流雲端運算 (cloud computing) 服務的負荷與提供

頻寬管理。更可憑藉臨近用戶設備 (UE) 的優勢就近享有雲端運算能力，實現虛擬實境(Virtual Reality, VR)、擴增實境(Augmented Reality, AR)、車聯網(Vehicle-to-Everything, V2X) 或無人飛行系統 (Unmanned Aerial Systems, UAS) 等低延遲和高頻寬通訊的第三方應用服務。

歐洲電信標準協會 (ETSI) 的多接取邊緣運算技術 (MEC) 標準工作組針對邊緣運算系統之規範 (1)(3)(4)，由多接取邊緣運算協作 (MEC Orchestrator) 對邊緣應用伺服器 (EAS) 內部的資源/服務進行管控，並藉由 Naf 介面提供多接取邊緣運算 (MEC) 中的服務資訊給連結管理功能 (SMF)，使之建立與調整用戶設備 (UE) 存取至邊緣應用伺服器 (EAS) 的連線。

3.4 專網 (Non-Public Networks, NPN)

一種專門佈署用醫療、交通、製造、智慧城市等公部門應用，以及企業總部、工廠、醫院、娛樂展場、運動 場館、零售門市等私企業應用的網路 (5)。專網可以分為 3GPP TS 23.501 (6) 的第 5.3.2 小節所定義之獨立佈建專網 (Stand-alone Non-Public Network, SNPN)」以及與 3GPP TS 23.501 (6) 的第 5.3.3 小節所定義之「與公網整合專網 (Public Network integrated Non-Public Network, PNiNPN)」兩種佈建型態。

3.5 用戶設備 (User Equipment, UE)

由通用積體電路卡 (Universal Integrated Circuit Card, UICC) 和移動式設備 (Mobile Equipment, ME) 組成 (7)，其中移動式設備可進一步由處理通訊功能的移動式終端 (Mobile Termination, MT) 和終端設備 (Terminal Equipment, TE) 組成。

3.6 存取網路 (Access Network, AN)

透過無線接取介面連接用戶設備 (UE)，提供增強型行動寬頻通訊 (Enhanced Mobile Broadband, eMBB)、超可靠度和低延遲通訊 (Ultra-reliable and Low Latency Communications, URLLC)、大量機器類通訊 (massive Machine-Type Communications, mMTC) 以及車聯網通訊 (Vehicle-to-Everything, V2X) 等服務 (6)(7)。

3.7 5G 基地臺 (gNodeB, gNB)

是固定在一個地方的多通道雙向無線電傳送機，提供用戶設備 (UE) 雙向無線通訊，依據發射功率可以分為大型基地臺 (Marco Cell) 以及小型基地臺 (Small Cell)。大型基地臺搭載巨量天線 (Massive antennas)，主要布建位置為高塔及建物樓頂，用來提供基本的 5G 戶外訊號涵蓋以及有限度的室內訊號涵蓋。小型基地臺則用來提高基地臺的部署密度，填補大型基地臺訊號死角與加強室內的訊號涵蓋以及提升熱點的系統容量。

3.8 5G 基地臺集中單元 (gNB Central Unit, gNB-CU)

是一個網路元件負責 5G 基地臺 (gNB) 中無線資源控制 (Radio Resource Control, RRC) 與服務數據適配協定 (Service Data Adaptation Protocol, SDAP) 以及分封數據匯聚協定 (Packet Data Convergence Protocol, PDCP) 等網路功能 (8)。

3.9 5G 基地臺分散單元 (gNB Distributed Unit, gNB-DU)

是一個網路元件負責 5G 基地臺 (gNB) 中無線鏈路控制 (Radio Link Control, RLC) 與媒體存取控制 (Media Access Control, MAC) 以及實體層 (Physical layer, PHY) 等網路功能 (8)。

3.10 5G 基地臺集中單元-控制平面 (gNB-CU Control Plane, gNB-CU-CP)

是一個網路元件負責 5G 基地臺集中單元 (gNB-CU) 中無線資源控制 (Radio Resource Control, RRC) 與分封數據匯聚協定 (Packet Data Convergence Protocol, PDCP) 等控制平面的網路功能 (8)。

3.11 5G 基地臺集中單元-用戶平面 (gNB-CU User Plane, gNB-CU-UP)

是一個網路元件負責 5G 基地臺集中單元 (gNB-CU) 中服務數據適配協定 (Data Adaptation Protocol, SDAP) 以及分封數據匯聚協定 (Packet Data Convergence Protocol, PDCP) 等用戶平面的網路功能 (8)。

3.12 5G 核心網路 (5G Core Network, 5GC)

透過控制平面 (Control Plane) 與使用者平面 (User Plane) 分離技術實現以服務為基礎 (Service Based Architecture, SBA) 之網路功能虛擬化 (Network Function Virtualization, NFV) 架構 (6)，5G 核心網路透過下一代應用協定 (Next Generation Application Protocol, NGAP) 與通用封包無線服務隧道協定-使用者平面 (GPRS Tunnel Protocol–User Plane, GTP-U) 連接基地台 (gNB)。

3.13 存取與行動管理功能 (Access and Mobility Management Function, AMF)

負責用戶設備 (UE) 進入行動網路的註冊管理與身份驗證、非存取層 (Non Access Stratum, NAS) 傳訊的加密與完整性保護、緊急電話 (emergency call) 的定位服務管理、用戶設備移動換手管理以及合法監聽 (Lawful Interception, LI) 等功能 (6)。

3.14 連結管理功能 (Session Management Function, SMF)

負責用戶設備 (UE) 對話建立/修改/釋放之管理、DHCP 功能與 IP 地址分配管理、ARP 代理管理、配置用戶平面功能 (UPF) 的流量控制、對話和服務連續性 (Session and Service Continuity, SSC) 模式、收集電信營運商收費資訊、使用者平面安全策略管理以及合法監聽等功能 (6)。

3.15 用戶平面功能 (User Plane Function, UPF)

負責用戶設備 (UE) 上網連線、資料封包檢查與路由和轉發、使用者平面的流量監控與服務品質 (QoS) 管理、連接外部資料網路 (DN) 的管理、使用者平面部分策略規則管理以及合法監聽等功能 (6)。

3.16 認證伺服器功能 (Authentication Server Function, AUSF)

提供用戶設備 (UE) 雙向身份認證與單一認證框架的功能，並負責產生加解密與完整性檢查的金鑰 (6)。

3.17 統一資料管理功能 (Unified Data Management, UDM)

由應用前端 (front end, FE) 與用戶資料庫 (user data repository, UDR) 兩部分組成。統一資料管理功能前端 (UDM-FE) 可以訪問儲存在用戶資料庫中的用戶資訊，同時負責處理存取授權、註冊與移動性管理、位置管理以及簡訊管理等功能 (6)。

3.18 網路資料庫功能 (Network Repository Function, NRF)

支援 5G 核心網路元件的服務探索功能，同時負責維護 5G 核心網路中所有網路元件的資訊以及支援的服務。當一個核心網路元件收到服務探索請求時，被探索的核心網路元件將回復該探索請求。

3.19 網路曝光功能 (Network Exposure Function, NEF)

主要包含監控、支援、策略/計費等三種功能。其中監控功能主要是監控用戶設備 (UE) 透過網路曝光功能 (NEF) 向外傳輸的資料；支援功能指外部單元可以通過網路曝光功能獲得用戶設備 (UE) 的移動性與連結管理等資訊；策略/計費功能指外部單元單元通過網路曝光功能傳遞服務品質 (QoS) 與計費的策略 (policy)。

3.20 政策控制功能 (Policy Control Function, PCF)

該網路元件支援網路政策管理的統一框架；連接用戶資料庫 (user data repository, UDR) 獲取用戶政策資訊，並提供政策規則給控制平面執行。

3.21 應用功能 (Application Function, AF)

該網路元件提供應用服務路由、訪問網路曝光功能 (NEF)，並透過政策控制功能 (PCF)進行用戶政策管控。

3.22 資料網路 (Data Network, DN)

係指電信網路服務(如 VOD 隨選服務等) 或第三方資料網路 (6) (如 Youtube 等)。

3.23 來賓作業系統 (Guest Operating System, Guest OS)

係指安裝在網路設備虛擬機器 (Virtual Machine, VM) 上的作業系統 (Operating System, OS) 軟體 (35)。

3.24 應用程式介面 (Application Programming Interface, API)

規定執行一個銜接不同應用程式系統的協定 (7)，由複雜且大量的函數與副程式所組成，協助不同程式在交換資料、執行指令時，得以順利溝通並保證無誤。可以間接促成系統形成鬆耦合關係，降低彼此之間的依賴性，並提高系統的可用性 (Availability) 與可擴充性 (Scalability)。

4. 符號及縮寫

3GPP: 3rd Generation Partnership Project

5GC: 5G Core Network

5G-GUTI: 5G Globally Unique Temporary Identifier

5G-PPP: 5G Infrastructure Public Private Partnership

AAA: Authentication, Authorization, Accounting

AEF: API Exposure Function

AF: Application Function

AI: Artificial Intelligence

AIoT: Artificial Intelligence and Internet of Things

AMF: Access and Mobility Management Function,

AN: Access Network

API: Application Programming Interface

AR: Augmented Reality

ARIB: Association of Radio Industries and Business

ARPF: Authentication credential Repository and Processing Function

ATIS: Alliance for Telecommunications Industry Solutions

AUSF: Authentication Server Function

B2B: Business to Business

CAG: Closed Access Group

CAPIF: Common Application Programming Interface Framework

CCF: CAPIF Core Function

CCSA: China Communications Standards Association

CGI: Common Gateway Interface

CIoT: Cellular Internet of Things

C-RAN: Centralized/Cloud Radio Access Network

CSA: Cloud Security Alliance

CU: Centralized Unit

DevOps: Development and Operations

DN: Data Network

DU: Distributed Unit

EAS: Edge Application Server

EC: Edge Computing

eMBB: Enhanced Mobile Broadband

ETSI: European Telecommunications Standards Institute

FAE: FoF Application Enabler

FE: Front End

FMC: Fixed-Mobile Convergence

FoF: Factories of the Future

FRMCS: Future Railway Mobile Communication System

GDPR: General Data Protection Regulation

gNB: gNodeB

gNB-CU: gNB Central Unit

gNB-DU: gNB Distributed Unit

gNB-CU-CP: gNB-CU Control Plane

gNB-CU-UP: gNB-CU User Plane

gPTP: generic Precision Time Protocol

GSM: Global System for Mobile communications

GTP-C: GPRS Tunnel Protocol–Control Plane

GTP-U: GPRS Tunnel Protocol–User Plane

GVNP: Generic Virtualized Network Product

HIPAA: Health Insurance Portability and Accountability Act

HPC: High-Performance Computing

HTTP: HyperText Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

IACS: Cyber Security for Industrial Automation and Control

ICMPv4: Internet Control Message Protocol version 4

ICMPv6: Internet Control Message Protocol version 6

IE: Information Element

IEC: International Electrotechnical Commission

IETF: The Internet Engineering Task Force

IIoT: Industry Internet of Thing

iMEC: Intelligent Mobile Edge Computing

IMS: IP Multimedia Subsystem

IMSI: International Mobile Subscriber Identity

IOPS: Isolated E-UTRAN Operation for Public Safety

IoT: Internet of Things

IP: Internet Protocol

IPsec: IP Security

IPX: IP eXchange

ISA: International Society of Automation

JSON: JavaScript Object Notation

JWS: JSON Web Signature

K8S: Kubernetes

LAN: Local Area Network

LEA: Law Enforcement Agency

LI: Lawful Interception

MAC: Media Access Control

MANO: Management and Orchestration

MBMS: Multimedia Broadcast/Multicast Service

ME: Mobile Equipment

MEC: Mobile Edge Computing

MEC: Multi-access Edge Computing

MitM: Man-in-the-Middle

mMTC: massive Machine-Type Communications

MT: Mobile Termination

N3IWF: Non-3GPP Inter-Working Function

NAS: Non-Access Stratum

NEF: Network Exposure Function

NF: Network Function

NFV: Network Function Virtualization

NFVI: Network Functions Virtualization Infrastructure

NGAP: Next Generation Application Protocol

NGMN: Next Generation Mobile Network

NPN: Non-Public Networks

NRF: Network Repository Function

NWDAF: Network Data Analytics Function

OMA: Open Mobile Alliance

OpenNESS: Open Network Edge Service Software

OPNFV: OpenStack Network Function Virtualization

OS: Operating System

PCF: Policy Control Function

PDCP: Packet Data Convergence Protocol

PHY: Physical layer

PLMN: Public Land Mobile Network

PNiNPN: Public Network integrated Non-Public Network

QoS: Quality of Service

RLC: Radio Link Control

RRC: Radio Resource Control

SaaS: Security-as-a-Service

SBA: Service Based Architecture

SCEF: Service Capability Exposure Framework

SDAP: Service Data Adaptation Protocol

SDN: Software Defined Network

SEAL: Service Enabler Architecture Layer for Verticals

SECOP: Service Communication Proxy

SEPP: Security Edge Protection Proxy

SMF: Session Management Function

SS7: Signalling System No. 7

SSC: Session and Service Continuity

SSI: Server Side Includes

SNPN: Stand-alone Non-Public Network

SUPI: Subscription Permanent Identifier

TE: Terminal Equipment

TEID: Tunnel Identifier

TLS: Transport Layer Security

TSC: Time Synchronization

TSDSI: Telecommunications Standards Development Society, India

TSN: Time Sensitive Networking

TTA: Telecommunication Technical Assembly

TTC: Telecommunication Technology Committee

UAS: Unmanned Aerial Systems

UDM: Unified Data Management

UDR: User Data Repository

UE: User Equipment

UICC: Universal Integrated Circuit Card

UPF: User Plane Function

URLLC: Ultra-Reliable Low-Latency Communication

USS: UAS Service Supplier

UTM: UAS Traffic Management

V2X: Vehicle-to-Everything

VAE: V2X Application Enabler

VAL: Vertical Application Layer

VIM: Virtualised Infrastructure Manager

VM: Virtual Machine

VNC: Virtual Network Console

VNF: Virtual Network Function

VNFM: Virtualized Network Function Manager

VoD: Video on Demand

WLAN: Wireless Local Area Network

5. 5G 專網多接取邊緣運算架構分析

雲端虛擬化技術持續地蓬勃發展，為符合更多應用服務對於低延遲時間或移動性管理的需求，進而衍生了透過與行動核心網路整合的分散式邊緣運算技術，讓內容服務或應用服務供應商能夠透過行動網路邊緣之處，適時卸載雲端運算 (cloud computing) 服務的負荷與提供頻寬管理。在「TAICS 企業組網情境與架構研究報告」[1] 中已經闡述現有營運商預想的 5G 專網多接取邊緣運算 (MEC) 應用情境與系統架構，本節將闡述現有國際5G專網多接取邊緣運算架構發展趨勢與國內5G專網多接取邊緣運算架構，並在下節探討相關的安全性議題。

5.1 5G 專網多接取邊緣運算架構的國際發展趨勢

當企業欲建立起 5G 專網環境時，可透過租用電信營運商的 5G 網路達成，但礙於企業的資訊需要保密，故需要將邊緣運算 (Edge Computing, EC) 平台部署於企業網路中。同時為了實現低延遲率與高可靠度以及高傳輸速率的垂直領域應用服務，需將 5G 專網多接取邊緣運算與電信業者無線接取網路及核心網路的通訊設備緊密整合，所以5G專網多接取邊緣運算是未來部署5G企業專網的關鍵。目前要進入垂直領域市場所面臨到最大障礙是缺乏各領域的專業知識，所以第三代合作夥伴計畫 (3GPP) 自從 2018 年 6 月完成第十五版 (Release 15) 的 5G 行動通訊的基礎設施技術標準後，緊接著就有來自航太、車輛、農業、零售、製造等各垂直領域業者積極參與，並於 2019 年 12 月完成第十六版 (Release 16) 的 5G 專網相關應用的最終標準制定。目前也已有如汽車大廠賓士 (Mercedes-Benz)、奧迪 (Audi)、福斯汽車 (Volkswagen)，以及博世 (Bosch)、諾基亞 (Nokia) 等全球知名企業陸續宣布在自家工廠建置 5G 專網的案例。

5.1.1 5G 專網多接取邊緣運算與專網架構的標準化

5G 專網多接取邊緣運算 (MEC) 技術在靠近 (proximity) 用戶設備 (UE)的網路位置，提供雲端運算的服務及儲存能力，藉以達成提供超低延遲時間 (ultra-low latency) 及高頻寬 (high bandwidth) 的服務的目的。以制定行動通訊系統架構相關標準為主要任務的架構工作組 (SA2 - Architecture) 在完成以服務基礎架構 (Service-Based

Architecture, SBA) 為導向之網路功能虛擬化 (NFV) 後，更進一步對於 3GPP TR 23.748 [2] 之 5G 專網多接取邊緣運算架構的標準技術規格，使電信運營商可以實現視訊分析、健康醫療或企業服務等不同類型的低延遲 5G 應用服務。

依據 3GPP TS 23.501 (6) 與 3GPP TR 23.748 [2] 標準文件所定義之 5G 獨立網組 (Standalone, SA) 之多接取邊緣運算架構由用戶設備 (User Equipment, UE)、存取網路 (Access Network, AN)、邊緣運算 (Edge Computing, EC) 及 5G 核心網路 (5G Core Network, 5GC) 所組成，其中 5G 核心網路(5GC) 由多個「網路功能服務」的模組構成，並透過「以服務為基礎之介面」來實現網路功能 (Network Function, NF) 。而網路資料庫功能 (Network Function Repository Function, NRF) 支持網路功能 (NF) 服務註冊與狀態監測等機制，以實現網路功能 (NF) 服務自動化管理。並透過控制平面 (Control Plane) 與使用者平面 (User Plane) 分離，可以為網路功能虛擬化 (Network Function Virtualization, NFV) 及多接取邊緣運算 (Multi-access Edge Computing, MEC) 提供較為完善的網路架構。

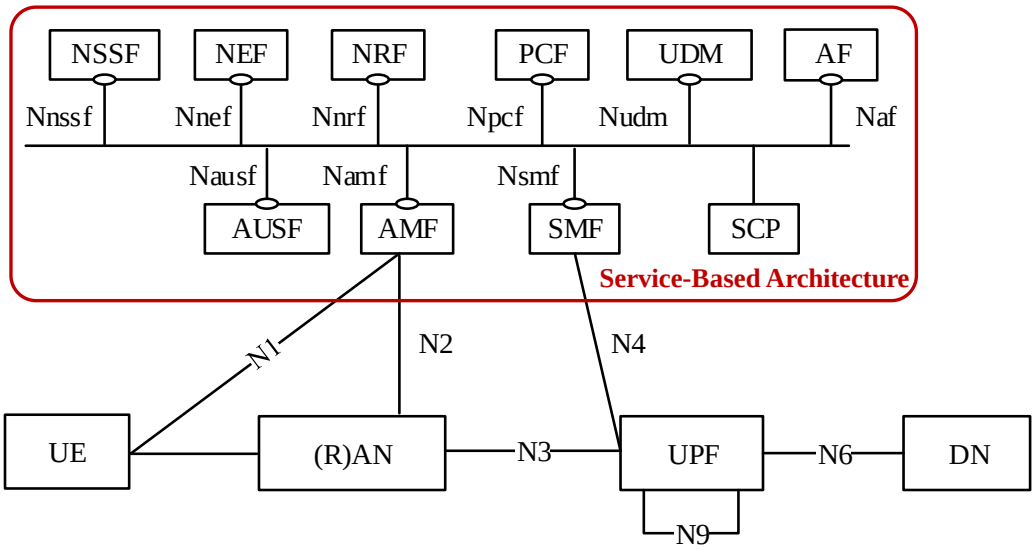


圖 4 以服務基礎架構為導向的系統架構 (3)

5G 專網多接取邊緣運算的佈建型態依據 3GPP TS 23.501 (6) 的規範分為由企業建構的「獨立佈建專網 (Stand-alone Non-Public Network, SNPN)」以及由電信營運商主導的「與公網整合專網 (Public network integrated Non-Public Network, PNiNPN)」兩大類。

當企業欲建立起 5G 專網環境時，可透過租用電信營運商的 5G 網路達成與公網整合專網 (PNiNPN) 的佈建型態，如圖 5 所示。

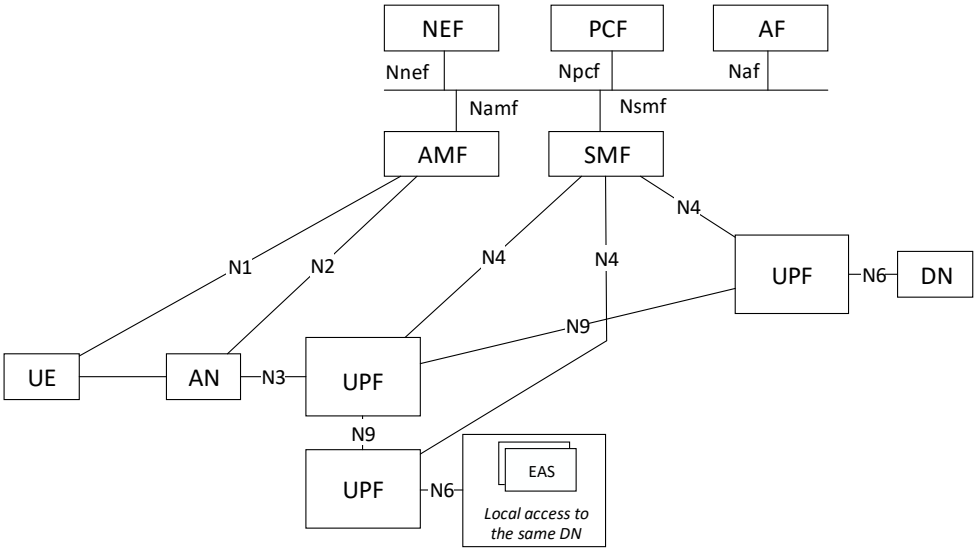


圖 5 與公網整合專網 (PNiNPN) 的系統架構 [2]

針對與公網整合專網可以進一步分為三種佈建型態模式：(1) 在公有電信網路透過網路切片方式切一塊專屬企業用專網、(2) 建置企業專用基地台與邊緣應用伺服器 (EAS)、(3) 建置企業專用基地台與企客共用邊緣應用伺服器 (EAS) 提供跨廠區服務。

當企業需要超可靠度和低延遲通訊 (Ultra-reliable and Low Latency Communications, URLLC) 的專網環境時，則需要採用獨立的核心網路加上獨立基地台的 5G 獨立佈建專網 (SNPN)，如圖 6 所示。

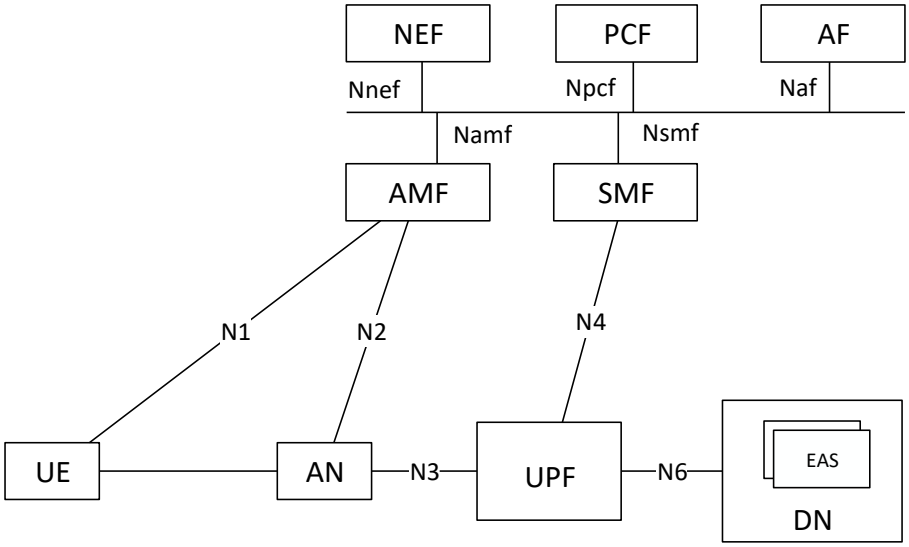


圖 6 獨立佈建專網(SNPN)的系統架構 [2]

早期電信事業若有基站建置需求都必須向傳統電信設備商購買 5G 基地台設備。 當 5G 行動通訊網路導入 5G 基地臺集中單元與分散單元分離網路架構後 (如圖 7 所示)，電信事業可跳過傳統電信設備商，直接向硬體設備業者採購電信設備，有利於創建高靈活性的 5G 行動通訊網路。其中 5G 基地臺集中單元 (gNB-CU) 負責無線資源控制 (RRC) 與服務數據適配協定 (SDAP) 以及分封數據匯聚協定 (PDCP) 等網路功能，而 5G 基地臺分散單元 (gNB-DU) 則負責無線鏈路控制 (RLC) 與媒體存取控制 (MAC) 以及實體層 (PHY) 等網路功能。當 5G 基地臺集中單元 (gNB-CU) 進一步導入之控制平面與用戶平面分離架構後 (如圖 8 所示)，5G 基地臺集中單元拆分為 5G 基地臺集中單元-控制平面 (gNB-CU-CP) 與 5G 基地臺集中單元-用戶平面 (gNB-CU-UP)。

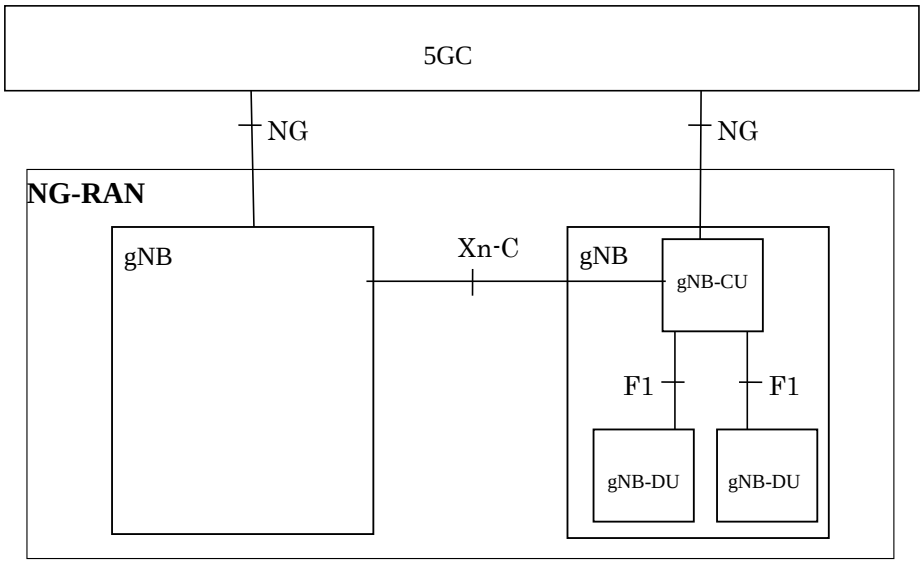


圖 7 5G 基地臺集中單元與分散單元分離架構 (8)

