5G開放架構網路端對端整合營管

作者/霍冠樺、徐鈺澄、張昇賀、邱祈榮

提要

一、5G網路通訊技術巨幅影響軍事作戰能力，但傳統行動網路屬封閉式網路架構，[1]造成「供應商綁定」(Vendor Lock-in)的現象。若軍方建置5G企業專網，將被限制與其他廠商合作發展軍事通訊技術應用的空間。

二、5G行動網路架構採開放式架構，將傳統網路架構解構成不同的網路元件。藉由定義每一個網路元件間的開放通訊介面，讓不同的設備供應商的設備彼此間可以互相溝通交流，驅動設備製造商在O-RAN和5GC投入更多研究與開發資源，降低供應的風險，並促進國軍5G技術於軍事領域的發展。

三、本文提出一種新型監控整合系統，確保5G開放架構整體運作狀態、服務效能及資訊安全，提升運行5G開放網路之維運效率。

關鍵詞：5G開放架構網路、5G核心網路、營運維運管理系統、網路管理系統

前言

5G網路通訊技術具備大連結、高速率和低延遲的特性，不僅改變產業與生活應用，進而影響軍事作戰能力，例如無人機偵查、作戰、攻擊和防禦，以及車聯網、車隊管理等。

5G企業專用網路是指在企業場域內建置部署企業的行動網路，企業內部可共享資訊、操作系統及各種應用程式的服務(APP)。企業在此特定區域範圍內，5G行動用戶或裝置(終端設備)連上基站(Base Station)，基站內包含多個基地台(Cell)，通常僅限企業內部員工或特定裝置使用，非企業相關人員及設備需透過身分認證或授權，才能使用企業專網的資源，是企業內部獨立運作的行動網路。企業專網具備資訊安全和獨立運作兩大優勢。在資訊安全方面，提供更完整安全性與網路控制權，並將企業網路與公用網路隔離，保障企業的資訊安全。在獨立性方面，企業專網可以獨立運作，又能依據工作場域不同需求，設置不同的網路功能，更能彈性化調整。

1 〈5G Moves towards Open and Interoperable Network Architecture〉，《Edge-core Networks》，https://www.edge-core.com/news-inquiry.php?cls=3&id=514 closed-type network，2020年7月16日，(檢索日期：2023年6月15日)

5G企業專網使用頻段分為「共頻專網」和「專頻專網」。共頻專網就是5G企業專網和公網使用同一個頻段，即電信業者向政府競標取得5G專網商用的頻段。專頻專網則使用政府釋出特定頻譜上建立專用網路，獨立於公共網路使用的商用頻段。[2]專用網路與公共網路實體隔離，不受公網影響，確保通訊品質，也避免機敏資料外流風險。我國數位發展部開放4.8至4.9GHz頻段供企業申請5G專頻專網。為了推動5G創新應用發展，執照申請後可使用10年，前兩年有零至四折優惠，第三年是六折優惠，第四年是八折優惠。[3]根據規劃，5G專網每MHz 1,326元乘上頻寬，再乘上折扣係數，以建物投影面積算場域係數，再加管理費3.3萬元，每一個單位、每年頻譜使用費僅3萬至5萬元。[4]依據使用經驗，一般企業一年的費用約十幾萬元。

5G企業專網有四種建置方式，分別為混合建置(共享型/專用型)、獨立建置和網路切片(架構整理如圖1)：[5]

一、混合建置(共享型/專用型)

藉由多接取邊緣運算(Mobile/Multi-access Edge Computing, MEC)技術實現5G高速率、低延遲和大連結的三大特性。先在企業內部建置專屬基地台，再透過MEC技術將資料運算、儲存和應用程式設置在最靠近企業端的行動網路邊緣，5G行動用戶不需等待遠端運算的回應，經由前置處理縮減資料量後，僅將少量且必要的資料傳送給遠端的運算中心處理，解決傳遞資料延遲的問題。混合建置共享型為多家企業共用MEC，每家企業可選擇使用專屬或共用基地台；專用型則企業有專屬的MEC和基地台。

二、獨立建置

在企業內部場域直接部署專用基地台和專用核心網路，透過專用核心網路將網路訊務傳送至企業端網路。此方式不需與其他企業共用核心網路，是獨立5G企業專網，安全等級最高。

三、網路切片

5G網路服務初期仰賴LTE 4G網路基礎建設，核心網路採用非獨立(Non-Standalone, NSA)架構，但獨立(Standalone,SA)核心網路架構才提供網路切

2 蘇文彬，〈Gb級5G來了，企業架構無線內網有新方法〉《iThome》，https://www.ithome.com.tw/news/138728，2020年7月10日，(檢索日期：2023年8月8日)

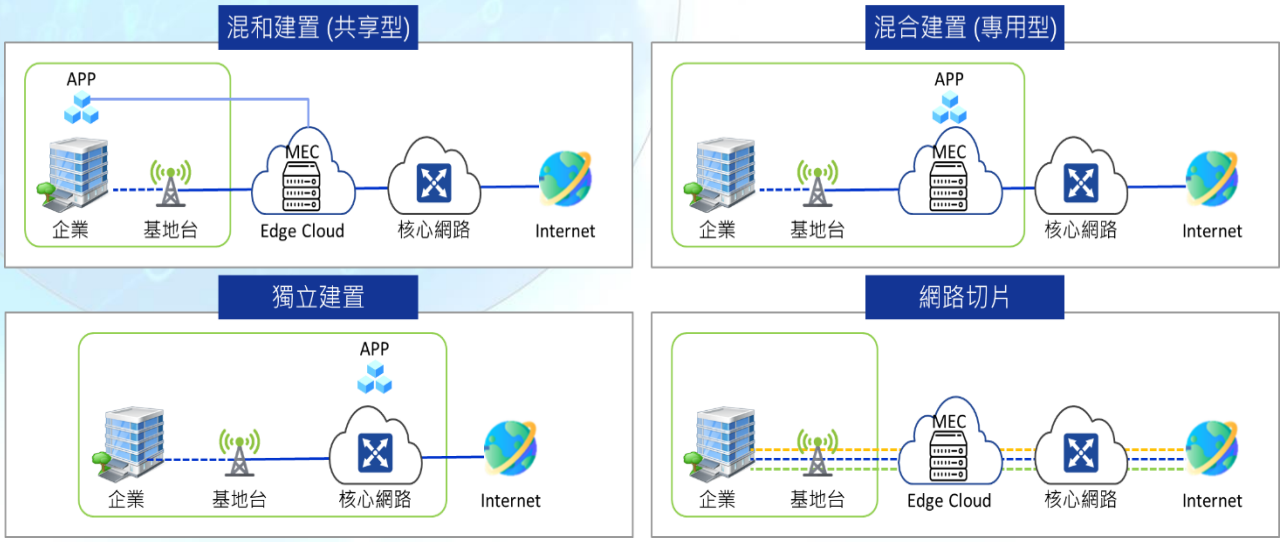
3 馬瑞璿，〈5G專頻專網辦法正式上路 數位部：6月5日開始受理申請〉《經濟日報》，https://money.udn.com/money/story/5612/7208779，2023年6月2日，(檢索日期：2023年8月8日)

4 小丰子3C俱樂部，〈5G專網頻率使用費將大打折，有用嗎?〉《小丰子3C俱樂部》，https://tel3c.tw/blog/post/40183，2023年6月2日，(檢索日期：2023年8月8日)

5 中華電信，〈企業專網〉《中華電信》，https://www.cht.com.tw/home/enterprise/mobile/5genterprise/712，(檢索日期：2023年7月31日)

片功能。網路切片技術是在實體網路上建立多個邏輯網路，每個切片均互相隔離，達到高資安的特性。[6]

圖1　5G企業專網實現方式



資料來源：作者繪製(整理)

另外，攜帶式5G企業專網可以滿足機動式通訊需求，將應用在防救災、軍事演習、軍事作戰等，或者緊急部署情境，如大型研討會、展場、大型活動、演唱會等(攜帶式5G企業專網架構圖如圖2)，將軟體式的MEC和核心網路建置在伺服器上，再將伺服器和軟體定義網路(Software-Defined Networking, SDN)交換器裝載入攜行箱，置於行動車上。

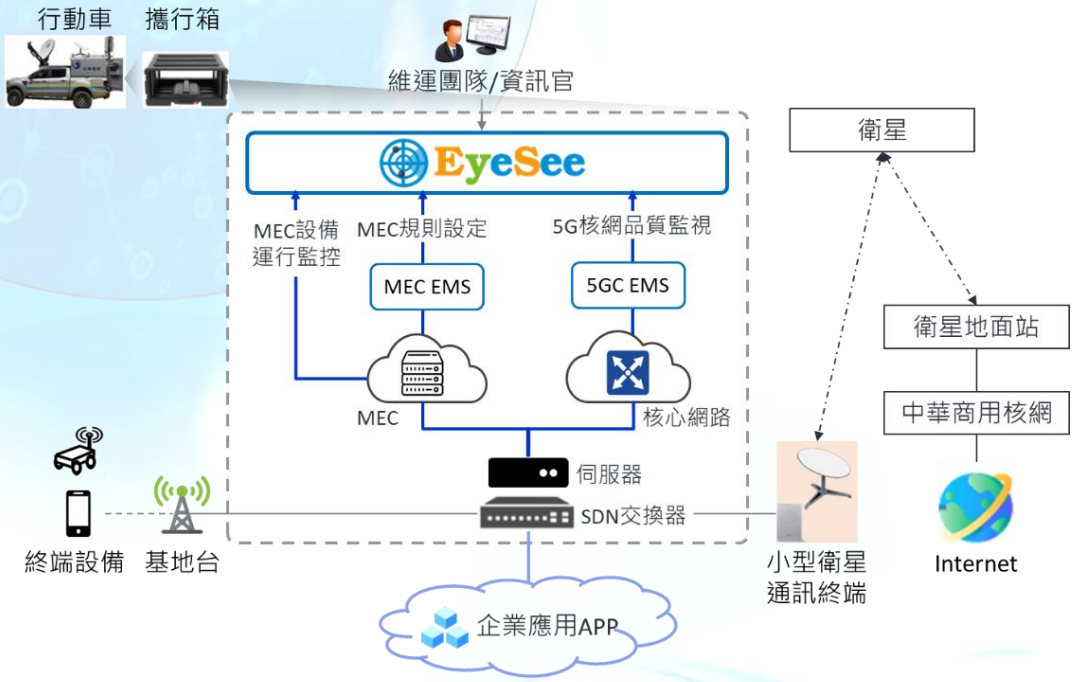
隨著基礎網路設施技術不停演進與升級，驅使網路發展從傳統4G封閉式網路，邁向5G開放式網路架構(如圖3)。在5G核心網路中，有一個相當關鍵的重要特徵，就是服務導向的架構(Service-based Architecture)。它讓不同的網路功能(Network Functions)之間透過基於表現層狀態轉移(Representational State Transfer)介面(REST-based Interface)能互相通訊交流。[7]由此看來，將一個較大的網路功能，解耦成更多、更小、更特定的功能用途，具體實現開放式的5G核心網路。其他系統也能藉著這些標準的介面連接至5G核心網路。關於傳統接取網路(Radio Access Network, RAN)的部分，也轉變為開放式

6 中華電信，〈中華電信推出5G 獨立式組網(SA)服務 提供更多元的垂直場域應用 加速產業升級〉《中華電信》，https://www.cht.com.tw/zh-tw/home/cht/messages/2021/1019-1440，2021年10月19日，(檢索日期：2023年7月31日)

7 Alan Weissberger，〈5G Security explained: 3GPP 5G core network SBA and Security Mechanisms〉《IEEE Communications Society》，https://techblog.comsoc.org/2022/01/01/5g-network-security-threats-and-3gpp-security-mechanisms/，2022年1月1日，(檢索日期：2023年6月16日)

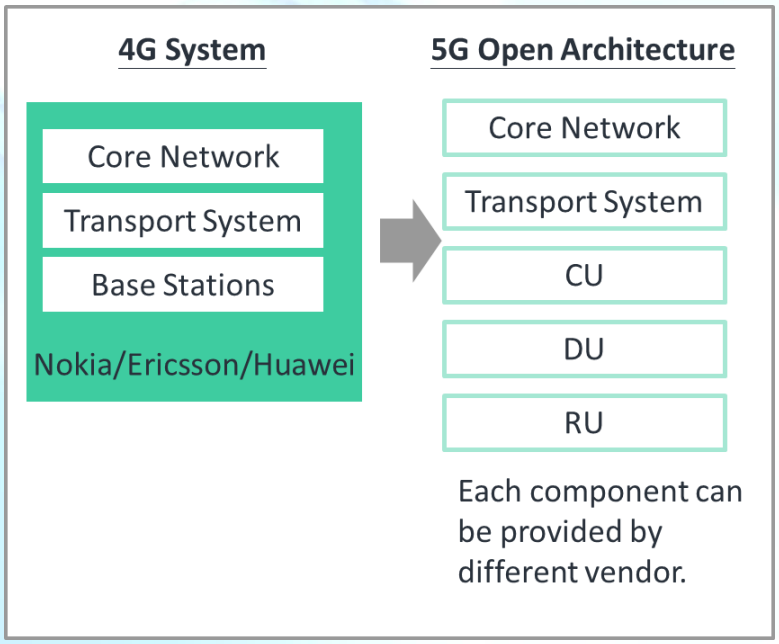
接取網路(Open RAN, O-RAN)，這是一種虛擬化的開放式架構。這種架構將基站切分為無線電單元(Radio Unit, RU)、分布單元(Distribution Unit, DU)和中央單元(Central Unit, CU)，正因如此，軟體、韌體和硬體全部皆能獨立且分離。

圖2　攜帶式5G企業專網架構圖



資料來源：作者繪製(整理)

圖3　4G與5G架構的轉變



資料來源：作者繪製(整理)

5G核心網路和開放式接取網路透過網路功能虛擬化架構(Network Function Virtualization Infrastructure)，整合各式各樣的網路元件。不同網路元件之間使用開放通訊介面，讓不同設備供應商所製造的設備彼此間能互相通訊，避免「供應商綁定」情況。觀察美國軍方也積極與業界合作發展5G開放架構網路，推動5G Open RAN生態系統發展。故5G開放式架構除了大幅降低資本支出外，還能使供應鏈更加多樣化，[8]促進國軍與多家廠商合作發展各種軍事技術的機會與可能性。

然而，我們發現擁有虛擬化特性的5G開放式網路，有可能造成多個網路元件分散於不同的實體地點，同時需整合多家廠商的網路元件，推升管理的困難度與複雜度。而且在開放的架構下，可能出現更多的安全漏洞，嚴重暴露資安隱憂。所以我們的研究目標期望解決在5G開放架構網路中如何整合管理多家廠商、多種網路元件和資安管理問題。例如能快速查詢各家廠商和各種設備的健康度、監控指標、統計分析、歷史趨勢報表，以及進行障礙偵測、事件告警通知等。於是，我們提出了一個EyeSee系統，是一個5G開放架構網路端對端整合營管系統，藉由建立通用的資料儲存框架，並將關鍵指標參數作正規化處理，提供網路元件的拓撲圖、即時品質、運行狀態和歷史紀錄等資訊。再用跨域障礙整合日誌收容不同的告警資料，提供5G專網相關共十五項告警項目。另外，整合資安檢測工具，呈現資安檢測報告。總之，EyeSee管理三家廠商的網路元件，提供Level 1儀表板及Level 2的監測報表，統整所有監控資訊、告警功能和資安檢測報告，解決維運團隊或國軍資訊官的5G專網維運管理問題與資安議題。

國際5G專頻專網政策

一、德國

主管機關配發3.7至3.8GHz頻段作為區域型網路服務使用，補充全區5G網路涵蓋不足，而無法兼顧區域或地方產業的需求。性質上，較屬於區域型公眾電信網路

二、法國

法國政府核發2.6GHz (TDD)頻段(2570-2620)作為行動專用電信網路，提供特定垂直應用場域之企業或組織使用，例如特定5G應用情境的連線需求

8 關河鳴，〈5G Open-RAN與台灣的機會認識5G專網與公網〉《農業數位學堂》，https://www.intelligentagri.com.tw/files/file_pool/1/0L229531656944067938/%284-2%29%E8%AA%8D%E8%AD%98%205G%20%E5%B0%88%E7%B6%B2%E8%88%87%E5%85%AC%E7%B6%B2.pdf，2021年8月16日，(檢索日期：2023年6月16日)

。此網路專門提供給企業應用，並非一般公眾電信服務。

三、日本

日本則開放4.6至4.9GHz和28.2至29.1GHz作為特定地區5G執照使用(稱之為Local 5G)。與日本全國性電信採用的5G不相同，Local 5G以地區的企業或政府為主。

四、香港

香港政府規劃「地區性無線寬頻服務執照」，在26/28GHz頻段釋出400MHz頻寬(27.95-28.35GHz)，讓特定區域、特定用戶群，以5G或其他先進技術提供創新無線寬頻服務使用，同時禁止一般大眾行動服務，如行動語音、行動寬頻等。[9]

各國5G網路軍事應用概況

一、美國

美國國防部於2020年「5G戰略及實施計畫」[10]中，提出5G應用願景及實施規畫，並與民間合作，啟動12座軍事基地之5G試驗，強調未來戰爭將應用5G網路傳輸大量資料，可連結士兵、武器、感測器等，能透過演算法協助指揮官進行更佳的環境狀況理解與技術戰略調整。同時，美國也注意到敵對國家在夥伴國家5G市場的影響力，而且透過供應鏈、惡意程式等方式，對網路資安造成威脅。

5G戰略設定三大目標，包括提升美國及相關夥伴之5G能力、對5G風險的關注提升至國家安全層級和發展可保障5G基礎設施及技術之方法。

5G戰略提出的四項實施要點：

(一)促進技術發展

包含進行5G試驗、發展毫米波、動態頻譜共享、開放架構、培育人才等。

(二)針對5G弱點進行評估、減輕與運行

含威脅情資、最小化5G基礎設施風險、全球行動、資安評估、零信任等。

(三)影響5G標準及政策

9 國家通訊傳播委員會，〈行動寬頻專用電信網路(4.8-4.9GHz)政策諮詢文件〉《國家通訊傳播委員會》，https://www.ncc.gov.tw/chinese/files/21041/54_45934_210413_1.pdf，2021年4月，(檢索日期：2023年8月8日)

10工商時報，〈美國防部推5G戰略 提升軍民雙邊能量〉《工商時報名家評論》，https://view.ctee.com.tw/technology/49428.html，2023年4月12日，(檢索日期：2023年7月27日)

包含標準組織參與、頻譜管理、5G應用操作概念、技術控制措施等方向。

(四)協同合作夥伴

包含同盟國及夥伴國、產業、國會等合作。

美國國防部5G戰略的實施要點中，5G試驗為重要施行環節，期望5G技術未來可以更快、更低成本的方式進行部署。軍事相關的5G試驗採分期分階段進行，於2019年底至2020年在5座軍事基地推動第一期的試驗計畫。目前第一期計畫大多完成第一階段解決方案開發和原型開發等內容，並延長合作廠商合約，進行第二、第三階段作業，例如解決方案調整、部署測試等。美國國防部於2020年中宣布於7座軍事基地進行第二期的試驗計畫，目前尚在第一階段。前兩期計畫多以推動軍民合作5G研發為主，並以訓練、後勤為主要應用情境，如C-17運輸機的虛擬實境訓練(Virtual Reality Training)、倉儲物流等。[11]由5G和VR構成高速網路虛擬實境系統，有效整合遠端的人機介面，大幅度提升虛擬實境的軍事實用性，而且遠端操控的無人載具的戰場應用在未來更具潛力。而5G高速寬頻網路進行倉儲物流測試，以加速後勤補給作業流程。

此外，開放架構網路為其技術發展目標之一，與業界合作推動開放架構網路發展，亦能作完整資安評估。透過試驗計畫，為5G核網、邊緣系統、無線接取和網路切片技術，提出更安全的設計。美國國防部與國家電信暨資訊管理局(NTIA)於2022年3月發起「5G挑戰」活動，促進5G Open RAN生態系統發展。