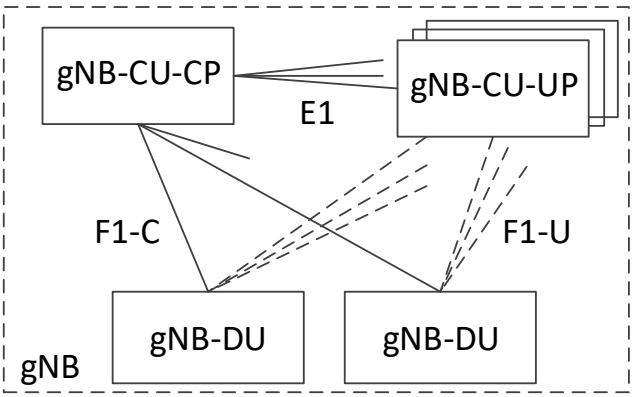


圖 8 5G 基地臺集中單元之控制平面與用戶平面分離架構 (8)

依據前述的 5G 網路架構標準，5G 專網多接取邊緣運算平台架構可以分為圖 2 之「獨立佈建多接取邊緣運算網路架構」以及圖 3 之「與公網整合多接取邊緣運算網路架構」兩類。當存取網路 (Access Network, AN) 採用 5G 基地臺集中單元與分散單元分離時，5G 基地臺集中單元 (gNB-CU) 將會邊緣運算 (Edge Computing) 整合共同部屬於 5G 多接取邊緣運算 (MEC) 的平台上 (圖 1 與圖 2 中紅色虛線框部分)，以實現超低延遲時間 (ultra-low latency) 及高頻寬 (high bandwidth) 的服務。

5.1.2 5G 專網多接取邊緣運算支援多元應用情境

以制定關鍵型應用程序相關標準為主要任務的關鍵任務應用工作組 (SA6 - Mission-critical applications) 在完成包括未來鐵道行動通訊系統 (Future Railway Mobile Communication System, FRMCS) 和獨立運作式公共安全 (Isolated E-UTRAN Operation for Public Safety, IOPS) 等關鍵任務運營服務後，現階段正將關鍵任務應用服務的技術規格移植到各垂直領域的應用服務。透過應用層功能元件和應用程式介面 (Application Programming Interface, API) 的標準技術規格，來滿足鏈結到各垂直行業的 5G 專網生態系統需求，進一步為 5G 提供垂直應用程序的通用服務平台做準備。

為了達成低延遲和高頻寬通訊的垂直領域應用服務，5G 專網佈建時需要垂直領域的邊緣應用伺服器 (EAS) 與電信業者間進行緊密整合，如圖 9 所示。透過啟用邊緣應用程序 (Application Architecture for enabling Edge Applications, EDGEAPP) 相關標準規範的制定，可以將用戶設備的資料導流至邊緣應用伺服器 (EAS)，以實現視訊分析、無人車、智慧製造、健康醫療或企業服務等不同類型的低延遲 5G 應用服務。

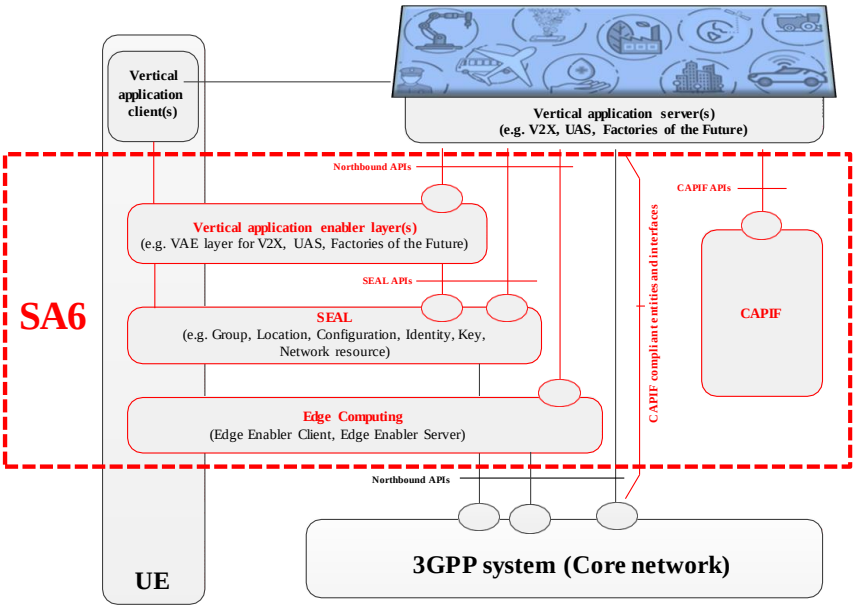


圖 9 緊密整合垂直應用服務與 5G 多接取邊緣運算示意圖 (9)

5.1.2.1 啟用邊緣應用程序架構

啟用邊緣應用程序架構 (Application Architecture for enabling Edge Applications, EDGEAPP) 支援在 5G 專網多接取邊緣運算平台上開發和託管應用程序的架構體，依據 3GPP TR 23.758 [3] 之技術規格研究報告，其包括如用戶設備移動性，邊緣應用程序可移植性，服務差異化和靈活部署，並提供邊緣應用程序對應之北向應用程式介面 (Northbound API) 使 5G 專用網路功能與邊緣運算服務 (Edge Computing Service) 之間緊密整合。

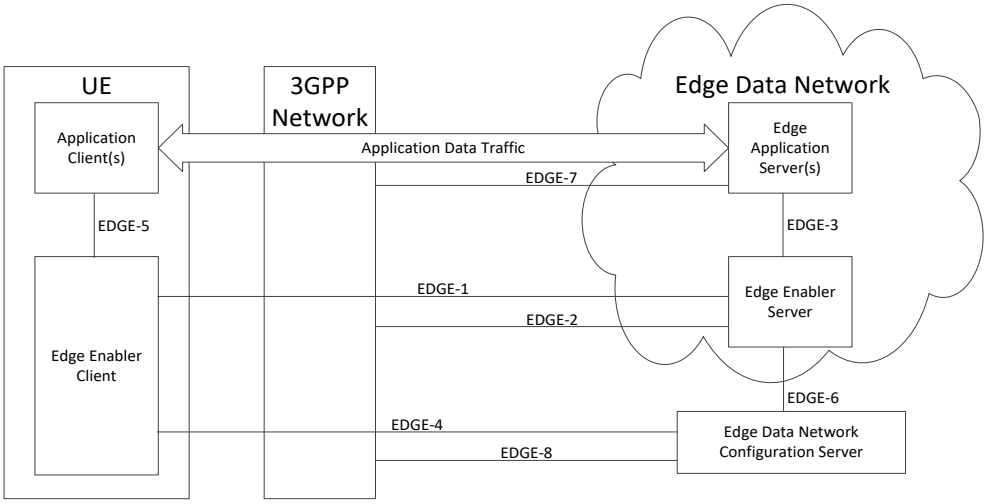


圖 10 啟用邊緣應用程序架構(EDGEAPP)

共用應用程式介面構架 (Common Application Programming Interface Framework, CAPIF) 主要是參考開放行動通訊聯盟 (Open Mobile Alliance, OMA) 以及歐洲電信標準協會 (ETSI) 的 5G 專網多接取邊緣運算 (MEC) 之應用程式介面 (API) 框架制定 3GPP TS 23.222 (10) 的技術標準規格。該標準規格結合 SA2 架構工作組所制定之服務能力揭露框架 (Service Capability Exposure Framework, SCEF) 與網路曝光功能 (Network Exposure Function, NEF) 之北向應用程式介面 (Northbound APIs) (11) 以及編碼工作組 (SA4 - Codec) 制定之多媒體廣播多點服務 (Multimedia Broadcast/Multicast Service, MBMS)的 xMB 之北向應用程式介面 (12)，建立一個承載電信 5G 專網垂直領域應用服務框架的統一北向應用程式介面框架標準。

其允許第三方垂直領域業者藉由該共用應用程式介面構架來提供用戶設備相關垂直應用服務，同時導入兩個第三方垂直領域業者間透過共用應用程式介面構架相互連接以及以聯盟形式部署垂直應用服務的關鍵功能。並由共用應用程式介面構架核心功能 (CAPIF Core Function, CCF)、應用程式介面揭露功能 (API Exposure Function, AEF) 與應用程式介面調用者 (API Invoker) 等三個主要實體組成，以支援第三方業者透過共用應用程式介面構架進行垂直領域應用服務分散式部署。

(a) 應用程式介面構架核心功能 (CCF) 提供所有應用程式介面的核心功能與存儲資料庫，包含各垂直領域應用服務註冊 (registration)、註銷(de-registration)、服務發現 (service discovery)、身份驗證 (authentication) 和授權 (authorization)、收費 (charging) 和日誌記錄所需使用的介面與相關功能。

(b) 應用程式介面揭露功能 (AEF) 提供第三方垂直領域業公開的應用程式介面 (API)。

(c) 應用程式介面調用者 (API Invoker) 可以透過如網路曝光功能 (NEF) 的應用程式介面揭露功能 (AEF) 訪問應用程式介面構架核心功能 (CCF) ，以執行如服務註冊 (registration)以及身份驗證 (authentication) 和授權 (authorization)的服務。

5.1.2.2 垂直服務致能架構層

垂直服務致能架構層 (Service Enabler Architecture Layer for Verticals, SEAL) 的系統架構包含用戶設備 (UE) 上的垂直服務致能架構層用戶端 (SEAL client) 以及提供 5G 垂直服務致能架構層服務器 (SEAL server)，依據 3GPP TS 23.434 (13) 之標準技術規格，垂直服務致能架構層允許跨不同垂直領域成員使用功能服務並透過使用者平面進行配置管理、位置管理、身份與金鑰管理以及網路資源管理。垂直服務致能架構層上是垂直應用層 (Vertical Application Layer, VAL)，垂直應用層透過垂直服務致能架構層來實現 5G 垂直應用服務。並能夠在多個垂直服務致能架構層服務器之間建立相互連線和通信，以實現分散式垂直服務致能架構層部署，同時允許用戶設備基於特定位置建立群組服務。該技術規格設計允許用戶設備在連線網路 (on-network) 與離線網路 (off-network) 兩種模式下，均支援垂直服務致能架構層的企業對企業 (Business to business, B2B) 服務。

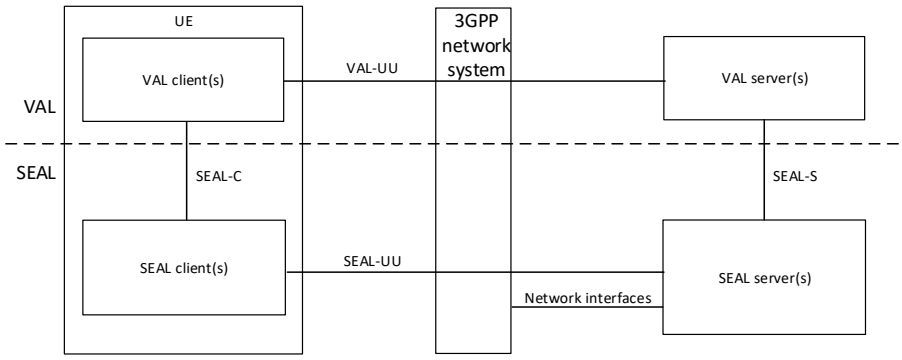


圖 11 垂直服務致能架構層(SEAL)

垂直服務致能架構層能夠提供包含支援車聯網 (Vehicle-to-Everything services, V2X)、未來工廠 (Factories of the Future, FoF) 與無人飛行系統系統 (Unmanned Aerial Systems, UAS) 等垂直應用服務。依據 3GPP TS 23.286 (14) 之技術研究報告，評估在系統上部署車聯網 (V2X) 服務的支援車聯網服務應用層 (Application layer support for Vehicle-to-Everything (V2X) services, V2XAPP) 的必要需求和相對應的解決方案。並且基於垂直服務致能架構層 (SEAL) 上發展一個或多個車聯網垂直應用致能器 (V2X Application Enabler, VAE)。

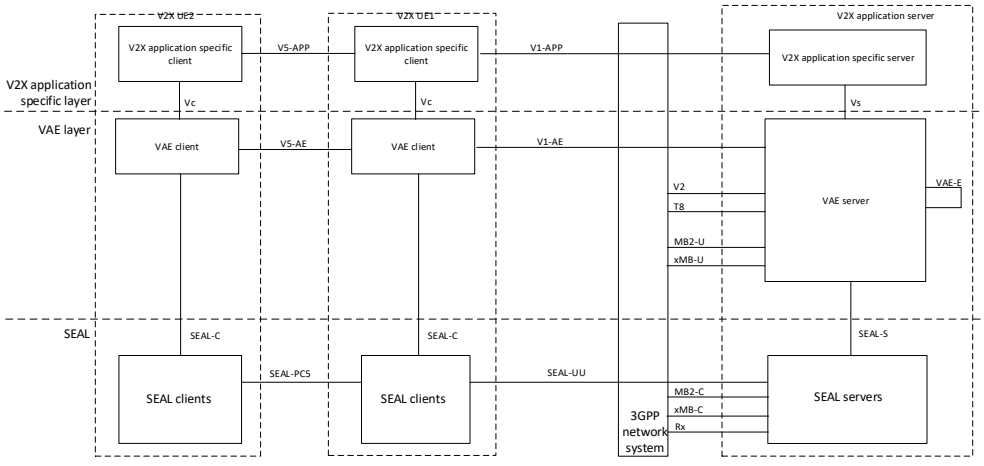


圖 12 支援車聯網服務的應用層(V2XAPP)

依據 3GPP TR 23.755 (15) 之技術研究報告，評估無人飛行系統應用服務必要的應用層架構需求和相對應的解決方案，以實現 5G 專網無人飛行系統 (Unmanned Aerial

Systems, UAS) 的飛行路線授權、位置管理與群組通信等無人飛行系統航路管理 (UAS Traffic Management, UTM) 等應用服務。

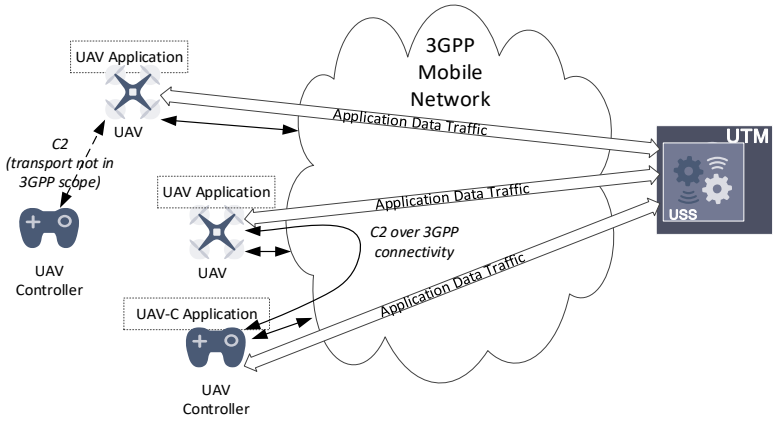


圖 13 支援無人飛行系統應用的情境

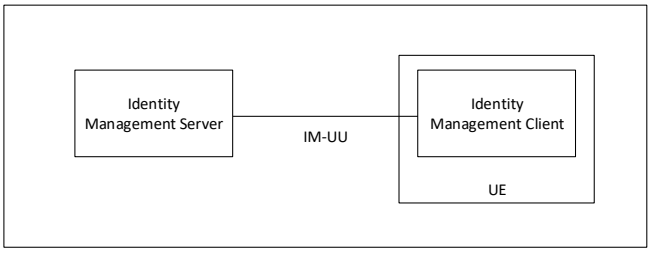


圖 14 垂直服務致能架構層(SEAL)身份管理功能模型

依據 3GPP TR 23.745 (16) 之技術研究報告，根據未來工廠 (FoF) 的垂直應用服務需評估支援未來工廠的應用層 (Application layer support for Factories of the Future, FFAPP) 的必要需求和相對應的解決方案，以確保在未來工廠部署時能夠有效使用 5G 專網的服務。並且基於垂直服務致能架構層 (SEAL) 上發展未來工廠垂直應用致能器 (FoF Application Enabler, FAE)。

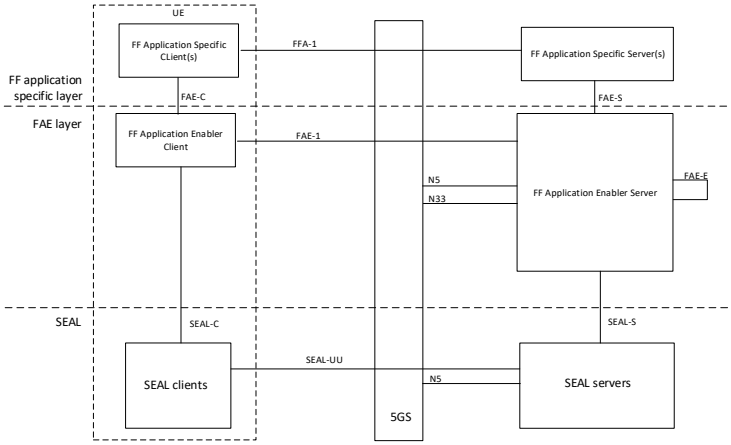


圖 15 支援未來工廠的應用層(FFAPP)

此外，未來工廠 (FoF) 對於無線端對端通訊要求相對於傳統無線通訊要求要高得多，對於不同的應用場景、網路的服務品質機制 (Quality of Service, QoS)、可靠性與安全性要求皆大不相同，故，5G 多接取邊緣運算平台需要導入超可靠度和低延遲通訊 (Ultra-reliable and Low Latency Communications, URLLC) 與時間敏感網路 (Time Sensitive Networking, TSN) 以及 5G 區域網路型態服務 (5G LAN-type service) 等重要技術。

5.1.2.3 時間敏感網路

5G 系統與時間敏感網路 (Time Sensitive Networking, TSN) 整合的技術是透過 IEEE 802.1Qcc (17) 技術標準規格支援時間敏感網路 (TSN) 的控制器協作，並通過 IEEE 802.1AS (18) 技術標準規格針對單一時域來實現時間敏感網路 (TSN) 的同步 (Time Synchronization)，以及藉由 IEEE 802.1Qbv (19) 與 IEEE 802.1CB (20) 技術標準規格來達成時間敏感網路 (TSN) 的限制延遲 (Bounded Latency) 與可靠性等要求。

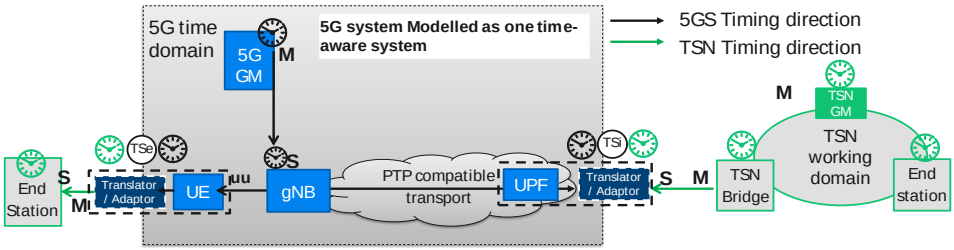


圖 16 時間敏感網路(TSN)的系統架構示意圖[4]

5G 系統可透過用戶平面功能 (UPF) 做為與時間敏感網路 (TSN) 整合的橋樑，並於用戶設備 (User Equipment, UE) 端和終端站 (End Station) 導入解讀通用精準時間協議 (generic Precision Time Protocol, gPTP) 協定的機制，以實現傳輸時域和同步訊號的協同工作。

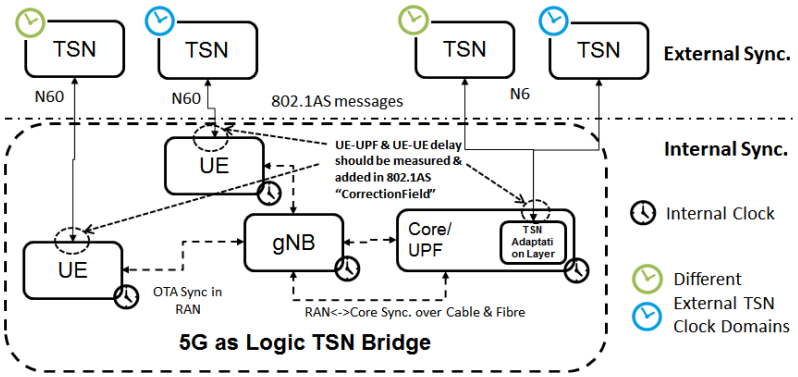


圖 17 並存多個時間敏感網路(TSN)的佈建情境 [4]

5.1.2.4 5G 區域網路型態服務

光纖固網傳輸通訊架構為智慧連網工廠的根基，工業 4.0 的控制級無線通訊對於即時性要求必須達到毫秒等級的超低延遲 (ultra low latency)以及 99.9999%之超高可靠度 (ultra high reliablity) 的水準，且抗干擾性和通訊安全性的要求等級也相對較高，透過固定網路與行動網路融合 (Fixed-Mobile Convergence, FMC) 技術標準規格，可以讓 5G 專網透過 3GPP TR 23.734 [4] 規範中的 5G 區域網路型態服務 (5G LAN-type service) 支援工廠所需超低延遲與超高可靠度的通訊服務。

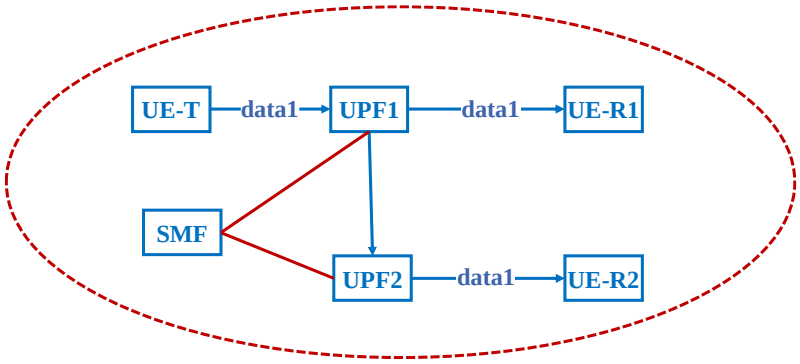


圖 18 5G 區域網路型態服務(5G LAN-type service)的情境 [4]

5.2 台灣廠商 5G 專網多接取邊緣運算平台

台灣廠商透過 5G 專網多接取邊緣運算平台實現虛擬實境(VR)、擴增實境(AR)、未來工廠、智慧醫療、智慧零售和無人駕駛等垂直領域應用服務領域，下列章節分別描述各家的特點。

5.2.1 英特爾的平台

Intel® Smart Edge 產品 (21) 基於開放網路邊緣服務軟體 (Open Network Edge Service Software, OpenNESS) 打造，是一個 5G 多接取邊緣運算 (MEC) 平台。英特爾 (Intel) 的開源軟體工具集開放網路邊緣服務軟體 (OpenNESS) (22)，讓開發者能透過應用程式介面 (Application Programming Interface, API) 來部署、管理、與自動化 5G 多接取邊緣運算的叢集與叢集上方的應用。要讓製造業、零售業、智慧城市和其他產業能夠輕鬆部署和管理專用無線網路應用環境，提供邊緣調度的框架搭配 OpenStack、Kubernetes 的功能，同時支援了歐洲電信標準協會 (ETSI) 的 5G 多接取邊緣運算以及以第三代合作夥伴計畫 (3GPP) 標準規格為基礎的 5G 佈建。並於 2019 年 17 日攜手鴻海科技、凌華科技、研華科技、威強電工業電腦、威聯通科技等台灣廠商搶先佈局工業電腦於 5G 多接取邊緣運算應用的商機 (23)。

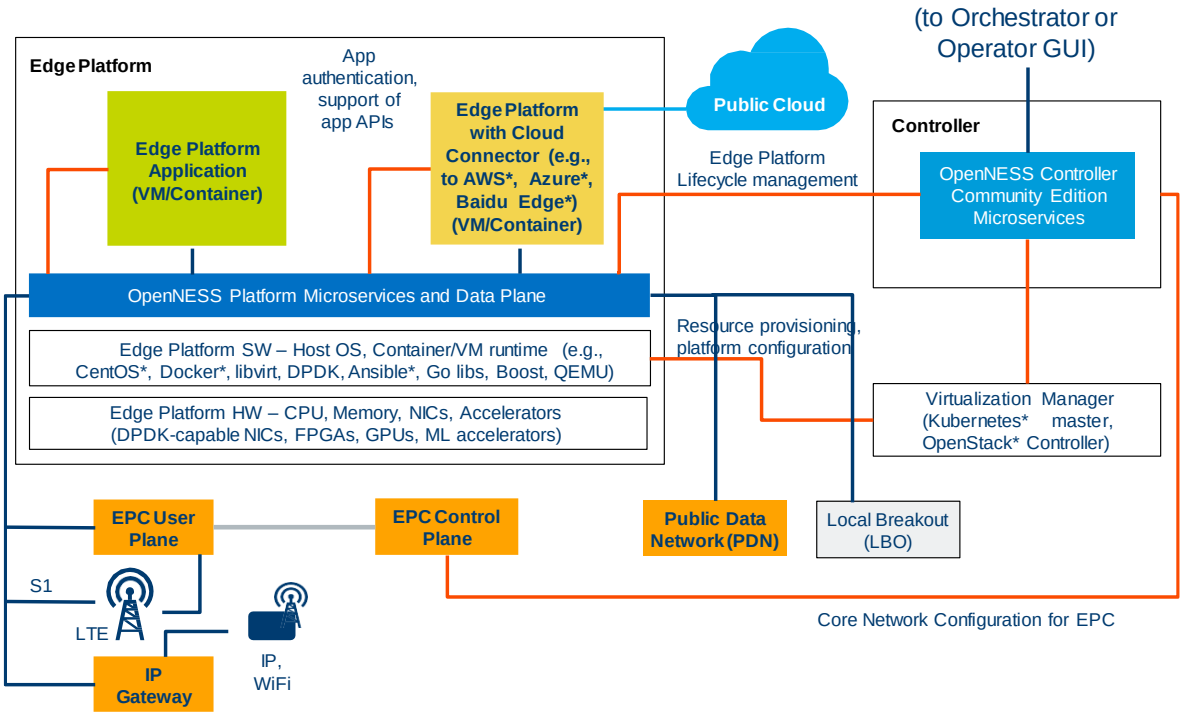


圖 19 英特爾 OpenNESS 的多接取邊緣運算平台架構圖 (22)

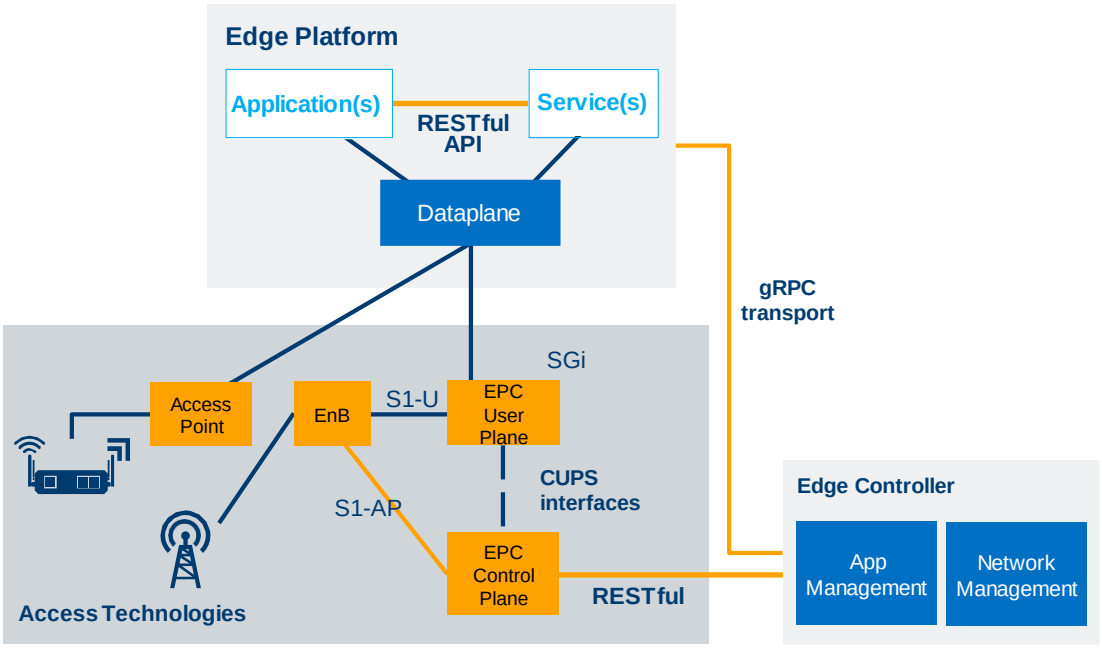


圖 20 英特爾 OpenNESS 的多接取邊緣運算網路架構圖 (22)