美國國防部除了重視5G開放架構網路外，資安計畫也是發展重點之一，並將5G風險提升至國家安全層級，關注程度可見一斑。

二、中共

中共工信部於2019年發放5G牌照，為中共5G商用元年，[12]積極布局5G應用與技術。中共5G應用揚帆行動計畫顯示中共大力推動5G的全面發展，並且推進深入各行各業。[13]2023年中共國際信息通信展覽會中國電信展示5G網聯無人機駕駛艙互動體驗區，觀眾體驗坐在北京的無人機駕駛艙內，觀看全國

11蘇紫雲，〈美國防部啟動軍用5G測試與產業合作〉《國防安全雙週報》，https://indsr.org.tw/respublicationcon?uid=12&resid=756&pid=2847，2020年1月31日，(檢索日期：2023年7月27日)

12中國新聞網，〈【十年中國風】“5G+萬物”，中國人闖出數字生活新天地〉《人民網》，http://finance.people.com.cn/BIG5/n1/2022/1004/c1004-32539375.html，2022年10月4日，(檢索日期：2023年7月28日)

13工信部聯通信，〈5G應用“揚帆”行動計劃〉《工業和信息化部網站》，http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/zhengceku/2021-07/13/content_5624610.htm，2021年7月5日，(檢索日期：2023年7月28日)

各地的美景。2023年世界行動通訊大會中國聯通展示5G無人機巡檢、擴增實境(Augmented Reality, AR)遠端協助等應用。[14]

事實上，中共的5G網路技術與國家軍民融合戰略息息相關，[15]觀察中興通訊、中國聯通、中國航天科工集團等關鍵行業皆為5G技術軍民融合應用產業聯盟的一員，在促進軍事及民用發展的同時，也能促進國防和商業應用。中共5G的發展進程可能與其極權統治和國防訊息化戰略相關，並應用人工智慧(Artificial Intelligence, AI)技術，改善中共軍隊指揮自動化系統能力，實現軍事智能化。例如，珠海一家生產無人艇的民營企業，成功轉型為無人艇反潛，想進一步實現無人艇為攻航母。[16]

三、南韓

南韓自從5G商轉後，也積極發展軍事應用，[17]如發展無人機沿海搜索和營地安全。目前無人機僅作為眼睛的輔助應用，希望能導入AI與大數據技術，實現軍事補給和攻擊、防禦等應用。南韓國防部與LG Uplus計畫展開無人地雷清除的研究項目，解決極度危險的地雷搜索清除任務。

5G也加速虛擬實境(Virtual Reality, VR)和AR在軍事領域的應用。韓國陸軍士官學校與SK Telecom發展VR的精確射擊訓練模擬器，例如特殊氣候或環境等訓練，提高單兵和部隊作戰能力。AR眼鏡可協助指揮官做最佳決策，提供各種作戰區域的地形、建築物、各方訊息等。

5G網路整合管理系統現況

本節介紹兩個5G企業專網整廠輸出方案(Turnkey Solution)及一篇亞太地區網路研究與管理論壇國際學術研討會(Asia Pacific Network Operations and Management Symposium, APNOMS)論文。

第一個整廠輸出方案是Celona，於2020年11月推出企業專網平台，[18]目標是讓4G/5G企業專網能像Wi-Fi一樣容易部署和使用。Celona整合企業專網所

14經濟參考報，〈5G：從“建得好”向“用得好”加速升級〉《新華網》，http://big5.news.cn/gate/big5/www.xinhuanet.com/tech/20230703/e499367af8264e46b3aec8b80f758917/c.html，2023年7月3日，(檢索日期：2023年7月28日)

15李清怡，〈為什麼中共想在下一代5G技術上擊敗美國？〉《新紀元》，https://www.epochweekly.com/b5/623/19344.htm，2019年3月6日，(檢索日期：2023年7月31日)

16黃皓頤，〈金一南看5G的軍事戰略意義 指揮無人機無人艇和機器人〉《中國文化研究院》，https://www.ourchinastory.com/zh/2912，2021年11月24日，(檢索日期：2023年7月31日)

17盧碧瑩，〈南韓5G提升軍事作戰能力：電信營運商與軍方合作〉《科技政策研究與資訊中心》，https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=15517，2019年4月26日，(檢索日期：2023年6月29日)

18Celona，〈PRIVATE WIRELESS FOR THE ENTERPRISE〉《Celona》，https://www.celona.io/，(檢索日期：2023年6月17日)

需的軟硬體資源，使企業能「一站式」購足企業專網所需的設備。整廠輸出方案包含SIM卡、RAN、Edge和Orchestrator。Celona的Orchestrator提供使用者監控企業專網運作品質。

第二個整廠輸出方案是Ananki，於2021年9月從開放網路基金會(Open NetworkFoundation, ONF)分拆出來的新公司。[19]Ananki成立的目的是整合ONF開源解決方案，協助企業佈建5G企業專網。開源專案包括Aether、軟體定義RAN (Software-Defined RAN, SD-RAN)、軟體定義網路架構(Software-Defined Fabric, SD-Fabric)和軟體定義核心網路(Software-Defined Core, SD-Core)，涵蓋企業專網的基站、核心網路、傳輸網路和網管功能。整廠輸出方案包含SIM卡、小型基地台(Small Cell)、儀表板(Dashboard)，只要簡單的步驟就可完成安裝。

Celona Orchestrator和Anaki 儀表板都是網路管理系統，提供端對端(End-to-End)的整合監控。不同於這兩個整廠輸出方案，我們所提出的解決方案整合資安檢測工具，監控運行平台的資訊安全。此外，我們亦將監控延伸至終端設備，進一步掌握多元終端設備的運作品質。

5G Open RAN的網管系統設計(Design of a Network Management System for5G Open RAN)，[20]是2021年於APNOMS發表的論文，我們提出一個利用O-RAN網路管理系統(Network Management System, NMS)平台監控多種廠牌的Open RAN基站。

5G開放架構網路端對端整合營管系統-EyeSee

一、EyeSee系統概述

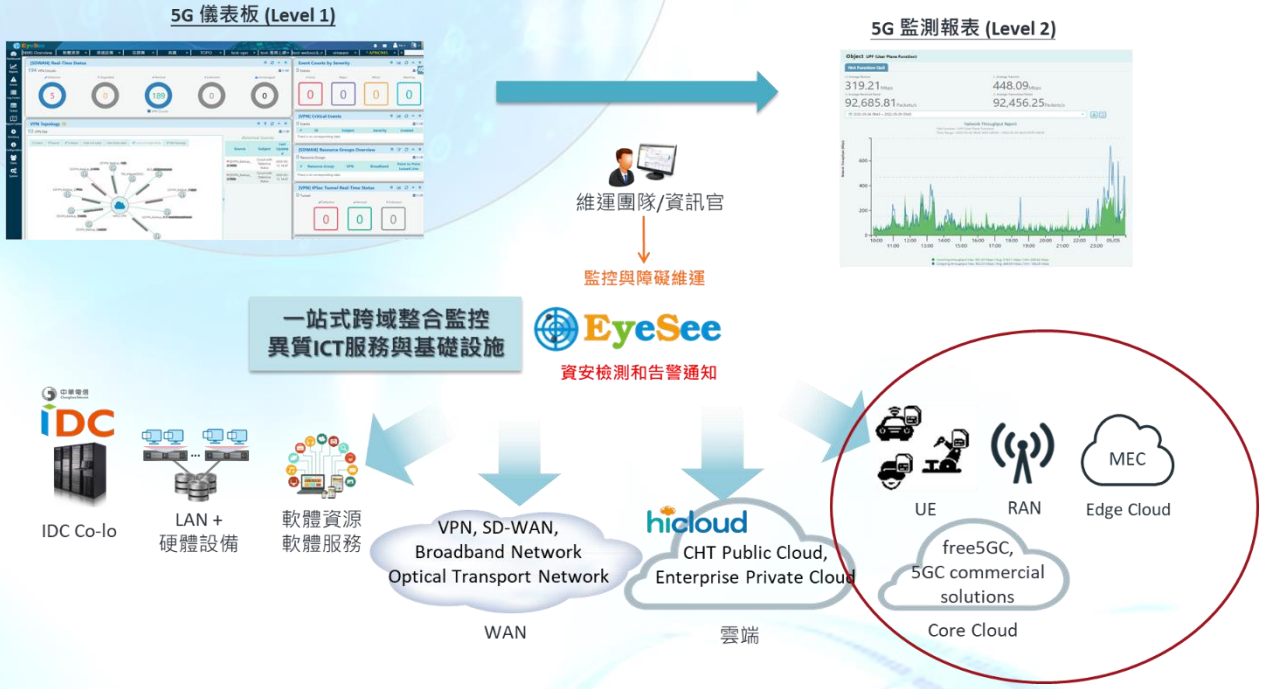
EyeSee為一站式跨域整合營管系統(如圖4)，用來監控異質的資訊與通訊科技(Information and Communication Technology, ICT)服務與基礎設施，涵蓋硬體設備、軟體資源、虛擬機和軟體服務。為了給維運團隊或國軍資訊官更全面的網路管理工具，我們強化EyeSee在5G專網的監控能力(圖4深紅色圓圈)，包括用戶設備(User Equipment, UE)、MEC、RAN和5G核心元件。因具備跨域整合營運與維運的能力，EyeSee提供維運團隊或國軍資訊官完善的5

19Ray Le Maistre，〈ONF spin-out Ananki offers to make private 5G as simple as wi-fi〉《TELECOM TV》，https://www.telecomtv.com/content/5g/onf-spin-out-ananki-offers-to-make-private-5g-as-simple-as-wi-fi-42491/，2021年9月28日，(檢索日期：2023年6月18日)

20Tse-Han Wang、Yen-Cheng Chen、Sin-Jie Huang、Kai-Sheng Hsu、Chung-Hua Hu，〈Design of a Network Management System for 5G Open RAN〉《IEEE》，https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9562627，2023年1月，(檢索日期：2023年6月19日)