5.2.2 工研院的平台

工研院 5G 智慧型行動邊緣運算 (Intelligent Mobile Edge Computing, iMEC) 平台於行動網路邊緣與鄰近基地台的位置提供雲端運算能力以及應用服務的管理。5G 智慧型行動邊緣運算 (iMEC) 上的邊緣運算應用程式平台服務 (MEC APP Platform Services) 可以提供行動邊緣運算應用程式 (MEC APP) 的管理，包含上下架、生命週期與流量規則 (Traffic Rules) 等，邊緣運算應用程式 (MEC APP) 可佈建與運行於混合式的 (Network Function Virtualization, NFV) 平台上。

由於 5G 智慧型行動邊緣運算能滿足低延遲的需求、資料分析輔助與區域性關聯的各種服務，因此將原本需傳回雲端處理的資料，依照用戶設備 (UE) 的位置，提供使用者低延遲之視訊觀賞服務體驗。基於「TAICS 企業組網情境與架構研究報告」[1]，現有工研院的多接取邊緣運算佈署 iMEC 之系統架構與公網整合專網之情境，如下：

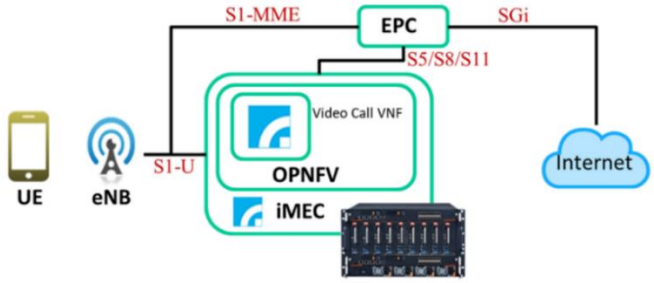


圖 21 iMEC 之系統架構圖 [1]

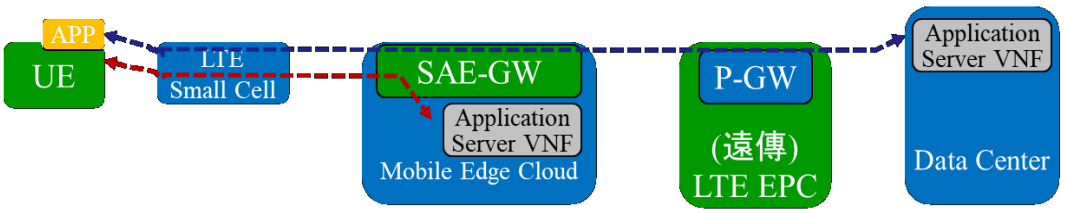


圖 22 iMEC 與公網整合專網之佈建情境 [1]

其用戶設備 (UE) 辨識解決方案 (24) 將企業認證機制與多接取邊緣運算整合，由智慧型行動邊緣運算 (iMEC) 提供身分認證的資料，並利用認證協定與企業認證、授權與計費 (Authentication, Authorization and Accounting, AAA) 伺服器進行認證，通過認

證的用戶即可取得授權。此方法用戶的認證行為仍保留在企業端，兼顧用戶及企業的安全性及隱私，並提供最低限度的資訊給多接取邊緣運算進行網路用戶及企業用戶的資訊比對，使智慧型行動邊緣運算 (iMEC) 可辨識出不同權限等級的用戶設備 (UE) 進行路由控制。

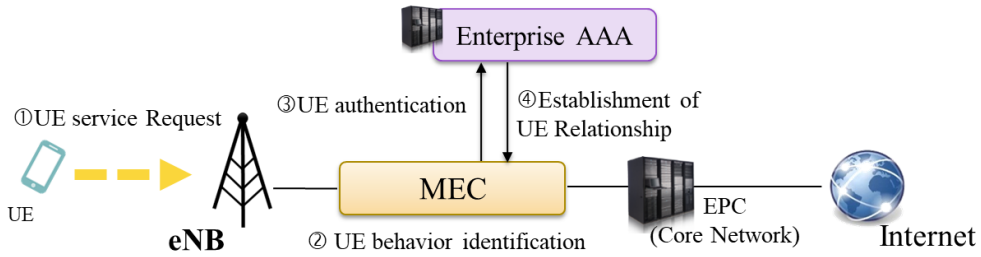


圖 23 用戶設備辨識解決方案 (24)

為了使用戶、企業及電信商達到彈性的多接取邊緣運算部署及私有服務存取機制，智慧型行動邊緣運算 (iMEC) 可部署在企業內部機房或是電信業者的機房，當企業欲使用電信網路存取私有服務時，除了將服務上架至多接取邊緣運算，尚須提供該服務的認證流程，並設定用戶認證後的相關權限及服務存取的路由至智慧型行動邊緣運算 (iMEC) 進行管理。

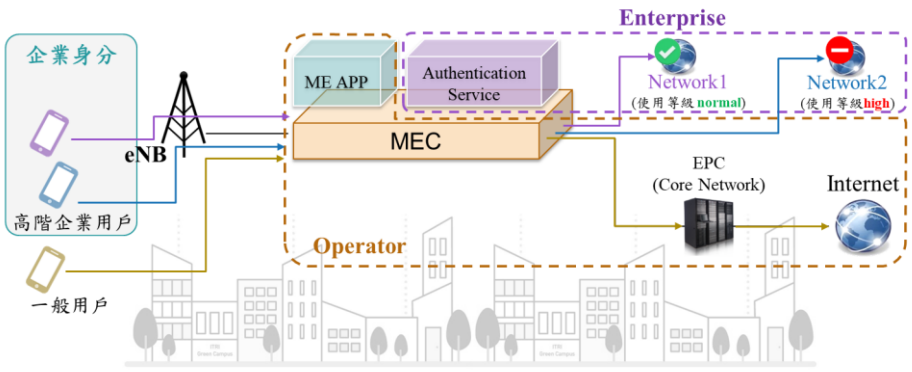


圖 24 不同身分別的用戶設備進行路由控制 (24)

5.2.3 鴻海科技的平台

鴻海積極開發應用於集團的 Local 5G 邊緣解決方案瞄準 5G 企業專網，鴻海集團針對智慧製造、5G 多接取邊緣運算 (Multi-access Edge Computing, MEC) 及高效能伺服器設備 (High-Performance Computing, HPC) 等領域尋求市場突破點，未來會陸續將 5G 垂直應用導入與落地。以智慧製造來說，鴻海 BEACON 平台將工廠中的機台每天所產生的數據蒐集起來，再去跟軟體結合、進而與市場資訊結合起來，希望達到實際上的產出如何與數據做結合、成為真正的智慧製造。自 2019 年 7 月起應用英特爾開放網路邊緣服務軟體 (OpenNESS) 來開發 5G 企業專網解決方案，而推出的 5G 企業專網解決方案，搭配的是通用型的硬體伺服器，企業可以將整套設備部署在 5G 基地臺附近，再透過應用程式介面 (Application Programming Interface, API) 執行人工智慧物聯網 (Artificial Intelligence (AI) and Internet of Things (IoT), AIoT) 的應用。

5.2.4 技嘉科技的平台

技嘉科技的伺服器作為 5G 多接取邊緣運算 (Multi-access Edge Computing, MEC) 平台的硬體基礎支援新一代 5G 應用 (25)，5G 多接取邊緣運算 (MEC) 結合了網路功能虛擬化 (NFV) 將行動數據回傳的頻寬需求降至最低，提供超低延遲的邊緣雲端平台，是降低建置基礎設施成本的理想方法，讓電信公司能夠成功地將 4G 網路轉換成支援 5G 網路。

該 5G 多接取邊緣運算 (MEC) 平台採用工研院的智慧型行動邊緣運算 (iMEC) 技術，可以同時支援 OpenStack 網路功能虛擬化 (OPNFV) 和 Kubernetes 網路功能虛擬化 (K8S NFV) 基礎架構解決方案，並為虛擬機器和容器應用程式服務提供統一的管理界面以易於應用端服務的快速部署。該平台提供動態路徑判斷，並支援指定無線存取點名稱 (Access Point Name, APN) 的流量卸載功能、使用者數據資料封包將直接傳送到網路功能虛擬化 (NFV) 的 5G 多接取邊緣運算 (MEC) 平台。

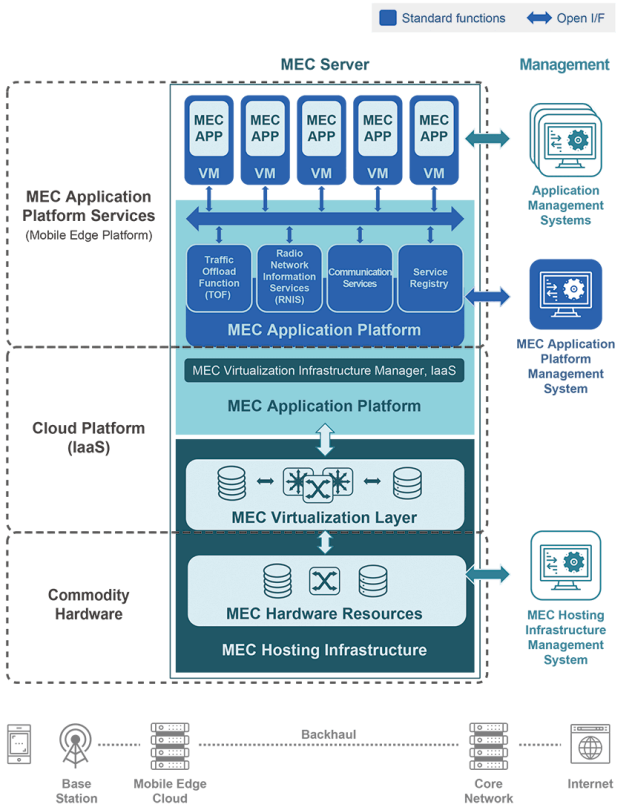


圖 25 技嘉科技的 5G 多接取邊緣運算平台 (25)

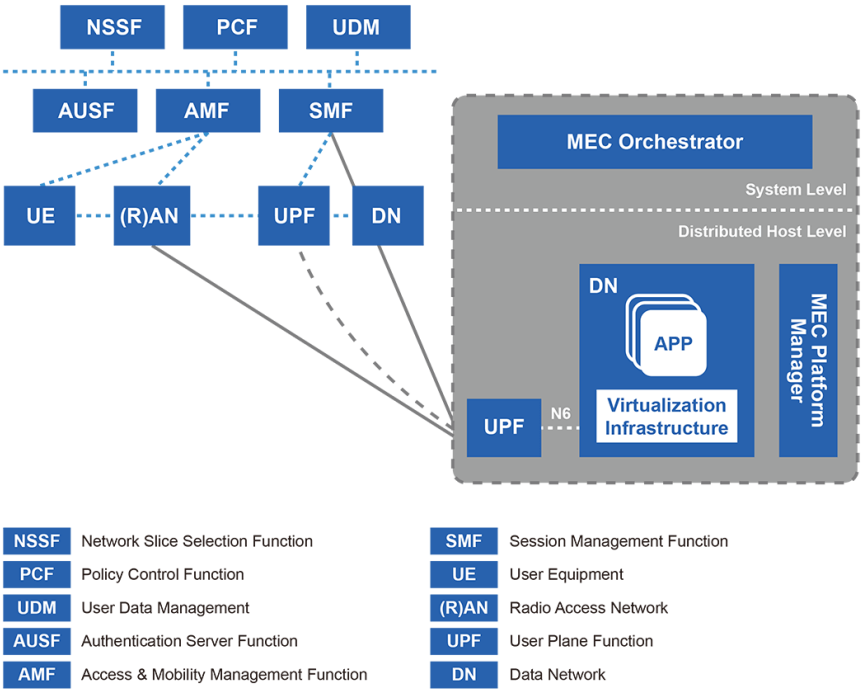


圖 26 技嘉科技的 5G 邊緣運算網路架構 (25)

5.2.5 凌華科技的平台

凌華科技的 OCCERA 平台 (26) 為集中式無線接取網 (Centralized/Cloud Radio Access Network, C-RAN) 提供高密度運算資源與更靈活的部署模式，除了提供更高的頻寬外，並且滿足嚴苛的戶外應用環境，以適合不同的運營環境。

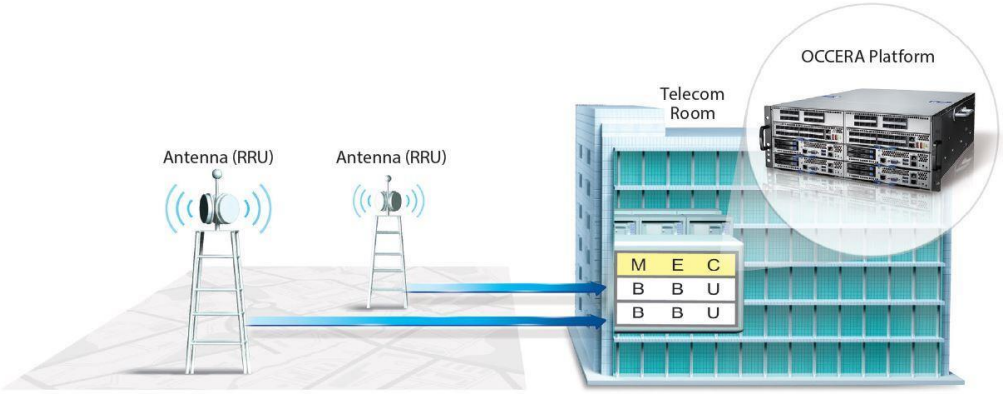


圖 27 凌華科技的 5G 多接取邊緣運算之應用情境 (26)

集中式無線接取網 (C-RAN) 的系統採用集中單元 (Centralized Unit, CU) 與分散單元 (Distributed Unit, DU) 分割的功能分離 (function split) 架構，由支援網路功能虛擬化 (Network Function Virtualization, NFV) 的通用處理器建構集中式的基頻處理池，基頻處理池中多個基頻處理單元之間通過支援軟體定義網路 (Software Defined Network, SDN) 的高頻寬交換器連接起來，結合網路功能虛擬化技術可以實現基頻資源池內的資源分享和動態調度。

5.2.6 研華科技的平台

研華科技藉由 4K/8K 核心技術、5G 多接取邊緣運算伺服器與虛擬化網路，提供虛擬實境 (VR)、擴增實境 (AR)、智慧醫療、智慧零售和無人駕駛等垂直領域應用服務領域，讓 5G 網路營運商從核心基礎架構到 5G 多接取邊緣運算 (MEC) 平台全面最佳化，其 5G 多接取邊緣運算技術以低延遲的超高解析度視訊處理平台，以更有效率運用行動邊緣和核心網路的頻寬，提升全新行動視訊基礎架構的壓縮效能。

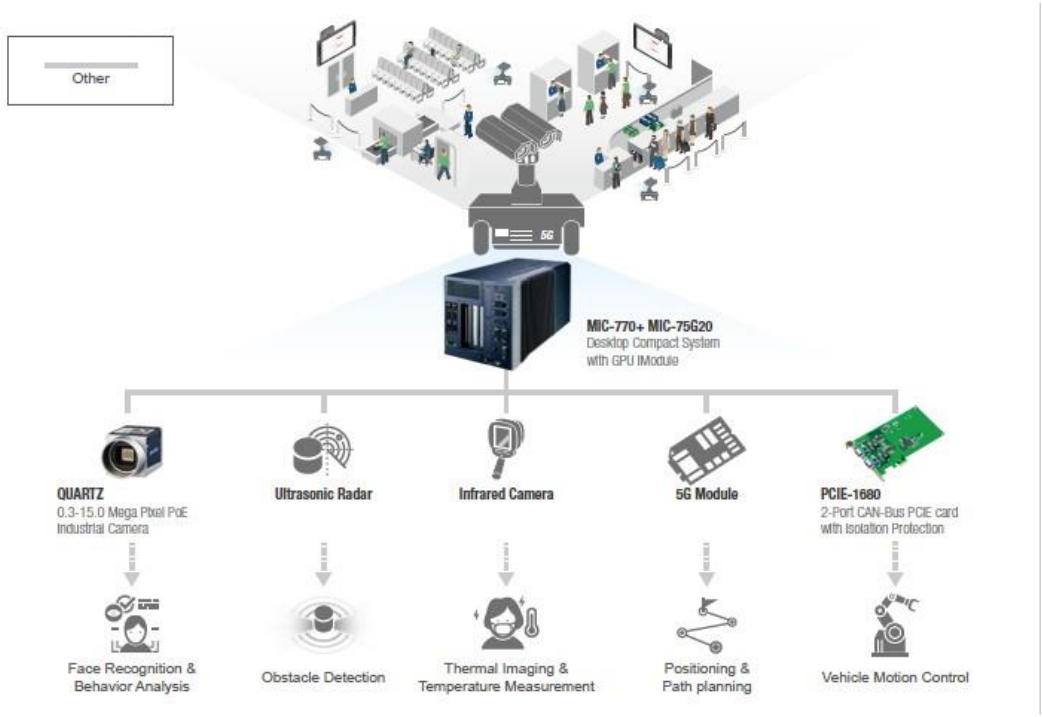


圖 28 研華科技的 5G 多接取邊緣運算之應用情境 (28)

6. 5G 專網多接取邊緣運算資安風險探討

5G 專網多接取邊緣運算 (Mobile Edge Computing, MEC) 為了實現低延遲率與高可靠度以及高傳輸速率的垂直領域應用服務，需將 5G 專網多接取邊緣運算與電信業者無線接取網路及核心網路的通訊設備緊密整合如圖 29 所示，所以探討 5G 專網多接取邊緣運算資安風險之前需要先了解 5G 資安的關鍵議題，故第 6.1 小節探討 5G 專網行動通訊系統的資安關鍵議題後，緊接著於第 5.2 小節與第 6.3 小節分別討論 5G 專網多接取邊緣運算的資安風險分析與安全解決方案。

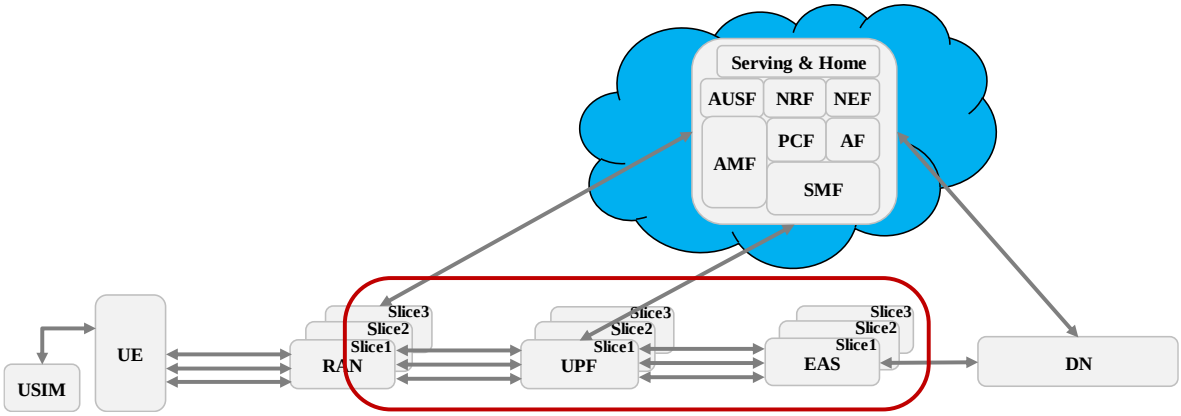


圖 29 5G 行動通訊系統架構

6.1 5G 行動通訊系統的資安關鍵議題

6.1.1 5G 資安國際發展趨勢

5G 世代的應用多元，各類新服務、新架構、新技術對安全和用戶隱私保護也都帶來新的挑戰。如何設計更完備的第五代行動通訊網路安全機制，且在維護基本通訊安全要求同時，還能夠因應不同應用場景以適應多種網路接取與新型網路架構，進而提供差異化安全服務、保護用戶隱私，將是標準制定者、技術設備與應用開發者的第一要務。然而不同的應用場景，所要對應的第五代行動通訊網路資安面向也不盡相同。有鑑於此，標準化機構如第三代合作夥伴計劃 (3GPP)、雲端安全聯盟 (Cloud Security

Alliance, CSA)、新世代行動網路聯盟 (Next Generation Mobile Network Alliance, NGMN Alliance)、網際網路工程小組 (The Internet Engineering Task Force, IETF)、歐洲電信標準協會 (ETSI)、第五代行動通訊基礎設施公私合作伙伴關係 (5G Infrastructure Public Private Partnership, 5G-PPP) 等已經開始研究第五代行動通訊網路資安相關問題。

表 1 探討 5G 資安的國際標準組織

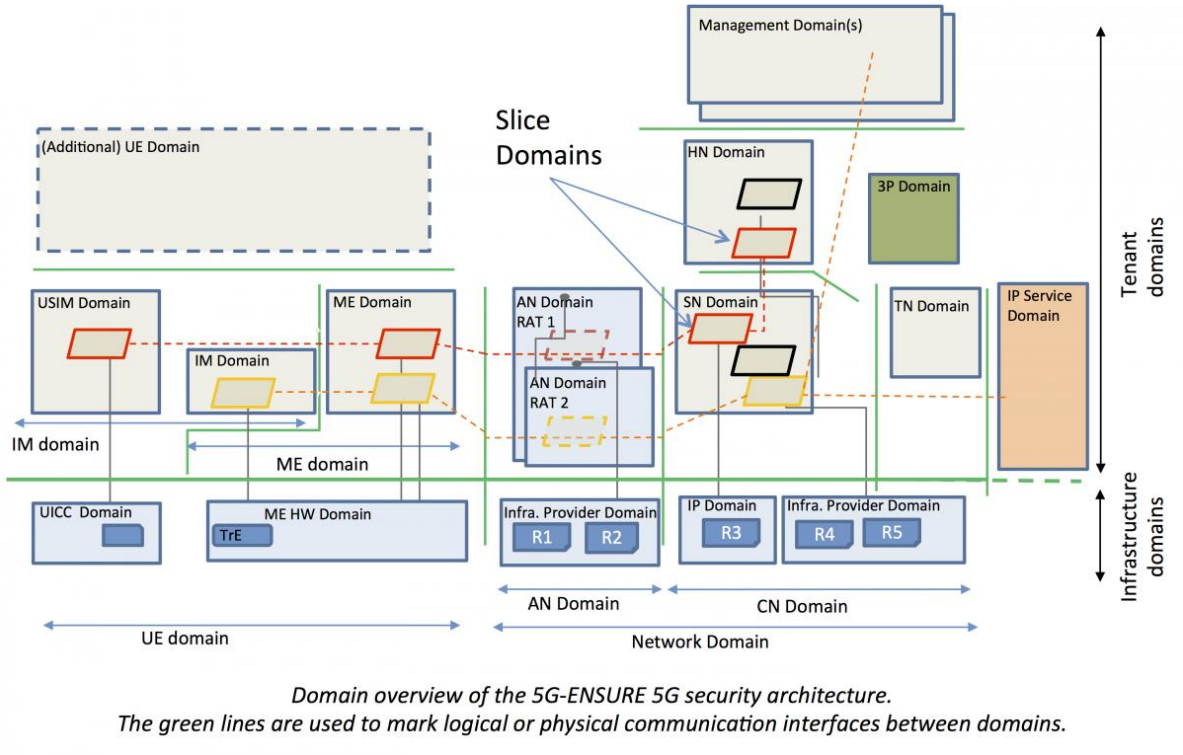
標準組織	工作組	主責安全議題	產出物
3GPP	Service and System Aspects (SA3)	Security architecture RAN security Authentication mechanism Subscriber privacy Network slicing	TR 33.899 Study on the security aspects of the next generation system TS 33.501: Security architecture and procedures for 5G system
5GPPP	5G Security WG	Security architecture Subscriber privacy Authentication mechanism	5G PPP Security Landscape (White Paper) June 2017.
IETF	I2NSF DICE WG ACE WG DetNet WG	Security solutions for massive IoT device in 5G User privacy Network security functions	RFC 8192 RFC 7744 Deterministic Networking (DetNet) Security Considerations
NGMN	NGMN 5G security group (NGMN P1 WS1 5G security group)	Subscriber privacy Network slicing MEC security	5G security recommendations: Package 1 and Package 2 5G security: Package 3
ETSI	ETSI TC CYBER ETSI NFV SEC WG	Security architecture, NFV security, MEC security, privacy	ETSI GS NFV-SEC 010 ETSI GS NFV-SEC 013 ETSI GS NFV-SEC 006 ETSI GS MEC 009

同時主要的設備供應大廠，也著手進行第五代行動通訊網路安全架構與相關技術的研發。例如強化設備終端與雲端連接的信任關係上，藉由對所有傳輸資料數據進行加密處理，並根據正在傳輸的資料價值，以智慧化的方式選擇各節點間的安全架構；或是針對物聯網的信令安全要求，透過多種協定組合方案作簡化管理，且藉由即時數據分析進行檢測與保護等方式。未來，大廠們也思考著將機器學習納入網路安全架構設計的一環，經由更先進的訊號監控機制，主動過濾且更為強大的分析功能，以確保第五代行動通訊網路安全不受侵犯，同時保護用戶隱私與資訊安全。

6.1.2 5G-PPP 發表的 5G 資安關鍵議題

第五代行動通訊公私合營聯盟基礎建設 (5G-PPP) 在 2017 年 6 月 12 日發表第五代行動通訊公私合營聯盟基礎建設第一階段安全白皮書 (29)，概述 5G 安全將面臨的風險與挑戰。針對新興 5G 關鍵安全風險與需求，諸如未經授權接取訪問或資產使用、弱切片 (weak slices) 隔離與連接、難以管理垂直服務層級協議 (Service Level Agreement, SLA) 與遵從規範、切片與中立性、信任管理複雜性等面向進行研究，並討論安全層級、安全自動化、安全管理與監控、啟用端對端 (end to end) 加密增值服務、5G 租戶 (inter-tenant)/切片隔離 (slice isolation) 等相關研究項目。

面對 5G 世代新型態的服務、網路架構與價值鏈，在營運商與服務商以及垂直產業間的網路更需要有新的信任模型，加上任務關鍵性的服務對於資訊安全威脅之考量。第五代行動通訊公私合營聯盟基礎建 (5G-PPP) 設對於 5G 安全架構提出了幾點設計原則，包含應打造一邏輯凌駕於實體的安全架構，設計一分布式、分級與遞迴的方法，藉由工業網路級的軟體定義網路 (Software Defined Network, SDN) 與網路功能虛擬化 (Network Function Virtualization, NFV) 支持內部與外部領域垂直產業服務商與營運商之間的協調，打造資安即服務 (Security-as-a-Service, SaaS) 概念之網路架構。同時，該網路架構必須能靈活且具擴展性、支持大規模與任務關鍵性物聯網服務，因此提出了更高級層級的安全架構設計概念，如下圖。



Domain overview of the 5G-ENSURE 5G security architecture.
The green lines are used to mark logical or physical communication interfaces between domains.

圖 30 各領域之 5G 安全架構 (29)

針對認證、授權與計費 (Authentication, Authorization and Accounting, AAA) 服務在 5G 安全相關技術發展中至關重要，至少必須做到在接取過程中，保護頻率與無線通訊資源之功能，並且能按需提供 5G 網路服務，遵守不同的約束規則。在 5G 未來在物聯網應用接取安全的需求上，輕量認證與密鑰協議群組相關技術的發展，將協助驗證未來在 5G 網路上持續增加的物聯網設備安全的重要解決方案之一。而基於團體的認證與密鑰協議群組則允許服務網路對一組設備進行認證，並降低家庭網路信令與通訊的延遲。面對 5G 隱私議題的利益相關者，如用戶、服務供應商、執法機關所需網路架構進行設計，潛在的推動力和未來的發展方向之需求也提供客製化設定。

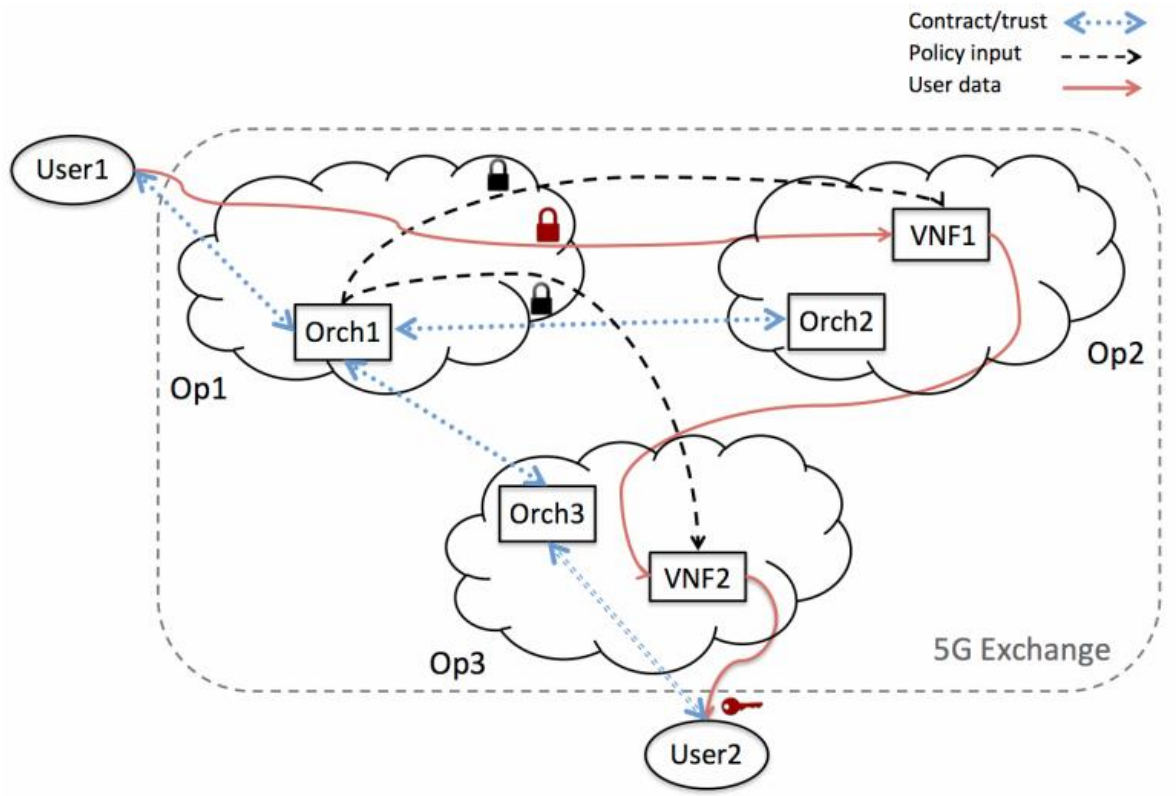


圖 31 多營運商服務鏈 (29)

5G 系統架構針對利益關係者發展信賴模型 (trust model)，該模型需要評估利益關係者在網路的可信度，並衡量利益關係者的網路與服務的安全能力，同時量化網路中利益關係者的行為，並透過利益關係者之間的互動降低風險或移除可能的弱點。針對網路實體特徵包含軟體定義網路 (SDN) 控制器、協調器、實體與虛擬網路功能等的信賴模型 (trust model)，主要是評估網路實體可信度，透過網路實體的使用機制衡量其安全能力等級，量化網路實體在網路中的行為，以及自主移除網路實體間運作互動產生的風險與漏洞。

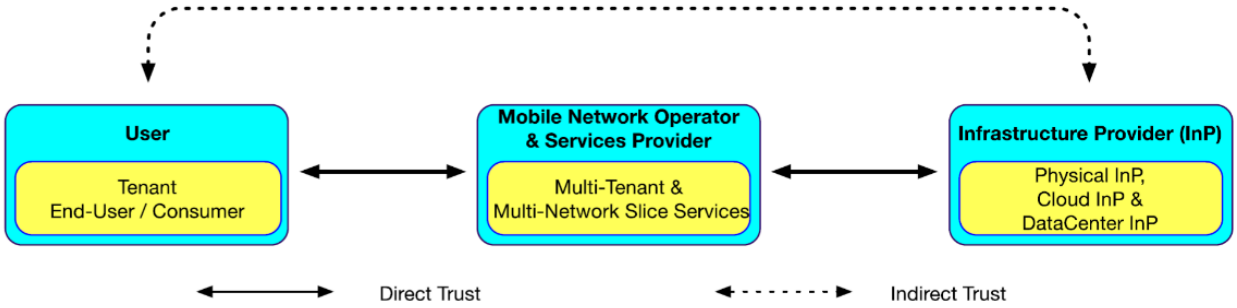


圖 32 5G 信賴模型 (29)

針對 5G 軟體定義網路 (SDN) 與網路功能虛擬化 (NFV) 等通訊關鍵基礎建設的新型態安全風險需要持續被監控與管理。尤其在軟體定義網路 (SDN) 與網路功能虛擬化 (NFV) 環境中將會帶來額外的安全風險，如數據偽造、應用程式介面 (API) 的濫用等。因此控制器與管理開發需要有更適當的機制，諸如強化認證、訪問控制、應用程式隔離與沙盒，串流完整性與衝突解決方案，以及加密介面等。

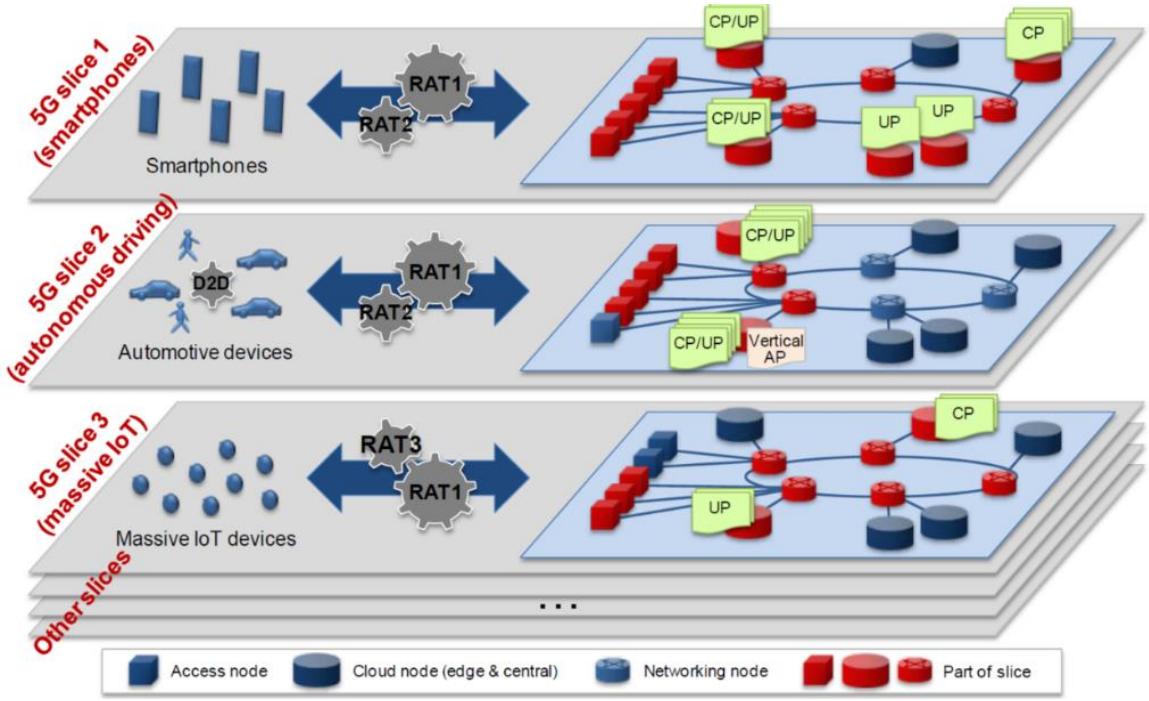


圖 33 5G 切片模型 (29)

此外，包含異質網路設備與多元化的服務將對行動網路帶來極大的安全性挑戰，而網路切片 (network slicing) 面臨的安全問題在於對不同網路切片應有隔離機制，以防止各網路切片 (network slicing) 內的資源被其他類型的網路切片 (network slicing) 非法存取，即便是同一應用領域的網路切片之間也有隔離的需求。因此第五代行動通訊公私合營聯盟基礎建設 (5G-PPP) 從各切片層級，含無線接取網路的切片 (RAN network slicing)、核心網路的切片 (core slicing)、應用級的切片 (application-level slicing) 的安全性需求進行研究，最後期望 5G 安全能形成統一標準。

6.1.3 台灣 TTC 發表的 5G 資安關鍵議題

依據財團法人電信技術中心 (TTC) 發表的「5G 釋照之先期資通安全法規整備計畫」(30)，除了新增加 5G 多接取邊緣運算 (MEC) 以外將 5G 網路系統的威脅分為無線電接取網路、傳輸網路與核心網路等三部分來敘述如圖 29 與表 2 所示。

表 2 5G 系統的威脅 (30)

類別	威脅種類	內容簡述
無線電接取網路	實體層攻擊	5G 將大量引入並安裝更便宜的小型基地臺。這些安裝在公共場所的基地臺較容易遭受物理破壞，並允許攻擊者實體接觸基地臺的網路介面。
	用戶隱私資料竊聽與阻斷服務攻擊	國際行動用戶識別碼擷取器 (IMSI-Catcher)的出現，導致用戶隱私被攔截、竊聽的威脅。攻擊者可能利用用戶設備在開始接入基地臺過程中，通過中間人攻擊來偽裝用戶，竊取客戶流量或發起阻斷服務攻擊。
	惡意基地臺	攻擊者可以試圖將惡意基地臺引入網路，模擬電信業者的節點，並攔截來自用戶設備的語音和數據傳輸，達到竊聽或重新導向用戶到不同的網路。
	數據完整性攻擊	在 4G 網路中，用戶平面之數據傳輸，並沒有完整性保護機制。控制平面的數據也缺乏完整性與不可否認性的安全保護。
	空中介面威脅	空中介面之安全性仰賴於位元層級之串流加密法，倘若密鑰長度及加密演算法強度不足將導致竊聽、中間人攻擊等可能性。
傳輸網路	傳輸網路竊聽	目前 LTE 基地臺架構中，從空中介面解密後，到核心網路之前的鏈路傳輸並無採取任何加密保護措施。針對 5G 基地臺開放式網路將會開啟 IPsec 功能進行防護，並新增 DTLS 以提升用戶隱私性保護強度。
	阻斷服務攻擊	由於 5G 時代物聯網設備將呈現指數型成長，而且較一般終端設備更容易被植入惡意程式或遭駭客入侵；數以百萬計的僵屍

		設備將用來發動阻斷式巨大流量攻擊，讓網路效能與可用性大幅下降，甚至造成服務無法運作。
	數據完整性攻擊	現行 LTE 傳輸網路從空中介面解密後到核心網路間並無任何加密保護機制要求，並使用既有老舊的互聯傳輸標準，容易遭受惡意人士竄改攻擊，竊取其個人資料與權限。
核心網路	IP 多媒體子系統威脅 (IMS)	未經授權的接取：IMS 的開放和分布式架構產生了眾多必須保護的節點，通常位於半可信區域，這可能使 IMS 核心易受攻擊。服務濫用與盜竊服務：攻擊者可通過受感染的 UE 接取 IMS，導致攻擊者繼續保持與媒體流的連接時系統不會計費。網路竊聽與會話脅持：攻擊者攔截 SIP 會話中兩個用戶之間的數據傳輸，劫持並插入惡意數據包，替換流量和破壞完整性，影響 QoS。
	5G 功能暴露	5G 將其核心網路驗證功能與無線電接取網路之連線功能向外暴露給垂直應用業者，攻擊者可利用旁通道攻擊，攻擊存在同一實體資源的用戶。
	竊取用戶身份	5G 中提供輔助身份驗證功能，當此身分驗證機制遭受攻擊，除可取得用戶行動數據外，還可竊取其個人的資料與權限，甚至金錢。由 SS7 或 Diameter 所引起一系列安全問題已經獲得監理機關與各大電信業者的關注。鑑於 5G 系統也需與舊系統保持互通，故依然會引入上述安全議題。

6.2 5G 專網多接取邊緣運算的資安風險分析

本節將以歐洲電信標準協會 (ETSI) 與以第三代合作夥伴計畫 (3GPP) 標準規範為主探討 5G 專網多接取邊緣運算的資安風險分析。從其 5G 專網多接取邊緣運算平台與 5G 專網多接取邊緣運算網路架構可以歸納出八大類安全面向的威脅，分別為 5G 核心網路元件的安全威脅、5G 基地臺集中單元的安全威脅、傳輸網路的安全威脅、以服務基礎架構為導向之專網架構的安全威脅、5G 專網垂直應用的安全威脅、平台與網路虛擬層的安全威脅、平台架構的安全威脅以及應用服務的安全威脅。於第 6.2.1 小節先討論「5G 專網多接取邊緣運算平台」的威脅分析，緊接著於第 6.2.2 小節與第 6.2.3 小節討論「獨立佈建 5G 多接取邊緣運算網路架構」以及「與公網整合 5G 專網多接取邊緣運算網路架構」兩種佈署型態的威脅分析，針對 5G 專網多接取邊緣運算平台與網路功能虛擬化的威脅分析列於第 6.2.4 小節，最後於第 5.2.5 小節探討 5G 專網多接取邊緣運算多元應用情境的資安風險分析。

6.2.1 5G 專網多接取邊緣運算平台的威脅分析

依據圖 1 所示的 5G 專網多接取邊緣運算平台，可以歸納出的威脅分析如圖 34 所示，涵蓋平台與網路虛擬層的安全威脅、平台架構的安全威脅與應用服務的安全威脅。

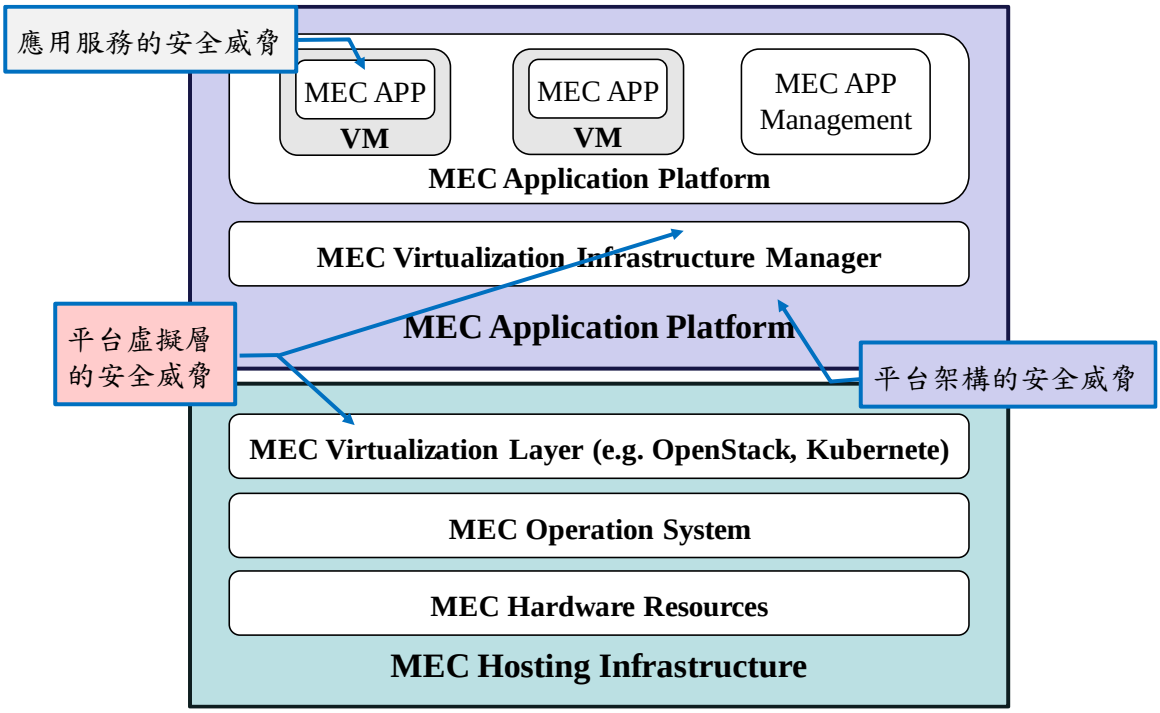


圖 34 5G 多接取邊緣運算平台的威脅分析

依據「5G 釋照之先期資通安全法規整備計畫」(30)提出的 5G 多接取邊緣運算(MEC)威脅分析如表 3 所示。

表 3 5G 多接取邊緣運算威脅分析 (30)

威脅種類	內容簡述
多接取邊緣運算本身威脅	系統結構方面，多接取邊緣運算節點更貼近用戶，更容易受到物理層面攻擊。服務提供方面，受託管多個第三方邊緣計算應用程序需要在不同程序間、以及網路元件間進行良好隔離。營運模式方面，需要長期累積多接取邊緣運算平臺和第三方應用管理和營運經驗，才能建立完整有效的防禦機制。
針對多接取邊緣運算租用戶之雲端應用層的攻擊	多接取邊緣運算可能需要連結外部雲端網路，不直接由電信業者控制，存在耗盡網路資源的風險。可能因應用程序缺陷導致遭受攻擊或被駭客入侵，甚至埋入惡意應用程式。
多接取邊緣運算部署帶來的計費風險	多接取邊緣運算中大量數據直接在用戶設備和網路邊緣流動，遠比核心更容易受到攻擊，可能產生帳單錯誤、帳單欺詐、計費不足等風險。
與網路功能在同一平臺上的第三方應用程式	隨 5G NFV 引入，多接取邊緣運算可能將邊緣計算應用程式與網路元件結合於相同平臺，存在獨佔網路資源的風險外，還可能因應用程式設計不當、被惡意程式滲透操控。
允許第三方應用程式影響網路	一些不良應用程式可能會搶奪無線資源，導致其他用戶的體驗嚴重降低或遭受拒絕服務。
多重接取邊緣計算環境中的用戶平面攻擊	網路邊緣服務伺服器使用 HTTP/HTTP 協定，存在既有弱點，除伺服器和暫存的傳統攻擊外，針對內容暫存的新型攻擊(暫存中毒攻擊)也將可能發生，
在邊緣儲存的敏感性資產或資料	儲存在邊緣計算的虛擬化主機的敏感性資產或資料較容易遭到偷竊或損害。
核心和多重接取邊緣運算平臺間的敏感性資料交換	如果在交換敏感性資料時遭受到入侵或攻擊，則攻擊者可能連接核心網路進行欺騙， 竊聽或數據操縱等攻擊。
與多接取邊緣運算協調器進行通信的安全性	邊緣計算網路的物理連接常發生在良好防護機房之外，因此實體或邏輯鏈路很容易受到侵入或破壞。
多接取邊緣運算部署的通信監察要求	在多接取邊緣運算的網路邊緣周圍放置多個合法監聽 (Lawful Interception, LI) 節點，將帶來更多的安全風險，更容易受到攻擊而失效。

6.2.2 獨立佈建多接取邊緣運算網路架構的資安風險分析

獨立佈建多接取邊緣運算網路架構運作獨立，可申請使用專網頻譜執照，不受公共網路壅塞影響，故能確保感測設備聯網的通訊品質，保障物聯網應用的可靠性，且專網與公共網路實體隔離，避免組織機敏資料外流，其架構的威脅分析如圖 35 所示。當存取網路 (Access Network, AN)採用 5G 基地臺集中單元與分散單元分離的架構情境下時 (如圖 35 中紅色虛線框部分)，3GPP TS 33.501 (31) 的安全標準規範要求考量 5G 基地臺集中單元 (gNB-CU) 與 5G 基地臺分散單元 (gNB-DU) 間 F1 介面的連線安全。

當 5G 基地臺集中單元 (gNB-CU) 進一步導入之控制平面與用戶平面分離架構後，需要進一步 5G 考量基地臺集中單元-控制平面 (gNB-CU-CP) 與 5G 基地臺集中單元-用戶平面 (gNB-CU-UP) 間 E1 介面的連線安全。

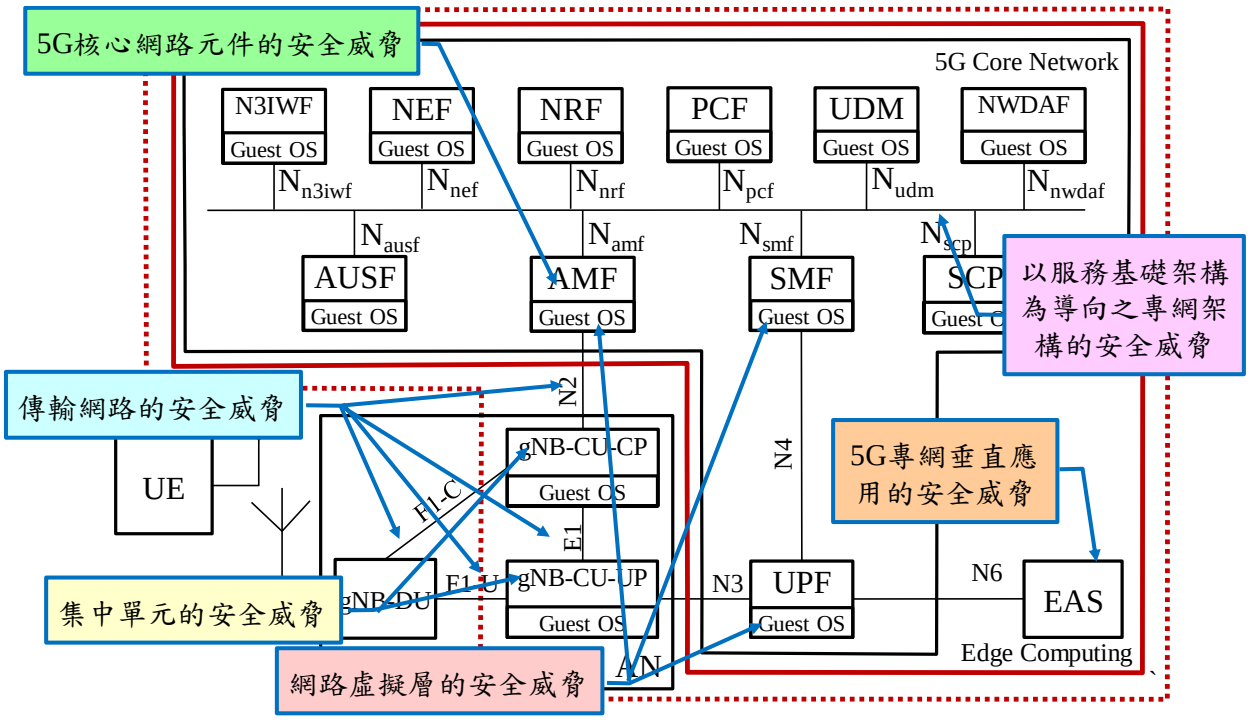


圖 35 獨立佈建多接取邊緣運算網路架構的威脅分析

5G 獨立佈建多接取邊緣運算標準架構的核心網路採用以服務基礎架構為導向 (Service-Based Architecture, SBA) (6)，基於雲端原生 (Cloud Native) 的「微服務架構 (Micro-services)」構架來設計行動網路的主要功能，同時導入軟體開發人員 (Development, Dev)」和「資訊科技維運技術人員 (Operations, Ops)」間溝通合作的 DevOps 機制 (32)，以實現彈性交付、重複性和可靠性。核心網路透過控制平面 (Control Plane) 與使用者平面 (User Plane) 分離，可以為網路功能虛擬化 (Network Function Virtualization, NFV) 及 5G 多接取邊緣運算 (Multi-access Edge Computing, MEC) 提供較為完善的網路架構，其中 5G 網路功能虛擬化的威脅分析列於第 6.2.4 小節。

然而，以服務基礎架構為導向 (SBA) 的核心網路衍生了新的資安問題，而第五代行動通訊公私合營聯盟基礎建設 (5G-PPP) 安全工作組在 5G 安全標準化上的貢獻，主要有四個面向：(1) 影響 5G 包含無線接取、核心網、應用服務等各方面的安全要求發

展；(2) 透過識別 5G 所需要的安全功能與機制，設定基於一致性技術和程序的最小安全基準；(3) 提供基於安全基準的安全架構設計；(4) 增加可根據特定服務或應用稽核的安全功能。為了確保 5G 以服務基礎之架構 (SBA) 不受網路攻擊威脅以及用戶隱私保障上有所保障，第三代合作夥伴計畫 (3GPP) 訂定 3GPP TR 33.855 (33) 之技術研究報告提出安全威脅如表 4。

表 4 以服務基礎架構為導向 (SBA) 的安全威脅

關鍵議題[1]	議題標題	安全威脅
1	傳訊資訊的機密性保護	- 洩漏行動通訊用戶的敏感資訊，如 SUPI 或位置。 - 洩漏有關陸地行動通信網路(PLMN)本身的潛在敏感資訊。 - 盜竊未經加密傳輸之身份驗證資訊/授權憑據的用戶服務。
2	允許修改之傳訊資訊的完整性保護	- 主動修改網路功能(NF)間傳訊訊息的中間人(MitM)攻擊。 - 傳輸過程中未察覺篡改資訊，導致格式錯誤而不能使用。 - 對電信由運商的盜竊與欺詐。
3	傳訊資訊重送保護	- 盜用服務。 - 洩漏行動通訊用戶和網路本身的潛在敏感資訊。 - 重播授權憑證後將喪失控制權。
4	網路功能(NF)間認證	- 惡意網路功能(NF)向合法網路功能(NF)請求某些服務或資訊，導致盜用服務或數據洩漏。 - 對一個陸地行動通信網路(PLMN)的合法網路功能(NF)間進行中間人(MitM)攻擊。
5	網路功能(NF)間授權	- 成功向網路功能(NF)獲取被禁止的第三方服務，如藉以獲得網路的潛在敏感資訊。 - 透過強制網路功能(NF)進行資源請求，導致阻斷服務。
6	網路功能(NF)與網路資料庫功能(NRF)間認證	- 對一個陸地行動通信網路(PLMN)的合法網路功能(NF)與合法網路資料庫功能(NRF)間，進行中間人(MitM)攻擊。 - 將一個惡意網路功能(NF)註冊到一個陸地行動通信網路(PLMN)的合法網路資料庫功能(NRF)。 - 誘導合法網路功能(NF)註冊到一惡意的網路資料庫功能(NRF)而不是一個陸地行動通信網路(PLMN)的合法網路資料庫功能(NRF)。
7	網路功能(NF)與網路資料庫功能(NRF)間授權	- 從受到攻擊者控制的惡意網路功能(NF)發送註冊請求 - 向網路功能(NF)請求被禁止的第三方服務，藉以獲得有關陸地行動通信網路(PLMN)的機密資訊 - 大量向網路資料庫功能(NRF)請求資源，導致阻斷服務
8	網路資料庫功能(NRF)間認	- 對本地網路資料庫功能(NRF)與漫遊夥伴的合法網路資料庫功能(NRF)間，進行中間人攻擊。