G專網端對端整合營管監控功能，如儀表板、統計分析、歷史報表及資源健康狀態的視覺化圖表，監控標的包含邊緣伺服器(Edge Server)、網路和基站。不僅如此，EyeSee加入資安漏洞檢測功能及資安防護機制，當異常的事件發生時，會自動觸發告警通知維運人員。

圖4　EyeSee 5G開放架構網路端對端整合營管系統



資料來源：作者繪製(整理)

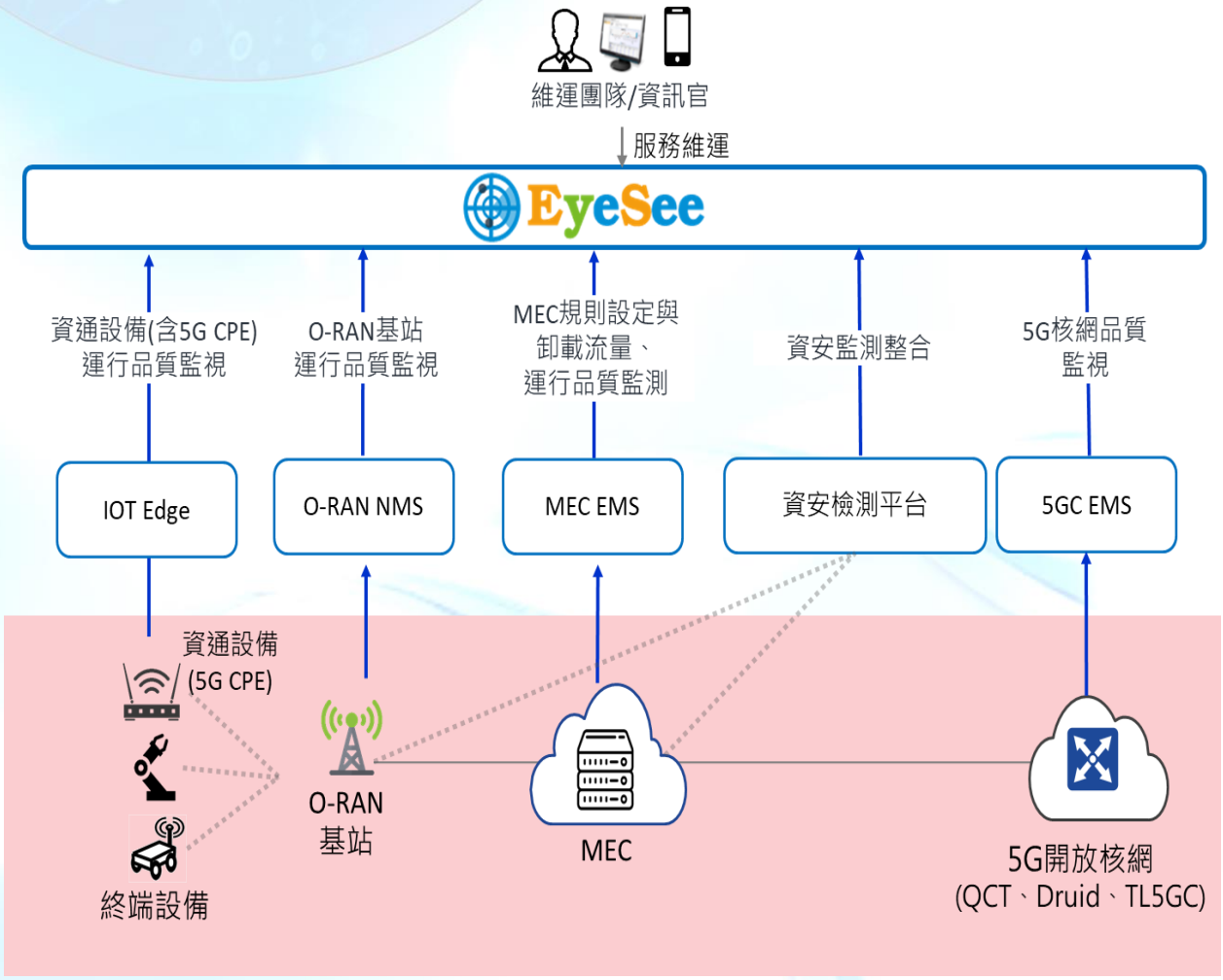
然而，對EyeSee來說，如何從這些異質資源蒐集並分析資料是一個相當困難的挑戰。因為不同的資源設備具有不同的特徵資訊，所以監控這些跨域的資源設備時，蒐集的規則方式和通訊協定不盡相同，導致我們無法只用一種方法就蒐集到所有資源設備的資料。除此之外，收集大量裝置的原始資料是非常巨量可觀的，還會造成系統運行效能的議題。所以，我們在系統的架構中，融入分治法(Divide and Conquer)的概念來解決這些重要的議題。

二、EyeSee系統整體架構

「開放架構網路」是5G企業專網的一種實踐方式，在企業或軍方場域建置專屬基站和專屬核網，同時依據企業或軍方需求，可選擇部署中華電信自主開發的MEC方案。在開放架構網路中，EyeSee扮演端對端整合監控的角色(如圖5)，維運團隊或國軍資訊官登入EyeSee單一監控管理平台，掌握5G專網跨域異質資源的運行品質。監控對象包括企業或軍方多元的終端設備、多廠

牌的 O-RAN、MEC和多廠牌的5G核網設備等。EyeSee介接IoT Edge系統取得終端設備、資通設備(5G CPE)等運行品質監視資料；藉由O-RAN NMS系統獲得各家廠牌O-RAN基站的監視資料；EyeSee透過MEC EMS系統設定MEC規則及監測卸載流量與運行品質；EyeSee還藉著5GC EMS系統進行5G核網品質監視。另外，EyeSee串整中華電信自主開發的「資安檢測工具」，提供O-RAN、MEC和其他系統的資安檢測報告。

圖5　EyeSee系統整體架構



資料來源：作者繪製(整理)

EyeSee採取高可用性(High Availability, HA)的部署架構，達到高可靠、高效能、高彈性、高可用與其他能力。在使用者登入EyeSee網頁前，負載平衡(Server Load Balancer, SLB)預先處理(Pre-streaming)，接著後端資料層(Back-end Data Layer)使用快取叢集(Cache Cluster)和資料庫叢集機制，確保資料層(Data Plan)的持續性和延展性。EyeSee也研發自己的HA模組，能自動

化監控主機的運作狀態，提供後端主被動伺服器的即時切換功能。

三、EyeSee監控5G Core

接下來說明5G核心網路(5G Core, 5GC)介接的部分。目前與三家廠商共同協作，包括雲達科技(Quanta Cloud Technology, QCT)、開放原始碼5G核心網路(Free5GC)和Druid。我們完成QCT 5GC的監控功能，正在進行中華電信研究院(Telecom Laboratories, TL) 5GC和Druid 5GC的介接研發。

與這三家廠商討論介接與功能過程中，我們發現需要克服困難的議題：

(一)系統架構皆不相同

從圖6可以看出QCT是以2部伺服器和3部交換器組成單一主機(Active-Standby)架構，承載6個虛擬網元；[21]TL 5GC則是1部伺服器和1部交換器承載9個虛擬網元；而Druid是在伺服器上運行基於核心的虛擬機器(Kernel-based Virtual Machine, KVM)，再承載存取與移動管理功能(Access and Mobility Management Function, AMF)、會話管理功能(Session Management Function, SMF)與用戶面管理功能(User Plane Function, UPF)。[22]

(二)支援的北向介面不同

QCT以主動式的安全檔案傳輸協定(SSH File Transfer Protocol, SFTP)和遵循REST架構風格的應用程式介面(RESTful Application Programming Interface, RESTful API)機制傳遞資料給EyeSee；而TL 5GC和Druid則提供被動式的RESTful API讓EyeSee主動定時查詢。

(三)提供之資料結構不同

雖然都是5GC，但是因為三家廠商的架構不同，所提供的資料結構不盡相同。QCT是以功能分類；TL 5GC是以虛擬網元來分類，而Druid則是以虛擬網元和用戶來分類。