	證	- 向從網路資料庫功能(NRF)查詢網際網路協定(IP)位置資訊，導致洩漏有關陸地行動通信網路(PLMN)的機密數據。
9	網路資料庫功能(NRF)間授權	- 從受到攻擊者控制的惡意網路資料庫功能(NRF)發送探索請求。 - 向網路資料庫功能(NRF)請求被禁止的第三方服務，如藉以獲得有關陸地行動通信網路(PLMN)的機密資訊。
20	服務通訊代理(SeCoP)介面防護	- 服務通訊代理(SeCoP) 若未經授權訪問，可能導致欺騙攻擊、盜用服務以及服務通訊代理(SeCoP)與網路功能(NF)或網路資料庫功能(NRF)間的中間人(MitM)攻擊。 - 缺乏機密性保護可能會導致洩漏敏感資訊。 - 缺乏完整性保護可能會導致傳輸資訊遭受未察覺的篡改。 - 缺乏重播保護可能會導致如盜用服務、洩漏敏感資訊或喪失控制權等負面影響。
21	透過服務通訊代理(SeCoP)傳送安性資訊	- 服務通訊代理(SeCoP)若缺乏機密性保護可能會導致洩漏敏感資訊。 - 服務通訊代理(SeCoP)若缺乏完整性保護可能會導致傳輸資訊遭受未察覺的篡改。 - 服務通訊代理(SeCoP)若缺乏重播保護可能會導致如盜用服務、洩漏敏感資訊或喪失控制權等負面影響。
22	間接通信的網路功能(NF)服務訪問授權	- 不適用 (Not applicable)
23	間接通信的網路功能(NF)間認證與授權	- 惡意網路功能(NF)獲得某些服務或資訊，導致盜用服務或數據洩漏。 - 對一個陸地行動通信網路(PLMN)與任意合法網路功能(NF)間的，進行中間人(MitM)攻擊。
24	基於網路功能集(NF Set)的服務訪問授權	- 從網路功能(NF)實體或網路功能(NF)服務實體獲取有關網路服務的敏感資訊。 - 透過在網路功能(NF)上執行資源請求來達成阻斷服務攻擊。
25	漫遊情境下的間接通信	- 不適用 (Not applicable)
26	N9 介面防護	- 缺乏對陸地行動通信網路(PLMN)間 N9 介面的用戶流量保護，將導致洩漏敏感資訊和未經授權修改資訊。
27	支援 N9 介面的用戶平面閘道器	- 不適用 (Not applicable)
28	委派訂閱通知情境的服務訪問授權	- 如果針對委派訂閱通知(delegated subscribe-notify)情境沒有特定授權機制，任一網路功能可以在未經授權的情下代表其他網路功能進行訂閱服務。
29	網路功能(NF)用戶的資源級	- 向網路功能(NF)請求被禁止的第三方服務，藉以獲得有網路的敏感資訊。

	別授權	- 透過在網路功能(NF)上執行資源請求來達成阻斷服務攻擊。
30	未委派訂閱通知情境的服務訪問授權	- 如果針對未委派訂閱通知(non-delegated subscribe-notify)情境沒有特定授權機制，任一網路功能可以在未經授權的情下代表其他網路功能進行訂閱服務，導致阻斷服務攻擊。

註 1: 3GPP TR 33.855 之關鍵議題 (Key Issue) 編號

此外，依據 3GPP TR 33.819 [6] 之技術研究報告，獨立佈建專網 (SNPN) 還需要解決下列的安全威脅。

表 5 獨立佈建專網的安全威脅

關鍵議題 [1]	議題標題	安全威脅
1.1	獨立佈建專網的 AKA 驗證安全機制	- 如果對多個獨立佈建專網使用相同的憑證，則用戶設備可能會嘗試連接到其他的獨立佈建專網。 - 當用戶設備嘗試連接到公網時可能會連接到獨立佈建專網。
5.1	專網的金鑰階層	- 密鑰層次結構應支持除了 EAP-AKA'以外的 EAP 身份驗證安全機制。
5.2	專網用戶的認證和授權	- 文件無安全威脅描述

註 1: 3GPP TR 33.819 之關鍵議題 (Key Issue) 編號

5G 行動通訊系統導入 5G 基地臺集中單元與分散單元分離的網路架構，該架構進一步將 5G 基地臺 (gNB) 分割為 5G 基地臺集中單元 (gNB-CU) 與 5G 基地臺分散單元 (gNB-DU)。由於 5G 基地臺集中單元 (gNB-CU) 的分封數據匯聚協定 (PDCP) 網路功能負責執行用戶平面 (user plane) 和控制平面(control plane) 封包的完整性 (integrity) 和機密性 (confidentiality)，故 5G 基地臺分散單元 (gNB-DU)不會涉及到用戶設備 (UE) 的完整性和機密性 (27)，但當其遭受攻擊時仍然會影響 5G 行動通訊網路用戶設備 (UE) 的可用性 (availability)。

6.2.3 與公網整合多接取邊緣運算網路架構資安風險分析

5G 在制定技術規格時讓網路組建方式有許多彈性，因此建議可採用與公網整合專網 (PNiNPN) 之獨立多接取邊緣運算 (MEC)、與公網共享多接取邊緣運算以及透過公

網做虛擬專網網路切片 (Network Slicing) 等三種 5G 專網建置，透過企業與電信業者合作使建置成本更為低廉，其架構的的威脅分析如圖 36 所示。當存取網路 (AN) 採用 5G 基地臺集中單元與分散單元分離的架構情境下時 (如圖 36 中紅色虛線框部分)，3GPP TS 33.501 (31) 的安全標準規範要求考量 5G 基地臺集中單元 (gNB-CU) 與 5G 基地臺分散單元 (gNB-DU) 間 F1 介面的連線安全。當 5G 基地臺集中單元 (gNB-CU) 進一步導入之控制平面與用戶平面分離架構後，需要進一步 5G 考量基地臺集中單元-控制平面 (gNB-CU-CP) 與 5G 基地臺集中單元-用戶平面 (gNB-CU-UP) 間 E1 介面的連線安全。

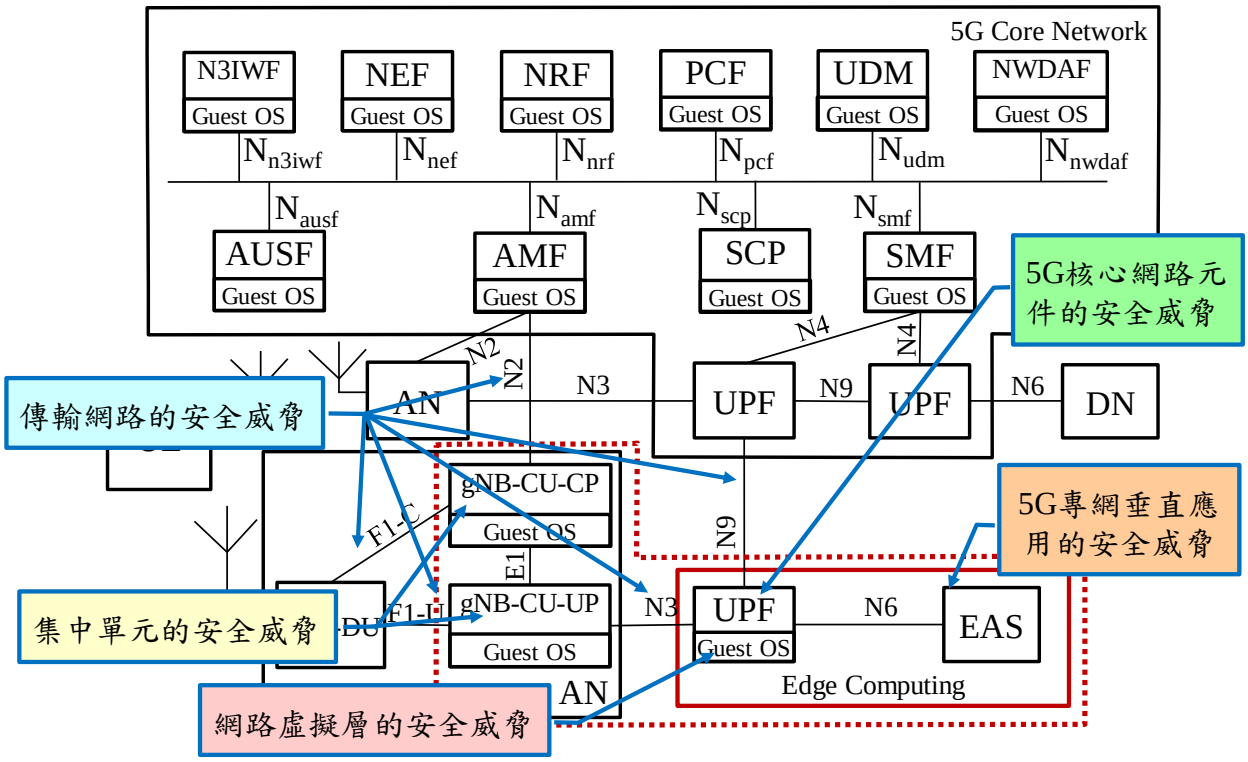


圖 36 與公網整合多接取邊緣運算網路架構的威脅分析

依據 3GPP TS 23.501 (6) 之技術標準規格，核心網路由多個「網路功能服務」的模組構成，並通過「以服務為基礎之介面」來實現網路功能 (Network Function, NF) 。其中網路資料庫功能 (Network Function Repository Function, NRF) 支持網路功能 (NF) 服務註冊與狀態監測等機制，以實現網路功能 (NF) 服務自動化管理。並透過控制平面與使用者平面分離，可以為網路功能虛擬化 (NFV) 及 5G 多接取邊緣運算 (MEC) 提供較為完善的網路架構，其中 5G 網路功能虛擬化的威脅分析列於第 6.2.4 小節。

依據 3GPP TR 33.819 [6] 之技術研究報告，與公網整合專網 (PNiNPN)需要解決下列的安全威脅。

表 6 與公網整合專網的安全威脅

關鍵議題 [1]	議題標題	安全威脅
6.1	透過對閉架式群組(CAG)進行大量註冊請求之阻斷服務(DoS)/分散式阻斷服務(DDoS)攻擊攻擊	- 與公網整合專網(PNiNPN)應該提供一種用戶設備(UE)存取閉架式群組(CAG)的驗證機制。 - 當大量惡意 UE 向閉架式群組(CAG)進行網路註冊程序時，會導致 5G 系統核心網路(如統一資料數據功能管理 (Unified Data Management, UDM))遭受阻斷服務(DoS)/分散式阻斷服務(DDoS)攻擊。
6.2	閉架式群組(CAG)識別碼隱私性	- 竊聽者可以透過擷取閉架式群組(CAG)的廣播訊息，獲得提供關鍵基礎設施服務的用戶設備(UE)識別碼清單。 - 當用戶設備(UE) 進行網路註冊程序時，其閉架式群組(CAG)識別碼以明文發送，會來識別碼隱私性的安全威脅，例如竊聽者可以擷取執法機構(Law Enforcement Agency, LEA)專用閉架式群組(CAG) 的用戶設備(UE)識別碼。
6.3	未經授權刪除用戶設備的閉架式群組(CAG)允許清單之阻斷服務(DoS)攻擊	- 當用戶設備(UE)的註冊拒絕(Registration Reject)訊息未被保護時，攻擊者可以嘗試向用戶設備(UE)發送註冊拒絕訊息，來刪除用戶設備的閉架式群組(CAG)允許清單。導致用戶設備(UE)無法存取特定的閉架式群組(CAG)網路，當用戶設備(UE)的閉架式群組(CAG)允許清單被全數刪除後，將導致用戶設備(UE)遭受永久性的阻斷服務(DoS)。
2.1	專網和公網間交互工作、漫遊的驗證和授權	- 用戶設備未經過授權透過陸地行動通信網路(PLMN)存取專網(NPN)。 - 用戶設備未經過授權透過專網(NPN)存取陸地行動通信網路(PLMN)。
2.2	服務持續性和會談持續性的安全性和隱私性方面	- 現有 3GPP 標準文件已經解決該安全議題
2.3	專網和公網使用獨立憑證進行驗證和授權	- 陸地行動通信網路(PLMN)和專網(NPN)應該提供相互認證機制以確保僅提供授權用戶設備網路服務。如果陸地行動通信網路(PLMN)和專網(NPN)共用相同安全憑證，當安全憑證洩露可能導致共用相同安全憑證的所有網路都受害。

註 1: 3GPP TR 33.819 之關鍵議題 (Key Issue) 編號

6.2.4 網路功能虛擬化的威脅分析

5G 專網多接取邊緣運算平台支援第三代合作夥伴計畫 (3GPP) 的 5G 專網多接取邊緣運算網路虛擬化架構，故也為帶來新的資安挑戰。依據 3GPP TR 33.848 (34) 之技術研究報告，網路功能虛擬化需要解決下列的安全威脅。

表 7 網路功能虛擬化的安全威脅

關鍵議題 [1]	議題標題	安全威脅
1	建立網路功能的信賴區域	- 如果將具有不同安全等級的虛擬網路功能 (VNF) 放在同一個信賴區域 (trust domain) 中，則會因為對高信賴區域 (high trust domain) 訪問的安全性不足，而增加對高信賴關鍵安全功能的攻擊面。 - 權限較低的管理員或用戶可能可以入侵超出其權限級別的 3GPP 網路功能。 - 用戶或管理員可能會透過一個信賴區域 (trust domain) 入侵另一個信任域。
2	敏感資料的機密性	- 如果沒有適當的保護，攻擊者可以透過入侵虛擬層來竊取虛擬網路功能 (VNF) 的加密密鑰或關鍵機敏資訊。 - 如果沒有適當的保護，一個電信事業之虛擬網路功能 (VNF) 中的敏感資料，可能會洩漏到同一虛擬層上運行的其他電信事業之虛擬網路功能 (VNF)。
3	網路功能的可用性	- 虛擬化 3GPP 網路功能 (NF) 所需的共享資源如果沒有適當的保護可能，會被鄰近的虛擬機 (VM) 獨占，進而降低了虛擬化 3GPP 網路功能 (NF) 的功能可用性。
4	通用軟體環境	- 如果在多個虛擬化 3GPP 網路功能 (NF) 的軟體中發現相同漏洞，則攻擊者可以利用相同手法攻擊這些網路功能 (NF)。該漏洞可能允許攻擊者透過多個入口進入網路，或者是透過網路橫向移動。 - 透過軟體平台可能會向攻擊者提供更多關於如何入侵網路的資訊，所以當破解一個虛擬網路功能 (VNF) 後，將允許他們使用隱含信賴 (implicit trust) 在相連接的網路功能 (NF) 間移動。
5	資料的位置和生命週期	- 如果沒有適當限制在功能執行的位置或資料存放的位置時，一個虛擬網路功能 (VNF)的敏感隱私資訊可能面對不同的司法管轄權 (legal jurisdiction)。 - 如果沒有適當的生命週期保護時，一個虛擬網路功能 (VNF) 的敏感資訊可能會洩露給其他重複使用儲存資源得虛擬網路功能 (VNF)

6	功能隔離	- 如果沒有做好適當的功能隔離保護，惡意的功能可能會直接讀取其他功能的記憶體。
7	記憶體內省 (Introspection)	- 如果沒有做好適當的功能隔離保護，惡意的功能可能會直接讀取其他功能的記憶體。
8	測試隔離與確保	- 單獨測試虛擬網路功能 (VNF) 可能會遺漏虛擬網路功能 (VNF) 與電信事業網路中的網路元件交互運作產生的威脅和漏洞。 - 由於不同虛擬化環境可能對於應用層提供不同級別的資安防護，單獨測試虛擬網路功能 (VNF) 的資安防護等級將無法適用在所有虛擬化場域。 - 當虛擬網路功能 (VNF) 佈署在不同水平或垂直應用服務的虛擬化場域時，將需要滿足不同應用服務的資安防護需求。對於在特定隔離測試環境下單獨測試虛擬網路功能 (VNF)，將無法確保能夠同時滿足不同應用服務的資安防護需求。
9	信賴區域和切片隔離	- 攻擊者可以利用虛擬化環境的特性從低信任區域 (lower trust domain) 遷移到高信任區域 (higher trust domain)，或者在切片間 (slices) 遷移。 - 敏感資料可能因此出現在切片 (slice) 的外部。
10	單一管理區域 (Administrator Domain)	- 當攻擊者取得具有全域管理員帳戶 (global admin accoun) 登入權限後，可以登入所有的虛擬網路功能 (VNF) 包含統一資料管理功能 (UDM) 與認證憑證儲存和處理功能 (ARPF) 等高度安全性網路功能，並更改網路路由將資料轉送到其他位置，甚至可以關閉整個行動通訊網路。
11	金鑰和敏感資料存放的位置	- 高度安全性虛擬網路功能 (VNF) 可能會運行有弱點的主機，進而增加網路功能的資料遭受攻擊並破解的風險。
12	功能存取的區域	- 虛擬網路功能 (VNF) 可能被安裝或搬移到不適合提供服務甚至會違反法規的區域。
13	3GPP 功能級別的認證	- 如果從 3GPP 功能級別到硬體級別缺乏完整證明鏈 (full attestation chain)，則 3GPP 網路的應用層將無法驗證虛擬網路功能 (VNF) 或 NFVI 的信賴程度。所以一個虛擬網路功能 (VNF) 對於另一個網路功能 (VNF) 的信賴程度將受到限制。
14	跨接虛擬網路功能主機	- 攻擊者可以讀取傳輸中的資料。
15	加密資料處理	- 在不安全的環境中處理解密或未加密格式的資料，該資料可能會被攔截或複制。
16	混合部署虛擬和實體網路功能	- 實體網路功能 (PNF) 的弱點可以被當作攻擊虛擬網路功能 (VNF) 的入口，並可能利用虛擬網路功能 (VNF) 無法解讀之實體網路功能 (PNF) 的傳統安全機制。 - 虛擬網路功能 (VNF) 的弱點可以被當作將惡意訊息 (malicious messages) 轉傳至實體網路功能 (PNF) 的入口，而實體網路功能 (PNF) 尚無安全機制保護這類攻擊。

17	曝露軟體目錄的映像檔	- 如果沒有對保存虛擬網路功能 (VNF) 映像檔的軟體目錄做好完整性保護，則攻擊者可以利用目錄中的資訊對虛擬網路功能 (VNF) 發動攻擊。 - 如果沒有對保存虛擬網路功能 (VNF) 映像檔的軟體目錄做好完整性保護，則攻擊者可以在管理與協調流程 (MANO) 啟用該映像檔前，篡改目錄中的軟體套件。 - 如果沒有對啟用後的虛擬網路功能 (VNF) 軟體套件做好完整性保護，則攻擊者可以透過入侵管理與協調流程 (MANO) 來篡改實體化 (instantiate) 前虛擬網路功能 (VNF) 的軟體套件。 - 如果沒有對啟用時的虛擬網路功能 (VNF) 軟體套件做好機密性保護，則攻擊者可以透過入侵管理與協調流程 (MANO) 來竊取虛擬網路功能 (VNF) 中的敏感資訊。
18	起動悖論	- 如果透過管理與協調流程 (MANO) 頒布虛擬網路功能 (VNF) 授權憑證，則有權訪問管理與協調流程 (MANO) 的管理者可能破解其無權訪問的網路功能 (NF)。
19	變造時間	- 可以透過調整系統時鐘來混淆虛擬機 (VM) 的作業系統 (OS) 和虛擬網路功能 (VNF)，進而造成如篡改安全日誌、使用憑證過期或用戶設備 (UE) 與網路不同步等多種威脅。 - 網路可能會受到變造網路時間同步來源或虛擬網路功能 (VNF) 時鐘的攻擊而破解。
20	第三方託管環境	- 當使用未受電信事業控制且沒有適當的保護的第三方主機環境部署時，虛擬網路功能 (VNF) 的敏感資料可能會在第三方主機遭受破解。
21	虛擬機和虛擬機監控程序中斷	- 如果在完全虛擬化網路中的通用虛擬化平台沒有適當的保護，則攻擊者可能會利用一個被破解虛擬網路功能 (VNF) ，透過突破虛擬機監控程序或虛擬層 (VM) 入侵另一個虛擬網路功能 (VNF)。 - 攻擊者可能會入侵虛擬網路功能 (VNF) 並在虛擬層或 NFVI 中獲得執行程式碼。
22	管理與協調流程單點故障	- 攻擊者可以透過沒有適當保護的管理與協調流程 (MANO) 系統來破解虛擬網路功能 (VNF)。 - 攻擊者可以透過沒有適當保護的管理與協調流程 (MANO) 系統來竊聽或篡改虛擬網路功能 (VNF) 中的資料。 - 虛擬網路功能 (VNF) 可能會因為沒有適當保護而被破解的管理與協調流程 (MANO) 系統誤導，而收到來自 OSS / BSS 或 EM 的錯誤管理資訊，亦或不會收到相關的管理資訊。
23	網際網路協定層與應用層安全性	- 如果兩端 (both ends) 或中繼段 (both hops) 都位於相同的虛擬化平台中，則虛擬機管理程序等虛擬層以上網際網路協定層或應用程序層之端對端 (end-to-end) 或逐中繼段 (hop-by-hop) 間的安全機制，可能無法讓虛擬網路功能 (VNF) 獲得與實體網路功能 (PNF) 相同級別的資安防護。

24	通過網料進行資料同步	- 如果沒有適當的保護，攻擊者可能會入侵 NFVI 中的多個邏輯位置，以獲得虛擬網路功能 (VNF) 的內部資訊，緊接著在網路中移動以獲取用戶在不同介面上的相同資料，並透過資料與信令的關聯性發起攻擊行動。且洩露的資料甚至可能暴露用戶隱私。

註 1: 3GPP TR 33.848 之關鍵議題 (Key Issue) 編號

依據 3GPP TR 33.818 (35) 之技術研究報告與 ETSI NFV-SEC 001 (36) 之標準技術規格，將 5G 網路虛擬化分為三種部署模式如下：

(a) 部署模式 1：電信網路運營商從供應商處購買 3GPP 虛擬網路功能 (Virtual Network Functions, VNF)，並將其部署在第三方網路功能虛擬化基礎建設 (Network Functions Virtualization Virtualization, NFVI) 上。

(b) 部署模式 2：電信網路運營商從供應商處購買 3GPP 虛擬網路功能 (VNF) 和虛擬層 (virtualization layer)，並部署在第三方硬體層 (hardware layer) 上。

(c) 部署模式 3：電信網路運營商從供應商處購買和部署 3GPP 虛擬網路功能 (VNF)、虛擬層 (virtualization layer) 和硬體層 (hardware layer)。

電信網路運營商所不論採用何種型態的網路虛擬化部署，其虛擬化產品要經過資安測試和評估。電信網路運營商的三種部署模式分別對應到三種通用虛擬化網路產品 (Generic Virtualized Network Product, GVNP) 型態如下：

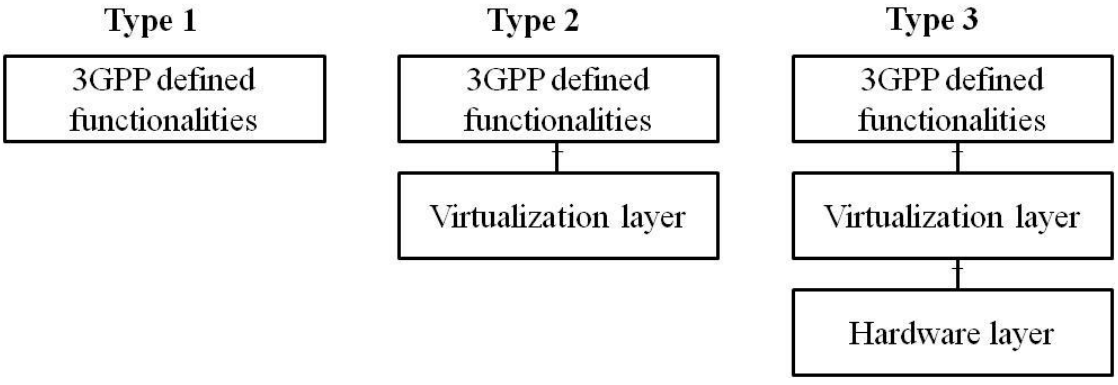


圖 37 三種網路虛擬化產品型態

6.2.4.1 通用虛擬化網路產品型態 1

通用虛擬化網路產品型態 1 僅部署第三代合作夥伴計畫 (3GPP) 定義的行動網路功能，如下：

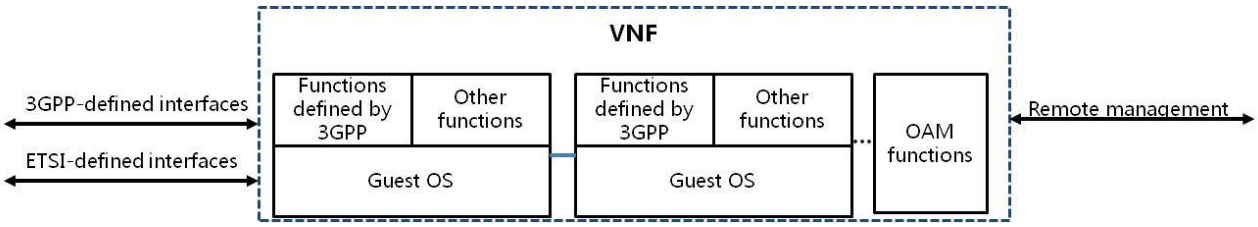


圖 38 通用虛擬化網路產品型態 1 的架構

通用虛擬化網路產品型態 1 的威脅分析與既有 3GPP TR 33.926 (37) 的網路產品威脅比較，如下：

表 8 通用虛擬化網路產品型態 1 的威脅分析表

威脅種類	威脅細節	與既有 3GPP TR 33.926 威脅比較
3GP 定義的網路介面威脅	-	適用 3GPP TR 33.926 之第 5.3.2 節的威脅
ETSI 定義的網路介面威脅	-	新類型威脅 - 虛擬網路功能與虛擬網路功能管理 (Virtualized Network Function Manager, VNFM) 間介面的威脅 - 虛擬網路功能與虛擬層間介面的威脅
識別碼欺騙 (Spoofing identity)	預設帳戶 (Default Accounts)	類似 3GPP TR 33.926 之第 5.3.3.1 節的威脅，但是該威脅透過虛擬網路控制台 (Virtual Network Console, VNC) 介面而不是實體控制介面進行訪問。
	弱密碼政策(Weak Password Policies)	類似 3GPP TR 33.926 之第 5.3.3.2 節的威脅，但是該威脅透過虛擬網路控制台 (VNC) 介面而不是實體控制介面進行訪問。
	窺視密碼 (Password peek)	類似 3GPP TR 33.926 之第 5.3.3.3 節的威脅，但是該威脅透過虛擬網路控制台 (VNC) 介面而不是實體控制介面進行訪問。
	直接根存取 (Direct Root Access)	適用 3GPP TR 33.926 之第 5.3.3.4 節的威脅

	網際通訊協定欺騙 (IP Spoofing)	類似 3GPP TR 33.926 之第 5.3.3.5 節的威脅，但是該威脅攻擊目標是虛擬網路功能 (VNF) 並不是實體電腦。
	惡意程式 (Malware)	適用 3GPP TR 33.926 之第 5.3.3.6 節的威脅
	竊聽 (Eavesdropping)	適用 3GPP TR 33.926 之第 5.3.3.7 節的威脅
竄改 (Tampering)	軟體竄改 (Software Tampering)	適用 3GPP TR 33.926 之第 5.3.4.1 節的威脅
	所有權檔案誤用(Ownership File Misuse)	適用 3GPP TR 33.926 之第 5.3.4.2 節的威脅
	開機竄改 (Boot tampering for GVNP of type 1)	定義於 3GPP TR 33.818 之第 5.2.4.2.2.5.3 節的威脅
	日誌竄改 (Log Tampering)	適用 3GPP TR 33.926 之第 5.3.4.4 節的威脅
	營運管理與維護流量竄改 (OAM traffic Tampering)	適用 3GPP TR 33.926 之第 5.3.4.5 節的威脅
	檔案寫入權限濫用 (File Write Permissions Abuse)	適用 3GPP TR 33.926 之第 5.3.4.6 節的威脅
	用戶通信期竄改 (User Session Tampering)	適用 3GPP TR 33.926 之第 5.3.4.7 節的威脅
否認性 (Repudiation)	缺乏用戶活動記錄 (Lack of User Activity Trace)	適用 3GPP TR 33.926 之第 5.3.5.1 節的威脅
資訊揭露 (Information disclosure)	不良金鑰產生 (Poor key generation)	適用 3GPP TR 33.926 之第 5.3.6.1 節的威脅
	不良金鑰管理 (Poor key management)	適用 3GPP TR 33.926 之第 5.3.6.2 節的威脅
	弱密碼演算法 (Weak cryptographic algorithms)	適用 3GPP TR 33.926 之第 5.3.6.3 節的威脅
	不安全資料儲存 (Insecure Data Storage)	適用 3GPP TR 33.926 之第 5.3.6.4 節的威脅
	系統指紋 (System Fingerprinting)	適用 3GPP TR 33.926 之第 5.3.6.5 節的威脅
	惡意程式 (Malware)	適用 3GPP TR 33.926 之第 5.3.6.6 節的威脅
	個人識別資訊違規(Personal Identification Information Violation)	適用 3GPP TR 33.926 之第 5.3.6.7 節的威脅
	不安全預設組態 (Insecure Default Configuration)	適用 3GPP TR 33.926 之第 5.3.6.8 節的威脅
	檔案/目錄讀出權限濫用 (File/Directory Read Permissions Misuse)	適用 3GPP TR 33.926 之第 5.3.6.9 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.6.10 節的威脅
	非必要服務 (Unnecessary Services)	適用 3GPP TR 33.926 之第 5.3.6.11 節的威脅
	日誌揭露 (Log Disclosure)	適用 3GPP TR 33.926 之第 5.3.6.12 節的威脅
	非必要應用 (Unnecessary	適用 3GPP TR 33.926 之第 5.3.6.13 節的威脅

	Applications)	
	竊聽 (Eavesdropping)	適用 3GPP TR 33.926 之第 5.3.6.14 節的威脅
	缺乏通用網路產品流量隔離導致安全威脅 (Security threat caused by lack of GNP traffic isolation)	適用 3GPP TR 33.926 之第 5.3.6.15 節的威脅
阻斷服務 (Denial of Service)	被破解/行為異常用戶設備 (Compromised/Misbehaving User Equipment)	適用 3GPP TR 33.926 之第 5.3.7.1 節的威脅
	實作缺陷 (Implementation Flaw)	適用 3GPP TR 33.926 之第 5.3.7.2 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.7.3 節的威脅
	人為錯誤 (Human Error)	適用 3GPP TR 33.926 之第 5.3.74 節的威脅
	未經授權更改虛擬化資源 (changing virtualisation resource without authorization)	定義於 3GPP TR 33.818 之第 5.2.4.2.2.8 節的威脅
提高特權 (Elevation of privilege)	授權使用者誤用 (Misuse by authorized users)	適用 3GPP TR 33.926 之第 5.3.8.1 節的威脅
	超過特權的程序/服務(Over-Privileged Processes/Services)	適用 3GPP TR 33.926 之第 5.3.8.2 節的威脅
	資料夾寫入權限濫用 (Folder Write Permission Abuse)	適用 3GPP TR 33.926 之第 5.3.8.3 節的威脅
	根所屬檔案寫入權限濫用 (Root-Owned File Write Permission Abuse)	適用 3GPP TR 33.926 之第 5.3.8.4 節的威脅
	高特權檔案 (High-Privileged Files)	適用 3GPP TR 33.926 之第 5.3.8.5 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.8.6 節的威脅
	透過非必要網路服務提高特權 (Elevation of Privilege via Unnecessary Network Services)	適用 3GPP TR 33.926 之第 5.3.87 節的威脅

6.2.4.2 通用虛擬化網路產品型態 2

通用虛擬化網路產品型態 2 部署第三代合作夥伴計畫 (3GPP) 定義的行動網路功能和虛擬層 (virtualization layer)，如下：

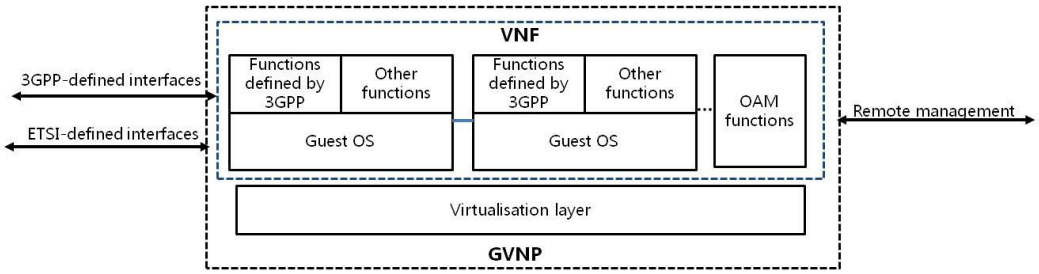


圖 39 通用虛擬化網路產品型態 2 的架構

通用虛擬化網路產品型態 2 的威脅分析與既有 3GPP TR 33.926 (37) 的網路產品威脅比較，如下：

表 9 通用虛擬化網路產品型態 2 的威脅分析表

威脅種類	威脅細節	與既有 3GPP TR 33.926 威脅比較
3GP 定義的網路介面威脅	-	適用 3GPP TR 33.926 之第 5.3.2 節的威脅
ETSI 定義的網路介面威脅	-	新類型威脅 - 虛擬網路功能與虛擬網路功能管理(VNFM)間介面的威脅 - 虛擬網路功能與虛擬層間介面的威脅 - 虛擬層與虛擬網路功能間介面的威脅 - 虛擬層與硬體層間介面的威脅 - 虛擬層與虛擬架構管理 (Virtualised Infrastructure Manager, VIM) 間介面的威脅
識別碼欺騙 (Spoofing identity)	預設帳戶 (Default Accounts)	類似 3GPP TR 33.926 之第 5.3.3.1 節的威脅，但是該威脅透過虛擬網路控制台 (VNC) 介面而不是實體控制介面進行訪問。
	弱密碼政策(Weak Password Policies)	類似 3GPP TR 33.926 之第 5.3.3.2 節的威脅，但是該威脅透過虛擬網路控制台 (VNC) 介面而不是實體控制介面進行訪問。
	窺視密碼 (Password peek)	類似 3GPP TR 33.926 之第 5.3.3.3 節的威脅，但是該威脅透過 VNC 介面而不是實體控制介面進行訪問。
	直接根存取 (Direct Root Access)	適用 3GPP TR 33.926 之第 5.3.3.4 節的威脅
	網際通訊協定欺騙 (IP Spoofing)	類似 3GPP TR 33.926 之第 5.3.3.5 節的威脅，但是該威脅攻擊目標是虛擬網路功能 (VNF) 並不是實體電腦。

	惡意程式 (Malware)	適用 3GPP TR 33.926 之第 5.3.3.6 節的威脅
	竊聽 (Eavesdropping)	適用 3GPP TR 33.926 之第 5.3.3.7 節的威脅
竄改 (Tampering)	軟體竄改 (Software Tampering)	適用 3GPP TR 33.926 之第 5.3.4.1 節的威脅
	所有權檔案誤用(Ownership File Misuse)	適用 3GPP TR 33.926 之第 5.3.4.2 節的威脅
	開機竄改 (Boot tampering for GVNP of type 2)	定義於 3GPP TR 33.818 之第 5.2.4.3.2.5.3 節的威脅
	日誌竄改 (Log Tampering)	適用 3GPP TR 33.926 之第 5.3.4.4 節的威脅
	營運管理與維護流量竄改 (OAM traffic Tampering)	適用 3GPP TR 33.926 之第 5.3.4.5 節的威脅
	檔案寫入權限濫用 (File Write Permissions Abuse)	適用 3GPP TR 33.926 之第 5.3.4.6 節的威脅
	用戶通信期竄改 (User Session Tampering)	適用 3GPP TR 33.926 之第 5.3.4.7 節的威脅
否認性 (Repudiation)	缺乏用戶活動記錄 (Lack of User Activity Trace)	適用 3GPP TR 33.926 之第 5.3.5.1 節的威脅
資訊揭露 (Information disclosure)	不良金鑰產生 (Poor key generation)	適用 3GPP TR 33.926 之第 5.3.6.1 節的威脅
	不良金鑰管理 (Poor key management)	適用 3GPP TR 33.926 之第 5.3.6.2 節的威脅
	弱密碼演算法 (Weak cryptographic algorithms)	適用 3GPP TR 33.926 之第 5.3.6.3 節的威脅
	不安全資料儲存 (Insecure Data Storage)	適用 3GPP TR 33.926 之第 5.3.6.4 節的威脅
	系統指紋 (System Fingerprinting)	適用 3GPP TR 33.926 之第 5.3.6.5 節的威脅
	惡意程式 (Malware)	適用 3GPP TR 33.926 之第 5.3.6.6 節的威脅
	個人識別資訊違規(Personal Identification Information Violation)	適用 3GPP TR 33.926 之第 5.3.6.7 節的威脅
	不安全預設組態 (Insecure Default Configuration)	適用 3GPP TR 33.926 之第 5.3.6.8 節的威脅
	檔案/目錄讀出權限濫用 (File/Directory Read Permissions Misuse)	適用 3GPP TR 33.926 之第 5.3.6.9 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.6.10 節的威脅
	非必要服務 (Unnecessary Services)	適用 3GPP TR 33.926 之第 5.3.6.11 節的威脅
	日誌揭露 (Log Disclosure)	適用 3GPP TR 33.926 之第 5.3.6.12 節的威脅
	非必要應用 (Unnecessary Applications)	適用 3GPP TR 33.926 之第 5.3.6.13 節的威脅
	竊聽 (Eavesdropping)	適用 3GPP TR 33.926 之第 5.3.6.14 節的威脅
	缺乏通用網路產品流量隔離	適用 3GPP TR 33.926 之第 5.3.6.15 節的威脅

	導致安全威脅 (Security threat caused by lack of GNP traffic isolation)	
阻斷服務 (Denial of Service)	被破解/行為異常用戶設備 (Compromised/Misbehaving User Equipment)	適用 3GPP TR 33.926 之第 5.3.7.1 節的威脅
	實作缺陷 (Implementation Flaw)	適用 3GPP TR 33.926 之第 5.3.7.2 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.7.3 節的威脅
	人為錯誤 (Human Error)	適用 3GPP TR 33.926 之第 5.3.74 節的威脅
	未經授權更改虛擬化資源 (changing virtualisation resource without authorization)	定義於 3GPP TR 33.818 之第 5.2.4.3.2.8 節的威脅
提高特權 (Elevation of privilege)	授權使用者誤用 (Misuse by authorized users)	適用 3GPP TR 33.926 之第 5.3.8.1 節的威脅
	超過特權的程序/服務(Over-Privileged Processes/Services)	適用 3GPP TR 33.926 之第 5.3.8.2 節的威脅
	資料夾寫入權限濫用 (Folder Write Permission Abuse)	適用 3GPP TR 33.926 之第 5.3.8.3 節的威脅
	根所屬檔案寫入權限濫用 (Root-Owned File Write Permission Abuse)	適用 3GPP TR 33.926 之第 5.3.8.4 節的威脅
	高特權檔案 (High-Privileged Files)	適用 3GPP TR 33.926 之第 5.3.8.5 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.8.6 節的威脅
	透過非必要網路服務提高特權 (Elevation of Privilege via Unnecessary Network Services)	適用 3GPP TR 33.926 之第 5.3.8.7 節的威脅

6.2.4.3 通用虛擬化網路產品型態 3

通用虛擬化網路產品型態 3 部署第三代合作夥伴計畫 (3GPP) 定義的行動網路功能、虛擬層 (virtualization layer) 和硬體層 (hardware layer)，如下：

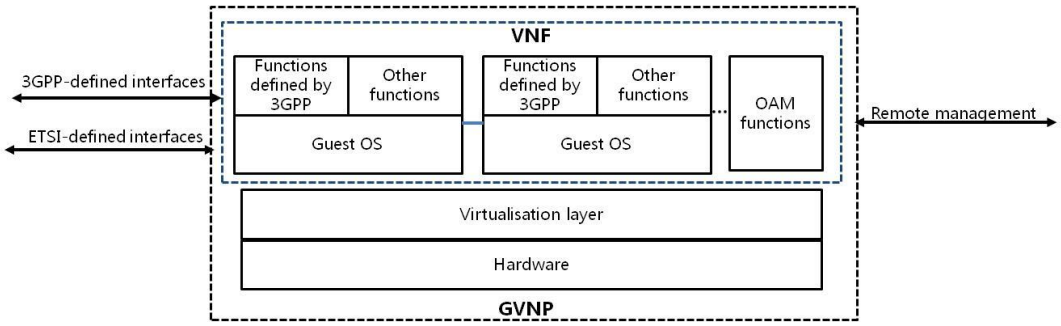


圖 40 通用虛擬化網路產品型態 3 的架構

通用虛擬化網路產品型態 3 的威脅分析與既有 3GPP TR 33.926 (37) 的網路產品威脅比較，如下：

表 10 通用虛擬化網路產品型態 3 的威脅分析表

威脅種類	威脅細節	與既有 3GPP TR 33.926 威脅比較
3GP 定義的網路介面威脅	-	適用 3GPP TR 33.926 之第 5.3.2 節的威脅
ETSI 定義的網路介面威脅	-	新類型威脅 - 虛擬網路功能與虛擬網路功能管理 (VNFM) 間介面的威脅 - 虛擬網路功能與虛擬層間介面的威脅 - 虛擬層與虛擬網路功能間介面的威脅 - 虛擬層與硬體層間介面的威脅 - 硬體層與虛擬層間介面的威脅 - 虛擬層與虛擬架構管理(VIM)間介面的威脅 - 硬體層與虛擬架構管理(VIM)間介面的威脅
識別碼欺騙 (Spoofing identity)	預設帳戶 (Default Accounts)	類似 3GPP TR 33.926 之第 5.3.3.1 節的威脅，但是該威脅透過虛擬網路控制台 (VNC) 介面而不是實體控制介面進行訪問。
	弱密碼政策(Weak Password Policies)	類似 3GPP TR 33.926 之第 5.3.3.2 節的威脅，但是該威脅透過虛擬網路控制台 (VNC) 介面而不是實體控制介面進行訪問。
	窺視密碼 (Password peek)	類似 3GPP TR 33.926 之第 5.3.3.3 節的威脅，但是該威脅透過虛擬網路控制台 (VNC) 介面而不是實體控制介面進行訪問。
	直接根存取 (Direct Root Access)	適用 3GPP TR 33.926 之第 5.3.3.4 節的威脅

	網際通訊協定欺騙 (IP Spoofing)	類似 3GPP TR 33.926 之第 5.3.3.5 節的威脅，但是該威脅攻擊目標是虛擬網路功能 (VNF) 並不是實體電腦。
	惡意程式 (Malware)	適用 3GPP TR 33.926 之第 5.3.3.6 節的威脅
	竊聽 (Eavesdropping)	適用 3GPP TR 33.926 之第 5.3.3.7 節的威脅
竄改 (Tampering)	軟體竄改 (Software Tampering)	適用 3GPP TR 33.926 之第 5.3.4.1 節的威脅
	所有權檔案誤用(Ownership File Misuse)	適用 3GPP TR 33.926 之第 5.3.4.2 節的威脅
	開機竄改 (Boot tampering for GVNP of type 3)	定義於 3GPP TR 33.818 之第 5.2.4.4.2.5.3 節的威脅
	日誌竄改 (Log Tampering)	適用 3GPP TR 33.926 之第 5.3.4.4 節的威脅
	營運管理與維護流量竄改 (OAM traffic Tampering)	適用 3GPP TR 33.926 之第 5.3.4.5 節的威脅
	檔案寫入權限濫用 (File Write Permissions Abuse)	適用 3GPP TR 33.926 之第 5.3.4.6 節的威脅
	用戶通信期竄改 (User Session Tampering)	適用 3GPP TR 33.926 之第 5.3.4.7 節的威脅
否認性 (Repudiation)	缺乏用戶活動記錄 (Lack of User Activity Trace)	適用 3GPP TR 33.926 之第 5.3.5.1 節的威脅
資訊揭露 (Information disclosure)	不良金鑰產生 (Poor key generation)	適用 3GPP TR 33.926 之第 5.3.6.1 節的威脅
	不良金鑰管理 (Poor key management)	適用 3GPP TR 33.926 之第 5.3.6.2 節的威脅
	弱密碼演算法 (Weak cryptographic algorithms)	適用 3GPP TR 33.926 之第 5.3.6.3 節的威脅
	不安全資料儲存 (Insecure Data Storage)	適用 3GPP TR 33.926 之第 5.3.6.4 節的威脅
	系統指紋 (System Fingerprinting)	適用 3GPP TR 33.926 之第 5.3.6.5 節的威脅
	惡意程式 (Malware)	適用 3GPP TR 33.926 之第 5.3.6.6 節的威脅
	個人識別資訊違規(Personal Identification Information Violation)	適用 3GPP TR 33.926 之第 5.3.6.7 節的威脅
	不安全預設組態 (Insecure Default Configuration)	適用 3GPP TR 33.926 之第 5.3.6.8 節的威脅
	檔案/目錄讀出權限濫用 (File/Directory Read Permissions Misuse)	適用 3GPP TR 33.926 之第 5.3.6.9 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.6.10 節的威脅
	非必要服務 (Unnecessary Services)	適用 3GPP TR 33.926 之第 5.3.6.11 節的威脅
	日誌揭露 (Log Disclosure)	適用 3GPP TR 33.926 之第 5.3.6.12 節的威脅
	非必要應用 (Unnecessary	適用 3GPP TR 33.926 之第 5.3.6.13 節的威脅

	Applications)	
	竊聽 (Eavesdropping)	適用 3GPP TR 33.926 之第 5.3.6.14 節的威脅
	缺乏通用網路產品流量隔離導致安全威脅 (Security threat caused by lack of GNP traffic isolation)	適用 3GPP TR 33.926 之第 5.3.6.15 節的威脅
阻斷服務 (Denial of Service)	被破解/行為異常用戶設備 (Compromised/Misbehaving User Equipment)	適用 3GPP TR 33.926 之第 5.3.8.1 節的威脅
	實作缺陷 (Implementation Flaw)	適用 3GPP TR 33.926 之第 5.3.8.2 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.8.3 節的威脅
	人為錯誤 (Human Error)	適用 3GPP TR 33.926 之第 5.3.8.4 節的威脅
	未經授權更改虛擬化資源 (changing virtualisation resource without authorization)	定義於 3GPP TR 33.818 之第 5.2.4.4.2.8 節的威脅
提高特權 (Elevation of privilege)	授權使用者誤用 (Misuse by authorized users)	適用 3GPP TR 33.926 之第 5.3.8.5 節的威脅
	超過特權的程序/服務 (Over-Privileged Processes/Services)	適用 3GPP TR 33.926 之第 5.3.8.6 節的威脅
	資料夾寫入權限濫用 (Folder Write Permission Abuse)	適用 3GPP TR 33.926 之第 5.3.87 節的威脅
	根所屬檔案寫入權限濫用 (Root-Owned File Write Permission Abuse)	適用 3GPP TR 33.926 之第 5.3.8.4 節的威脅
	高特權檔案 (High-Privileged Files)	適用 3GPP TR 33.926 之第 5.3.8.5 節的威脅
	不安全網路服務 (Insecure Network Services)	適用 3GPP TR 33.926 之第 5.3.8.6 節的威脅
	透過非必要網路服務提高特權 (Elevation of Privilege via Unnecessary Network Services)	適用 3GPP TR 33.926 之第 5.3.8.7 節的威脅

6.2.5 5G 專網多接取邊緣運算多元應用情境的資安風險分析

5G 專網多接取邊緣運算多元應用情境包含支援車聯網 (Vehicle-to-Everything services, V2X)、未來工廠 (Factories of the Future, FoF)、無人飛行系統系統 (Unmanned Aerial Systems, UAS)、遠距醫療 (Telemedicine) 與虛擬實境 (Virtual Reality, VR) 以及擴增實境 (Augmented Reality, AR) 等垂直應用服務。

5G 專網多接取邊緣運算除了要考量資訊安全外，還需要滿足使用穿戴式物聯網 (Wearable IoT) 技術實現遠距醫療 (Telemedicine) 的病患以及透過車聯網 (V2X) 實現自動駕駛 (Autopilot) 的乘客之隱私權保障，故於第 6.2.5.1 小節探討隱私的資安風險分析。

由於 5G 應用情境多，部份的安全威脅仍然在討論中，其中車聯網 (V2X)、無人飛行系統系統 (UAS)、未來工廠 (FoF) 以及遠距機器人手術 (Remote Robotic Surgery) 等應用情境需要依賴超高可靠度和低延遲通訊 (Ultra-reliable and Low Latency Communications, URLLC) 技術，將於第 6.2.5.2 小節描述其的資安風險分析。

而未來工廠在建置 5G 專網多接取邊緣運算平台時，需要新增如時間敏感網路 (Time Sensitive Networking, TSN) 以及 5G 區域網路型態服務 (5G LAN-type service) 等特定技術功能於 5G 專網多接取邊緣運算平台上，這些技術的資安風險議題都需要被納入考量，分別於第 6.2.5.3 小節與第 6.2.5.4 小節討論。

6.2.5.1 隱私的資安風險分析

5G 專網多接取邊緣運算仰賴標準化的先進技術實現萬物相連的多元應用情境，用戶設備 (UE) 由於經常處於聯網狀態，會在不知情的情況下將使用數據傳送到網路上，因此增加個人資料外洩的隱私問題和資安威脅如表 11。

表 11 隱私 (Privacy) 的安全威脅

威脅議題	安全威脅
用戶隱私資料竊聽	- 行動用戶永久識別碼 (Subscriber Permanent Identifier, SUPI) 擷取器 (Catcher) 導致用戶隱私被攔截與竊聽的威脅。
竊取用戶身份	- 5G 中提供輔助身份驗證功能，當此身分驗證機制遭受攻擊，可竊取行動用戶的個人資料與位置等隱私資訊。

此外，依據 3GPP TR 33.861 (38) 與 3GPP TR 33.836 (39) 之技術研究報告，5G 物聯網 (IoT) 與車聯網 (V2X) 需要面對下列的隱私安全威脅。

表 12 物聯網 (IoT) 的隱私安全威脅

關鍵議題 [1]	議題標題	安全威脅
12	非存取層 (NAS)資訊包含的行動通訊物聯網 (CIoT) 新參數的隱私保護	- 要防範透過交換參數以及和用戶設備 (UE) 行為關聯達成重新標識用戶設備 (UE) 的威脅。

註 1: 3GPP TR 33.836 之關鍵議題 (Key Issue) 編號

表 13 車聯網 (V2X) 的隱私安全威脅

關鍵議題 [1]	議題標題	安全威脅
1	透過 PC5 的單播資訊隱私保護	- 能夠將 L2 識別碼與應用層 ID 真實或長期的識別碼做鏈結，進一步在時空上追蹤特定終端。這種可追蹤性 (trackability) 和可鏈結性 (linkability) 將對端點的隱私造成威脅。
3	透過 PC5 的群播資訊隱私保護	- 能夠將 L2 識別碼與應用層 ID 真實或長期的識別碼做鏈結，進一步在時空上追蹤特定終端。這種可追蹤性 (trackability) 和可鏈結性 (linkability) 將對端點的隱私造成威脅。
8	透過 PC5 的廣播資訊隱私保護	- 能夠將 L2 識別碼與應用層 ID 真實或長期的識別碼做鏈結，進一步在時空上追蹤特定終端。這種可追蹤性 (trackability) 和可鏈結性 (linkability) 將對端點的隱私造成威脅。
9	最小化隱私保護機制對於應用層通訊的影響	-

註 1: 3GPP TR 33.836 之關鍵議題 (Key Issue) 編號

6.2.5.2 超可靠度和低延遲通訊的資安風險分析

超可靠度和低延遲通訊 (URLLC) 在車聯網 (V2X)、未來工廠 (FoF)、無人機控制 (UAS) 等應用上扮演著重要的角色，由於超可靠度和低延遲通訊極度嚴格的延遲與可靠度需求將對現有網路通訊系統與安全性帶來巨大的挑戰。依據 3GPP TR 33.825 (40) 之技術研究報告，其應解決的安全威脅如表 14。

表 14 超可靠度和低延遲通訊 (URLLC) 的安全威脅

關鍵議題 [1]	議題標題	安全威脅
1	冗餘 (redundant) 傳輸的安全性	- 攻擊者可以監視資料流 (data streams) 並識別兩個資料流是否被用於冗資料流傳輸。如果相應的無線電承載 (Radio Bearer) 或 N3 隧道缺乏完整性、機密性和重播保護，則攻擊者可以利用此類資訊針對超可靠度和低延遲通訊 (URLLC) 服務發動攻擊。
2	支援用戶平面(UP)冗餘資料高可靠性傳輸的安全性	- 兩個或多個用戶平面 (UP) 路徑必須採用同等的安全性保護，才能實現用戶平面(UP) 冗餘資料通信的高度可靠性。破壞其中一個用戶平面 (UP) 路徑將使超可靠度和低延遲通訊 (URLLC) 服務尚失高度可靠性。
3	處理建立多個協定資料單元(PDU)會話的冗餘資料傳輸之用戶平面 (UP) 安全策略	- 當攻擊者知道在第一條路徑上啟用了完整性保護而第二條路徑上未啟用完整性保護時，攻擊者可透過干擾第一條路徑並竄改第二條路徑從 5G 基地臺 (gNB) 轉發到用戶平面功能 (UPF) 的用戶平面資料。
4	超可靠度和低延遲通訊服務的安全策略	- 如果超可靠度和低延遲通訊 (URLLC) 服務的用戶平面沒有完整性保護，則可能在傳輸期間遭受竄改。 - 如果超可靠度和低延遲通訊 (URLLC) 服務的用戶平面使用完整性保護，則可能導致無法接受的時間延遲。 - 如果超可靠度和低延遲通訊 (URLLC) 服務沒有採用特定服務的安全策略，則可能導致服務沒有採用足夠保護的風險。
5	低延遲換手的安全性	- 當介面 (如 N2 介面) 沒有安全保護時，攻擊者可以竊聽、注入或竄改介面上傳輸的金鑰和安全參數。 - 如果存取與行動管理功能 (AMF) 遭到入侵 ● 且用戶設備 (UE) 的金鑰不具有後向安全性 (backward security)，那麼攻擊者將能夠解密用戶設備先前與網路間的傳輸資料。 ● 且用戶設備 (UE) 的金鑰不具有前向安全性 (forward security)，那麼攻擊者將能夠解密用戶設備未來與網路間的傳輸資料。 - 如果存取與行動管理功能 (AMF) 遭到入侵，或裝置遭受到中間人 (Men in the Middle, MiTM) 攻擊，則攻擊者可以將演算法降階為容易破解的演算法設定。 -