統整比較三家廠商架構與資料的異同之處，歸納出三個解決方法：

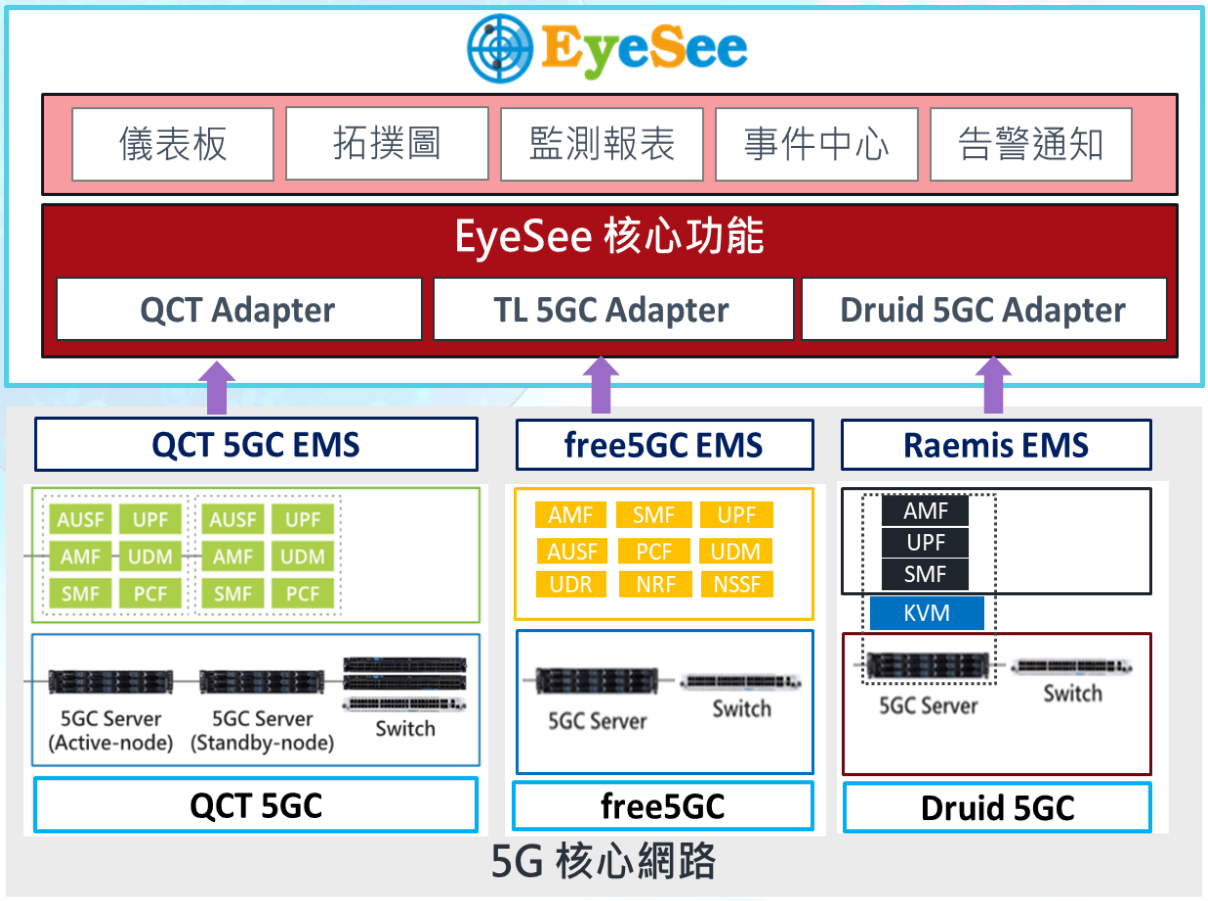
(一)重構5GC的網路管理架構

跳脫已實作的QCT原有資料框架，建立新的通用的資料儲存框架，加速第二家和第三家廠商介接與協作。

21QCT，〈QCT 5G OAM〉《QCT》，https://go.qct.io/telco/omnipod-enterprise-5g/qct-oam/，(檢索日期：2023年6月19日)

22英菲達科技，〈CELLULAR NETWORK TECHNOLOGY〉《英菲達科技》，https://www.innotrust.com.tw/druid.html，(檢索日期：2023年8月1日)

圖6　EyeSee監控5G核網



資料來源：作者繪製(整理)

(二)將5GC關鍵指標正規化

從組態管理(Configuration Management, CM)、效能管理(Performance Management, PM)和障礙管理(Fault Management, FM)的資料中，精煉最重要的參數進行分析，並將這些參數進行歸類與標準化。若未來需監控更多廠商的5GC核網設備，即可基於這些規範與廠商討論資料介接的方式。

(三)跨域障礙整合日誌收容不同的告警資料

以「跨域障礙整合日誌」來收容告警資料，使用原始資料(Raw Data)的方式收集5GC廠商所提供的FM資料，提升FM格式的彈性，並且快速、廣泛地收容各種形式的告警內容。

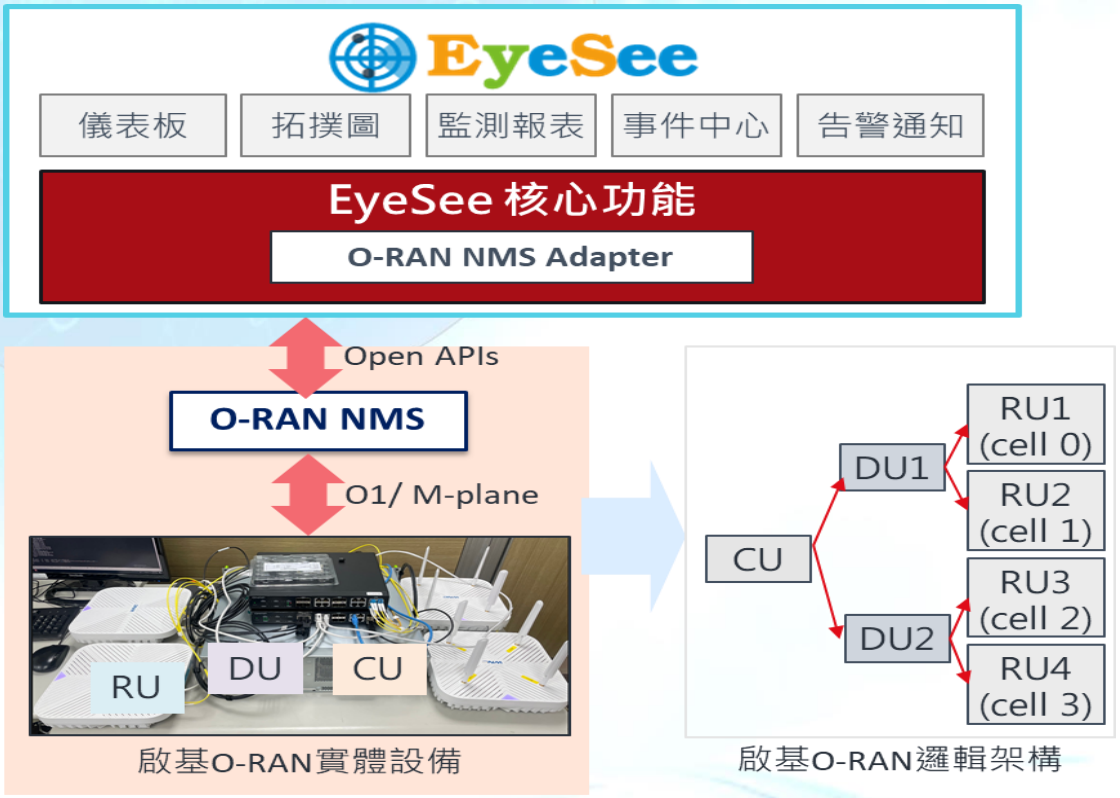
完成重構後，EyeSee在Level 1儀表板提供5GC的虛實資源拓撲圖和即時品質，以及Level 2監測報表提供網元與設備為單位組態資訊、運行狀態和歷史紀錄。

四、EyeSee監控O-RAN

中華電信自主研發的O-RAN網路管理系統，透過O1和M-Plan介面監控O

-RAN基站的運行狀態，而EyeSee則是藉助O-RAN NMS的能力來監控不同廠牌的O-RAN(如圖7)。

圖7　EyeSee監控啟碁設備架構



資料來源：作者繪製(整理)

EyeSee透過O-RAN NMS所提供的統一介面與格式取得O-RAN監控資訊。以O-RAN廠商啟碁為例，O-RAN NMS提供的CM資料包含CU、DU和RU的組態資訊，PM資料提供8項關鍵效能指標(Key Performance Indicators, KPI)，包括每個細胞(Cell)的資源使用率(Physical Resource Block, PRB)、連線成功率(Data Radio Bearer, DRB)、所連接的裝置數與上/下流量的統計等，FM則涵蓋十五項告警項目。

在EyeSee 使用者介面(User Interface, UI)的網頁上，以每個細胞為單位呈現效能指標和歷史趨勢，讓維運團隊或國軍資訊官可以明確了解基站中每個細胞的運作狀態。

五、EyeSee整合資安檢測平台

5G行動開放架構網路採開放式的介面、多樣的軟體和多廠牌的硬體設計，使電信設備更容易升級、採購與調整部署。然而，這種彈性的架構隨之而來的是資安漏洞議題。為此，EyeSee整合資安檢測平台(Information Security

Detection Platform, ISDP)，提供整體開放架構網路的完善資安防護。

資安檢測平台針對5G開放專網提供O-RAN、MEC及雲負載平台等三種監控標的安全檢測。首先，關於O-RAN的部分，針對第三代合作夥伴計劃(3rd Generation Partnership Project, 3GPP)無安全規格要求的O-RAN開放介面，包含O1介面、M-Plane、U-Plane和S-Plain進行資安檢測；其次，MEC乃針對安全設定進行檢測；最後，雲負載平台包含Docker與Kubernetes等檢測，防止雲原生基礎環境設定錯誤造成資料被竊聽、權限盜用、受駭橫向擴散、映像檔被惡意竄改等事故發生。

當資安漏洞檢測執行完成後，上述三種監控標的統一採用JSON格式進行正規化，再將檢測報告收攏至EyeSee。Level 1儀表板用兩種方式顯要呈現檢測漏洞，其中一種在儀表板最上方呈現關鍵指標，以紅色標示高風險漏洞總數，綠色表示無高風險漏洞，讓使用者快速掌握資安檢測重點結果。另一種是監控元件(Widget)，以監控標的(O-RAN、MEC、雲負載平台)和風險嚴重程度(高、中、低)分類，提供更細節的資安檢測結果。另外，還具有逐層展開(Drill-Down)功能，點選關鍵指標和監控元件的檢測數量，能進一步查詢且快速瀏覽分析報告列表，協助使用者檢視5G營運環境的資安風險。

六、EyeSee與IoT物聯網協同合作

EyeSee除了具備5G企業專網管理功能外，更延伸擴大管控領域至IoT (Internet of Things)物聯網，打造了一條完整由IoT整合5G網路設備，並透過基站傳輸，與企業既有的私雲整合應用。

參考圖8架構圖，EyeSee管控IoT Edge平台，[23]該平台負責設定感測裝置參數及接收樹莓派終端設備的空氣品質感測資料，如溫度、濕度、懸浮微粒(PM 2.5)、硬體狀態等，透過Wi-Fi或5G路由器(Router)將感測裝置蒐集到的即時數據回傳至EyeSee，達成縮短障礙終端定位與應變時間，提升服務可用性。此外，EyeSee還蒐集5GC的CM、PM和FM資料。透過CM，可以讓使用者查詢和管理組態設定，例如選擇資安演算法。藉由PM，使用者可以查詢5GC重要的維運參數，如分組數據單元會話(Packet Data Unit Session, PDU Session)總數。FM則提供異常事件的資訊，如AMF失連等。

如前述章節所提資安檢測平台亦可針對IoT進行檢測，當樹莓派終端關鍵組態異動與非法登入被偵測時，亦可由EyeSee統籌顯示，提升服務安全性。

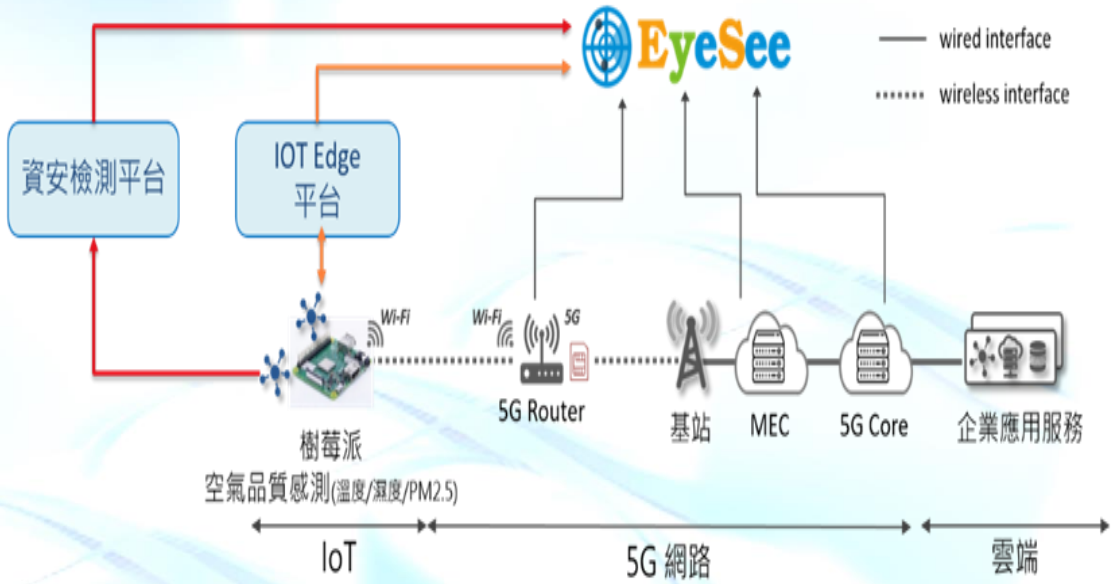
23中華電信股份有限公司，〈一起加入物聯網生態系〉《IoT智慧聯網大平台》，https://iot.cht.com.tw/iot/，(檢索日期：2023年6月20日)

此技術亦可應用於無人機或車聯網，如國軍場域進行無人機、車隊管理，軍官與資訊官皆可透過EyeSee豐富的儀表板和詳盡的監測報表，檢視重要關鍵參數及歷史趨勢報表，滿足維運管理需求。

七、EyeSee系統功能

現今軍事科技發達，機房內擁有眾多的資訊系統，如伺服器、防火牆、資料庫等。這些硬體設備、軟體資源有各自的監控機制與操作入口，管理相當不便。尤其障礙發生時，勢必在不同管理介面間切換，無法有效分析整體服務運行品質。導入5G企業專網後，除了管理原本資通設備、軟硬體資源外，更增加5G網路設備，例如5G終端設備、MEC設備、基站和5G核心網路元件等。故EyeSee系統以單一入口呈現各式軟硬體和5G企業專網的健康狀態以及資安檢測報告。

圖8　EyeSee管控IoT架構圖



資料來源：作者繪製(整理)

EyeSee設計Level 1視覺化儀表板，以便維運團隊和國軍資訊官清晰掌握5G企業專網運行況狀。EyeSee儀表板上方以紅、綠燈號呈現嚴重的障礙事件和資安高風險漏洞；下方可依需求自訂專屬監控儀表板，提供5G企業專網監控元件，如障礙事件統計、5G企業專網設備、基站、終端門號之即時運行狀態、設備總覽及門號訊務/應用服務網路流量統計、虛實資源拓撲圖、資安檢測結果。藉由拖曳監控元件調整擺放位置，並整合多層次報表，點選相關數值，可依需查詢細節資訊。

EyeSee提供Level 2監控報表以單一介面統整呈現5G企業專網設備資訊、終端門號訊務、應用服務訊務、O-RAN基站及MEC規則設定。5G企業專網設備總表顯示設備的即時運作狀態、效能資訊、重要相關參數、組態資訊和歷史趨勢圖表。設備運行狀態以紅、綠燈號呈現正常或失連；運行效能與程度則以紅、紫、黃和綠等顏色線條長度表示；另外，依選取的時間區間顯示歷史報表，並可匯出PDF或下載原始數據作後續分析。5G企業專網門號總表和應用服務總表顯示終端門號或應用服務最近1小時網路流入或流出的流量及歷史趨勢圖表。5G企業專網O-RAN顯示基站和細胞的吞吐量、PRB使用率與細胞可用度，以及歷史趨勢圖表。5G企業專網MEC規則設定可設置本地卸載規則、內網權限管控規則和DNS Proxy，進行終端設備連網權限管控。

EyeSee的事件中心功能，以同一操作介面收容異常的告警事件，可設定十五項告警規則。當異常障礙發生時，立即產生告警。亦可設定告警嚴重程度、Email/簡訊通知等。此外，還提供工單管理的障礙追蹤功能，讓維運團隊、國軍資訊官隨時掌握議題處理進度。

EyeSee系統5G企業專網應用現況

一、國外應用現況

EyeSee系統已經成功部署於泰國和越南等地。中華電信跨國與泰國國家電信、The WhiteSpace合作，實現5G+AIoT+雲端的智慧工廠應用，於2022年9月在泰國邦浦工業區一廠導入5G企業專網，主要應用於AR遠程協作、裝備培訓、操作輔助等工廠實踐及視覺化設備操作，支持和推動泰國數位政府4.0，進行後疫情時代的數位轉型。[24]

在越南方面，中華電信與和碩、越南電信合作，建置5G智慧工廠，導入AI視覺辨識平台、產線即時監測系統和AR遠端協作技術，使生產製造邁向高效率、現代化、智慧且安全的新里程碑。[25]

EyeSee系統主要應用於監控MEC設備運行狀態和管控終端設備門號，例如設定MEC權限管控規則、查詢門號流量、應用服務流量等。

二、國內應用現況

(一)國家兩廳院即時串流應用

24中華電信，〈中華電信偕同泰國國家電信與The WhiteSpace於泰達電泰國廠完成5G企業專網部署，協助泰達電於後疫情時代成功數位轉型〉《中華電信》，https://www.cht.com.tw/zh-tw/home/cht/messages/2022/0922-1600，2022年12年9月22日，(檢索日期：2023年9月11日)

25鉅亨網新聞中心，〈和碩攜手越南電信 建越南首座5G智慧工廠年底完工〉《鉅亨網》，https://news.cnyes.com/news/id/5261363，2023年7月24日，(檢索日期：2023年9月11日)

第一個開放5G企業專網的實際應用案例運用超過十家台灣的網路通信業者與硬體製造商組成的生態產業鏈，打造於國家兩廳院的5G專網即時串流技術。[26]

5G技術的網路低延遲、大頻寬特性，可滿足4K高畫質即時直播與異地共演，提供多視角自由選擇觀看的內容。透過5G與AR眼鏡的結合，將表演字幕即時傳送到AR眼鏡，提供翻譯字幕讓聽障朋友與國外觀眾用眼睛「看見」舞臺上的對話。[27]

5G的開放式架構替台廠帶來新商機，集結中華電信、友訊、譁裕、啟碁、廣達、可億隆、互動國際、研華、亞力、資策會等國內外超過十家網通業者所打造，也顯示50%以上的國內產業供應鏈體系能量已建構。

EyeSee負責管控網路設備，包含5G設備和Wi-Fi裝置。首先在監控5G企業專網設備方面，包含MEC、旁路交換器(Bypass Switch)、軟體定義網路交換器(SDN Switch)、第三層交換器(Layer 3 Switch, L3 Switch) 和Base Station，收攏所有設備運行的即時狀態、基礎效能與網路介面的資料，並可設定告警規則產製事件，通知維運人員。

接著，兩廳院的維運人員可自主透過網頁操作建置於網際網路(Internet)上的EyeSee雲端(Cloud)，設定進入企業內網之門號白名單，門號可選擇中華已設定之IP/網址；此外依據門號、時間與位置自行調整用戶頻寬與使用服務，當然所有的門號狀態、歷史流量皆可由EyeSee查詢，並可產製日、月的報表。

最後，除了門號具備管理方案，如其他User Equipment僅具Wi-Fi功能，用戶可透過非3GPP互通功能(Non-3GPP InterWorking Function, N3IWF)向5G核網進行註冊和身份認證，註冊成功後建立用戶和N3IWF 之間網際網路安全協定關聯(Internet Protocol Security Association, IPsec Security Association)，並能成功建立PDU Session進行各種服務品質(Quality of Service, QoS)資料流的傳輸。而EyeSee可以藉由媒體存取控制位址(Media Access Control Address, MAC Address)和帳號密碼來管控Wi-Fi AP認證白名單。

(二)IoT空氣品質感測應用

5G開放架構網路結合IoT樹莓派空氣品質感測裝置應用案例，用來

26Interface，〈5G毫米波藝文展演就在兩廳院 高通攜手中華電信實現600Mbps上傳速度〉《Interface》，https://theinterface.asia/article/6291-5g-mmwave/，2021年12月28日，(檢索日期：2023年6月21日)

27國家通訊傳播委員會，〈NCC 展現5G創新應用成果 開創5G藝術展演新時代〉《國家通訊傳播委員會》，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=46946，2021年12月17日，(檢索日期：2023年6月21日)

蒐集溫度、濕度、PM 2.5及硬體狀態。樹莓派上的感測裝置產生空氣品質感測資料後，透過Wi-Fi傳輸至5G路由器，經由5G網路傳送感測資料至基站，然後匯集於IoT Edge平台，最後由EyeSee展示物與網路管理的一體化呈現。

EyeSee在主動品保面向，提供完善的物、端、網狀態關聯拓樸圖以統籌呈現重要硬體元件，包含樹莓派、IoT感測裝置、網路設備(Wi-Fi、5G Router、MEC)與空品偵測管理系統。於被動品保面向，EyeSee可設定告警規則，當裝置失連時，EyeSee的拓撲圖顯示裝置的狀態，並產生告警事件通報維運人員，盡速追蹤與定位問題來源。終端可視性縮短障礙終端定位與應變時間，提升服務可用性。

EyeSee不僅即時監控IoT裝置，也能管控5G路由器存取控制清單(Access Control List, ACL)規則，達到強化資安保護的能力。當駭客攻擊IoT裝置，預先安裝於裝置上的代理模組，偵測到違法登入或組態設定被竄改時，EyeSee揭露終端受駭及可疑活動。維運人員也會收到資安告警通知，立即隔離終端禁止入網，阻斷橫向攻擊，提升服務安全性。

三、小結

5G網路帶來各產業的技術革新，5G應用成功拓展至國外，實現智慧工廠，促進產業轉型與升級。期望未來能複製泰國、越南等成功經驗，擴展至其他國家。在國內，5G開放架構網路帶動國內多家廠商協同合作，完成AR即時串流與IoT空氣品質感測應用，使得國內5G產業供應鏈更加興盛。

EyeSee主要負責監控5G網路設備，包括MEC設備、基站等運行狀態、效能資訊及相關歷史趨勢圖表，以及終端設備之門號，如白名單管理與狀態、流量歷史趨勢圖表。另外，還提供IoT感測資料及關聯拓撲圖。在事件告警方面，EyeSee具備十五項關鍵告警項目，當異常發生時，立即通報相關人員。

結論

國軍的5G企業專網可應用於無人機、後勤、軍事訓練和指揮控制。其中，無人機在俄烏戰中扮演至關重要的角色。俄烏戰爭是很明顯實力不對等的軍事衝突，烏軍採取不對稱打擊的城鎮作戰，運用小型防空飛彈、反裝甲飛彈、無人機對俄軍進行視距內精準打擊，有效消耗俄軍戰力。由此可見，不對稱作戰結合城鎮戰與視距內精準打擊為小國反擊確實有效的作戰方式。[28] 特別是，無人機可創造局部的制空權優勢，進行偵查敵方軍事活動，如防禦

28馬振坤，〈俄烏戰爭及共軍圍台軍演對台灣防衛的啟示〉《財團法人國策研究院文教基金會》，http://inpr.org.tw/m/405-1728-25892,c113.php?Lang=zh-tw，2022年10月，(檢索日期：2023年9月14日)

據點、火砲陣地、油庫、彈藥庫或指揮所等，爾後再進行精準打擊。不僅如此，無人機還能執行定位追蹤、戰鬥打擊和後勤補給任務。[29]鑒於我國地理位置與地形環境，可強化濱海灘岸及城鎮作戰的防衛能力，無人機皆能達到小兵立大功的作用。因此，可以常態納入無人機作戰和反制作戰訓練。

無人機主要透過無線通訊從遠端操控，上面搭載全球定位系統(GPS)和慣性導航系統(IMU)等，進行半自動或全自動導航飛行。無人機應用於農藥噴灑、物流遞送、災害巡檢、空中通訊平台等。另外，結合AI辨識技術、邊緣運算技術，能作場域巡檢，發現可疑人士或車輛立即發出告警，達到空中巡邏效果。亦可作設施巡檢，找出設施異常情況，如辨識橋梁是否有異常繡蝕或裂縫。無人機主要藉由飛航任務管理系統(UTM)進行管理，所有飛行中的無人機即時狀態皆傳送到雲端UTM納入控管，操作人員以管理者身分對無人機進行監視與管理。UTM系統主要功能包括無人機管理、飛行任務管理、禁航區顯示、電子圍籬和飛行紀錄等。通常UTM系統會藉著5G網路和邊緣運算技術，傳輸即時影像至AI辨識引擎，例如即時辨別可疑人員或車輛，讓管理者隨時掌握場域安全狀況。而且無人機完成任務，會自動返航無人機停機坪，並自動充電，無須人工手動操作替換電池。[30]

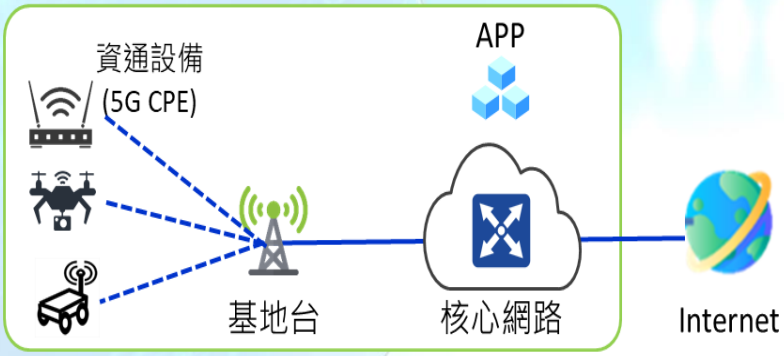
在後勤方面，智慧倉儲在軍事應用也佔有一席之地，透過自動化後勤紀錄和物流追蹤，能減少後勤資訊整合負擔。在軍事訓練方面，藉由AR和VR技術立體展現作戰地區，進行不同戰場情境訓練。最後，指揮控制是軍隊中最關鍵的核心能力，蒐集巨量的裝備、人員等感測、偵測、戰場資料，匯集並用AI進行數據統計分析，幫助指揮人員獲得更即時、更全面的資訊。

5G專網結合無人機和AI技術、AIoT技術，發揮最大優勢與綜效。若國軍發展5G企業專網相關軍事應用，可採專頻專網獨立建置方式，在軍方規劃5G訊號覆蓋場域範圍內部署專用基站和專用核心網路，完全未與其他企業共用，符合網路隔離需求。建設基地台以大型基地台為主，再搭配微型基地台補足5G訊號涵蓋問題。抑或建置攜帶式5G企業專網和基地台，滿足高機動需求。通常，軍方AI應用系統或其他應用服務系統(如圖9中的APP)直接連至專用核心網路，達到5G網路大連結、高速率、地延遲的特性。一般終端設備，如無人機或各種感測裝置上安裝SIM卡，連上5G基地台，就可以和AI應用系統、應用服務系統進行5G網路通訊，例如傳送即時影像作AI辨識分析。

29全球防衛雜誌，〈美中無人機的後勤發展與應用，台灣如何借鏡？〉《鳴人堂》，https://opinion.udn.com/opinion/story/120902/7141161，2023年5月4日，(檢索日期：2023年9月14日)

30林俊佑，〈論無人機商用服務與整合技術〉《中國工程師學會》，http://www.cie.org.tw/cms/JournalFiles/10912_chapter07.pdf，2020年12月，(檢索日期：2023年9月14日)

圖9　軍方建置5G企業專網架構示意圖



資料來源：作者繪製(整理)

傳統封閉式網路架構容易造成「供應商綁定」的形況，而採用開放式的5G網路則可解決此問題，讓設備供應商能共同投資開發5G通訊設備，使軍方能與多家廠商共同合作發展軍事5G技術與應用。本文提出EyeSee解決兩大議題。第一個議題，在預先整合開放架構網路的軟硬體設備，EyeSee 藉由IoT Edge平台監控多元的終端設備，及透過中華電信的MEC方案監控MSISDN的流量和相關規則設定。EyeSee還介接不同的廠商，取得5GC設備的運作狀態。EyeSee也藉著O-RAN NMS來監控多廠牌的O-RAN設備。第二個議題，在資訊安全漏洞方面，EyeSee整合資安檢測平台，收容O-RAN、MEC和雲端平台的資安漏洞資訊。相較於Celona和Anamki網路管理系統，僅能監測他們自己的核心網路和基站，而EyeSee則可以監控多廠牌的5GC和O-RAN，也可以提供資安檢測報告。另外，EyeSee已成功應用於5G和AR即時串流及IoT空氣品質感測，期望未來能應用於軍事AR模擬訓練、無人機與車聯網車隊管理等領域。

目前EyeSee開放架構網路持續研發精進，期許EyeSee整合更多家5G Core和O-RAN的廠商，讓企業或軍方可以建置更多種、更彈性的企業專網。另外，5G網路切片是非常重要的關鍵特性，讓軍方多場域5G企業專網間的網路通訊更加安全，因此我們致力於納入網路切片監控。

參考文獻

一、小丰子3C俱樂部，〈5G專網頻率使用費將大打折，有用嗎?〉《小丰子3C俱樂部》，https://tel3c.tw/blog/post/40183，2023年6月2日，(檢索日期：2023年8月8日)

二、工信部聯通信，〈5G應用“揚帆”行動計劃〉《工業和信息化部網站》，http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/zhengceku/2021-07/

13/content_5624610.htm，2021年7月5日，(檢索日期：2023年7月28日)
三、工商時報，〈美國防部推5G戰略 提升軍民雙邊能量〉《工商時報名家評論》，https://view.ctee.com.tw/technology/49428.html，2023年4月12日，(檢索日期：2023年7月27日)
四、中國新聞網，〈【十年中國風】“5G+萬物”，中國人闖出數字生活新天地〉《人民網》，http://finance.people.com.cn/BIG5/n1/2022/1004/c1004-32539375.html，2022年10月4日，(檢索日期：2023年7月28日)
五、中華電信，〈中華電信偕同泰國國家電信與The WhiteSpace於泰達電泰國廠完成5G企業專網部署，協助泰達電於後疫情時代成功數位轉型〉《中華電信》，https://www.cht.com.tw/zh-tw/home/cht/messages/2022/0922-1600，2022年12年9月22日，(檢索日期：2023年9月11日)
六、中華電信，〈中華電信推出5G 獨立式組網(SA)服務 提供更多元的垂直場域應用 加速產業升級〉《中華電信》，https://www.cht.com.tw/zh-tw/home/cht/messages/2021/1019-1440，2021年10月19日，(檢索日期：2023年7月31日)
七、中華電信，〈企業專網〉《中華電信》，https://www.cht.com.tw/home/enterprise/mobile/5genterprise/712，(檢索日期：2023年7月31日)
八、中華電信股份有限公司，〈一起加入物聯網生態系〉《IoT智慧聯網大平台》，https://iot.cht.com.tw/iot/，(檢索日期：2023年6月20日)
九、全球防衛雜誌，〈美中無人機的後勤發展與應用，台灣如何借鏡？〉《鳴人堂》，https://opinion.udn.com/opinion/story/120902/7141161，2023年5月4日，(檢索日期：2023年9月14日)
十、李清怡，〈為什麼中共想在下一代5G技術上擊敗美國？〉《新紀元》，https://www.epochweekly.com/b5/623/19344.htm，2019年3月6日，(檢索日期：2023年7月31日)
十一、林俊佑，〈論無人機商用服務與整合技術〉《中國工程師學會》，http://www.cie.org.tw/cms/JournalFiles/10912_chapter07.pdf，2020年12月，(檢索日期：2023年9月14日)
十二、英菲達科技，〈CELLULAR NETWORK TECHNOLOGY〉《英菲達科技》，https://www.innotrust.com.tw/druid.html，(檢索日期：2023年8月1日)
十三、馬振坤，〈俄烏戰爭及共軍圍台軍演對台灣防衛的啟示〉《財團法人國策研究院文教基金會》，http://inpr.org.tw/m/405-1728-25892,c113.php?Lang=zh-tw，2022年10月，(檢索日期：2023年9月14日)

十四、馬瑞璿，〈5G專頻專網辦法正式上路 數位部：6月5日開始受理申請〉《經濟日報》，https://money.udn.com/money/story/5612/7208779，2023年6月2日，(檢索日期：2023年8月8日)

十五、國家通訊傳播委員會，〈NCC 展現5G創新應用成果 開創5G藝術展演新時代〉《國家通訊傳播委員會》，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=46946，2021年12月17日，(檢索日期：2023年6月21日)

十六、國家通訊傳播委員會，〈行動寬頻專用電信網路(4.8-4.9GHz)政策諮詢文件〉《國家通訊傳播委員會》，https://www.ncc.gov.tw/chinese/files/21041/54_45934_210413_1.pdf，2021年4月，(檢索日期：2023年8月8日)

十七、黃皓頤，〈金一南看5G的軍事戰略意義 指揮無人機無人艇和機器人〉《中國文化研究院》，https://www.ourchinastory.com/zh/2912，2021年11月24日，(檢索日期：2023年7月31日)

十八、經濟參考報，〈5G：從“建得好”向“用得好”加速升級〉《新華網》，http://big5.news.cn/gate/big5/www.xinhuanet.com/tech/20230703/e499367af8264e46b3aec8b80f758917/c.html，2023年7月3日，(檢索日期：2023年7月28日)

十九、鉅亨網新聞中心，〈和碩攜手越南電信 建越南首座5G智慧工廠年底完工〉《鉅亨網》，https://news.cnyes.com/news/id/5261363，2023年7月24日，(檢索日期：2023年9月11日)

二十、盧碧瑩，〈南韓5G提升軍事作戰能力：電信營運商與軍方合作〉《科技政策研究與資訊中心》，https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=15517，2019年4月26日，(檢索日期：2023年6月29日)

二一、闕河鳴，〈5G Open-RAN與台灣的機會認識5G專網與公網〉《農業數位學堂》，https://www.intelligentagri.com.tw/files/file_pool/1/0L229531656944067938/%284-2%29%E8%AA%8D%E8%AD%98%205G%20%E5%B0%88%E7%B6%B2%E8%88%87%E5%85%AC%E7%B6%B2.pdf，2021年8月16日，(檢索日期：2023年6月16日)

二二、蘇文彬，〈Gb級5G來了，企業架構無線內網有新方法〉《iThome》，https://www.ithome.com.tw/news/138728，2020年7月10日，(檢索日期：2023年8月8日)

二三、蘇紫雲，〈美國防部啟動軍用5G測試與產業合作〉《國防安全雙週報》，https://indsr.org.tw/respublicationcon?uid=12&resid=756&pid=2847，20

20年1月31日，(檢索日期：2023年7月27日)

二四、〈5G Moves towards Open and Interoperable Network Architecture〉，《Edge-core Networks》，https://www.edge-core.com/news-inquiry.php?cls=3&id=514closed-type network，2020年7月16日，(檢索日期：2023年6月15日)

二五、Alan Weissberger，〈5G Security explained: 3GPP 5G core network SBA and Security Mechanisms〉《IEEE Commu-nications Society》，https://techblog.comsoc.org/2022/01/01/5g-network-security-threats-and-3gpp-security-mechanisms/，2022年1月1日，(檢索日期：2023年6月16日)

二六、Celona，〈PRIVATE WIRELESS FOR THE ENTERPRISE〉《Celona》，https://www.celona.io/，(檢索日期：2023年6月17日)

二七、Interface，〈5G毫米波藝文展演就在兩廳院 高通攜手中華電信實現600Mbps上傳速度〉《Interface》，https://theinterface.asia/article/6291-5g-mmwave/，2021年12月28日，(檢索日期：2023年6月21日)

二八、QCT，〈QCT 5G OAM〉《QCT》，https://go.qct.io/telco/omnipod-enterprise-5g/qct-oam/，(檢索日期：2023年6月19日)

二九、Ray Le Maistre，〈ONF spin-out Ananki offers to make private 5G as simple as wi-fi〉《TELECOM TV》，https://www.telecomtv.com/content/5g/onf-spin-out-ananki-offers-to-make-private-5g-as-simple-as-wi-fi-42491/，2021年9月28日，(檢索日期：2023年6月18日)

三十、Tse-Han Wang、Yen-Cheng Chen、Sin-Jie Huang、Kai-Sheng Hsu、Chung-Hua Hu，〈Design of a Network Management System for 5G Open RAN〉《IEEE》，https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9562627，2023年1月，(檢索日期：2023年6月19日)

中英文對照表

供應商綁定 Vendor Lock-in
擴增實境 Augmented Reality, AR
虛擬實境 Virtual Reality, VR
基站 Base Station
基地台 Cell
多接取邊緣運算 Mobile/Multi-access Edge Computing, MEC
非獨立架構 Non-Standalone, NSA
獨立架構 Standalone, SA
軟體定義網路 Software-Defined Networking, SDN
服務導向架構 Service-based Architecture
網路功能 Network Functions
表現層狀態轉移 Representational State Transfer, REST
基於 REST 介面 REST-based Interface
接取網路 Radio Access Network, RAN
開放式接取網路 Open RAN, O-RAN
無線電單元 Radio Unit, RU
分布單元 Distribution Unit, DU
中央單元 Central Unit, CU
網路功能虛擬化架構 Network Function Virtualization Infrastructure
虛擬實境訓練 Virtual Reality Training
整廠輸出方案 Turnkey Solution
亞太地區網路研究與管理論壇國際學術研討會 Asia Pacific Network Operations and Management Symposium, APNOMS
開放網路基金會 Open Network Foundation, ONF
軟體定義 RAN Software-Defined RAN, SD-RAN
軟體定義網路架構 Software-Defined Fabric, SD-Fabric
軟體定義核心網路 Software-Defined Core, SD-Core
小型基地台 Small Cell
儀表板 Dashboard
端對端 End-to-End
5G Open RAN 的網管系統設計 Design of a Network Management System for 5G Open RAN

網路管理系統 Network Management System, NMS
資訊與通訊科技 Information and Communication Technology, ICT
用戶設備 User Equipment, UE
邊緣伺服器 Edge Server
分治法 Divide and Conquer
高可用性 High Availability, HA
負載平衡 Server Load Balancer, SLB
預先處理 Pre-streaming
後端資料層 Back-end Data Layer
快取叢集 Cache Cluster
資料層 Data Plan
5G 核心網路 5G Core, 5GC
雲達科技 Quanta Cloud Technology, QCT
開放原始碼 5G 核心網路 Free5GC
電信研究院 Telecom Laboratories, TL
單一主機架構 Active-Standby
基於核心的虛擬機器 Kernel-based Virtual Machine, KVM
存取與移動管理功能 Access and Mobility Management Function, AMF
會話管理功能 Session Management Function, SMF
用戶面管理功能 User Plane Function, UPF
安全檔案傳輸協定 SSH File Transfer Protocol, SFTP
遵循 REST 架構風格的應用程式介面 RESTful Application Programming Interface, RESTful API
組態管理 Configuration Management, CM
效能管理 Performance Management, PM
障礙管理 Fault Management, FM
原始資料 Raw Data
關鍵效能指標 Key Performance Indicators, KPI
細胞 Cell
資源使用率 Physical Resource Block, PRB
連線成功率 Data Radio Bearer, DRB
使用者介面 User Interface, UI
資安檢測平台 Information Security Detection Platform, ISDP

第三代合作夥伴計畫 3rd Generation Partnership Project, 3GPP
逐層展開 Drill-Down
物聯網 Internet of Things, IoT
路由器 Router
分組數據單元會話 Packet Data Unit Session, PDU Session
旁路交換器 Bypass Switch
軟體定義網路交換器 SDN Switch
第三層交換器 Layer 3 Switch, L3 Switch
網際網路 Internet
雲端 Cloud
非 3GPP 互通功能 Non-3GPP InterWorking Function, N3IWF
網際網路安全協定關聯 Internet Protocol Security Association, IPsec Security Association
服務品質 Quality of Service, QoS
媒體存取控制位址 Media Access Control Address, MAC Address
存取控制清單 Access Control List, ACL
全球定位系統 Global Positioning System, GPS
慣性導航系統 Inertial Measurement Unit, IMU
飛航任務管理系統 UAS Traffic Management, UTM

作者簡介

霍冠樺，國立中央大學資訊工程研究所碩士。現任中華電信研究院網路管理研究所高級研究員，從事網路及客戶服務品質相關技術研究。

徐鈺瀅，交通大學資訊工程與科學系碩士。現任中華電信組織暨人才發展處高級工程師。

張昇賀，國立臺灣師範大學資訊教育所碩士。現任中華電信研究院網路管理研究所高級研究員，從事網路及客戶服務品質相關技術研究。

邱祈榮，美國加州大學洛杉磯分校統計碩士。現任中華電信研究院網路管理研究所高級研究員，從事網路及客戶服務品質相關技術研究。