6	保留存取層 (AS) 金鑰支援用戶平面冗餘資料傳輸	-
7	服務品質 (QoS) 監控保護	- 當端對端服務品質(E2E QoS)的監視過程缺乏安全保護時，攻擊者可能會修改資料封包或訊息導致系統獲得錯誤的延遲報告 (latency report)。
8	加速認證和密鑰協商過程以降低延遲	-
9	低延遲重新認證過程的安全性	-
10	低延遲的用戶平面安全性	-

註 1: 3GPP TR 33.825 之關鍵議題 (Key Issue) 編號

6.2.5.3 時間敏感通訊的資安風險分析

5G 通訊與時間敏感網路 (TSN) 的整合是 5G 做為工業通訊系統中非常重要的組成，像是 5G 通訊需要支援時間敏感網路的控制器協作、時間同步 (Time Synchronization)、時間敏感網路限制延遲 (Bounded Latency) 與時間敏感網路可靠性要求等面向。依據 3GPP TR 33.819 [6]之技術研究報告，時間敏感通訊 (Time Synchronization , TSC) 應解決的安全威脅如表 15。

表 15 時間敏感通訊 (TSC) 的安全威脅

關鍵議題 [1]	議題標題	安全威脅
4.1	保護 5G 系統與時間敏感網路間的交互作用介面	- 如果與時間敏感網路通訊的介面缺乏機密性保護、完整性保護以及重播保護，則攻擊者可能會竊聽資料、修改資料以及發動重播攻擊
4.2	時間敏感通訊的時間同步	5G 通訊與時間敏感網路的橋接器可能以下弱點： - 阻斷使用嚴格延遲邊 (strict latencies boundaries)的確定性傳輸 (deterministic transmission)。 - 變造主/從網路單元間的時鐘同步和全域時間基準的主時鐘 (Grand Master)。 - 變造時間感知排程 (Time aware Scheduling) 和流量整形 (traffic shaping)。

		- 變造通信路徑的選擇以及預留的頻寬和時間間隔 (timeslot)。

註 1: 3GPP TR 33.819 之關鍵議題 (Key Issue) 編號

6.2.5.4 5G 區域網路的資安風險分析

固網與行動融合 (Fixed and Mobile Convergence, FMC) 技術讓 5G 無線接入技術與現有固定 (local area network, LAN) 及無線區域網路 (wireless local area network, WLAN) 共同使用核心網路組成 5G 區域網路 (5G LAN) 架構。依據 3GPP TR 33.819 [6] 之技術研究報告，其應解決的安全威脅如表 16。

表 16 5G 區域網路的安全威脅

關鍵議題 [1]	議題標題	安全威脅
3.1	5G 區域網路通訊的用戶設備認證和授權	- 5G 區域網路服務系統應提供一種相互身份驗證和授權機制，以確保僅提供授權的用戶設備使用 5G 區域網路群組服務。 - 如果不進行身份驗證和授權，則任何未經授權的用戶設備都可獲得 5G 區域網路群組(5GLAN group)服務，導致 5G 區域網路群組通信遭到盜用服務和阻斷服務的風險。
3.2	5G 區域網路群組的使用者平面安全政策	- 如果屬於同一 5G 區域網路群組 (5GLAN group) 的用戶設備 (UE) 和 5G 基地台 (gNB) 間的用戶平面流量中最弱的安全等級將成為整個 5G 區域網路群組的通信路徑安全等級。 - 如果其中一個用戶設備關閉機密功能，縱使 5G 區域網路群組的其他用戶設備的通信路徑均被加密，但其交換的資訊仍然會被竊聽。

註 1: 3GPP TR 33.819 之關鍵議題 (Key Issue) 編號

6.3 5G 專網多接取邊緣運算平台的安全解決方案

5G 專網多接取邊緣運算 (MEC) 採用以服務基礎架構 (SBA) 為導向之網路功能虛擬化 (NFV)，是行動網路中連接到包括營運管理與維護 (OAM) 系統、用戶平面功能 (UPF)、合法監聽 (Lawful Interception, LI) 等多個行動網路實體的同時，還連接到第三方應用伺服器，甚至容納第三方應用程式 (41)。因為現有台灣廠商大多採用英特爾 (Intel) 或工研院 (ITRI) 的邊緣運算平台架構，故於第 6.3.1 小節描述 5G 專網多接取邊

緣運算平台與網路架構的安全解決方案；同時為了確保安全解決方案符合相關的資安規範，於第 6.3.2 小節探討 5G 專網多接取邊緣運算相關的資安確保技術；最後統整前述 5G 專網多接取邊緣運算的威脅與安全解決方案涵蓋資安確保技術於第 6.3.3 小節中。

6.3.1 5G 專網多接取邊緣運算的安全解決方案

5G 專網多接取邊緣運算的安全解決方案已訂定於第三代合作夥伴計畫 (3GPP) 的相關安全標準技術規格中，然而 5G 多接取邊緣運算平台的虛擬環境維護、邊緣應用伺服器與 5G 垂直領域應用服務的安全標準規範尚在討論與制定中，故分別於第 6.3.1.1 小節、第 6.3.1.3 小節與第 6.3.1.3 小節作簡介。

6.3.1.1 5G 多接取邊緣運算平台的虛擬環境維護方案

依據 3GPP TR 32.842 (42) 之第 5.5.10 小節，當 5G 專網多接取邊緣運算平台的虛擬網路功能 (VNF) 的軟體套件需要進行更新時，將透過管理與協調流程 (MANO) 系統地網路功能虛擬化協調器 (NFV orchestrator, NFVO) 執行網路服務的資源規劃和生命週期管理，來更新軟體目錄下的虛擬網路功能 (VNF) 映像檔。並透過 3GPP TR 32.842 (42) 之第 5.1.8 小節描述的虛擬網路功能快照 (VNF snapshot capture) 機制，來實現虛擬網路功能的生命週期管理 (VNF lifecycle management) 以及快速虛擬網路功能佈署 (fast VNF deployment)。

6.3.1.2 邊緣應用伺服器的安全解決方案

5G 專網多接取邊緣運算 (MEC) 的具體安全是物理設施保護，鄰接部署為用戶提供優質服務的同時，也縮短了攻擊者與邊緣應用伺服器間的距離，使攻擊者更容易與伺服器接觸造成實體入侵破壞、服務中斷、用戶隱私泄露等威脅。邊緣應用伺服器也可能面臨著各種自然災害和工業災害的威脅，導致邊緣應用伺服器間受到直接損害和服務突然中斷，因此需要為邊緣應用伺服器配置相應的保護措施。

5G 專網多接取邊緣運算的安全挑戰主要來自重要軟體組成部分與廣泛的應用服務等關鍵技術創新所帶來的安全性更新，與軟體有關的安全風險漏洞管理十分重要，不良的軟體開發流程 使攻擊者容易植入難以被發現的惡意軟體。電信運營商要為邊緣應用伺服器 (EAS) 中的應用程式提供防禦惡意攻擊的服務，並檢查第三方應用程式的安

全漏洞，以避免惡意應用程式在邊緣應用伺服器 (EAS) 上惡意占用資源，使伺服器上的其他應用程式失效，並防止惡意應用程式也可以透過應用程式介面 (API) 更改網路的配置，進一步損害整個網路的效能。

針對應用服務的安全威脅有必要建立一個的安全評估系統來評估邊緣應用伺服器 (EAS) 中應用程式的安全性以及應用程式和網路間應用程式介面 (API) 通訊安全。然後需要建立用戶設備 (UE)、邊緣應用伺服器 (EAS)、邊緣運算應用程式 (MEC APP)、核心網路 (5GC) 構建共擴展的信任關係，以便合法用戶設備使用 5G 邊緣應用服務。

在邊緣應用伺服器和邊緣運算應用程式間建立信任關係以防止惡意應用程式接管用戶服務；在邊緣應用伺服器與用戶設備間建立的信任關係以確認合法性，防止惡意的邊緣應用伺服器竊取用戶資訊。最後需要配備隱私泄露保護措施，嚴格控制第三方邊緣應用伺服器的行為，防止其泄露和濫用用戶設備的隱私資訊。

6.3.1.3 5G 垂直領域應用服務的安全解決方案

當 5G 專網多接取邊緣運算平台未來採用第三代合作夥伴計畫 (3GPP) 訂定共用應用程式介面構架核心功能 (CAPIF) 的系統架構時，依據 3GPP TS 33.122 (43) 之安全標準技術規格，於 3GPP TS 23.222 (10) 所制定之共用應用程式介面構架核心功能 (CAPIF Core Function, CCF)、應用程式介面揭露功能 (API Exposure Function, AEF) 與應用程式介面調用者 (API Invoker) 等三個共用應用程式介面構架 (CAPIF) 主要實體，需滿足下圖的共用應用程式介面構架 (CAPIF) 的功能安全模型。

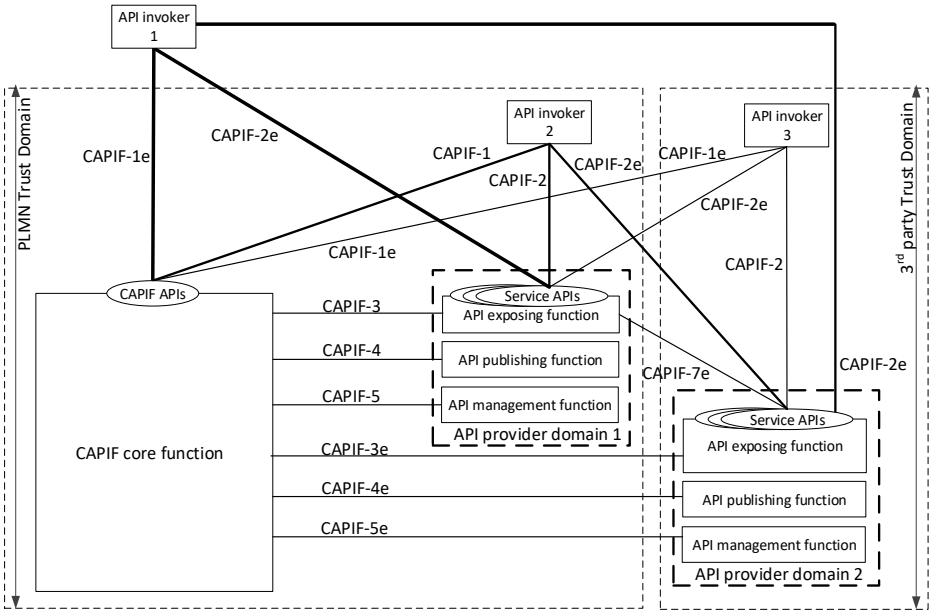


圖 41 共用應用程式介面構架 (CAPIF) 的功能安全模型

此外，當其 5G 專網多接取邊緣運算平台的多元應用服務未來採用垂直服務致能架構層 (SEAL) 的系統架構時，依據 3GPP TS 33.434 (44) 之標準技術規範，其系統架構的安全需求如表 17。

表 17 垂直服務致能架構層 (SEAL) 的系統架構的安全需求

需求編號 [1]	安全需求
4.1-a	垂直服務致能架構層服務的所有用戶均應經過驗證
4.1-b	在向垂直服務致能架構層服務用戶設備提供服務前，垂直服務致能架構層用戶端應和伺服器進行交互身份驗證。
4.1-c	網路中合法授權的垂直服務致能架構層伺服器與用戶設備間的傳輸應受到機密性與完整性以及重播保護。
4.1-d	垂直服務致能架構層服務應採取措施來偵測和輕減阻斷服務 (DoS) 攻擊，以大幅減少對網路和用戶的影響。
4.1-e	垂直服務致能架構層服務應提供用戶身份的機密性的機制。
4.1-f	垂直服務致能架構層服務應提供垂直服務致能架構層傳訊的機密性。
4.2-a	垂直服務致能架構層系統應採取保護措施免受到外部攻擊。

註 1: 3GPP TS 33.434 之需求編號

6.3.2 5G 專網多接取邊緣運算的資安確保

為了確保 5G 專網多接取邊緣運算符合相關的資安標準與規範，第三代合作夥伴計畫 (3GPP) 針對 5G 虛擬化架構與 5G 核心網路以及 5G 基地臺的相關資安確保標準，分別於第 6.3.2.1 小節與第 6.3.2.12 小節以及第 5.3.2.3 小節作簡介；然而第三代合作夥伴計畫並未針對 5G 多元應用服務的部分訂定相關資安確保標準，其仰賴相關領域的資安標準與各區域的資安法規，將於第 5.3.2.4 小節探討相關的資安確保規範與標準。

6.3.2.1 5G 虛擬化架構的通用資安確保標準

依據 3GPP TR 33.818 (35) 網路虛擬化之威脅和關鍵資產的安全保證規範研究報告認為既有的 5G 產品通用資安確保標準適用於虛擬化架構的產品，故參考 3GPP TS 33.117 (45) 技術標準規格之第 4.2.2 小節，其安全測試項目如下：

表 18 5G 虛擬化架構的產品資安確保標準 (SCAS)

分類		標準章節	測試項目
以服務為基礎架構之安全性		4.2.2.2.2	傳輸層的保護
		4.2.2.2.3.1	處理同一陸地行動通信網路的授權許可證驗證失敗
		4.2.2.2.3.2	處理不同陸地行動通信網路的授權許可證驗證失敗
保護數據和資訊		4.2.3.2.1	通則
		4.2.3.2.2	未經授權的檢視
		4.2.3.2.3	保護存儲中的數據和資訊
		4.2.3.2.4	保護傳輸中的數據和資訊
		4.2.3.2.5	記錄訪問個人數據的事件
保護可用性和完整性		4.2.3.3.1	系統處理過載的情況
		4.2.3.3.2	僅從預設的存儲設備開機
		4.2.3.3.3	系統處理過度過載的情況
		4.2.3.3.4	系統針對非預期輸入的強健性
		4.2.3.3.5	網路產品軟體的完整性驗證
認證與授權	認證政策	4.2.3.4.1.1	未經成功認證和授權，不得使用或訪問系統功能
		4.2.3.4.1.2	網路產品應使用明確標識的用戶帳戶
	認證屬性	4.2.3.4.2.1	至少透過一個身份驗證屬性保護帳戶
		4.2.3.4.2.2	預設帳戶應刪除或禁用
		5.2.3.4.2.3	預設認證屬性應刪除或禁用
	密碼政策	4.2.3.4.3.1	密碼複雜度規則
		4.2.3.4.3.2	密碼變更
		4.2.3.4.3.3	防止暴力和字典攻擊
		4.2.3.4.3.4	隱藏密碼顯示

	特定身份驗證案例	4.2.3.4.4.1	網路產品管理和維護界面
	因應連續登錄失敗	4.2.3.4.5	有關連續嘗試登錄失敗的策略
	控制授權和訪問	4.2.3.4.6.1	授權政策
		4.2.3.4.6.2	基於角色的訪問控制
保護會話		4.2.3.5.1	保護會話－登出功能
		4.2.3.5.2	保護會話－不活動逾時
記錄		4.2.3.6.1	安全事件記錄
		4.2.3.6.2	日誌傳輸到集中存儲
		4.2.3.6.3	保護安全事件日誌文件
作業系統	可用性和完整性	4.2.4.1.1.1	動態增長的內容不應影響系統功能
		4.2.4.1.1.2	處理網際網路控制訊息協定第四版 (Internet Control Message Protocol version 4, ICMPv4) 和網際網路控制訊息協定第六版 (ICMPv6) 封包
		4.2.4.1.1.3	不處理具有非必選或延伸標頭的網際網路協定 (Internet protocol, IP)封包
	認證與授權	4.2.4.1.2.1	僅允許經過身份驗證的特權升級
	UNIX®	4.2.4.2.1	通則
		4.2.4.2.2	系統帳號識別
	安全強化 (hardening)	4.3.3.1.1	因應網際網路協定 (IP) 來源位置欺騙
		4.3.3.1.2	核心網路功能最小化
		4.3.3.1.3	沒有自動開啟可移除式媒體
		4.3.3.1.4	預防請求洪水 (Syn Flood)
		4.3.3.1.5	防止緩衝器溢位的保護機制
		4.3.3.1.6	限制安裝外部檔案系統
網頁伺服器	網頁安全	4.2.5.1	超文本傳輸安全協定 (HyperText Transfer Protocol Secure, HTTPS)
		4.2.5.2.1	網頁伺服器日誌記錄
		4.2.5.3	用戶會話
		4.2.5.4	輸入驗證
	安全強化 (hardening)	4.3.4.1	通則
		4.3.4.2	網頁伺服器沒有系統特權
		4.3.4.3	未使用的超文本傳輸協定 (HyperText Transfer Protocol, HTTP) 的方法 (methods) 應被停用
		4.3.4.4	應停用不需要的附加元件
		4.3.4.5	沒有通過共同閘道介面 (Common Gateway Interface, CGI) 或其他伺服器端腳本編寫的編譯器、解釋器或殼層 (Shell)
		4.3.4.6	沒有用於上傳的共同閘道介面 (CGI) 或其他腳本
		4.3.4.7	不使用伺服器端包含變數值 (Server Side Includes, SSI) 執行系統命令
		4.3.4.8	管理網頁伺服器的權限僅應授予網頁伺服器的所有者或具有系統特權的用戶

		4.3.4.9	應刪除預設的內容
		4.3.4.10	沒有目錄列表/目錄瀏覽
		4.3.4.11	應最小化超文本傳輸協定 (HTTP) 標頭中有關網頁伺服器的資訊
		4.3.4.12	應刪除網頁伺服器中的錯誤資訊頁面
		4.3.4.13	應刪除不需要的檔案類型或腳本映射
		4.3.4.14	網頁伺服器僅交付必要的檔案
		4.3.4.15	僅在共同閘道介面 (CGI) 與腳本目錄中具有執行權限
網路裝置	保護可用性和完整性	4.2.6.2.1	封包過濾
		4.2.6.2.2	發送到網路設備的變造封包不應導致可用性降低
		4.2.6.2.3	通用封包無線服務隧道協定-控制平面 (GTP-C) 封包過濾
		4.2.6.2.3	通用封包無線服務隧道協定-用戶平面 (GTP-U) 封包過濾
	安全強化	4.3.5.1	流量分離
	以服務為基礎架構之安全強化	4.3.6.2	JavaScript 物件表示法 (JavaScript object notation, JSON) 解析器不應包含外部資源或執行程式
		4.3.6.3	資訊元件 (Information Element, IE) 值的唯一性
		4.3.6.4	資訊元件 (IE)格式和數值範圍的有效性
安全強化的技術準則		4.3.2.1	沒有不必要或不安全的服務與協議
		4.3.2.2	網路產品應限制服務的可達性
		4.3.2.3	卸載或不得安裝未使用的軟體
		4.3.2.4	未使用的網路產品軟硬體功能應被停用
		4.3.2.5	網路產品不得包含供應商、生產商或開發人員不再支援的軟硬體元件。
		4.3.2.6	限制特權用戶從遠端登錄
		4.3.2.7	檔案系統需要授權特權
基本弱點		4.4.2	通訊埠掃描
		4.4.3	弱點掃描
		4.4.4	強健性模糊測試

註: 部分虛擬化架構的測試項目還在訂定中

6.3.2.2 5G 核心網路的產品資安確保標準

針對 5G 核心網路安全上的威脅，國際標準作法第三代合作夥伴計畫 (3GPP) 的安全性工作群組 (SA3 Security) 訂定一系列的 5G 核心網路產品資安確保標準 (Security Assurance Specification, SCAS)，如下：

表 19 核心網路產品資安確保標準 (SCAS)

核心網路元件	標準編號
用戶平面功能 (User Plane Function, UPF)	3GPP TS 33.513
存取與行動管理功能 (Access and Mobility management Function, AMF)	3GPP TS 33.512
連結管理功能(Session Management Function, SMF)	3GPP TS 33.515
認證伺服器功能 (Authentication Server Function, AUSF)	3GPP TS 33.516
統一資料管理功能 (Unified Data Management, UDM)	3GPP TS 33.514
網路資料庫功能 (Network Repository Function, NRF)	3GPP TS 33.518
網路揭露功能 (Network Exposure Function, NEF)	3GPP TS 33.519
安全邊緣防護代理 (Security Edge Protection Proxy, SEPP)	3GPP TS 33.517
非 3GPP 元件互通功能 (Non-3GPP Inter-Working Function, N3IWF)	3GPP TS 33.520*
服務通訊代理 (Service Communication Proxy, SECOP)	3GPP TS 33.522*
網路數據分析功能 (Network Data Analytics Function, NWDAF)	3GPP TS 33.521*

註*: 該技術標準開始制定，標準規格文件尚在制定中

依據 3GPP TS 33.513 (46) 技術標準規格之第 4.2.2 小節，用戶平面功能 (User Plane Function, UPF) 的行動通訊安全檢測項如下：

表 20 用戶平面功能的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.1	通過 N3 介面傳輸之用戶數據的機密性保護
4.2.2.2	通過 N3 介面傳輸之用戶數據的完整性保護
4.2.2.3	通過 N3 介面傳輸之用戶數據的重播保護
4.2.2.4	同一個陸地行動通信網路(PLMN)內通過 N9 介面傳輸之用戶數據的保護
4.2.2.5	傳訊數據保護
4.2.2.6	通道辨識碼 (Tunnel Identifier, TEID)的唯一性

依據 3GPP TS 33.512 (47) 技術標準規格之第 4.2.2 小節，存取與行動管理功能 (AMF) 的行動通訊安全測試項目如下：

表 21 存取與行動管理功能的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.1.1	同步失敗處置
4.2.2.1.2	RES* 驗證失敗處置
4.2.2.3.1	非存取層傳訊訊息的重播保護
4.2.2.3.2	非存取層無 (NULL) 完整性保護
4.2.2.3.3	非存取層完整性演算法的選擇與使用
4.2.2.4.1	避免 Xn 介面換手的降級威脅
4.2.2.4.2	存取與行動管理功能變更時非存取層保護演算法的選擇
4.2.2.5.1	5G 全球唯一識別符 (5G Globally Unique Identifier, 5G-GUTI) 配置
4.2.2.6.1	無效或不能接受的戶設備安全能力處置

依據 3GPP TS 33.515 (48) 技術標準規格之第 4.2.2 小節，連結管理功能 (SMF) 的行動通訊安全測試項目如下：

表 22 連結管理功能 (SMF) 的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.1.1	用戶平面之安全策略的優先順序
4.2.2.1.2	通道辨識碼 (TEID) 的唯一性
4.2.2.1.3	會話管理功能檢查用戶平面之安全策略的功能需求
4.2.2.1.4	計費識別碼的唯一性

依據 3GPP TS 33.516 (49) 技術標準規格認證伺服器功能 (AUSF) 的無行動通訊安全測試項目。依據 3GPP TS 33.514 (50) 技術標準規格之第 4.2.2 小節，統一資料管理功能 (UDM) 的行動通訊安全測試項目如下：

表 23 統一資料管理功能 (UDM) 的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.1	同步失敗處置
4.2.2.2	統一數據管理存儲的用戶設備身份驗證狀態

依據 3GPP TS 33.518 (51) 技術標準規格之第 4.2.2 小節，網路資料庫功能 (NRF) 的行動通訊安全測試項目如下

表 24 網路資料庫功能 (NRF) 的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.2.1	探索特定網路功能切片的授權

依據 3GPP TS 33.519 (52) 技術標準規格之第 4.2.2 小節，網路曝光功能 (NEF) 的行動通訊安全測試項目如下：

表 25 網路曝光功能 (NEF)的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.1.1	應用功能認證
4.2.2.1.2	北向應用程式介面的授權

依據 3GPP TS 33.517 (53) 技術標準規格之第 4.2.2 小節，安全邊緣防護代理功能 (Security Edge Protection Proxy, SEPP) 的行動通訊安全測試項目如下：

表 26 安全邊緣防護代理功能 (SEPP) 的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.2	正確處置安全邊緣防護代理功能 (SEPP) 和網際網路協定交換服務 (IP eXchange service, IPX) 提供者的加密材料
4.2.2.3	網際網路協定交換服務 (IPX) 提供者之特定連接範圍的加密素材
4.2.2.4	正確處理服務陸地行動通信網路識別碼 (PLMN ID) 不匹配問題
4.2.2.5	在原始 N32-fv 訊息中使用空 (NULL) 替換機密資訊元件 (IE)
4.2.2.6	正確處置保護策略不匹配問題
4.2.2.7	JavaScript 物件表示法網頁簽章 (JSON Web Signature, JWS) 組態限制
4.2.2.8	網際網路協定交換服務 (IPX)不會在 JavaScript 物件表示法 (JSON) 對像中誤植已加密的資訊元件 (IE)

6.3.2.3 5G 基地台集中單元的產品資安確保標準

由於集中單元 (CU) 的分封數據匯聚協定 (PDCP) 網路功能負責執行用戶平面 (user plane) 和控制平面 (control plane) 封包的完整性 (integrity) 和機密性 (confidentiality)，故 5G 基地台 (gNB) 的產品資安確保規範適用於 5G 基地台集中單元 (gNB-CU)。依據 3GPP TS 33.511 (57) 技術標準規格之第 4.2.2 小節，其行動通訊安全測試項目如下：

表 27 5G 基地台集中單元 (CU) 的行動通訊安全檢測項目總表

標準章節	測試項目
4.2.2.1.1	無線資源控制傳訊的完整性保護
4.2.2.1.2	用戶設備和基地臺間的用戶數據資料完整性保護
4.2.2.1.4	無線資源控制完整性檢查失敗
4.2.2.1.5	用戶平面完整性檢查失敗
4.2.2.1.6	無線資源控制傳訊加密
4.2.2.1.7	用戶設備和基地臺間的用戶平面資料加密
4.2.2.1.8	用戶設備與基地臺間的用戶數據資料重播攻擊保護
4.2.2.1.9	無線資源控制傳訊重播攻擊保護
4.2.2.1.10	基於連結管理功能傳送的安全策略對用戶平面資料進行加密
4.2.2.1.11	基於連結管理功能傳送的安全策略對用戶平面資料進行完整性保護
4.2.2.1.12	5G 基地台存取層加密和完整性演算法優先順序
4.2.2.1.13	5G 基地台金鑰更新
4.2.2.1.14	防範 Xn 介面交遞中的降階攻擊
4.2.2.1.15	於 5G 基地變更時存取層安全演算法選擇
4.2.2.1.16	控制平面資料在 N2 與 Xn 介面的機密性保護

4.2.2.1.17	控制平面資料在 N2 與 Xn 介面的完整性保護
4.2.2.1.18	雙連線的 5G 基地台金鑰更新

6.3.2.4 5G 多元應用服務的資安確保規範與標準

5G 多元應用服務的資安確保仰賴相關領域的資安標準與各區域的資安法規做規範。針對遠距醫療 (Telemedicine) 安全保護的部份，依據「智慧醫療關鍵議題與對策之研究」(58) 歸納出保護健康資訊技術所衍生隱私安全與權益如表 28 所示。

表 28 保護健康資訊技術所衍生隱私安全與權益 (58)

策略[1]	保護健康資訊技術所衍生隱私安全與權益
4.B.1	釐清關於安全保障、可性的健康資訊交換所需的期望與條件限制，必須與針對隱私安全的法規、個人偏好設定相符合
4.B.2	持續發展、管理、強化健康保險流通與責任法案 (HIPAA) 隱私與針對健康保險流通與責任法案 (HIPAA) 所涵蓋相關單位及商業夥伴的安全法規
4.B.3	在隱私適用的法規之下，持續強化健康保險流通與責任法案 (HIPAA) 不涵蓋單位對於安全隱私的條件限制
4.B.4	根據 ONC's Health IT Certification Program，將健康資訊科技產品進行認證檢測，確保符合隱私安全限制
4.B.5	制定並實施政策、行動措施與利用教學工具來促進系統互通性，使權益相關者對於維護隱私安全的部份具有信心
4.B.6	在開發技術使用時也需傳達網絡安全的疑慮
4.B.7	支持推廣並加強資訊的分享，如在公共健康單位間進行關於網路威脅議題雙向的資訊傳輸，或私人醫療照護機構與聯邦政府間的資訊漏洞
4.B.8	朝向一致的政策發展、利用電子技術紀錄下個人的偏好選擇，當個人有篩選資料需求時，能夠透過系統中統一的數據格式取得

註 1: 智慧醫療關鍵議題與對策之研究之策略編號

其中，隱私安全保護的部分需要符合各區域的法規，以最嚴苛的歐盟一般資料保護規範 (General Data Protection Regulation, GDPR) 為例，其清楚規範了與歐洲公民相關的各種個人資料收集、使用的權利。包含 200 多條規範的 GDPR 大致上可分為 8 個原則：取得限制 (Collection Limitation Principle)、資料質量 (Data Quality Principle)、確切目的 (Purpose Specification Principle)、使用限制 (Use Limitation Principle)、安全保障 (Security Safeguards Principle)、開放原則 (Openness Principle)、個體參與 (Individual Participation Principle)、責任原則 (Accountability Principle)。

針對智慧工廠的部分，因其採用工業物聯網 (Industry Internet of Thing, IIoT) 技術，讓許多系統中的設備都有連網能力。依據行政院資通安全處發布的「關鍵資訊基礎設施資安防護建議」(59)，為了有效處理整體安全議題以確保工業自動化和控制系統安全，就需要符合工業自動化控制系統 (Cyber Security for Industrial Automation and Control, IACS) 訂定的 ISA/ IEC 62443 標準如下。

表 29 ISA/ IEC 62443 標準 (59)

類別	標準編號	標準內容
共同(General)	62443-1-1	於 2007 年發行初版，內容介紹 62433 系列概念與模組。
	62443-1-2	說明 62443 系列所使用的專有名詞與名詞縮寫之技術報告。
	62443-1-3	描述 62443 系列基礎與系統之相關量化方法標準。
	62443-1-4	使用範例說明 IACS 元件層的生命週期安全技術報告。
政策與程序 (Policies and Procedures)	62443-2-1	此標準於 2009 年發行初版，內容要求與定義 IASC 網路安全管理系統，包含使用者與設備擁有者等相關權責。
	62443-2-2	提供 IASC 網路安全管理系統營運要求指引標準。
	62443-2-3	於 2015 年由 ISA 與 IEC 共同發表 IACS 之更新管理指引告。
	62443-2-4	對其他控制系統供應商的要求準則之標準。
系統要求(System Requirements)	62443-3-1	描述在 IACS 環境所使用的安全技術報告。
	62443-3-2	強調 IACS 系統安全設計與風險評估標準。
	62443-3-3	於 2013 年發行，針對系統安全與安全層級要求之標準。
元件要求 (Component Requirements)	62443-4-1	適用開發產品之要求標準。
	62443-4-2	對子系統、系統組成元件及其他控制系統供應商等列入系統規範要求之標準。

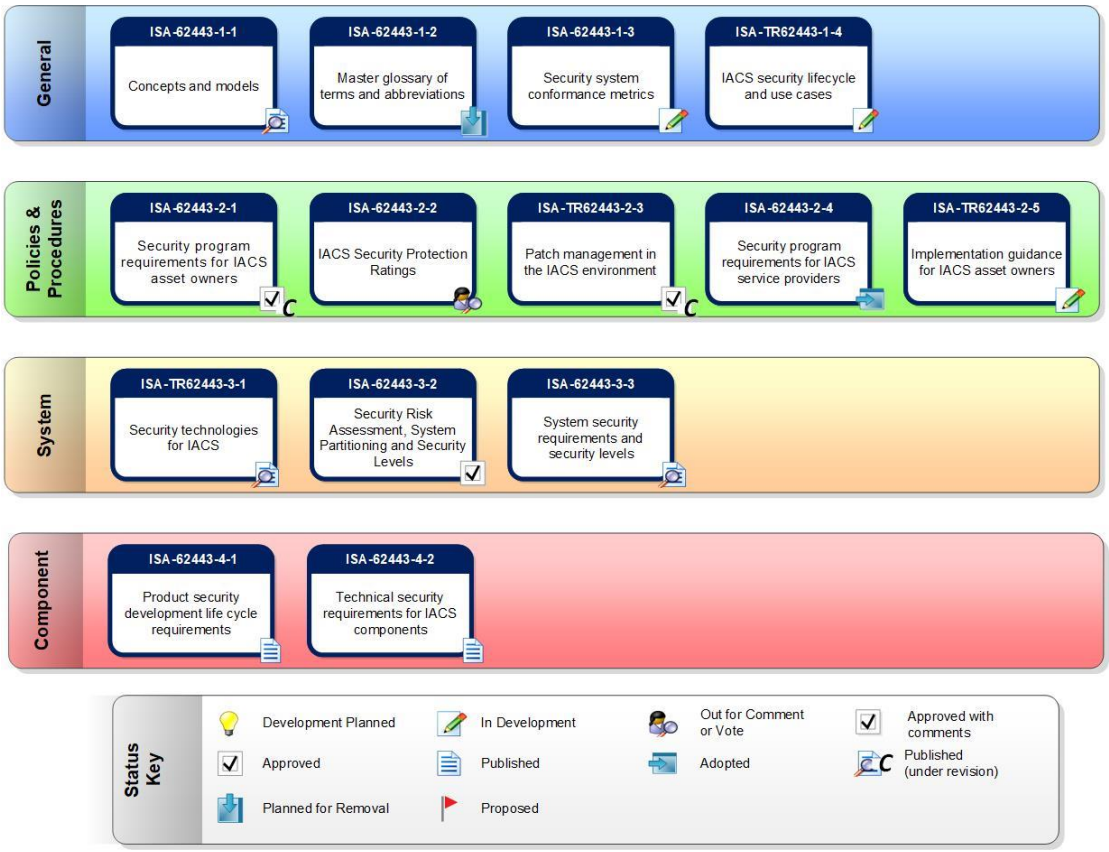


圖 42 ISA/ IEC 62443 的規格表 (59)

6.3.3 統整 5G 專網多接取邊緣運算的威脅與安全解決方案

針對5G專網多接取邊緣運算平台架構的5G核心網路元件、集中單元、傳輸網路、以服務基礎架構為導向之專網架構、5G 專網垂直應用、平台與網路虛擬層、平台架構以及應用服務的威脅與安全解決方案涵蓋資安確保技術統整於表 30。

表 30 5G 專網多接取邊緣運算平台的安全解決方案涵蓋資安確保技術

威脅種類	威脅細節	解決方案
5G 核心網路元件	用戶平面功能 (UPF)	需要讓核心網路元件滿足 5G 核心網路產品資安確保規範，來解決核心網路元件的資安問題。(見第 6.3.2.2 小節)
	存取與行動管理功能 (AMF)	
	連結管理功能(SMF)	
	認證伺服器功能 (AUSF)	
	統一資料管理功能 (UDM)	
	網路資料庫功能 (NRF)	
	網路揭露功能 (NEF)	
	安全邊緣防護代理 (SEPP)	

集中單元	集中單元 (CU)	需要讓核心網路元件滿足 5G 基地台集中單元的產品資安確保規範，來解決集中單元的資安問題。(見第 5.3.2.3 小節)
傳輸網路	傳輸網路 F1-C 介面	可以透過網際網路安全協定 (IP security protocol, IPsec)、傳輸層安全性協定(Transport Layer Security, TLS)、防火牆等防護技術阻止傳輸網路的資安問題。
	傳輸網路 F1-U 介面	
	傳輸網路 E1 介面	
	傳輸網路 N2 介面	
	傳輸網路 N3 介面	
	傳輸網路 N4 介面	
	傳輸網路 N9 介面	
以服務基礎架構為導向之專網架構	網路元件間傳訊資訊的機密性	以服務基礎之邊緣運算架構的資安問題仍然在討論中。(見第 6.2.2 小節)
	網路元件間傳訊資訊的完整性	
	網路元件間認證與授權	
	獨立佈建專網 (SNPN) 的驗證安全機制	獨立專網邊緣運算架構的資安問題仍然在討論中。(見第 6.2.2 小節)
	專網的認證和授權	
	時間敏感通訊的安全	
	5G 區域網路的安全	
	與公網整合專網 (PNiNPN) 之阻斷服務 (DoS)/分散式阻斷服務(DDoS) 攻擊	與公網整合專網邊緣運算架構的資安問題仍然在討論中。(見第 5.2.3 小節)
	與公網整合專網 (PNiNPN) 之閉架式群組 (CAG) 識別碼隱私性	
	專網和公網間交互工作、漫遊、使用獨立憑證進行驗證和授權	
	服務持續性和會談持續性的安全性和隱私性方面	
平台與網路虛擬層	模式 1：電信網路運營商從供應商處購買 3GPP 虛擬網路功能，並將其部署在第三方網路功能虛擬化基礎建設上。	需要讓核心網路元件滿足 5G 虛擬化架構的產品資安確保，來解決 5G 網路虛擬層的資安問題。(見第 6.3.2.1 小節)
	模式 2：電信網路運營商從供應商處購買 3GPP 虛擬網路功能和虛擬層，並部署在第三方硬體層上。	
	模式 3：電信網路運營商從供應商處購買和部署 3GPP 虛擬網路功能、虛擬層和硬體層。	
	平台虛擬層的安全威脅	需滿足 OpenStack 網路功能虛擬化 (OPNFV) 和 Kubernetes 網路功能虛

		擬化 (NFV) 的基本資安要求。
5G 專網垂直應用	未來工廠 (FoF)	5G 垂直領域應用服務的資安問題仍然在討論中 (見第 6.3.1.3 小節)，但多元應用服務本身仍然需要滿足如歐盟一般資料保護規範(GDPR)、健康保險流通與責任法案 (HIPAA) 與 ISA/ IEC 62443 標準等相關規範(見第 5.3.2.4 小節) 。
	無人飛行系統系統 (UAS)	
	車聯網 (V2X)	
	物聯網 (IoT)	
	遠距醫療 (Telemedicine)	
	虛擬/擴增實境 (VR/AR)	
平台架構	多接取邊緣運算本身威脅	採用 3GPP TS 33.117 (45) 通用安全保證規範的檢測機制確保產品的安全性。(見第 6.3.1.3 小節)
	在邊緣儲存的敏感性資產或資料	
	與多接取邊緣運算協調器進行通信的安全性	採用網路元件間傳訊資訊的機密性、完整性以及認證與授權的安全解決方案。(見第 6.2.2 小節)
	多接取邊緣運算部署的通信監察要求	
應用服務	邊緣運算應用程式 (MEC APP)	電信運營商要為邊緣應用伺服器 (EAS) 中的應用程式提供防禦惡意攻擊的服務，並檢查第三方應用程式的安全漏洞。(見第 6.3.1.3 小節)
	允許第三方應用程式影響網路	

6.3.4 制定 5G 專網多接取邊緣運算資安測試規範-通則

5G 專網多接取邊緣運算會因為 5G 垂直應用服務的差異而採用不同的網路架構，故未來針對 5G 專網多接取邊緣運算平台架構制定檢測規範時，因該先針對 5G 專網多接取邊緣運算的基本網路架構 (如圖 43 所示) 制定「5G 專網多接取邊緣運算資安測試規範-通則」，基本網路架構中之網路元件的威脅與資安確保技術統整於表 31。

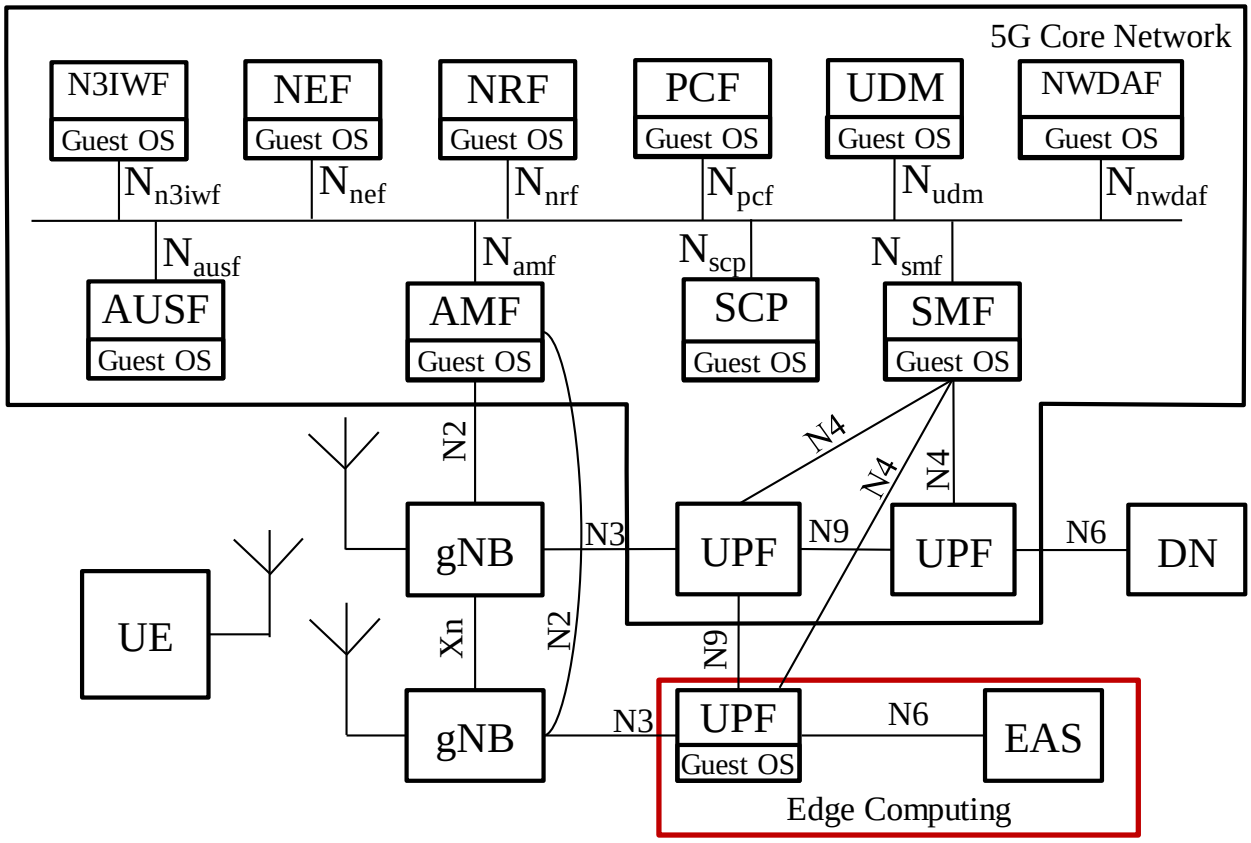


圖 43 5G 專網多接取邊緣運算基本網路元件架構示意圖

表 31 5G 專網多接取邊緣運算基本網路元件的威脅與資安確保技術

威脅種類	威脅細節	解決方案
5G 核心網路元件	用戶平面功能 (UPF)	滿足 5G 用戶平面功能 (UPF)產品資安確保規範。(見第 6.3.2.2 小節)
傳輸網路	傳輸網路 N2 介面	透過 IPsec、TLS、防火牆等防護技術阻止傳輸網路的資安問題。
	傳輸網路 N4 介面	
	傳輸網路 N9 介面	
平台與網路虛擬層	模式 1	滿足 5G 虛擬化架構的產品資安確保。(見第 6.3.2.1 小節)
	模式 2	
	模式 3	
	平台虛擬層的安全威脅	需滿足 OPNFV 和 Kubernetes NFV)的基本資安要求。
平台架構	多接取邊緣運算本身威脅	採用通用安全保證規範的檢測機制。(見第 6.3.1.3 小節)
	在邊緣儲存的敏感性資產或資料	
	與多接取邊緣運算協調器進行通信的安全性	可以採用網路元件間傳訊資訊的機密性、完整性以及認證與授權的安全解決方案。(見第 6.2.2 小節)
	允許第三方應用程式影響網路	

7. 結論與建議

本研究報告先探討 5G 專網多接取邊緣運算的系統架構，並收集與分析台灣現有 5G 專網多接取邊緣運算伺服器廠商的相關資料；從收集到的資訊來看台灣現有廠商的 5G 多接取邊緣運算平台架構為了互通性都支援第三代合作夥伴計畫的標準技術規格；而依據前述 5G 多接取邊緣運算平台的分析結果來看，其採用 OpenStack 或 Kubernetes 網路功能虛擬化的架構，且依相關技術標準規格網路架構可以分為「獨立佈建多接取邊緣運算網路架構」以及「與公網整合多接取邊緣運算網路架構」兩類；透過前述的 5G 專網多接取邊緣運算網路架構，得以實現未來工廠、無人飛行系統系統、車聯網、物聯網、遠距醫療以及虛擬與擴增實境等各種垂直應用服務。為了確保前述 5G 專網多接取邊緣運算平台間的互通性與服務性能一致性，建議未來可以進一步導入第三代合作夥伴計畫訂定的垂直服務致能架構層以及啟用邊緣應用程序架構標準規範。

針對前述 5G 專網多接取邊緣運算平台的資安風險分析結果，本研究報告可以歸納出八大類安全面向的威脅，同時於報告中統整相關的安全解決方案，供 5G 專網系統整合商與 5G 專網多接取邊緣運算伺服器製造商因應布建時會面臨的安全威脅。其中，關於 5G 核心網路元件、集中單元、傳輸網路、與網虛擬層等 5G 網路功能的安全威脅，建議可以參考第三代合作夥伴計畫訂定的相關標準規範中的安全解決方案；但為了確保設備商在實作相關網路產品的安全標準規範落實度，就需要藉由 5G 虛擬化架構與 5G 核心網路以及 5G 基地臺等資安確保標準 (SCAS) 來驗證。而關於應用服務的安全威脅部分，建議服務營運商在提供 5G 專網垂直領域應用服務時有必要建立安全評估機制，來評估邊緣應用伺服器中應用程式的安全性，以及應用程式和網路間應用程式介面通訊安全；此外，該安全評估機制同時需要納入相關垂直領域的資安規範，如歐盟一般資料保護規範 (GDPR)、健康保險流通與責任法案 (HIPAA) 與 ISA/ IEC 62443 標準等，以確保垂直領域應用服務的安全合規性。

從前述的資訊來看台灣工業電腦與伺服器廠商積極投入 5G 專網多接取邊緣運算的市場，且 5G 應用服務商也透過 5G 專網多接取邊緣運算技術實現各種垂直應用服務。由於目前台灣缺乏 5G 專網多接取邊緣運算網路架構以及 5G 垂直應用服務的資安標準規範，故建議未來應該先依據 5G 專網多接取邊緣運算 (MEC) 的基本網路架構，制定「5G 專網多接取邊緣運算資安測試規範-通則」，以協助台灣伺服器廠商與檢測實驗室

建立 5G 專網多接取邊緣運算的資安檢測能量。最後，期望 5G 垂直應用服務商與電信事業未來在營運時，能夠透過本研究報告獲得 5G 專網多接取邊緣運算的基本資安防護知識，以確保 5G 專網多接取邊緣運算與垂直應用服務的安全性。

參考資料

(1) 3GPP enables MEC over a 5G core, Sami Kekki & Alex Reznik, ETSI ISG MEC (https://www.3gpp.org/news-events/partners-news/1969-mec)
(2) 我國 5G 頻譜政策與專網發展，行政院科技會報辦公室，台灣
(3) MEC in 5G networks (https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf)
(4) Developing Software for Multi-Access Edge Computing (https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp20ed2_MEC_SoftwareDevelopment.pdf)
(5) 3GPP TS 22.261-h30 Service requirements for the 5G system; Stage 1 (Release 17)
(6) 3GPP TS 23.501-g51 System Architecture for the 5G System (5GS); Stage 2 (Release 16)
(7) 3GPP TR 21.905-h00 Vocabulary for 3GPP Specifications (Release 16)
(8) 3GPP TS 38.401-g20 NG-RAN; Architecture description (Release 16)
(9) 3GPP SA6 initiatives to enable new vertical applications
(10) 3GPP TS 23.222-h10 Common API Framework for 3GPP Northbound APIs (Release 17)
(11) 3GPP TS 29.522-g40 Network Exposure Function Northbound APIs (Release 16)
(12) 3GPP TS 26.348-g30 Northbound Application Programming Interface (API) for Multimedia Broadcast/Multicast Service (MBMS) at the xMB reference point (Release 16)
(13) 3GPP TS 23.434-g40 Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows (Release 16)
(14) 3GPP TS 23.286-g30 Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows
(15) 3GPP TR 23.755-090 Study on application layer support for Unmanned Aerial Systems (UASAPP)
(16) 3GPP TR 23.745-090 Study on application layer support for Factories of the Future in the 5G network
(17) IEEE 802.1Qcc-2018 - IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks -- Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements

(18) IEEE 802.1AS-2020 - IEEE Standard for Local and Metropolitan Area Networks--Timing and Synchronization for Time-Sensitive Applications
(19) IEEE 802.1Qbv-2015 - IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic
(20) IEEE 802.1CB-2017 - IEEE Standard for Local and metropolitan area networks--Frame Replication and Elimination for Reliability
(21) Intel® Smart Edge (https://www.intel.com.tw/content/www/tw/zh/design/technologies-and-topics/edge-cloud-computing/smart-edge-software.html)
(22) Enabling the Deployment of Edge Services with the Open Network Edge Services Software (OpenNESS), Intel (https://www.slideshare.net/LizWarner6/enabling-the-deployment-of-edge-services-with-the-open-network-edge-services-software-openness-toolkit)
(23) 英特爾揪伴攻，經濟日報，台灣 (https://udn.com/news/story/7240/4233119)
(24) 多接取邊緣運算之用戶辨識技術，財團法人工業技術研究院，台灣 (https://ictjournal.itri.org.tw/content/Messagess/contents.aspx?PView=1&KeyWord=&SiteID=654246032665636316&MmmID=654304432061644411&SSize=10&MSID=10351440154701346 51)
(25) 5G 多接取邊緣運算(MEC)平台，技嘉科技股份有限公司，台灣 (https://www.gigabyte.com/tw/Solutions/Networking/5g-imec-networking-platform)
(26) 在行動邊緣運算(MEC)中的應用，凌華科技股份有限公司，台灣 (https://www.adlinktech.com/tw/OCCERA_Applications_for_MEC)
(27) Security in 5G RAN and core deployments, Ericsson (https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments)
(28) Advantech Edge Solutions: Empowering 5G Patrol Robots, 研華科技股份有限公司，台灣 (https://www.advantech.tw/resources/case-study/advantech-edge-solutions-empowering-5g-patrol-robots)
(29) 5G PPP Phase1 Security Landscape - Produced by 5GPPP Security WG, EU
(30) 「推動 5G 垂直應用場域實證規劃、法規調適暨資安法規整備計畫」之細部計畫二「5G 釋照之先期資通安全法規整備計畫」期末報告補正版，財團法人電信技術中心，台灣 (https://www.grb.gov.tw/search/planDetail?id=13215614)

(31) 3GPP TS 33.501-g30 Security architecture and procedures for 5G system (Release 16)
(32) 公有雲解決方案，中華電信，台灣 (https://www.cht.com.tw/home/campaign/gxc/c4/public-cloud/solution-1.html)
(33) 3GPP TR 33.855-g00 Study on security aspects of the 5G Service Based Architecture (SBA) (Release 16)
(34) 3GPP TR 33.848-050 Study on Security Impacts of Virtualisation (Release 16)
(35) 3GPP TR 33.818-070 Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products (Release 16)
(36) ETSI GS NFV-SEC 001 V1.1.1 Network Functions Virtualisation (NFV); NFV Security; Problem Statement
(37) 3GPP TR 33.926-g30 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (Release 16)
(38) 3GPP TR 33.861-g00 Study on evolution of Cellular IoT (CIoT) security for the 5G System; (Release 16)
(39) 3GPP TR 33.836-g00 Study on security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services (Release 16)
(40) 3GPP TR 33.825-g01 Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System (5GS) (Release 16)
(41) 5G security – Package 3 Mobile Edge Computing/Low Latency/Consistent User Experience, NGMN (20 February 2018)
(42) 3GPP TR 32.842-d10 Study on network management of virtualized networks (Release 13)
(43) 3GPP TS 33.122-g30 Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs (Release 16)
(44) 3GPP TS 33.434-g00 Service Enabler Architecture Layer (SEAL); Security aspects
(45) 3GPP TS 33.117-g50 Catalogue of general security assurance requirements (Release 16)
(46) 3GPP TS 33.513-g10 5G Security Assurance Specification (SCAS); User Plane Function (UPF) (Release 16)
(47) 3GPP TS 33.512-g20 5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF) (Release 16)
(48) 3GPP TS 33.515-g10 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class (Release 16)

(49) 3GPP TS 33.516-g10 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class (Release 16)
(50) 3GPP TS 33.514-g10 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class (Release 16)
(51) 3GPP TS 33.518-g10 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class (Release 16)
(52) 3GPP TS 33.519-g10 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class (Release 16)
(53) 3GPP TS 33.517-g10 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class (Release 16)
(54) 3GPP TS 33.520-010 Security Assurance Specification for Non-3GPP InterWorking Function (N3IWF) (Release 17)
(55) 3GPP TS 33.522-020 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP) (Release 17)
(56) 3GPP TS 33.521-010 Security Assurance Specification (SCAS) for the Network Data; Analytics Function (NWDAF) network product class; (Release 17)
(57) 3GPP TS 33.511-g40 5G Security Assurance Specification (SCAS); NR Node B (gNB) (Release 16)
(58) 智慧醫療關鍵議題與對策之研究, 國立臺灣大學, 台灣
(59) 關鍵資訊基礎設施資安防護建議, 行政院資通安全處, 台灣

版本修改紀錄

版本	時間	摘要
v1.0	2021/01/07	出版

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw