5G Open RAN 資安研究報告

Cybersecurity study report for 5G Open RAN

出版日期: 2022/01/06

終審日期: 2021/12/24

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 蔡正煜 主任

TC5 副主席：財團法人電信技術中心 林炫佑 副執行長

TC5 網路與資訊安全工作組組長：財團法人資訊工業策進會 柯盈圳 組長

技術編輯：財團法人資訊工業策進會 蔡宜學

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)：

中華資安國際股份有限公司、中華電信股份有限公司、台灣是德科技股份有限公司、宏達國際電子股份有限公司、亞太電信股份有限公司、和碩聯合科技股份有限公司、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、國立陽明交通大學、華電聯網股份有限公司、緯創資通股份有限公司。

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

國家通訊傳播委員會、雲達科技股份有限公司、耀睿科技股份有限公司。

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

開放式無線接取網路聯盟(Open Radio Access Network Alliance, O-RAN Alliance)是由雲端無線接取網路聯盟(Cloud Radio Access Network Alliance, C-RAN Alliance)與 xRAN 論壇(xRAN Forum)兩個組織合併組成。開放式無線接取網路聯盟(O-RAN Alliance)的主要任務是重新塑造無線接取網路(Radio Access Network, RAN)產業以達成智慧性虛擬化且完全開放互通的行動通訊網路。

以 AT&T 為首的電信事業深刻感受到需要透過新的 Open RAN 的網路標準規範，達成更具競爭性與動態彈性的無線接取網路(RAN)供應鏈，積極推動 Open RAN 的網路架構以打破過去軟硬體高度整合的常態。其將整個硬體架構分成無線電單元(Radio Unit, RU)、分散單元(Distributed Unit, DU)、集中單元(Central Unit, CU)等，與不同層之間的傳輸介面與控制管理軟體。以 Open RAN 開放式的介面軟硬體架構，實現 5G 快速彈性化布署與客製化的服務，讓電信事業可以更快速的布署應用服務，並達成降低設備成本的目標。

在 Open RAN 標準化與開放過程中，需要透過眾多產業間的合作與溝通，以便在全球推動無線開放網路、軟體和虛擬化的目標。過去所有技術與介面大多由電信設備大廠統籌負責，一旦發生問題，負責之對象明確。Open RAN 改變傳統電信基地臺由國際大型電信設備商壟斷的處境，但也隨著開放式架構的網通設備「白牌化」後，硬體軟體整合會有軟體相容性問題。市場也擔心開放架構會不會讓資安漏洞更多，且一旦出現資安疑慮，更會無從查起，這也讓資安問題更加複雜化。

為了解決 5G 開放式架構的資安議題，開放式無線接取網路聯盟(O-RAN Alliance)於 2021 年成立安全焦點小組(Security Focus Group, SFG)，專注於制定 Open RAN 網路產品的安全架構和安全保證規範，開放式無線接取網路安全架構與框架，同時也致力於開放測試與整合中心(Open Testing and Integration Centre, OTIC)推動產品資安保證評估驗證程序。

在經濟部技術處「5G 資安防護系統開發計畫」的支持下，資策會資安所團隊參考「5G 專網多接取邊緣運算資安研究報告」與無線接取網路聯盟(O-RAN Alliance)及第三代合作夥伴計畫(3GPP)之標準規範與技術研究報告，撰寫「5G Open RAN 資安研究報告」(以下簡稱本研究報告)，並在台灣資通產業標準協會(TAICS)平台聚集產業意見，

以提供 5G Open RAN 製造商了解使用技術會面臨的威脅與因應之道，並作為未來制定國內 5G Open RAN 資安測試規範之參考。

1. 適用範圍

本研究報告涵蓋 5G Open RAN(Open Radio Access Network)系統架構之資安研究分析。本研究報告之 5G Open RAN 架構以開放架構無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(Security Focus Group, SFG)所訂定的標準規範[10]與技術研究報告[11]以及第三代合作夥伴計畫(3GPP)之服務與系統第 3 工作組(Service and System Aspects#3, SA3)所訂定的標準規範[8][9]與技術研究報告[3][7]為主。Open RAN 系統的邏輯架構圖如圖 1 所示。

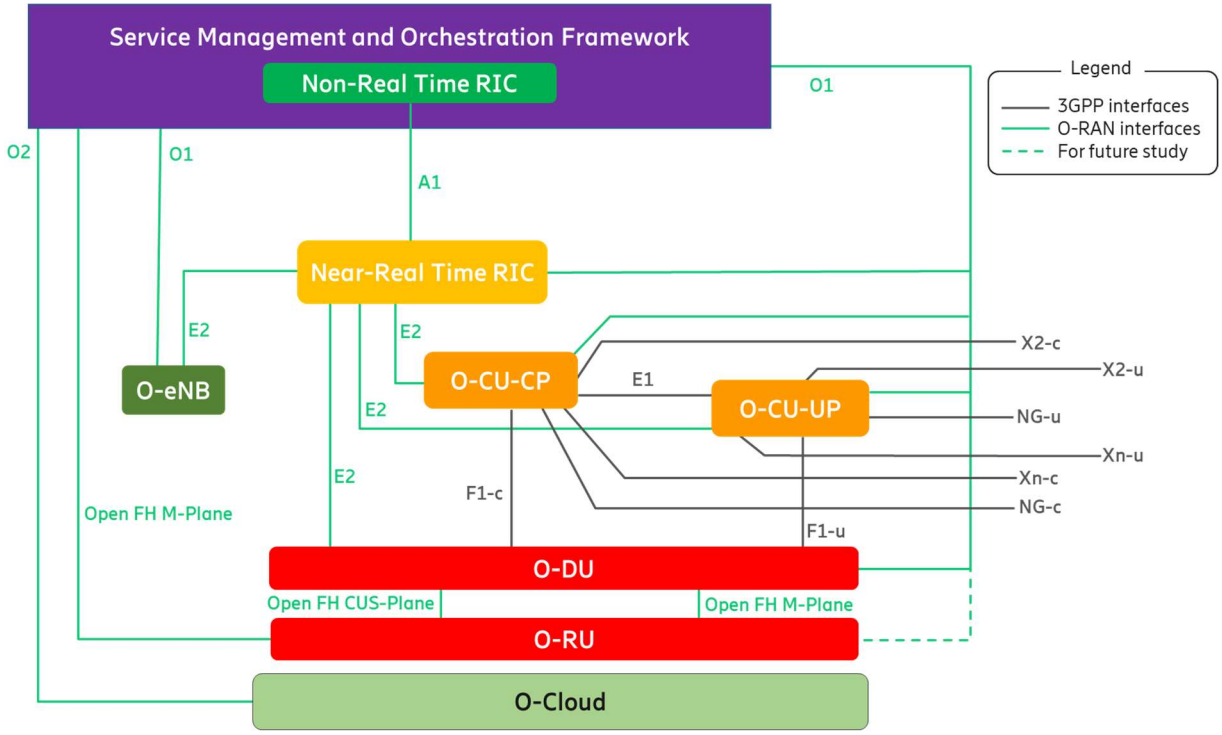

圖 1 Open RAN 系統架構[11]

*註圖中之網路元件與介面用語定義於第 3 節

2. 引用標準

下列標準因本研究報告所引用，成為本研究報告之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(包括補充增修)。無加註年份者，適用該最新版(包括補充增修)。

[1] TAICS TR-0017 v1.0, “5G 專網多接取邊緣運算資安研究報告”

[2] 3GPP TS 38.401-g70, “NG-RAN Architecture description” (https://www.3gpp.org/ftp/Specs/archive/38_series/38.401/38401-g70.zip)

[3] 3GPP TR 33.926- h20 “Security Assurance Specification (SCAS)threats and critical assets in 3GPP network product classes (Release 17)” (https://www.3gpp.org/ftp/Specs/archive/33_series/33.926/33926-h20.zip)

[4] 3GPP TR 38.801-e00, “Study on new radio access technology: Radio access architecture and interfaces (Release 14)” (https://www.3gpp.org/ftp//Specs/archive/38_series/38.801/38801-e00.zip)

[5] 3GPP TR 38.806-f00, “Study of separation of NR Control Plane (CP)and User Plane (UP)for split option 2;(Release 15)” (https://www.3gpp.org/ftp//Specs/archive/38_series/38.806/38806-f00.zip)

[6] 3GPP TR 38.816-f00, “Study on Central Unit (CU)- Distributed Unit (DU)lower layer split for NR (Release 15)” (https://www.3gpp.org/ftp//Specs/archive/38_series/38.806/38806-f00.zip)

[7] 3GPP TR 33.818-h10, “Security Assurance Methodology (SECAM); and Security Assurance Specification (SCAS)for 3GPP virtualised network products (Release 17)” (https://www.3gpp.org/ftp/Specs/archive/33_series/33.818/33818-h10.zip)

[8] 3GPP TS 33.511-h00 Security Assurance Specification (SCAS)for the next generation Node B(gNodeB)network product class (Release 17) (https://www.3gpp.org/ftp/Specs/archive/33_series/33.511/33511-h00.zip)

[9] 3GPP TS 33.117-g50 Catalogue of general security assurance requirements (Release 17) (https://www.3gpp.org/ftp/Specs/archive/33_series/33.117/33117-h00.zip)

[10] O-RAN SFG, “Security Test Specification - v01.00” (https://oranalliance.atlassian.net/wiki/download/attachments/2290581844/SFG.AO-2021.11.10-SFG-I-Security%20Test%20Specifications-v01.00.docx?api=v2 [Note: Draft specification for O-RAN Alliance members only])

[11] O-RAN WG1, “O-RAN Architecture Description 5.0 - July 2021” (https://www.o-ran.org/specifications)

[12] O-RAN SFG, “O-RAN Security Threat Modeling and Remediation Analysis 2.0 - July 2021” (https://www.o-ran.org/specifications)

[13] O-RAN SFG, “O-RAN Security Requirements Specifications 1.0 - July 2021” (https://www.o-ran.org/specifications)

[14] O-RAN SFG, “O-RAN Security Protocols Specifications 2.0 - July 2021” (https://www.o-ran.org/specifications)

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，提出一個能持續演進強化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 開放式無線接取網路聯盟 (Open Radio Access Network Alliance, O-RAN Alliance)

是一個成立於 2018 年 2 月的標準化機構，該機構由雲端無線接取網路聯盟(Cloud Radio Access Network Alliance, C-RAN Alliance)與 xRAN 論壇(xRAN Forum)兩個組織合併組成，以推動在全球無線網路方面的開放網路、軟體和虛擬化目標。在 Open RAN 標準化與開放過程中，需要透過眾多產業間的合作與溝通，以便在全球推動無線開放網路、軟體和虛擬化的目標。如透過開放性無線接取網路政策聯盟(Open RAN Policy Coalition)、開放測試與整合中心(Open Test and Integration Center, OTIC)、電信基礎架構專案(Telecom Infra Project, TIP)與開放網路基金會(Open Networking Foundation, ONF)和 Linux 基金會(Linux Foundation)以及全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)等不同層面的單位各自投入發展開放式軟硬體的架構。

3.3 資安評估準則 (Security Assurance Specification, SCAS)

涵蓋 5G 基地臺(Next Generation NodeB, gNB)及 5G 核心網路(5G Core Network, 5GC)的七大資安威脅面向與相關資安測試案例，針對生產製造的行動通訊裝置進行合規檢測，並由資安實驗室針對設備的弱點進行規範檢測及防駭漏洞檢測等兩階段資安檢測。

3.4 網路設備安全保證方案 (Network Equipment Security Assurance Scheme, NESAS)

包含了設備供應製造商的開發與產品生命週期之認證、測試實驗室之認證、網路設備之安全性測試評估規範，針對支援第三代合作夥伴計畫(The 3rd Generation Partnership Project, 3GPP)定義功能網路產品的供應商構建安全認證框架，以提升行動產業的安全層級。並由全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)負責管理、制定並定期修訂規範內容。

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(1)，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 5G 基地臺 (Next Generation NodeB, gNB/gNodeB)

5G 基地臺乃指 3GPP 5GNR 系統架構中，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布署密度，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。

3.7 5G 核心網路 (5G Core Network, 5GC)

乃指 3GPP 5G 系統中與 5G 接取網路相連，且透過控制平面(Control Plane)與用戶平面(User Plane)分割技術，實現以服務為基礎(Service Based Architecture, SBA)之網路虛擬化(Network Virtualization)架構(2)。5GC 透過下一代應用協定(NGAP)與通用封包無線服務隧道協定-用戶平面(GTP-U)連接 gNB。

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)以及封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)等網路功能[1]。

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[1]。

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

是負責 5G 基地臺(gNB)集中單元(gNB-CU)中，無線資源控制(Radio Resource Control, RRC)與封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)控制平面功能之網路元件[1]。

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

是負責 5G 基地臺(gNB)集中單元(gNB-CU)中，服務數據適配協定(Service Data Adaptation Protocol, SDAP)與封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)用戶平面功能之網路元件[1]。

3.12 服務管理與編排 (Service Management and Orchestration, SMO)

提供網路設施的管理服務，其管理介面及管理內容包括故障、組態、歸責、效能及安全管理(Fault Configuration Accounting Performance Security, FCAPS)，雲平台(O-Cloud)的資源及負載管理以及 O-RAN 無線電單元(O-RU)的管理。

3.13 非即時無線接取網路智能控制 (Non-Real Time Radio Access Network Intelligent Controller, Non-RT RIC)

位於服務管理與編排(Service Management and Orchestration, SMO)內，功能包括資料分析、訓練機器學習(Machine Learning, ML)模型、提供額外資訊(Enrichment Information)、設定方針(Policy)。

3.14 rApps 應用程式

位於非即時無線接取網路智能控制(Non-RT RIC)，提供非即時無線接取網路智能控制(Non-RT RIC)的資料分析與訓練機器學習(ML)模型功能，是從服務管理與編排(SMO)獲取無線接取網路(Radio Access Network, RAN)相關資料以及從應用服務端獲取用戶相關資料。並應用機器學習方法，針對個別目的，以離線(off-line)識別訓練或預測模型方式，將機器學習模型布署於近即時網路智能控制器(Near-RT RIC)，可因應流量與環境的變化，主動並提前調整網路資源配置。

3.15 近即時無線接取網路智能控制 (Near Real Time Radio Access Network Intelligent Controller, Near-RT RIC)

位於無線接取網路(Radio Access Network, RAN)內，接收與分析來自無線接取網路(RAN)的即時資訊，結合非即時無線接取網路智能控制(Non-RT RIC)提供的額外資訊，並利用非即時無線接取網路智能控制(Non-RT RIC)布署的機器學習模型，監控或預測用戶連線狀況的變化。

3.16 xApps 應用程式

位於近即時無線接取網路智能控制(Near-RT RIC)，利用機器學習模型，監控或預測用戶連線狀況的變化，一旦發現可能達不到非即時無線接取網路智能控制(Non-RT RIC)設定的方針，則需對無線接取網路(RAN)參數進行調整，例如調整資源分配、傳輸率、傳輸優先性、切換連接點、換手…等方式，使各用戶可繼續維持既定的方針目標。

3.17 O-RAN 集中單元 (O-RAN Central Unit, O-CU)

是一個網路元件負責 Open RAN 基地臺中，無線資源控制(Radio Resource Control, RRC)與服務數據適配協定(Service Data Adaptation Protocol, SDAP)以及封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)等網路功能[11]。

3.18 O-RAN 集中單元-控制平面 (O-CU Control Plane, O-CU-CP)

是一個網路元件負責 Open RAN 基地臺中，無線資源控制(Radio Resource Control, RRC)與封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)控制平面功能之網路元件[11]。

3.19 O-RAN 集中單元-用戶平面 (O-CU User Plane, O-CU-CP)

是一個網路元件負責 Open RAN 基地臺中，服務數據適配協定(Service Data Adaptation Protocol, SDAP)與封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)用戶平面功能之網路元件[11]。

3.20 O-RAN 分散單元/低層分割的集中單元 (O-RAN Distributed Unit/Lower Layer Split Central Unit, O-DU)

是一個網路元件負責 Open RAN 基地臺中，無線鏈路控制(Radio Link Control, RLC)與媒體存取控制(Media Access Control, MAC)以及上層實體層(Upper Physical layer, Upper-PHY)等網路功能[11](12)。

3.21 O-RAN 無線電單元 (O-RAN Radio Unit, O-RU)

是一個網路元件負責 Open RAN 基地臺中，下層實體層(Lower Physical layer, Lower-PHY)以及射頻(Radio Frequency, RF)信號處理等網路功能[11](12)。

3.22 下一代應用協定 (NG Application Protocol, NGAP)

為 5G 基地臺(gNB)和存取與移動管理功能(AMF)間處理 N2 介面(interface)之相關信令與程序(3)，該協定包含用戶設備(UE)設定更新和設定內容轉移、連線管理閒置(CM Idle)和連線管理連線(CM Connected)之用戶設備狀態管理、PDU 會話資源管理、用戶設備移動換手管理以及轉送上下行鏈路之非存取層(NAS)信令。

3.23 通用封包無線服務隧道協定-用戶平面 (GPRS Tunnel Protocol- User Plane, GTP-U)

是一個以網際網路協定(Internet Protocol, IP)為基礎的簡單穿隧協定(4)，該協定允許用戶設備(UE)與用戶平面功能(UPF)間建立隧道連線，使得用戶設備可以使用任意形式的封包協定(如 IPv4、IPv6 或 PPP 等協定)透過 5GC 傳送至資料網路(DN)。

3.24 Xn 應用協定 (Xn Application Protocol, XnAP)

為兩台 5G 基地臺(gNB)間處理 Xn 介面(interface)之相關信令與程序(5)，該協定包含用戶設備(UE)設定更新和設定內容轉移與用戶設備移動換手管理等。

3.25 F1 應用協定 (F1 Application Protocol, F1AP)

為 5G 基地臺集中單元(gNB-CU)或 5G 基地臺集中單元-控制平面(gNB-CU-CP)與 5G 基地臺分散單元(gNB-DU)間處理 F1-C 介面(interface)之相關信令與程序(6)，該協定包含傳送用戶設備(UE)的無線資源控制(Radio Resource Control, RRC)信令等資訊。

3.26 E1 應用協定 (E1 Application Protocol, E1AP)

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)間處理 E1 介面(interface)之相關信令與程序(7)，該協定包含傳送用戶設備(UE)的用戶平面安全設定等資訊。

3.27 E2 應用協定 (E2 Application Protocol, E2AP)

為 Open RAN 基地臺中近即時無線接取網路智能控制(Near-RT RIC)與 O-RAN 集中單元-控制平面(O-CU-CP)和 O-RAN 集中單元-用戶平面(O-CU-CP)與 O-RAN 分散單元(O-DU)間處理 E2 介面(interface)之相關信令與程序(8)。

3.28 A1 應用協定 (A1 Application Protocol, A1AP)

為 Open RAN 基地臺中非即時無線接取網路智能控制(Non-RT RIC)與近即時無線接取網路智能控制(Near-RT RIC)間，處理 A1 介面(interface)之相關信令與程序(9)。

3.29 O1 介面 (OAM Interface/O1 Interface)

為 Open RAN 基地臺中服務管理與編排(Service Management and Orchestration, SMO)與近即時無線接取網路智能控制(Near-RT RIC)、O-RAN 集中單元-控制平面(O-CU-CP)、O-RAN 集中單元-用戶平面(O-CU-CP)、O-RAN 分散單元(O-DU)與 O-RAN 無線電單元(O-RU)間，處理故障、組態、歸責、效能及安全管理(Fault Configuration Accounting Performance Security, FCAPS)之相關信令與程序(10)。

3.30 O2 介面 (O2 Interface)

為 Open RAN 基地臺中服務管理與編排(Service Management and Orchestration, SMO)與雲平台(O-Cloud)間，處理處理故障、組態、歸責、效能及安全管理(Fault Configuration Accounting Performance Security, FCAPS)之相關信令與程序(11)。

3.31 開放前傳介面/演進版通用公共無線電介面 (Open Fronthaul Interface(Open FH)/evolved Common Public Radio Interface, eCPRI)

是一個通用的無線電介面標準，定義 Open RAN 基地臺中無線電單元(O-RU)與無線電單元(O-RU)間介面的基頻 I/Q 訊號傳輸協定的控制、用戶和同步平面(Control, User and Synchronization Plane, CUS-Plane)以及管理平面(Management Plane, M-Plane)(12)。

3.32 服務數據適配協定 (Service Data Adaptation Protocol, SDAP)

主要功能就是對無線電承載(Data Radio Bearer, DRB)與傳輸資料的服務品質(QoS)間進行映射。由於用戶設備(UE)與 gNB 間透過下一代無線接取介面(NG RAN Air Interface)在封包資料匯聚通訊協定(PDCP)使用資料無線電承載(DRB)傳輸資料，而 5G 基地臺(gNB)與 5GC 間則是透過基於服務品質(QoS)為基礎的 N3 介面傳輸資料，因此需要透過服務數據適配協定(SDAP)層將資料無線電承載(DRB)與對應的服務品質(QoS)作映射。

3.33 無線電資源控制 (Radio Resource Control, RRC)

無線電資源控制是做無線電資源分配與管理，主要提供非存取層(NAS)系統資訊廣播；建立、維護和釋放用戶設備(UE)與 gNB 之間的無線電資源控制連線；臨時標識的分配和用於無線電資源控制連接信令的無線電承載(RB)配置；金鑰安全管理的功能；建立、配置、維護和釋放點對點的無線電承載(RB)；移動性功能包括用戶設備(UE)測量回報和選擇連線的 5G 基地臺(gNB)；服務品質(QoS)管理功能；非存取層(NAS)消息的傳輸等。

3.34 封包資料匯聚通訊協定 (Packet Data Convergence Protocol, PDCP)

主要負責網際網路協定(Internet Protocol, IP)表頭壓縮與解壓縮，數據與信令的加密及信令的初始化保護等功能。其中在控制平面部分必須啟用加密和初始保護，而在用戶平面部分必須啟用選強健標頭壓縮(Robust Header Compression, ROHC)功能，用戶平面的數據加密為可選擇的功能，其中用戶平面的數據包含應用層信令，如會談初始協

定(Session Initiation Protocol, SIP)或即時傳輸控制協定(Real-time Transport Control Protocol, RTCP)等。

4. 5G Open RAN 的國際發展趨勢與標準技術簡介

隨著行動資料量不斷地增加並支援各類新業務與應用場景，5G 系統預期將具有龐大的移動數據和設備連接，而無線接取網路(Radio Access Network, RAN)除了需考慮關鍵性能指標要求、網路商業營運能力以及具備持續演進能力這三方面的因素外，全球電信事業也希望與第三方設備供應商合作推動介面開放並標準化，以完全開放互通的介面並結合無線接取網路智能控制(Radio acess network Intelligent Controller, RIC)，來降低行動通訊網路設備建置的成本，因此 5G 無線接取網路的基礎架構有走向開放、虛擬化、高靈活性與節能的趨勢。

Open RAN 的網路架構打破過去軟硬體高度整合的常態，將整個硬體架構分成無線電單元(RU)、分散單元(DU)、集中單元(CU)等，與不同元件間的傳輸介面與控制管理軟體等，集中單元(CU)還可再拆分為集中單元-控制平面(CU-CP)以及集中單元-用戶平面(CU-UP)。以實現 5G 快速彈性化布署與客製化的服務，讓電信事業可以更快速的布署應用服務，並降低硬體設備採購與升級的成本。本節將闡述現有國際 Open RAN 架構的發展趨勢與標準技術，於 4.1 節介紹 Open RAN 的國際發展趨勢，4.2 節探討 3GPP 分散式基地臺(disaggregated gNB)標準技術後，緊接著於第 4.3 節討論 O-RAN 制定的 Open RAN 基地臺標準技術。

4.1 Open RAN 的國際發展趨勢

全球有越來越多主流電信事業都更積極參與了開放式無線接取網路聯盟(O-RAN Alliance)陣營，例如日本電信事業樂天(Rakuten)開始在日本一些都會區，透過 Open RAN 技術的網路架構提供無線電信服務；歐洲的電信事業沃達豐集團(Vodafone Group)與西班牙電信(Telefónica, S.A.)以及德國電信(Deutsche Telekom)已經準備好在某些歐洲區域進行 Open RAN 網路的布署。此外，許多供應商例如美國業者 Altiostar、Parallel Wireless 與 Mavenir 率先開發無線接取網路(Radio Access Network, RAN)網路功能虛擬化的軟體，而部分供應商 Airspan、富士通(Fujitsu)與日本電氣公司(Nippon Electric Company, NEC)則專門打造 O-RAN 無線電單元(O-RU)。

美國聯邦通訊委員會(FCC)於 2021 年 3 月對如何促進並支持開放架構之發展進行公眾意見徵詢(19)。

表 1 美國聯邦通訊委員會(FCC)諮詢意見–供應商多元性

業者	供應商多元性	
	正面意見	反面意見
電信事業	認同 Open RAN 有助於打破傳統設備壟斷。	大型電信事業傾向自己進行網路維運，但小型業者可能將維運外包給系統整合(System Integration, SI)業者。 在新技術或供應商能符合其功能、效能與可靠性等要求時才會大量採用。 設備採購是長期投資，且替換成本很高，故要朝開放架構前進，短期仍是專用設備與開放架構混合使用。 Open RAN 新業者必須證明有量產能量，才能與現有設備商競爭。 威訊通訊(Verizon)不認為未來選擇應只有開放網路。
系統設備大廠	Open RAN 有利於實現軟硬體供應商的多元性。 Open RAN 使美國電信事業可擺脫單一且非美國設備供應商狀況，進而提升美國國家安全。	網路基礎設備產業投資額大，且產量又要高，故本質上就不會有太多廠商。 Open RAN 並沒有很明確定義，很多號稱自己是開放架構的方案實際上只是幾個供應商之間彼此開放，而不是真正對整個技術聯盟作開放。 Open RAN 會造成供應商數量增加是政策的結果，且供應商數量增加並不代表技術有所進展。
晶片業者	網路軟硬體解構後會讓更多廠商進入，在競爭下可能使網路的效能更高，如 Wi-Fi 產業的狀態。	傳統設備商因有規模經濟，故能以較低的成本生產特殊應用積體電路(Application Specific Integrated Circuit, ASIC)晶片。Open RAN 目前沒有這種優勢。

業者	供應商多元性	
	正面意見	反面意見
IT/軟體業者	認同 Open RAN 有助於打破無線電單元(Radio Unit, RU)設備鎖死的現象。	無

資料來源：資策會產業情報研究所整理

表 2 美國聯邦通訊委員會(FCC)諮詢意見–互通性與效能

業者	互通性與效能	
	正面意見	反面意見
電信事業	樂天認為 Open RAN 生態系要發展必須要有系統整合(SI)業者，透過發展 RCP 平台來降低整合的複雜性。	採用 Open RAN 的第一步是找能相容開放網路的現有設備供應商。由於目前 NSA 架構 5G 設備以 4G 為基礎，無法與 Open RAN 相容，故採用上有困難。 Open RAN 的整合對電信事業是個難題，尤其是小型電信事業更沒能力處理整合。 Open RAN 可能不存在向後兼容的功能設備，故與既有系統互操作性變得不可能。
系統設備大廠	Open RAN 採用虛擬化技術，可快速配置、易於擴增容量。 Open RAN 標準與設備都以過去技術為基礎發展，故其效能與互通性等方面可被信任。	Open RAN 有許多整合問題、造成成本上升，且整體耗電較傳統高 40%。 需由系統整合(SI)業者整合，但系統整合(SI)業者也可能多無法負擔維運，電信商最後仍要找供應商負責。 設備需替換的多為小型電信事業，沒有人力來管理多供應的設備。 在 Open RAN 達到與傳統設備相同的效能、安全性與穩定性前，被採用的速度會很低。
晶片業者	網路功能虛擬化(Network Function Virtualization, NFV)使大量運算能在更有運算效率的資料中心進行處理。	無

業者	互通性與效能	
	正面意見	反面意見
IT/軟體業者	認為第三代合作夥伴計畫(3GPP)是由設備商主導，所以標準與介面並不朝開放與互通發展，使得電信設備都只能更同一家購買。	無

資料來源：資策會產業情報研究所整理

表 3 美國聯邦通訊委員會(FCC)諮詢意見–網路安全

業者	網路安全	
	正面意見	反面意見
電信事業	Open RAN 導入人工智慧(Artificial Intelligence, AI)和機器學習(Machine learning, ML)自動化管理，有助於降低人為錯誤發生；開放架構在軟體升級上更方便且快速，系統漏洞可快速更新修補。 開源軟體優點在於會有很多人會去看原始碼，且有漏洞也可以更快修補。 開放架構更能快速替換掉有資安疑慮的設備。 開放架構透明度有利於掌握資安狀況，並對各介面進行資安分析，能即時反應各種狀況。	Open RAN 依賴開源軟體也增加安全漏洞的潛在破口。 現階段沒有全面針對開放網路之安全評估或要求，任何存在的安全機制都是分散式架構，可能無法有效實行。
系統設備大廠	Open RAN 因有多個供應商，且容易替換，因而能有更高的安全性。 Open RAN 因更為透明，且更容易導入最佳資安實務，故更加安全。	Open RAN 有許多新介面與標準，相關資安議題尚未完整檢視討。目前業界並無最佳做法可用。 開放軟體即為網路安全最大風險來源。
晶片業者	Open RAN 設備解構是透過區隔化與容器化來達成，這有助於減少可以被攻破的點。	無

業者	網路安全	
	正面意見	反面意見
晶片業者	開源軟體社群已有相關的貢獻與檢視機制，在軟體碼成為商品前再加上進行安全與漏洞檢查有助於提升安全性。	
IT/軟體業者	認為開放架構具有透明、多供應商可選、且可使用共同的控制軟體，因而能進行更多網路安全控管。	無

資料來源：資策會產業情報研究所整理

表 4 美國聯邦通訊委員會(FCC)諮詢意見–產業政策

業者	產業政策	
	正面意見	反面意見
電信事業	提供更長的設備替換時限，讓電信事業可有更多時間評估與測試 Open RAN。 美國聯邦通訊委員會(FCC)應對頻譜與執照做更有效利用，搭配利用 Open RAN RU 同時支援 4G/5G 頻段使鄉村得到網路覆蓋。	美國聯邦通訊委員會(FCC)等監管機構不應發布有關使用開放 式網路技術的相關政策指令。 Open RAN 仍在發展前期，任何監管要求都為時過早。故政府不應強制要求使用 Open RAN 網路；也不應試圖通過監 管法令促進其發展。
系統設備大廠	Open RAN 列名在設備替換採購清單中，且優先購買美國供應商的產品，或設立基地臺由美國供應商供應的最低比重限制。	建議美國聯邦通訊委員會(FCC)不要用資助等機制去影響營運商在網路架構上的選擇。
晶片業者	對 Open RAN 發展提供資金，可資助國外企業共同研發，推動以美國與同盟國可信任供應商所組成的供應體系。 提出促使民間企業積極參與標準組織之誘因，如研發支出抵稅、直接提供資金等。 贊助 Open RAN 實驗室，以加速美國開放網路採用與系統整合。資助開放網路 Testbed，進行驗證與整合測試。	電信事業與企業會自己處理好 Open RAN 要大量布署前的所有工作，包括標準制定、研發與測試，故美國聯邦通訊委員會(FCC)並不需要用政策去介入。
IT/軟體業者		認為 FCC 應該只要維持對開放架構有利之無線網路創新就好，不應設立規範或偏好發展開放架構。

業者	產業政策	
	正面意見	反面意見
IT/軟體業者	贊助促進互操作性和集成為不同的開放網路解決方案供應商插拔大會，有助於支持開放網路生態發展。	

資料來源：資策會產業情報研究所整理

4.2 3GPP 分散式基地臺標準技術

當 5G 行動通訊網路導入 5G 基地臺集中單元與分散單元分割(CU-DU split)網路架構後，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。本節將闡述現有第三代合作夥伴計畫(The 3rd Generation Partnership Project , 3GPP)的 Open RAN 架構的標準技術，於第 4.2.1 節描述集中單元與分散單元分割標準技術，緊接著於第 4.2.2 節討論集中單元控制平面與用戶平面分離標準技術，最後於第 4.2.3 節探討分散單元與無線電單元分割的技術研究。

4.2.1 集中單元與分散單元分割標準技術

第三代合作夥伴計畫(3GPP)在分散式基地臺標準制定過程中，於3GPP TR 38.801 技術研究報告[4]中，提到集中單元(CU)與分散單元(DU)分割的好處在於能夠靈活搭配硬體以節省布署成本。報告中總共提出 8 種集中單元與分散單元分割架構的方案(如圖 2 所示)，分別為於無線資源控制(Radio Resource Control, RRC)和封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)間進行分割的第 1 方案(Option 1)、於封包數據匯聚協定(PDCP)和無線鏈路控制(Radio Link Control, RLC)間進行分割的第 2 方案(Option 2)、於上層無線鏈路控制(Upper-RLC)和下層無線鏈路控制(Lower-RLC)間進行分割的第 3 方案(Option 3)、於無線鏈路控制(RLC)和媒體存取控制(Media Access Control, MAC)間進行分割的第 4 方案(Option 4)、於上層媒體存取控制(Upper-MAC)和下層媒體存取控制(Lower-MAC)間進行分割的第 5 方案(Option 5)、於媒體存取控制(MAC)和實體層(Physical layer, PHY)間進行分割的第 6 方案(Option 6)、於上層實體層(Upper-PHY)和下

層實體層(Lower-PHY)間進行分割的第 7 方案(Option 7)以及於實體層(Physical layer, PHY)和射頻(Radio Frequency, RF)信號處理間進行分割的第 8 方案(Option 8)。

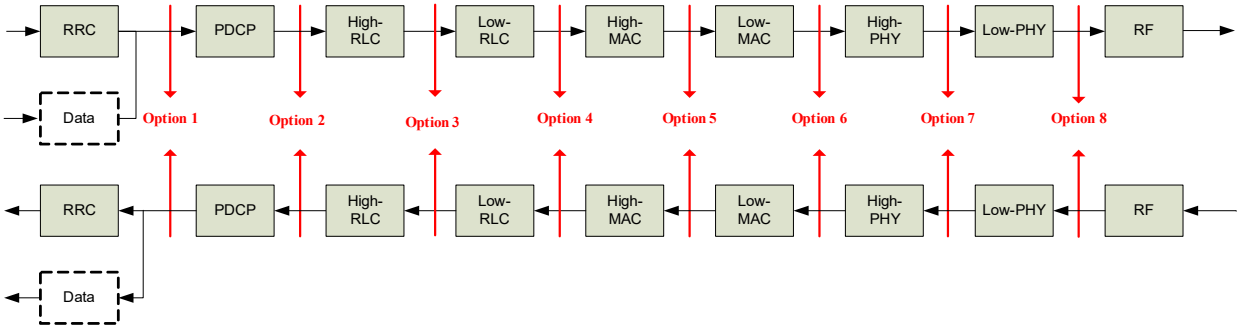

圖 2 集中單元與分散單元分割架構方案[4]

在考量集中單元(CU)與分散單元(DU)分割架構下[4]，為了實現性能和負載管理的協調以及落實網路功能虛擬化(Network Function Virtualization, NFV)的架構。最後 5G 基地臺集中單元(gNB-CU)與 5G 基地臺分散單元(gNB-DU)分割架構(如圖 3 圖 2 所示)採用了第 2 方案(Option 2)，兩者間透過 F1 介面連接。其中 5G 基地臺集中單元(gNB-CU)負責無 5G 基地臺中無線資源控制(Radio Resource Control, RRC)與服務數據適配協定(Service Data Adaptation Protocol, SDAP)以及封包數據匯聚協定(Packet Data Convergence Protocol, 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(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。

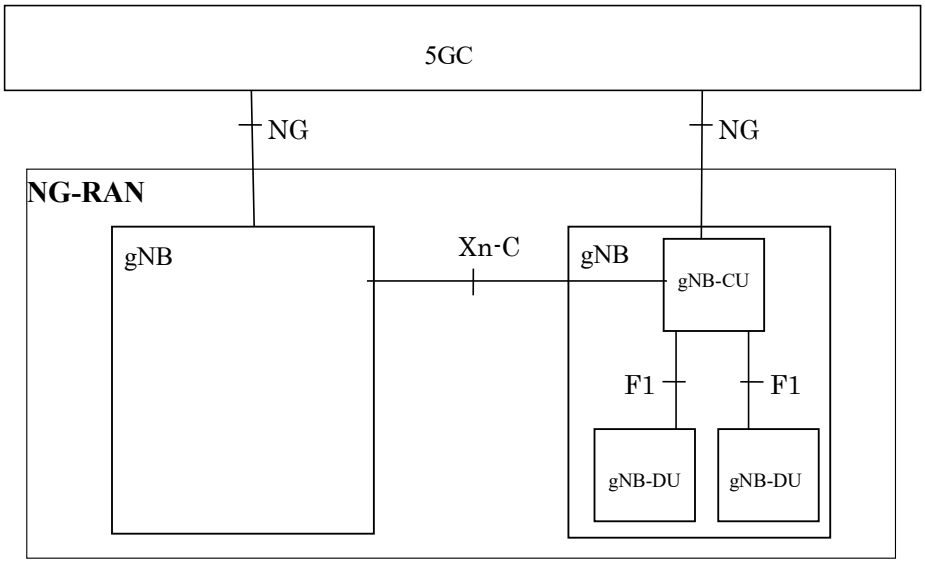

圖 3 5G 基地臺集中單元與分散單元分割架構[1]

4.2.2 集中單元控制平面與用戶平面分離標準技術

第三代合作夥伴計畫(3GPP)也基於第 2 方案(Option 2)之集中單元與分散單元分割標準架構[4]，探討並制定了支援集中單元控制平面與用戶平面分離(CP-UP Separation)的架構及相關介面(如圖 4 所示)[5]，將 5G 基地臺集中單元(gNB-CU)進一步拆分為 5G 基地臺集中單元-控制平面(gNB-CU Control Plane, gNB-CU-CP)與 5G 基地臺集中單元-用戶平面(gNB-CU User Plane, gNB-CU-UP)。優點包括增加網路運作管理的彈性與最佳化無線接取網路(RAN)功能的效率，及增加不同廠商間設備的互通性；然而相對也會增加網路的複雜度、維運工作及信令傳輸的延遲。

5G 基地臺集中單元-控制平面(gNB-CU-CP)主要負責 5G 基地臺中，無線資源控制(Radio Resource Control, RRC)與封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)控制平面功能，5G 基地臺集中單元-用戶平面(gNB-CU-UP)者則負責 5G 基地臺中，服務數據適配協定(Service Data Adaptation Protocol, SDAP)以及封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)用戶平面功能，兩者間透過 E1 介面連接。

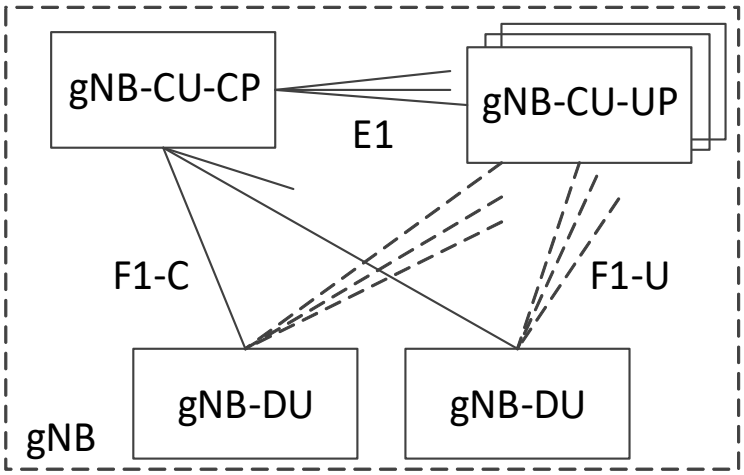

圖 4 5G 基地臺集中單元之控制平面與用戶平面分離架構[1]

在 3GPP TR 38.806 技術研究報告[5]所描述的分離架構中，一個 5G 基地臺(gNB)可由一個 5G 基地臺集中單元-控制平面(gNB-CU-CP)、多個 5G 基地臺集中單元-用戶平面(gNB-CU-UPs)以及多個 5G 基地臺分散單元(gNB-DUs)所組成。而一般電信事業在布署時，只會將一個 5G 基地臺集中單元-用戶平面(gNB-CU-UP)連接至一個 5G 基地臺集中單元-控制平面(gNB-CU-CP)，並將一個 5G 基地臺分散單元(gNB-DU)連接至一個 5G 基地臺集中單元-控制平面(gNB-CU-CP)，不過在高可用性(High availability, HA)的應用情境下，是可以連接至多個 5G 基地臺集中單元-控制平面(gNB-CU-CP)。

4.2.3 分散單元與無線電單元分割的技術研究

5G 基地臺(gNB)功能分割(functional split)的方式需要滿足不同應用場景的需求，如傳輸時延的多變性。於 3GPP TR 33.801 技術研究報告[4]中，提到如何對 5G 基地臺進行功能分割(functional split)取決於網路布署的場域、限制及服務等，如需要根據不同的應用服務設定低延遲與高傳輸率等不同的服務品質(Quality of Service, QoS)。

因為基於第 2 方案(Option 2)之集中單元與分散單元分割標準架構不適用於低延遲的布署場域，為了滿足超可靠度和低延遲通訊(Ultra-reliable and Low Latency Communications, URLLC)場域的需求，第三代合作夥伴計畫(3GPP)在分散式針對於上層實體層(Upper-PHY)和下層實體層(Lower-PHY)間進行分割的第 7 方案(Option 7)進一步進行分析討論。

在3GPP TR 38.816技術研究報告[6]中，提到在第6方案(Option 6)與第7方案(Option 7)進行低層分割(low layer split)，其中第 7 方案(Option 7)可以進一步分為第 7-1 方案(Option 7-1)、第 7-2 方案(Option 7-2)與第 7-3 方案(Option 7-3)等三個分割方案(如圖 5 所示)。

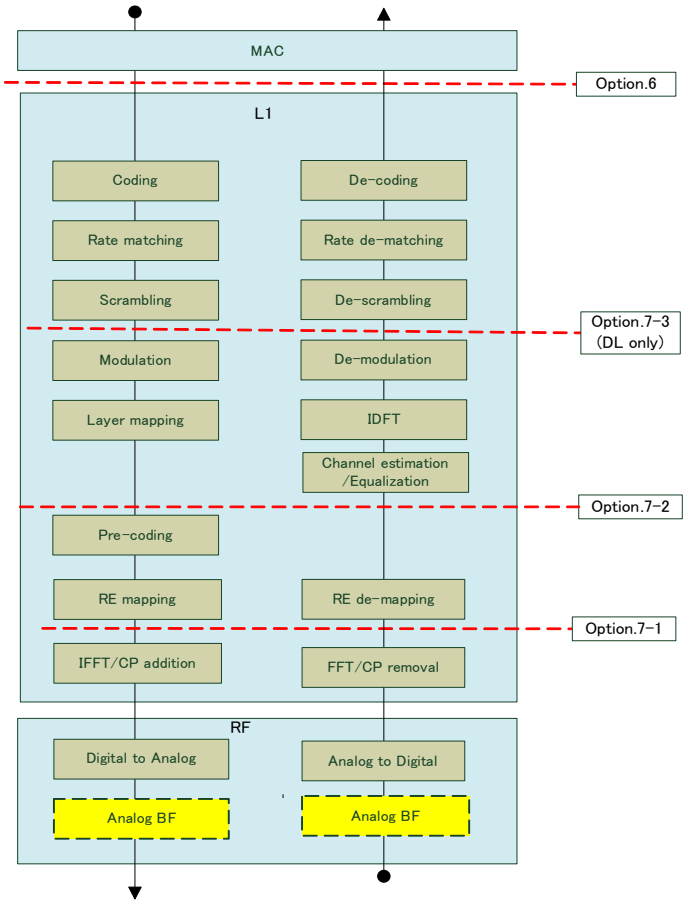

圖 5 5G 基地臺低層分割(low layer split)[6]

由於無線存取網路第 1 工作組(Radio Access Network 1, RAN1)認為低層分割依據實作需求不需要訂定單一標準[6]，且無線存取網路第 3 工作組(Radio Access Network 3, RAN3)對於低層分割方案無法達成共識，故第三代合作夥伴計畫(3GPP)現階段並未制訂低層分割標準。

4.3 O-RAN 制定的 Open RAN 基地臺標準技術

開放式無線接取網路聯盟(Open Radio Access Network Alliance, O-RAN Alliance)成立的目標是基於第三代合作夥伴計畫(3GPP)的 5G 基地臺(gNB)架構，發展一個開放式無線接取網路的管理架構，提供 5G 基地臺(gNB)的無線接取網路(Radio Access Network, RAN)網路功能虛擬化，同時在標準化介面的基礎之上使用商用產品(Commercial off the shelf, COTS)和開放原始碼軟體(Open Source Software)。透過開放降低白牌裝置的進入障礙，進而降低電信事業的整體建置成本，並提供 5G 眾多異質接取設備的最佳化管理。並導入嵌入式機器學習(Machine learning, ML)和人工智慧(Artificial Intelligence, AI)的即時分析，以開放架構與介面互通為目標來使行動通訊業者能滿足智慧城市、工業自動化和車聯網等新商機。

4.3.1 O-RAN 分散單元與無線電單元分割的標準技術

開放式無線接取網路聯盟(O-RAN Alliance)主要是制定第三代合作夥伴計畫(3GPP)沒有標準化的低層分割(low layer split)架構，並提供協定外的裝置管理為主，發展重點也著重於開放硬體架構，故 Open RAN 的架構不會重複定義 5G 基地臺集中單元-控制平面(gNB-CU Control Plane, gNB-CU-CP)與 5G 基地臺集中單元-用戶平面(gNB-CU User Plane, gNB-CU-UP)及 5G 基地臺分散單元(gNB-DU)。其所制定的 O-RAN 分散單元(O-RAN Distributed Unit, O-DU)又稱為低層分割的集中單元(Lower Layer Split Central Unit)，與 O-RAN 無線電單元(O-RAN Radio Unit, O-RU)透過通用公共無線電介面(Common Public Radio Interface, CPRI)或演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)介面相連(12)，開放式無線接取網路聯盟(O-RAN Alliance)所制定的 Open RAN 低層分割的架構如下圖 6 所示。

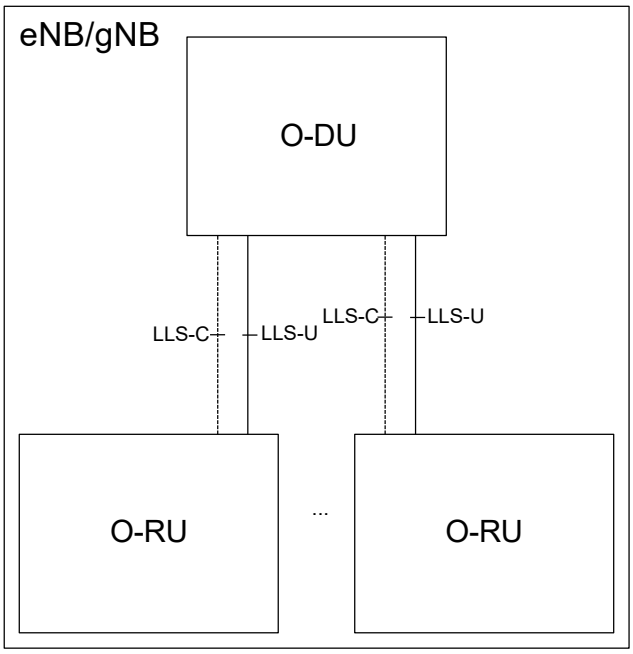

圖 6 O-RAN 基地臺低層分割(low layer split)(12)

4.3.2 無線接取網路智能控制的標準技術

開放式無線接取網路聯盟(O-RAN Alliance)在無線接取網路智能控制(Radio Access Network Intelligent Controller, RIC)的標準化上(如圖 7 所示)，專注於無線接取網路的開放式架構和標準化介面開發，搭配開放原始碼和白盒網路元件等軟硬體資源配合，並研究如何導入人工智慧(Artificial Intelligence, AI)和機器學習(Machine learning, ML)等智能技術，共同完成網路智慧化、架構和介面開放化、硬體設備白盒化與軟體開源化四大方向，為全球創建下一代靈活的無線網路。

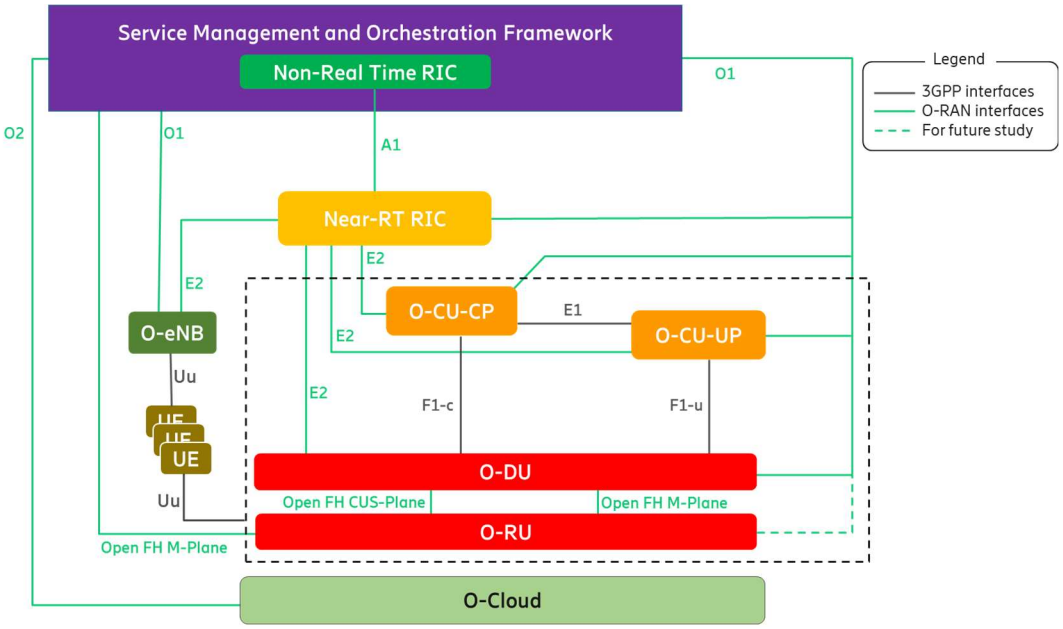

圖 7 Open RAN 系統架構[11]

5G 行動通訊技術在開放架構之解構下，未來廠商可藉由各模組間共通介面標準，依據不同應用情境需求，以 xApps 應用程式的模式提供智慧網路應用所需不同之資訊延遲品質需求、訊號覆蓋範圍與訊號強度。並針對不同應用之彈性預測與調整，反應無線通訊環境即時狀態，協助決策系統針對不同服務提供差異化通訊品質服務，透過 E2 及 O1 等介面達到整合開放式介面技術及接取網路智慧化控制技術。

服務管理與編排(Service Management and Orchestration, SMO)主要提供網路設備的管理服務，可透過 O1 介面進行故障、組態、歸責、效能及安全管理(Fault Configuration Accounting Performance Security, FCAPS)，同時進行雲端計算平台(O-Cloud)資源及負載管理，以及透過開放式前傳介面(Open Front-Haul, OFH)的管理平面(M-Plane)介面進行 O-RAN 無線電單元(O-RAN Radio Unit, O-RU)管理。服務管理與編排(SMO)內包含非即時無線接取網路智能控制(Non-Real Time Radio Access Network Intelligent Controller, Non-RT RIC)，主要功能為資料分析、訓練機器學習模型與提供額外資訊及政策制定。非即時無線接取網路智能控制(Non-RT RIC)分別從服務管理與編排(SMO)及應用服務端取得無線電接取網路(RAN)與用戶相關資料，再透過機器學習訓練識別及預測模型，透過 A1 介面將機器學習模型布署於非即時無線接取網路智能控制(Non-RT RIC)，使其可因應流量與環境的變化，主動或提前調整網路資源配置。

近即時無線接取網路智能控制(Near Real Time Radio Access Network Intelligent Controller, Near-RT RIC)位於無線電接取網路(RAN)內，接收與分析來自無線電接取網路(RAN)的即時資訊，結合非即時無線接取網路智能控制(Non-RT RIC)提供的額外資訊，利用非即時無線接取網路智能控制(Non-RT RIC)的機器學習模型監控或預測連線狀況的變化，並透過 E2 介面對無線電接取網路(RAN)進行參數調整，在近即時無線接取網路智能控制(Near-RT RIC)中，針對不同的應用有個別的 xApps 應用程式進行資料監控與對於無線電接取網路(RAN)功能進行參數調整。

5. 5G Open RAN 安全的國際發展趨勢與資安議題

O-RAN 改變傳統基地臺設備被國際大型電信設備商壟斷的困境，以產業分工提高整體產業效率和競爭力。但隨著 Open RAN 開放式架構的網通設備「白牌化」後，硬體軟體整合會有軟體相容性問題。市場也擔心開放架構會不會讓資安漏洞更多，且一旦出現資安疑慮更會無從查起，會讓資安問題更加複雜化。本節將闡述現有國際 5G Open RAN 架構的資安議題，於第 5.1 節介紹 Open RAN 安全的國際發展趨勢，探討 Open RAN 安全的國際政策與國際大廠對 Open RAN 資安議題的見解後，緊接著於第 5.2 節討論 3GPP 分散式基地臺的資安議題，最後於第 5.3 節簡述 Open RAN 基地臺的資安議題。

5.1 Open RAN 安全的國際發展趨勢

5.1.1 Open RAN 安全的國際政策

美國於 2020 年 3 月發布「安全可信通訊網路法(Secure and Trusted Communications Networks Act)」(13)，以保護國內的通訊網路以及 5G 技術之安全。該法案要求要求美國聯邦通訊委員會(Federal Communications Commission, FCC)公布造成國安威脅之法人名單；禁止以聯邦經費購買或租借具國安威脅的電信設備；補償拆除與更換具國安威脅的電信設備，成立 Open RAN 政策聯盟並與美國政府、產業緊密合作。

美國國防部(Department of Defense, DoD)於 2020 年 5 月發布「國防部 5G 戰略(Department of Defense 5G Strategy)」文件(14)，提及國防部的實驗計畫將提供 5G 核心與邊緣網路更安全的設計，包含開放架構與虛擬化網路切片等相關實驗，確保相關利益者提升安全。藉由大量的實驗場域驗證 5G 應用，推動技術發展；掌握 5G 資安威脅情報與威脅，評估、識別資安風險採取必要措施，並採取零信任(Zero Trust)反覆驗證之資安模式；積極加入 5G 技術相關標準訂定與規劃 5G 國防政策；吸引國際組織、國家與相關產業的合作夥伴，積極溝通協調以維持美國與合作夥伴間的共同利益，協助美國的盟友與合作夥伴識別 5G 風險。

美利堅合眾國眾議院(United States House of Representatives)於 2020 年 11 月通過的「美國電信法(USA Telecommunications Act)」，透過美國國家電信暨資訊管理局(National Telecommunications and Information Administration, NTIA)提供 7.5 億美元撥款，支援全美加速 5G Open RAN 架構網路的布署和使用，並於 2020 年 12 月提出將加速 Open RAN 架構網路的發展納入「2021 年國防授權法案(FY 2021 National Defense Authorization Act)」(15)中。

為了倡導推動建立「開放並可互操作」5G 網路架構(16)，美國聯合全球數十家科技和電信企業成立「開放無線接入網政策聯盟(Open RAN Policy Coalition)」，並由前美國國家電信暨資訊管理局(National Telecommunications and Information Administration, NTIA)代理行政長、前商務部負責電信和資訊事務代理助理部長戴安·李納多(Diane Rinaldo)擔任執行董事，該聯盟主要宗旨是推動各國政府政策支援「開放無線接入網」架構。

美國禁止和拆除華為(Huawei)設備之餘面臨的難題是缺乏本土公司選擇。而在 Open RAN 的網路架構下，電信事業可採用不同廠商的軟體和通用硬體，達成模組化混合組網，為美國本土企業參與競爭提供新機會。美國電信事業 AT&T 與威訊通訊(Verizon)及 Dish Networks 開始進行 Open RAN 架構網路的大規模的試營運，其中 AT&T 使用了三星(Samsung)與愛立信(Ericson)的設備在美國德州進行了大規模的網路測試，而 Dish Networks 也開始利用 Open RAN 技術建構一些大型私有網路。

美國聯邦通訊委員會(FCC)於 2020 年 9 月依據「美國 5G 科技加速方案(5G FAST Plan)」(17)，專就 5G Open RAN 架構舉行論壇(Forum on 5G Open Radio Access Networks)(18) 邀請專家分享，以提供傳統電信設備的替代方案，並藉此實踐供應商多樣性，提升網路安全同時降低成本。參與會議的 AT&T 與威訊通訊(Verizon)表達支持 5G Open RAN 的架構。『美國國務卿蓬佩奧(Mike Pompeo)在主題演講時說，美國希望各國選擇值得信賴的 5G 網路供應商，「而不是與中共有勾連的供應商。」委員會主席阿吉特·帕伊(Ajit Pai)則表示，「開放無線接入網」有可能成為華為設備的代替解決方案。美國將迎來供應商多樣性，且安全密鑰將掌握在網路商手中，而不是中國供應商。』(16)(18)

在美國等國家的推動之下，越來越多的電信事業開始採用 Open RAN 的網路架構建設 5G 無線通訊網路。在以國家安全為由禁止華為設備之後，日本電信設備供應商日本電氣公司(NEC)在 2020 年底開始在英國建設建立 Open RAN 架構網路的 5G 無線通訊網路，利用在日本支持 Open RAN 的網路架構商業布署的經驗，幫助電信事業在世界各地推出新架構網路。美國於 2021 年 1 月成立約 5 億美元的「跨國通訊安全基金」，邀請五眼聯盟國家與日本共同發展 5G 設備。

5.1.2 國際大廠對 Open RAN 資安議題的見解

開放式無線接取網路聯盟(O-RAN Alliance)基於第三代合作夥伴計畫(3GPP)的 5G 基地臺(gNB)架構，發展一個開放式無線接取網路的管理架構，兩者間的 5G 基地臺(gNB)架構差異比較如圖 8 所示。

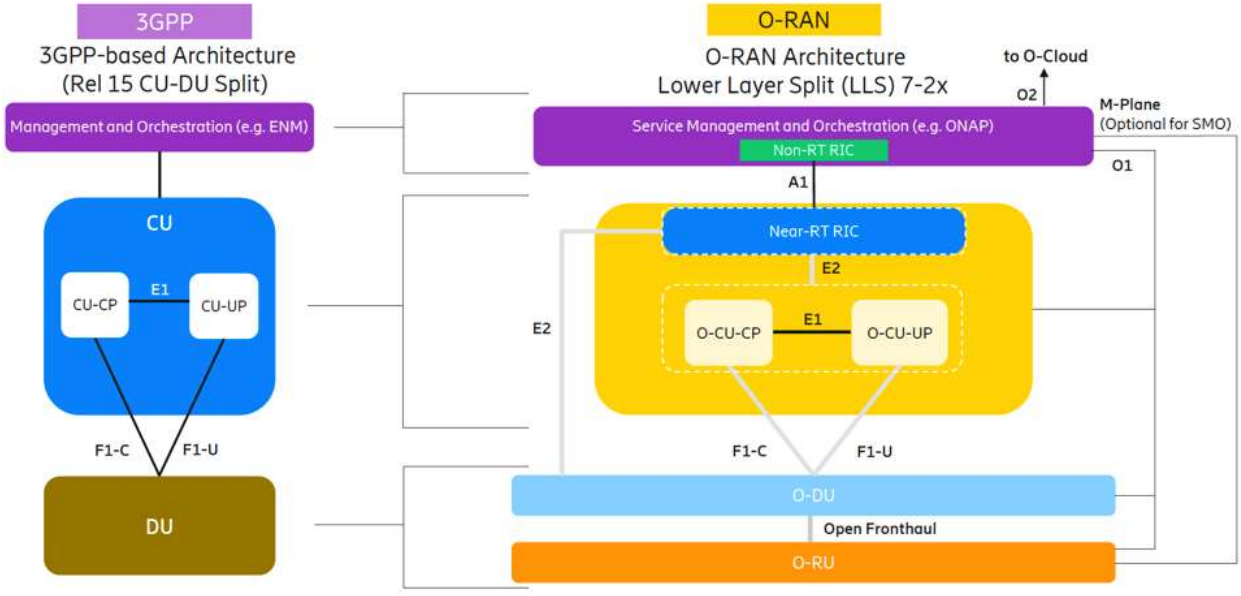

圖 8 O-RAN Alliance 與 3GPP 架構比較(21)

電信設備業者愛立信(Ericsson)認為相較於軟硬體高度整合的專有無線基礎設施，Open RAN 的基礎技術天生就不安全。其安全暨網路產品解決方案負責人在「確保開放性不會為 5G 網路的新風險開啟大門(Making sure that Open doesn’ t open the door for new risks in 5G)」一文(20)以及「開放式無線接取網路安全考量(Security Considerations of

Open RAN)」白皮書(21)中，具體指明在採用 Open RAN 架構之前必須要審慎考量的數個議題，並強調該種架構在被廣泛布署之前應該要考量其安全性。Open RAN 架構帶來了全新、額外的接觸點，以及軟體和硬體的脫鉤，這有可能從多個方面擴展威脅及網路攻擊面包括：

(a) A1 介面與 E2 介面以及開放前傳介面(front-haul interface)等新介面增加威脅面

(b) 近即時無線接取網路智能控制(Near-RT RIC)與 xApp 應用程式所帶來的新威脅

(c) 硬體脫鉤增加了對信任鏈(Trust Chain)的威脅

(d) 管理介面依據現有產業最佳實作規範(industry best practice)並不夠安全

(e) 開源軟體的風險威脅

任何新興技術，安全性都不是事後才想到的，而應該建立在安全設計的方法之上。愛立信(Ericsson)建議對於 Open RAN 應當落實下列安全機制：

(a) 應該擴大保護 Open RAN 更多的介面和功能。

(b) 限制與近即時無線接取網路智能控制(Near-RT RIC)相關的資安風險，尤其是與控制框架與策略指導能力以及 xApps 應用程式的潛在衝突等相關風險。

(c) 透過強制執行驗證硬體信任機制如憑證來解決功能脫鉤產生的信任鏈(Trust Chain)威脅。

(d) 依據產業最佳實作規範使用傳送層安全協定(Transport Layer Security protocol, TLS)和數位簽章來確保管理介面的安全性。

(e) 在使用開源代碼時，需透過實施安全成熟的 DevOps 以實踐更高層次的資安檢查。

(f) 實作實體攻擊防護。

相較於設備大廠如愛立信(Ericsson)、諾基亞(Nokia)與華為(Huawei)所提供的 5G 電信設備，Open RAN 透過將 5G 電信設備的不同元件分割的方式，讓電信事業能在同一個 5G 電信網路中混合設置來自不同供應商的產品，故能帶來更顯著的成本效益。然而，5G 電信產業也意識到 Open RAN 網路安全性是整個行動網路基礎架構中重要的元素。

5.2 3GPP 分散式基地臺的資安議題

第三代合作夥伴計畫(3GPP)標準規範定義之 5G 基地臺集中單元(gNB Central Unit, gNB-CU)與 5G 基地臺分散單元(gNB Distributed Unit, gNB-DU)分割架構(如圖 9 所示)，兩者間透過 F1 介面連接。同時也制定支援集中單元控制平面與用戶平面分割(CP-UP Separation)的架構及相關介面[5]，將 5G 基地臺集中單元(gNB-CU)進一步拆分為 5G 基地臺集中單元-控制平面(gNB-CU Control Plane, gNB-CU-CP)與 5G 基地臺集中單元-用戶平面(gNB-CU User Plane, gNB-CU-UP)，如圖 9 所示兩者間透過 E1 介面連接。

其中 5G 基地臺集中單元-控制平面(gNB-CU-CP)主要負責無線資源控制(Radio Resource Control, RRC)與封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)等控制平面的網路功能，涉及到用戶設備(UE)之控制平面(control plane)封包的完整性和機密性；5G 基地臺集中單元-用戶平面(gNB-CU-UP)者則負責服務數據適配協定(Service Data Adaptation Protocol, SDAP)以及封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)等用戶平面的網路功能，涉及到用戶設備(UE)之用戶平面(user plane)封包的完整性和機密性；而 5G 基地臺分散單元(gNB-DU)則負責無線鏈路控制(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，不會涉及到用戶設備(UE)的完整性和機密性(22)，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)。

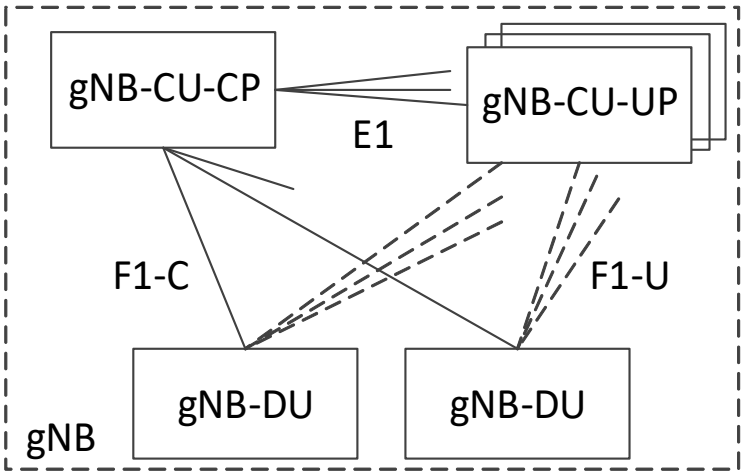

圖 9 5G 基地臺集中單元之控制平面與用戶平面分割架構[1]

5.2.1 5G 基地臺的資安威脅分析

依據 3GPP TR 33.926 網路產品類別之威脅和關鍵資產的安全保證規範研究報告[3]，可以將 5G 基地臺資安風險分析歸納為七種威脅層面的主要威脅，分別為 3GPP 定義的網路介面威脅(Threats relating to 3GPP-defined interfaces)、識別碼欺騙(Spoofing identity)、竄改(Tampering)、否認性(Repudiation)、資訊揭露(Information disclosure)、阻斷服務(Denial of Service)以及提高特權(Elevation of privilege)，其中針對 5G 基地臺風險分析如下。

表 5 5G 基地臺的資安威脅分析

威脅種類	威脅細節
3GPP 定義的網路介面威脅(Threats relating to 3GPP-defined interfaces)	N2 介面威脅
	N3 介面威脅
	Xn 介面威脅
	F1 介面威脅
	E1 介面威脅
	NR-Uu 介面威脅
識別碼欺騙(Spoofing identity)	預設帳戶(Default Accounts)
	弱密碼政策(Weak Password Policies)
	窺視密碼(Password peek)
	直接根存取(Direct Root Access)
	網際通訊協定欺騙(IP Spoofing)
	惡意程式(Malware)
	竊聽(Eavesdropping)

威脅種類	威脅細節
竄改(Tampering)	軟體竄改(Software Tampering)
	所有權檔案誤用(Ownership File Misuse)
	開機竄改(Boot tampering)
	日誌竄改(Log Tampering)
	營運管理與維護流量竄改 (OAM traffic Tampering)
	檔案寫入權限濫用(File Write Permissions Abuse)
	用戶通信期竄改(User Session Tampering)
否認性(Repudiation)	缺乏用戶活動記錄(Lack of User Activity Trace)
資訊揭露 (Information disclosure)	不良金鑰產生(Poor key generation)
	不良金鑰管理(Poor key management)
	弱密碼演算法(Weak cryptographic algorithms)
	不安全資料儲存(Insecure Data Storage)
	系統指紋(System Fingerprinting)
	惡意程式(Malware)
	個人識別資訊違規(Personal Identification Information Violation)
	不安全預設組態(Insecure Default Configuration)
	檔案/目錄讀出權限濫用(File/Directory Read Permissions Misuse)
	資訊揭露-不安全網路服務(Insecure Network Services)
	非必要服務(Unnecessary Services)
	日誌揭露(Log Disclosure)
	非必要應用(Unnecessary Applications)
	竊聽(Eavesdropping)
	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)
阻斷服務(Denial of Service)	被破解/行為異常用戶設備(Compromised/Misbehaving User Equipment)
	實作缺陷(Implementation Flaw)
	阻斷服務-不安全網路服務(Insecure Network Services)
	人為錯誤(Human Error)
提高特權(Elevation of privilege)	授權使用者誤用(Misuse by authorized users)
	超過特權的程序/服務(Over-Privileged Processes/Services)
	資料夾寫入權限濫用(Folder Write Permission Abuse)
	根所屬檔案寫入權限濫用(Root-Owned File Write Permission Abuse)
	高特權檔案(High-Privileged Files)
	提高特權-不安全網路服務(Insecure Network Services)
	透過非必要網路服務提高特權(Elevation of Privilege via Unnecessary Network Services)

5.2.2 虛擬化 5G 基地臺的資安威脅分析

依據 3GPP TR 33.818 網路虛擬化產品的安全確保方法和安全保證規範研究報告(Security Assurance Methodology(SECAM); and Security Assurance Specification(SCAS)for 3GPP virtualised network products)[7]，5G 網路虛擬化分為三種布署模式如下：

(a) 布署模式 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)，並將其布署在第三方網路功能虛擬化基礎建設(Network Functions Virtualization Virtualization, NFVI)上。

(b) 布署模式 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)，並布署在第三方硬體層(hardware layer)上。

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

電信網路運營商的三種布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：

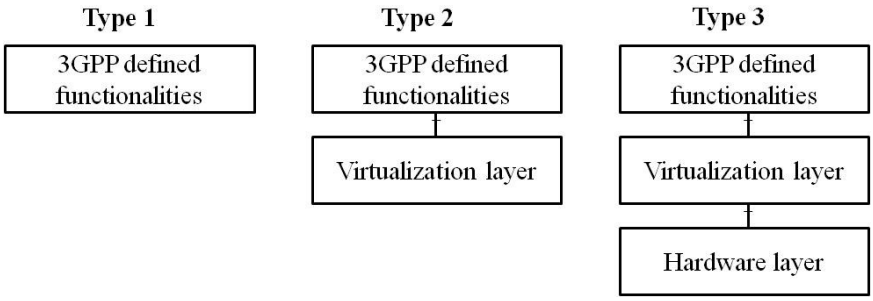

圖 10 三種網路虛擬化產品型態[7]

電信網路運營商在布署分散式虛擬化 5G 基地臺時，一般會採用通用虛擬化網路產品型態 3，其定義的行動網路功能、虛擬層(virtualization layer)和硬體層(hardware layer)，如下：

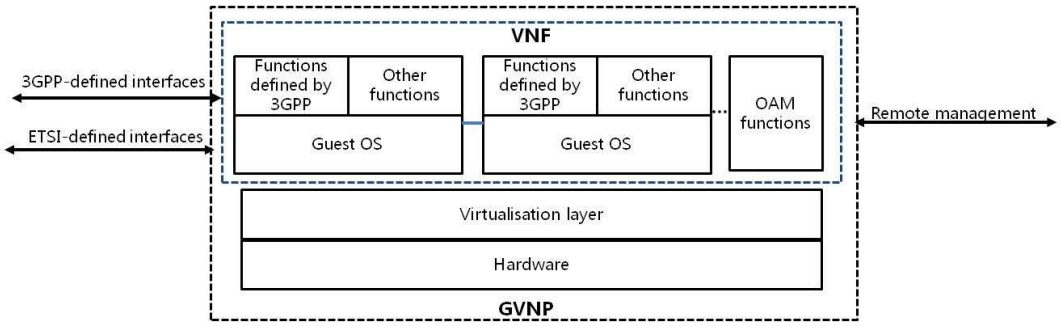

圖 11 通用虛擬化網路產品型態 3 的架構[7]

虛擬化 5G 基地臺的資安威脅分析與非虛擬化 5G 基地臺的資安威脅分析比較如下：

表 6 虛擬化 5G 基地臺的資安威脅分析表

威脅種類	威脅細節(TR 33.818)	與既有非虛擬化(TR 33.926)的威脅比較
3GP 定義的網路介面威脅	N2 介面威脅	適用 3GPP TR 33.926 之第 5.3.2 節的威脅
	N3 介面威脅	
	Xn 介面威脅	
	F1 介面威脅	
	E1 介面威脅	
	NR-Uu 介面威脅	
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(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。

威脅種類	威脅細節(TR 33.818)	與既有非虛擬化(TR 33.926)的威脅比較
識別碼欺騙(Spoofing identity)	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

威脅種類	威脅細節(TR 33.818)	與既有非虛擬化(TR 33.926)的威脅比較
資訊揭露(Information disclosure)	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

5.2.3 5G 基地臺的資安需求

第三代合作夥伴計畫(3GPP)標準規範定義之 5G 基地臺集中單元-控制平面(gNB-CU Control Plane, gNB-CU-CP)與 5G 基地臺集中單元-用戶平面(gNB-CU User Plane, gNB-CU-UP)以及 5G 基地臺分散單元(gNB Distributed Unit, gNB-DU)分割架構(如圖 9 所示)，依據第三代合作夥伴計畫(3GPP)TS 33.501 的安全標準規範，要求 5G 基地臺集中單元(gNB-CU)與 5G 基地臺分散單元(gNB-DU)間的 F1 介面連線安全，以及 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)間的 E1 介面連線安全，都需透過網際網路安全協定(Internet Protocol Security, IPSec)保護。依據 3GPP TS 33.501 5G 系統的安全架構與處理流程(Security architecture and procedures for 5G System)、3GPP TS 33.511 5G 基地臺產品類別的安全保證規範(Security Assurance Specification(SCAS)for the next generation Node B(gNodeB)network product class)[8]與 3GPP TS 33.117 通用安全保證規範(Catalogue of general security assurance requirements)[9]及 3GPP TR 33.818 網路虛擬化產品的安全確保方法和安全保證規範研究報告(Security Assurance Methodology(SECAM); and Security Assurance Specification(SCAS) for 3GPP virtualised network products)[7]，5G 基地臺的資安需求標準與資安測試標準對應表如下表 7 所示。

表 7 5G 基地臺的資安需求

需求標準	標題	3GPP 資安需求
TS 33.501 §5.1.1, §6.7.3.1 TS 33.511 §4.2.2.1.14	防範 Xn 介面交遞中的降階攻擊	即使用戶設備(User Equipment, UE)和網路實體都支援安全防護功能，攻擊者可以透過降階攻擊讓雙方相信對方不支援該安全防護功能。故應確保可以防止 Xn 介面交遞中的降階攻擊。
TS 33.501 §5.1.2	認證與授權	網路實體應該向用戶設備(UE)提供服務前先進行入網認證授權，該入網認證授權隱含在成功建立入網連線的信令中，並適用於所有類型的無線存取網路。
TS 33.501 §5.1.3	與 5G 基地臺的密鑰相關需求	5G 基地臺(gNB)必需使用 128 位元或 256 位元金鑰的加密和完整性保護演算法保護存取層(Access Satrum, AS)和非存取層(Non-Access Satrum, NAS)。
TS 33.501 §5.2.5	用戶隱私	除了行動國家代碼(Mobile Country Code, MCC)和行動網路代碼(Mobile Network Code，MNC)等路由資訊外，透過 5G 基地臺(gNB)傳輸的行動用戶永久識別碼(Subscriber Permanent Identifier, SUPI)不應該為明文。

需求標準	標題	3GPP 資安需求
TS 33.501 §5.3.2 TS 33.511 §4.2.2.1.6, §4.2.2.1.7, §4.2.2.1.10, §4.2.2.1.11	用戶數據和信令的機密性	5G 基地臺(gNB)應支援根據連結管理功能(Session Management Function, SMF)發送的安全策略啟用和用戶設備(UE)間的用戶數據加密保護。5G 基地臺(gNB)應支援選擇是否啟用無線電資源控制(Radio resource control, RRC)信令的加密保護。只要法規允許，就應使用加密保護措施。
TS 33.501 §5.3.3 TS 33.511 §4.2.2.1.1, §4.2.2.1.2, §4.2.2.1.8, §4.2.2.1.9	用戶數據和信令的完整性	5G 基地臺(gNB)應支援根據連結管理功能(Session Management Function, SMF)發送的安全策略啟用和用戶設備(UE)間的用戶數據完整性保護。5G 基地臺(gNB)應支援無線電資源控制(RRC)信令的完整性保護。除了使用緊急服務外，無線電資源控制(RRC)信令的加密保護是強制啟用。
TS 33.501 §6.5.1	無線資源控制完整性檢查失敗	無線電資源控制(RRC)信令的完整性檢查應在移動式設備(Mobile equipment, ME)和 5G 基地臺(gNB)中執行。在啟用完整性保護後，如果收到完整性檢查失敗的信令必需被丟棄。
TS 33.501 §6.6.4	用戶平面完整性檢查失敗	在啟用完整性保護後，如果 5G 基地臺(gNB)或用戶設備(UE)收到完整性檢查失敗的封包資料匯聚通訊協定(Packet data convergence protocol, PDCP)的協定資料單元(Protocol Data Unit, PDU)必需被丟棄。
TS 33.501 §5.3.4	5G 基地臺設定和配置的需求	設定和配置 5G 基地臺(gNB)的運維系統(O&M systems)需要進行身分驗證和授權，這樣攻擊者就不能通過本地或遠程訪問修改 5G 基地臺(gNB)設定和軟體配置。運維系統(O&M systems)和 5G 基地臺(gNB)間的通信應具備機密性、完整性和重播保護。
TS 33.501 §5.3.5	5G 基地臺內部密鑰管理的需求	應保護 5G 基地臺(gNB)中以明文形式存儲或處理的金鑰，如放置於實體保全環境以避免受實體攻擊。
TS 33.501 §5.3.6	處理 5G 基地臺用戶平面數據的需求	應保護 5G 基地臺(gNB)中以明文形式存儲或處理的用戶平面數據，如放置於實體保全環境以避免受實體攻擊。
TS 33.501 §5.3.7	處理 5G 基地臺控制平面數據的要求	應保護 5G 基地臺(gNB)中以明文形式存儲或處理控制平面數據，如放置於實體保全環境以避免受實體攻擊。
TS 33.501 §5.3.8	5G 基地臺的安全環境要求	實體保全環境應支援敏感數據的安全存儲和執行敏感功能與啟動過程中執行敏感功能，以及應確保實體保全環境的完整性。只有經過授權的用戶才能訪問實體保全環境

需求標準	標題	3GPP 資安需求
TS 33.501 §5.3.9, §9.8.2	5G 基地臺的 F1 介面要求	F1-C 介面應支持機密性、完整性和重放保護。集中單元與分散單元(CU-DU)介面上的管理流量都應受到完整性、機密性和重放保護。F1-U 介面應支持機密性、完整性和重放保護。F1-C 介面與集中單元與分散單元(CU-DU)介面上的管理流量需要跟 F1-U 介面分開保護。
TS 33.501 §5.3.10, §9.8.3	5G 基地臺的 E1 介面要求	E1 介面應支持機密性、完整性和重放保護。
TS 33.501 §9.2, §9.4 TS 33.511 §4.2.2.1.16, §4.2.2.1.17	N2/Xn 介面的安全機制	Xn/N2 介面的控制平面數據和用戶數據應具有完整性、機密性和重放保護。
TS 33.501 §6.7.3.0, §5.11.2 TS 33.511 §4.2.2.1.12	存取層安全防護演算法的選擇方式	行動網路應根據的用戶設備安全能力(UE security capabilities)和行動網路當前配置的安全能力允許列表，選擇要使用的安全演算法。每個 5G 基地臺(gNB)應該透過行動網路管理配置允許使用的完整性演算法列表以及加密演算法列表。
TS 33.501 §6.7.3.1, §6.7.3.2 TS 33.511 §4.2.2.1.15	於 5G 基地變更時存取層安全演算法選擇	目標 5G 基地臺(gNB)應該根據行動網路當前配置的安全能力允許的優先順序列表，從用戶設備安全能力(UE security capabilities)中選擇優先級最高的算法。如果目標 5G 基地臺(gNB)選擇與來源 5G 基地臺(gNB)不同的演算法，則應在 Handover Command 信令中指示用戶設備(UE)選定的新演算法。
TS 33.501 §6.10.2.1, §6.10.2.2.1 TS 33.511 §4.2.2.1.18	雙連線的 5G 基地臺金鑰更新	當對同一個次要節點(Secondary Node, SN)添加將後續的無線承載時，主要節點(Master Node, MN)應為每個新的無線承載分配一個自上次 KSN 更改後尚未用過的無線承載識別碼。如果主要節點(MN)無法為次要節點(SN)中分配尚未用過的無線承載識別碼時，主要節點(MN)應增加無法為次要節點(SN)的計數器，同時更新次要節點(SN)的 KSN。
TS 33.511 §4.2.3.2.2 TS 33.117 §4.2.3.2.2	未經授權的檢視	在非系統維護期間，系統功能不得向用戶和管理員明文傳輸任何系統內部機密資訊，例如本地或遠端營運管理與維護(Operations, administration and maintenance, OAM)的命令語言解譯器(Command-Line Interface, CLI)或圖形化使用者介面(Graphical User Interface, GUI)、日誌資訊、警報、匯出配置當案等。
TS 33.511 §4.2.3.2.3 TS 33.117 §4.2.3.2.3	保護存儲中的數據和資訊	對於永久或臨時存儲的敏感資訊應該限制其訪問存取權限。系統功能所需的檔案應受到保護以防止篡改。

需求標準	標題	3GPP 資安需求
TS 33.511 §4.2.3.2.4 TS 33.117 §4.2.3.2.4	保護傳輸中的數據和資訊	需要使用具有足夠安全措施和受到業界公認安全演算法保護的網路協定，且該協定不能有已知漏洞。
TS 33.511 §4.2.3.3 TS 33.117 §4.2.3.3.1	系統處理過度過載的情況	系統應提供安全措施來處理由於過載情況而發生的阻斷服務攻擊，以應避免損害系統的可用性。
TS 33.511 §4.2.3.3 TS 33.117 §4.2.3.3.2	僅從預設的存儲設備開機	網路產品只能從預設的存儲設備開機
TS 33.511 §4.2.3.3 TS 33.117 §4.2.3.3.3	系統處理過度過載的情況	系統於建構時應該能夠預測無法防止的過載情況，並讓過載情況受到控制以持續運行。同時應該確保系統不會因為過載情況而發生不安全的狀態。在喪失安全功能的極端故障情況下，應該關閉喪失安全防護的系統。
TS 33.511 §4.2.3.3 TS 33.117 §4.2.3.3.4	系統針對非預期輸入的強健性	網路產品在收到傳輸到系統的所有資料後，有必要進行輸入資料驗證再作資料處理，包括用戶輸入、陣列中的數值和協定的內容。
TS 33.511 §4.2.3.3 TS 33.117 §4.2.3.3.5	網路產品軟體的完整性驗證	軟體套件應在安裝或升級階段驗證其完整性，網路產品應支援軟體套件的完整性(如數位簽章)驗證。不得執行或安裝完整性檢查失敗的軟體套件。需要安全機制來確保只有經過授權的人員才能進行軟體套件更新。
TS 33.117 §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	應該防止未成功通過基用戶身分認證的人員使用系統功能，如網路服務、管理控制台的本地訪問、使用本地作業系統和應用程式。
TS 33.117 §4.2.3.4.1.2	網路產品應使用明確標識的用戶帳戶	網路產品應明確識別用戶，故應該支援為每個用戶分別配置帳戶，如個人帳戶(personal account)、機器帳戶(machine account)、應用程式帳戶(application account)或系統帳戶(system account)。且不得啟用群組帳戶(group account)，亦或多個用戶共享同一帳戶。
TS 33.511 §4.2.3.4.1 TS 33.117 §4.2.3.4.2.1	至少透過一個身分驗證屬性保護帳戶	應防止系統上各個用戶和機器帳戶被濫用，通常用戶名稱需要結合身分驗證屬性如密碼金鑰(Cryptographic Keys)、符記(Token)與密碼，以對授權用戶進行明確的身分驗證和識別。
TS 33.511 §4.2.3.4.1 TS 33.117 §4.2.3.4.2.2	預設帳戶應刪除或禁用	應刪除或禁用所有預定義帳戶或預設帳戶。如果無法刪除或禁用這些預設帳戶，則應該防止利用這些預設帳戶進行遠端登錄。

需求標準	標題	3GPP 資安需求
TS 33.511 §4.2.3.4.1 TS 33.117 §4.2.3.4.2.3	預設認證屬性應刪除或禁用	生產商、供應商或開發商通常會預先配置系統身分驗證的密碼或加密金鑰。此類身分驗證屬性在第一次登錄系統時，應透過自動強制手段要求用戶變更，亦或供應商應該提供手動變更的說明。
TS 33.117 §4.2.3.4.3.1	密碼複雜度規則	網路產品應該只接受符合密碼複雜度規則的密碼設定。如果使用集中式用戶身分驗證系統，則該系統應該執行符合密碼複雜度規則的密碼策略。
TS 33.117 §4.2.3.4.3.2	密碼變更	如果使用密碼作為身分驗證屬性時，則系統應提供用戶隨時更改其密碼的功能。首次登錄後將強制變更密碼。系統將根據密碼管理策略強制變更密碼，並於超過有效期限後強制用戶變更密碼。
TS 33.117 §4.2.3.4.3.3	防止暴力和字典攻擊	如果使用密碼作為身分驗證屬性，則應實施防止猜測密碼的暴力破解和字典攻擊的保護機制。
TS 33.117 §4.2.3.4.3.4	隱藏密碼顯示	密碼單字通常顯示為“*”等單字，不應該讓其他人員看到，可能允許在輸入期間短暫顯示密碼單字，但是永遠不會以明文形式顯示整個密碼。
TS 33.117 §4.2.3.4.4.1	網路產品管理和維護界面	網路產品管理應該支援交互認證機制。
TS 33.117 §4.2.3.4.5	有關連續嘗試登錄失敗的策略	電信事業應該可設定用戶帳戶允許連續登錄失敗的最大嘗試次數。在用戶連續登錄失敗次數超過允許的最大嘗試次數後，將要求用戶延遲一段時間再次嘗試登錄，亦可永久鎖定一般用戶帳戶。
TS 33.117 §4.2.3.4.6.1	授權政策	用戶帳戶和應用程式應該只要獲得執行任務所需的最低限度授權。對系統的授權應限制在用戶只能訪問執行任務過程需要的數據和使用相關功能。且不應該以管理員或系統權限執行應用程式。
TS 33.117 §4.2.3.4.6.2	基於角色的訪問控制	網路產品應該支援基於角色的訪問控制(Role Based Access Control, RBAC)，該系統控制用戶如何使用域(domain)和資源。域(domain)涵蓋故障管理(Fault Management, FM)、效能管理(Performance Management, PM)、系統管理(System Admin)等。
TS 33.511 §4.2.3.5 TS 33.117 §4.2.3.5.1	保護會話－登出功能	系統應該具有將已登錄的用戶隨時登出的功能，登錄用戶識別碼下所有的程序將在登出時終止。在沒有交談會話的情況下，網路產品應該能夠繼續運行。
TS 33.511 §4.2.3.5 TS 33.117 §4.2.3.5.2	安全事件記錄	在不使用會話時間逾時後，應該自動終止該營運管理與維護(OAM)用戶的會話。

需求標準	標題	3GPP 資安需求
TS 33.511 §4.2.3.6 TS 33.117 §4.2.3.6.1	安全事件記錄	安全事件應該一併記錄特有系統資訊如主機名、網際網路協定(IP)位址或媒體存取控制(Media Access Control, MAC)位址以及事件發生的確切時間。對於每個安全事件，日誌項目應包括用戶名稱、時間標籤、執行動作或結果、會話長度、超標數值或達成數值。
TS 33.511 §4.2.3.6 TS 33.117 §4.2.3.6.2	日誌傳輸到集中存儲	網路產品應支援將正在記錄的資安事件記錄數據傳輸到集中儲存區或系統外部。
TS 33.511 §4.2.3.6 TS 33.117 §4.2.3.6.3	保護安全事件日誌文件	安全事件日誌應受到文件訪問權限管制，僅有特定權限用戶才能訪問日誌文件。
TS 33.511 §4.2.4 TS 33.117 §4.2.4.1.1.1	動態增長的內容不應影響系統功能	如日誌文件、上傳等不斷動態增加的內容不應該影響到系統功能。檔案大小增長到最大極限時不應停止系統正常運行。
TS 33.511 §4.2.4 TS 33.117 §4.2.4.1.1.2	處理網際網路控制訊息協定第四版和網際網路控制訊息協定第六版封包	在網路產品應禁用處理非必要的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)數據封包的。
TS 33.511 §4.2.4 TS 33.117 §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封包	帶有非必選標頭或非必要延伸標頭的網際通訊協定(IP)數據封包不應處理，故啟用非必選標頭或非必要延伸標頭的數據封包應被過濾。
TS 33.511 §4.2.4 TS 33.117 §4.2.4.1.2.1	僅允許經過身分驗證的特權升級	在命令語言解譯器(CLI)或圖形化使用者介面(GUI)的交互式會話中不應有允許用戶無需重新認證從另一般帳戶獲得管理員或根權限的提權方法。
TS 33.511 §4.2.4 TS 33.117 §4.2.4.2.2	系統賬號識別	UNIX® 系統中的每個帳戶都應具有唯一識別符(Unique Identifier, UID)。
TS 33.511 §4.2.5 TS 33.117 §4.2.5.1	超文本傳輸安全協定	用戶端和網頁伺服器間的通信應採用傳輸層安全性協定(Transport Layer Security, TLS)保護。
TS 33.511 §4.2.5 TS 33.117 §4.2.5.2.1	網頁伺服器日誌記錄	網頁伺服器應記錄對服務器的訪問日誌，包含訪問時間標籤、網際通訊協定(IP)的來源位址、帳戶(如果已知)、嘗試登錄的帳戶名稱(如果關聯帳戶不存在)、超文本傳輸協定(HTTP)求中的相關資訊、 網頁伺服器響應的狀態代碼。

需求標準	標題	3GPP 資安需求
TS 33.511 §4.2.5 TS 33.117 §4.2.5.3	用戶會話	為保護用戶會話，網路產品應支援會話識別碼(ID)和會話訊錄(cookie)的相關要求。
TS 33.511 §4.2.5 TS 33.117 §4.2.5.4	輸入驗證	網路產品應有適當的機制來確保網頁應用程序不會受到命令注入或跨站點腳本攻擊的影響，故網路產品應驗證、過濾、轉義和編碼用戶控制的輸入。
TS 33.511 §4.2.6.2.1 TS 33.117 §4.2.6.2.1	封包過濾	網路產品應該提供一種過濾任何的網際網路協定(IP)介面上傳入的網際網路協定(IP)封包的機制。
TS 33.511 §4.2.6.2.2 TS 33.117 §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	網路設備的不應受到來自其他網路元件傳入的變造數據封包影響其可用性或強健性，所以應要偵測到無效的數據封包到並丟棄該封包，且不能影響網路設備的性能。
TS 33.511 §4.2.6.2.4 TS 33.117 §4.2.6.2.4	通用封包無線服務隧道協定-用戶平面封包過濾	對於基於通用封包無線服務隧道協定-用戶平面封包(GTP-U)的每個訊息，應該可以檢查該訊息的發送者是否被授權發送該訊息。至少應支援以下功能：丟棄(Discard)匹配的訊息、接受(Accept)匹配的訊息及計數(Account)匹配的訊息。
TS 33.117 §4.3.2.1	沒有不必要或不安全的服務與協議	網路產品應僅運行必備的協議處理程序和服務，且沒有任何已知的安全漏洞。
TS 33.117 §4.3.2.2	限制服務的可達性	網路產品的服務應該限制只能由合法的通信端透過必要的介面存取。
TS 33.117 §4.3.2.3	未使用的軟體應被卸載	網路產品運行或功能不需要使用的軟體元件不得安裝或應被卸載。
TS 33.117 §4.3.2.4	未使用的功能應被停用	系統運作不需要的硬體功能應永久停用，即使網路產品重新開機後也不會重新啟用。
TS 33.117 §4.3.2.5	不再支援的元件被移除	網路產品不應包含供應商、生產商或開發商不再支援的軟硬體元件。
TS 33.117 §4.3.2.6	限制特權用戶從遠端登錄	根權限或等效最高權限的用戶只能從系統控制台直接登錄。不允許根權限用戶從遠程登錄系統。
TS 33.117 §4.3.2.7	檔案系統需要授權特權	系統應確保只有被授權的用戶才能修改文件、數據、目錄或文件系統。
TS 33.117 §4.3.3.1.1	因應網際網路協定來源位置欺騙	如果透過進入介面(incoming interface)無法訪問其網址，則系統不處理該網際網路協定(IP)的封包。
TS 33.117 §4.3.3.1.2	核心網路功能最小化	網路功能運作不需使用的核心(Kernel)網路元件功能應該被停用。

需求標準	標題	3GPP 資安需求
TS 33.117 §4.3.3.1.3	沒有自動開啟可移除式媒體	當連接光碟(Compact Disc, CD)、數位影音光碟(Digital Video Disc, DVD)、通用序列匯流排棒(Universal Serial Bus Stick, USB-Stick)或通用序列匯流排儲存驅動機(USB Storage Drive)等可移動媒體設備時，網路產品應該禁止自動啟動任何應用程序。
TS 33.117 §4.3.3.1.4	預防請求洪水	網路產品應支援預防請求洪水攻擊的機制。
TS 33.117 §4.3.3.1.5	防止緩衝器溢位的保護機制	系統應支持緩衝區溢位保護機制。應提供如何檢查緩衝區溢出機制是否已啟用的描述文件檔案。
TS 33.117 §4.3.3.1.6	限制安裝外部檔案系統	如果允許一般用戶掛載外部文件系統，則作業系統的級別應設置適當限制，以防止掛載的外部文件系統進行提權攻擊。
TS 33.117 §4.3.4.2	網頁伺服器沒有系統特權	任何網頁伺服器程序應該在具有最低權限的帳戶下運行，且都不得以系統權限運行。
TS 33.117 §4.3.4.3	未使用的超文本傳輸協定的方法應被停用	未使用的超文本傳輸協定的方法將被停用。對網頁伺服器的標準請求僅能使用 GET、HEAD 和 POST 方法。
TS 33.117 §4.3.4.4	應停用不需要的附加元件	應停用網頁伺服器中所有不需要使用的可選附加元件。應停用不使用的共同閘道介面(Common Gateway Interface, CGI)或其他腳本組件、服務器端包含(Server Side Includes, SSI)和 WebDAV。
TS 33.117 §4.3.4.5	沒有通過共同閘道介面 或其他伺服器端腳本編寫的編譯器、解釋器或殼層	如果使用共同閘道介面(CGI)或其他腳本技術，共同閘道介面(CGI)目錄或其他對應的腳本目錄不應包含編譯器或解譯器。
TS 33.117 §4.3.4.6	沒有用於上傳的共同閘道介面或其他腳本	如果使用共同閘道介面(CGI)或其他腳本技術，應該禁止上傳檔案至相關的 CGI/script 目錄。
TS 33.117 §4.3.4.7	不使用伺服器端包含變數值執行系統命令	如果伺服器端包含(SSI)處於運作狀態，應停用執行系統命令的功能。
TS 33.117 §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	網頁伺服器的配置文件訪問權限應僅授予網頁伺服器的擁有者或系統權限的用戶。
TS 33.117 §4.3.4.9	應刪除預設的內容	應刪除網頁伺服器標準預先安裝的內容。
TS 33.117 §4.3.4.10	沒有目錄列表/目錄瀏覽	應停用目錄列表/索引和目錄瀏覽功能。

需求標準	標題	3GPP 資安需求
TS 33.117 §4.3.4.11	應最小化超文本傳輸協定標頭中有關網頁伺服器的資訊	超文本傳輸協定(HTTP)標頭不應包含有關網頁伺服器版本和所用模組及附加元件的資訊。
TS 33.117 §4.3.4.12	應刪除網頁伺服器中的錯誤資訊頁面	用戶定義的錯誤頁面不應包含有關網頁伺服器的版本資訊與所用的模組和附加元件。錯誤訊息不應包含內部伺服器名稱、錯誤代碼等內部資訊。網頁伺服器的預設錯誤頁面應替換為供應商定義的錯誤頁面。
TS 33.117 §4.3.4.13	應刪除不需要的檔案類型或腳本映射	應刪除不需使用的檔案類型或腳本映射，例如 php、phtml、js、sh、csh、bin、exe、pl、vbe、vbs。
TS 33.117 §4.3.4.14	網頁伺服器僅交付必要的檔案	在網頁伺服器檔案目錄中所有的文件應限制性訪問權限。
TS 33.117 §4.3.4.15	僅在共同閘道介面與腳本目錄中具有執行權限	如果使用共同閘道介面(CGI)或其他腳本技術，應該只允許 CGI/Scripting 目錄有執行權限。
TS 33.117 §4.3.5.1	流量分離	網路產品應支援實體上或邏輯上分離屬於不同網域的流量。
TS 33.117 §4.4.2	通訊埠掃描	應確保在所有網路介面上，只有傳輸層上記錄的埠才能回復來自系統外部的請求。
TS 33.117 §4.4.3	弱點掃描	弱點掃描的目的是確保網路產品的作業系統和應用程式不存在已知弱點。
TS 33.117 §4.4.4	強健性模糊測試	當收到非預期輸入時，應確保外部服務仍然具有一定的穩健性。
TR 33.818 §5.2.5.5.3.3.5.1 TR 33.848 §5.18.3	虛擬網路功能軟體包和虛擬網路功能映像檔的完整性	虛擬網路功能(Virtual Network Function, VNF)軟體包和映像檔應包含完整性驗證值。虛擬網路功能(VNF)軟體上架前應受到完整性保護，並由網路功能虛擬化協調器(NFV orchestrator, NFVO)驗證。
TR 33.818 §5.2.5.5.7.1	通用虛擬化網路產品(GVNP)生命週期管理安全	當虛擬網路功能與虛擬網路功能管理(Virtualized Network Function Manager, VNFM)與虛擬網路功能(VNF)進行通信時，虛擬網路功能(VNF)應驗證虛擬網路功能與虛擬網路功能管理(VNFM)。虛擬網路功能與虛擬網路功能管理(VNFM)應能夠與虛擬網路功能(VNF)建立安全的通信連線。當虛擬網路功能與虛擬網路功能管理(VNFM)訪問虛擬網路功能(VNF)的應用程式介面(API)時，虛擬網路功能(VNF)會檢查虛擬網路功能管理(VNFM)是否已經被授權。虛擬網路功能(VNF)應保留虛擬網路功能管理(VNFM)的管理操作記錄，以進行審計。

需求標準	標題	3GPP 資安需求
TR 33.818 §5.2.5.5.7.2	提供安全的執行環境	虛擬網路功能(VNF)應支援透過虛擬網路功能管理(VNFM)解析比較其擁有的資源狀態與虛擬網路功能描述(VNF Description, VNFD)的資源狀態。虛擬網路功能(VNF)可以從營運管理與維護(OAM)查詢虛擬網路功能管理(VNFM)的資源狀態解析。如果兩個資源狀態不一致，虛擬網路功能(VNF)將向 營運管理與維護(OAM)發送告警。
TR 33.818 §5.2.5.5.8.5.1 TS 33.117 §4.3.5.1	流量分離	虛擬化網路產品應支援邏輯上分離屬於不同網域的流量。
TR 33.818 §5.2.5.5.8.5.2	虛擬網路功能間與虛擬網路功能內流量分離	用於虛擬網路功能間(Inter-VNF)的通信網路和用於虛擬網路功能內(Intra-VNF)的通信網路應分開，以防止來自不同網路的安全威脅。
TR 33.818 §5.2.5.6.6.1 TR 33.848 §5.18.3	從受信賴的虛擬網路功能映像檔啟動虛擬網路功能	虛擬網路功能(VNF)應從一個或多個受信賴的虛擬網路功能(VNF)映像檔啟動。虛擬網路功能(VNF)映像檔應該包含授權運營商的數位簽章。
TR 33.818 §5.2.5.6.7.1	安全的虛擬化資源管理	為了防止被入侵的虛擬架構管理(Virtualised Infrastructure Manager, VIM)更改虛擬層的資源分配，虛擬網路功能(VNF)應向營運管理與維護(OAM)發出警報。虛擬網路功能(VNF)應記錄來自虛擬架構管理(VIM)的訪問。
TR 33.818 §5.2.5.6.7.2	建立安全的執行環境	當攻擊者篡改硬體的驅動程式並用於建立執行環境時，虛擬層會向管理員發出驅動程式錯誤警告，以便管理員日後可檢查警報並找到攻擊者。
TR 33.818 §5.2.5.6.7.3	虛擬機逃脫保護	為了防止攻擊者利用虛擬網路功能(VNF)的漏洞攻擊並控制虛擬層，虛擬化應拒絕來自虛擬網路功能(VNF)的異常訪問並記錄攻擊事件。
TR 33.818 §5.2.5.7.7.1	安全硬體資源管理	當被入侵的虛擬架構管理(Virtualised Infrastructure Manager, VIM)更改硬體資源配置時，該硬體應該觸發警報，以便管理員日後可檢查警報並找到攻擊者。
TR 33.818 §5.2.5.7.7.2	安全硬體資源管理資訊	當被入侵的虛擬層嘗試篡改硬體資源配置導致虛擬架構管理(VIM)收到硬體配置錯誤時，該硬體應該觸發警報，以便管理員日後可檢查警報並找到攻擊者。
TR 33.818 §5.2.5.7.7.3	可信平臺	主機系統應該使用可信平臺模組(Trusted Platform Module, TPM)或硬體安全模組(Hardware Security Module, HSM)等基於硬體根的信任(Hardware-Based Root of Trust, HBRT)作為初始信任根(Initial Root of Trust)。

5.3 Open RAN 基地臺的資安議題

為了解決 5G 開放式架構的資安議題，開放式無線接取網路聯盟(O-RAN Alliance)於 2021 年成立安全焦點小組(Security Focus Group, SFG)，專注於制定訂開放式虛擬無線接取網路(Open RAN)產品的安全架構和安全保證規範，開放式無線接取網路安全架構與框架，並定同時也致力於開放測試與整合中心(Open Testing and Integration Centre, OTIC)推動產品資安保證評估驗證程序。

5.3.1 Open RAN 基地臺的資安威脅分析

依據開放式無線接取網路聯盟(O-RAN Alliance)的安全焦點小組(SFG)所提出的 O-RAN 資安威脅建模和補救分析(O-RAN Security Threat Modeling and Remediation Analysis)研究報告[12]，列出 Open RAN 元件資產的資安分析與 Open RAN 元件的威脅分析分別如表 8 與表 9 所示。

表 8 Open RAN 元件資產的資安分析

資產編號	介面	元件	機密性	完整性	可用性	重播	認證
ASSET-D-01	前傳介面 S-Plane	Open RAN 分散單元、Open RAN 無線電單元		√		√	√
ASSET-D-02	前傳介面 M-Plane	Open RAN 分散單元、Open RAN 無線電單元、服務管理與編排	√	√		√	√
ASSET-D-03	O1 介面	近即時無線接取網路智能控制、非即時無線接取網路智能控制、Open RAN 集中單元、Open RAN 分散單元、服務管理與編排	√	√		√	√
ASSET-D-04	前傳介面 C-Plane	Open RAN 分散單元、Open RAN 無線電單元	√	√		√	√
ASSET-D-05	前傳介面 U-Plane	Open RAN 分散單元、Open RAN 無線電單元	√	√	√		

資產編號	介面	元件	機密性	完整性	可用性	重播	認證
ASSET-D-06	無線介面	Open RAN 無線電單元	√	√		√	√
ASSET-D-07	A1 介面	近即時無線接取網路智能控制、非即時無線接取網路智能控制	√	√			√
ASSET-D-08			√	√			√
ASSET-D-09	E2 介面	Open RAN 分散單元、Open RAN 集中單元、近即時無線接取網路智能控制	√	√		√	√
ASSET-D-12	O2 介面	服務管理與編排、雲平台(O-Cloud)	√	√		√	√
ASSET-D-13			√	√		√	√
ASSET-D-14			√	√		√	√
ASSET-D-16	前傳介面、O1 介面、O2 介面、E2 介面、A1 介面	全部(X.509 認證)		√		√	√
ASSET-D-17	前傳介面、O1 介面、O2 介面、E2 介面、A1 介面	全部(安全私密金鑰)	√	√		√	
ASSET-D-25	A1 介面、O1 介面、E2 介面	近即時無線接取網路智能控制、非即時無線接取網路智能控制、xApps 應用程式、rApps 應用程式	√	√		√	√
ASSET-D-30	A1 介面、E2 介面、O1 介面	近即時無線接取網路智能控制、非即時無線接取網路智能控制、服務管理與編排	√	√		√	√

表 9 Open RAN 元件的威脅分析

威脅編號	威脅對象	威脅標題
T-O-RAN-01	全部	攻擊者入侵缺乏安全設計的 Open RAN 元件
T-O-RAN-02	全部	攻擊者入侵錯誤或不當配置的 Open RAN 元件
T-O-RAN-03	全部	攻擊者透過網際網路入侵滲透弱認證與存取控制的 Open RAN 網路
T-O-RAN-04	全部	攻擊者透過物聯網設備(Internet of Things, IoT devices)干擾 Open RAN 網路的無線通訊信號
T-O-RAN-05	全部	攻擊者透過開放前傳介面(open front-haul interface)、O1 介面、O2 介面、A1 介面 和 E2 介面滲透破壞 Open RAN 系統
T-O-RAN-06	全部	攻擊者入侵滲透不完整或不適當之身分驗證和授權機制的 Open RAN 元件
T-O-RAN-07	全部	攻擊者入侵破壞 Open RAN 監控機制和日誌檔案的完整性和可用性
T-O-RAN-08	全部	攻擊者入侵破壞 Open RAN 數據的完整性、機密性和可追溯性
T-O-RAN-09	全部	攻擊者入侵破壞 Open RAN 元件的完整性和可用性
T-FRHAUL-01	前傳介面	攻擊者透過 Open RAN 無線電單元(O-RU)或前傳介面(Fronthaul interface)滲透 Open RAN 分散單元(O-DU)及其他元件
T-MPLANE-01	前傳介面的管理平面(M-Plane)	攻擊者透過中間人(Man in the Middle, MITM)攔截前傳介面(Fronthaul interface)的管理平面(M-Plane)的資訊
T-SPLANE-01	前傳介面同步平面(S-Plane)	攻擊者針對主時鐘(Master clock)進行阻斷服務(Denial of Service, DoS)攻擊
T-SPLANE-02	前傳介面的同步平面(S-Plane)	攻擊者針對精確時間協定(Precision Time Protocol, PTP)訊息進行中間人(MITM)攔截與選擇性的隨機延遲攻擊

威脅編號	威脅對象	威脅標題
T-CPLANE-01	前傳介面的控制平面(C-Plane)	攻擊者發送控制平面(C-plane)下行(Downlink, DL)與上行(Uplink, UL)的欺騙訊息
T-CPLANE-02	前傳介面的控制平面(C-Plane)	攻擊者針對 Open RAN 分散單元(O-DU)控制平面(C-plane)進行阻斷服務(DoS)攻擊
T-UPLANE-01	前傳介面的用戶平面(U-Plane)	攻擊者透過中間人(MITM)攔截前傳介面用戶平面(U-Plane)的資訊
T-ORU-01	Open RAN 無線電單元	攻擊者透過惡意 Open RAN 無線電單元(rogue O-RU)發動攻擊
T-NEAR-RT-01	近即時無線接取網路智能控制	攻擊者可以透過惡意 xApps 應用程式 來取得用戶終端(UE)識別碼、追蹤用戶終端(UE)位置和修改用戶終端(UE)優先權等級
T-NONRTRIC-01	非即時無線接取網路智能控制	攻擊者滲透非即時無線接取網路智能控制(Non-RT RIC)導致降低服務性能，亦或發動阻斷服務(DoS)攻擊
T-xApp-01	近即時無線接取網路智能控制	攻擊者利用 xApps 應用程式漏洞和錯誤配置發動攻擊
T-xApp-02	近即時無線接取網路智能控制	無意或惡意 xApps 應用程式的衝突會影響 Open RAN 系統功能，進而導致降低服務性能或阻斷服務(DoS)
T-xApp-03	近即時無線接取網路智能控制	攻擊者破壞 xApps 應用程式的安全隔離
T-rApp-01	非即時無線接取網路智能控制	攻擊者透過 rApps 應用程式漏洞和錯誤配置發動攻擊
T-rApp-02	非即時無線接取網路智能控制	攻擊者繞過身分驗證和授權發動攻擊
T-rApp-03	非即時無線接取網路智能控制	攻擊者破壞 rApps 應用程式的安全隔離
T-rApp-04	非即時無線接取網路智能控制	無意或惡意 xApps 應用程式的衝突會影響 Open RAN 系統功能，進而導致降低服務性能或阻斷服務(DoS)

威脅編號	威脅對象	威脅標題
T-SMO-01*1	服務管理與編排	攻擊者透過服務管理與編排(SMO)功能上不正確或缺乏身分驗證的弱點發動攻擊
T-SMO-02*1	服務管理與編排	攻擊者透過服務管理與編排(SMO)功能上不正確或缺乏身分驗證的弱點發動攻擊
T-SMO-03	服務管理與編排	對服務管理與編排(SMO)發動過載阻斷服務(DoS)攻擊

*1: T-SMO-01 與 T-SMO-02 的威脅標題(Threat title)相同但是引用標準[12]中的威脅描述(Threat description)不同。

5.3.2 Open RAN 基地臺的資安需求與安全協定標準

依據開放式無線接取網路聯盟(O-RAN Alliance)的安全焦點小組(SFG)所提出的 O-RAN 安全需求規範(O-RAN Security Requirements Specifications)[13]，列出 Open RAN 元件的安全需求規範如表 10 所示。而安全焦點小組(SFG)以第三代合作夥伴計畫(3GPP)分散式基地臺的介面安全方護機制為基準，提出的 O-RAN 安全協定標準(O-RAN Security Protocols Specifications)[14] 涵蓋安全外殼協定(Secure Shell, SSH)、傳送層安全協定(Transport Layer Security protocol, TLS)、資料包傳送層安全協定(Datagram Transport Layer Security protocol, DTLS)與網際網路安全協定(Internet Protocol Security, IPSec)等四大 Open RAN 基地臺介面安全方護機制的基本規範。

表 10 Open RAN 基地臺的資安需求

資安需求編號	元件/介面	Open RAN 資安需求
REQ-SEC-OCLOUD-1	O-Cloud	用戶必需透過身分驗證和授權。
REQ-SEC-OCLOUD-2	O-Cloud	應對不同用戶間的控制和資源實施隔離措施。
REQ-SEC-A1-1	A1 介面	A1 介面應支援機密性、完整性和重放保護以及資料來源驗證。
SEC-CTL-A1	A1 介面	A1 介面應透過傳送層安全協定(Transport Layer Security protocol, TLS)保護。
REQ-TLS-FUN-1	O1 介面	O1 介面應透過傳送層安全協定(TLS)保護。

資安需求編號	元件/介面	Open RAN 資安需求
REQ-NAC-FUN-1	O1 介面	使用網路組態協定(Network Configuration Protocol, NETCONF)的管理服務供應商和用戶應支援 RFC 8341 定義的網路組態存取控制模型(Network Configuration Access Control Model, NACM)，以限制將用戶存取權限。
REQ-NAC-FUN-2	O1 介面	O1 介面的 NETCONF 應該設置定下列網路組態存取控制模型(NACM)Global Enforcement Controls 得預設值。 enable-nacm = true read-default = permit write-default = deny exec-default = deny enable-external-groups = true
REQ-NAC-FUN-3	O1 介面	支援網路組態協定(NETCONF)管理服務的供應商應該在網路組態存取控制模型(NACM)中支援 O1_nacm_management、O1_user_management、O1_network_management、O1_ network_monitoring 與 O1_software_management 等預定義群組，以限制用戶對網路組態協定(NETCONF)協定的訪問權限。
REQ-NAC-FUN-4	O1 介面	分配到 O1_nacm_management 群組的用戶對 /nacm 物件和屬性及網路組態存取控制模型(NACM)Global Enforcement Controls 應具有讀寫的權限。
REQ-NAC-FUN-5	O1 介面	分配到 O1_user_management 群組的用戶對本地用戶的存儲物件和屬性，應具有讀寫的權限。
REQ-NAC-FUN-6	O1 介面	分配給 O1_network_management 群組的用戶應具有讀取、寫入和執行 <running> 存儲數據的權限，同時應具讀取、寫入、執行和提交 <candidate> 存儲數據的權限，但是不應具有對於 /nacm 物件的任何權限。
REQ-NAC-FUN-7	O1 介面	分配給 O1_network_monitoring 群組的用戶應具有讀取<running>存儲數據的權限，但是不應具有讀取/nacm 物件的權限。
REQ-NAC-FUN-8	O1 介面	分配到 O1_software_management 群組的用戶應有權安裝新軟體。
REQ-NAC-FUN-9	O1 介面	網路組態協定(NETCONF)端點應該支援下列一種與外部用戶的群組映射協定：支援 StartTLS 的輕型目錄存取協定(Lightweight Directory Access Protocol, LDAP)、OAuth 2.0、支援可延伸鑑別協定(Extensible Authentication Protocol, EAP)的遠程鑑別撥入用戶服務(Remote Authentication Dial In User Service, RADIUS)和終端訪問控制器訪問控制系統(Terminal Access Controller Access-Control System, TACACS/TACACS+)。
REQ-NAC-FUN-10	O1 介面	管理服務提供者可以允許在 <groups> 網路組態存取控制模型(NACM)物件中定義用戶。

資安需求編號	元件/介面	Open RAN 資安需求
REQ-SEC-O2-1	O2 介面	O2 介面應支援機密性、完整性和重放保護以及資料來源驗證。
SEC-CTL-O2	O2 介面	O2 介面應透過傳送層安全協定(TLS)保護。
REQ-SEC-E2-1	E2 介面	E2 介面應支援機密性、完整性和重放保護以及資料來源驗證。
SEC-CTL-E2	E2 介面	E2 介面應透過網際網路安全協定(Internet Protocol Security, IPSec)保護。
REQ-SEC-OFHPLS-1	開放前傳介面點對點網段	開放前傳介面應該提供開放前傳介面的網路設備間點對點網段來驗證和授權方式。
REQ-SEC-OFHPLS-2	開放前傳介面點對點網段	開放前傳介面應該提供一種偵測建立或中斷授權點對點網段的方法及回報機制。
SEC-CTL-OFHPLS-1	開放前傳介面點對點網段	運營商可以選擇每個開放前傳介面的點對點網段是否實施 IEEE 802.1X-2020 定義之以網路埠為基礎的存取控制。
SEC-CTL-OFHPLS-2	開放前傳介面點對點網段	開放前傳介面網路元件對於每個網路埠都應支援 IEEE 802.1X-2020 定義之功能。
SEC-CTL-OFHPLS-3	開放前傳介面點對點網段	任何開放前傳介面的網路設備都可以當身分驗證裝置。
SEC-CTL-OFHPLS-4	開放前傳介面點對點網段	開放前傳介面的網路設備中的驗證功能應該對於每個點對點網段支援 IEEE 802.1X-2020 定義以網路埠為基礎的存取控制。
SEC-CTL-OFHPLS-5	開放前傳介面點對點網段	開放前傳介面的網路設備中以網路埠為基礎的存取控制應該支援 IEEE 802.1X-2020 定義的可延伸鑑別協定(Extensible Authentication Protocol, eap)之傳送層安全協定(TLS)驗證。
SEC-CTL-OFHPLS-6	開放前傳介面點對點網段	Open RAN 分散單元(O-DU)必須支援 IEEE 802.1X-2020 驗證功能。
REQ-SEC-ALM-FUN2-1	通用應用程式軟體生命週期管理	應用程式軟體包應使用數位簽章。
REQ-SEC-ALM-FUN3-1	通用應用程式軟體生命週期管理	服務管理與編排(Service Management and Orchestration, SMO)應具備驗證應用程式軟體包數位簽章的能力。

6. 5G Open RAN 安全確保機制

依據歐盟與北約組織在 2019 年 5 月在 5G 安全會議所提出的「布拉格倡議(Prague Proposals)」(23)，可信任的 5G 網路軟硬體設備供應鏈管理將是 5G 資安管理最重要的關鍵議題。因此，5G 電信事業不僅需要可信任的網路軟硬體設備供應鏈業者，更必須有能力驗證 5G 相關網路軟硬體設備的安全性才行。5G 資安可以從制度面、管理面和技術面三個層次闡述，但最重要的內涵就是要做到預設安全(Security By Design)，也就是所有電信事業在進行 5G 網路建設之初，就必須納入資通安全防護機制。未來在營運時，也具備足夠的資安防護能量，真正做到確保 5G 網路的安全性，也可以進一步做到促進各種垂直應用場域及創新應用服務的發展。

開放式無線接取網路聯盟(Open Radio Access Network Alliance, O-RAN Alliance)的安全焦點小組(Security Focus Group, SFG)針對 Open RAN 開放式架構的安全確保機制，將採用全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)制定的網路設備安全保證方案(Network Equipment Security Assurance Scheme, NESAS)搭配第三代合作夥伴計畫(3GPP)制定的產品資安確保標準(Security Assurance Specification, SCAS)。本節將闡述現有國際 Open RAN 安全確保機制，於第 6.1 小節探討 GSMA 網路設備安全保證方案後，緊接著於第 6.2 小節與第 6.3 小節討論 3GPP 基地站安全確保機制與 O-RAN 安全確保機制，最後在第 6.4 小節分析 Open RAN 測試案例的缺口。

6.1 GSMA 網路設備安全保證方案

5G 網路將會帶動整個上下游供應鏈的發展，會以大量不同的設備供應商加入 5G 產業中，因此對於供應鏈、產品設備風險的議題當中，全球行動通訊系統協會(GSMA)與第三代合作夥伴計畫(3GPP)合作共同提出針對網路元件之網路設備安全保證方案(NESAS)(24)，適用於電信設備生命週期的安全保障，設備製造商可依循第三代合作夥伴計畫(3GPP)所制定之標準規範(SCAS)，設計其產品符合基本安全要求。其參考第三代合作夥伴計畫(3GPP)所制定之 SCAS 提出網路設備安全保證方案(NESAS)，針對支援第三代合作夥伴計畫(3GPP)定義功能網路產品的供應商構建安全認證框架，以提升行動產業的安全層級。

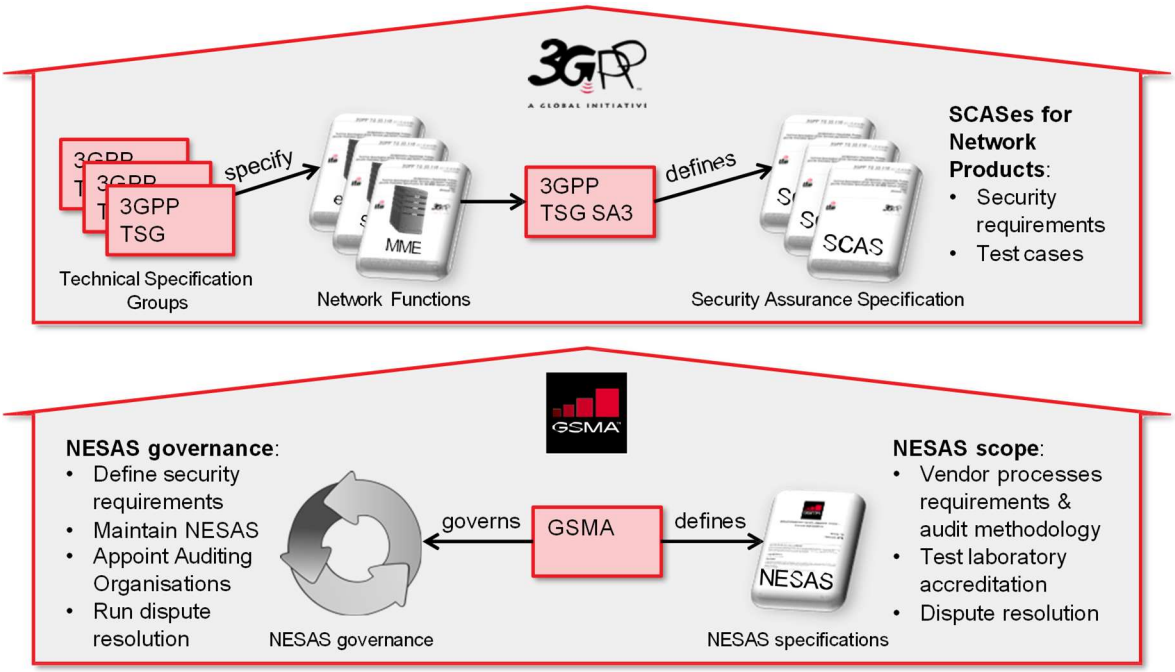

圖 12 NESAS 宗旨(24)

第一階段為針對產品開發及生命週期管理流程的評估著重於安全保證方法流程，期望電信設備製造商可透過認證之第三方實驗室，取得各元件之安全認證，此方法可做為未來電信事業採購設備時，對安全性的認定標準。第二階段是製造商須將網路設備產品提交給 3GPP 定義是否合格，且須透過 ISO/IEC 17025(25)認證的網路設備安全保證方案(NESAS)安全檢測實驗室，進行實質效益的網路產品安全測試評估，其內容包含：測試程序、文件體系、流程維護等。網路設備安全檢測實驗室可以由製造商自行建立，也可以是由外部的獨立第三方擔任，每一家實驗室都經過 ISO/IEC 17025 認證機構的檢驗，檢試實驗室最後將記錄評估結果並撰寫報告，之後再提供給製造商，由製造商自行決定是否將結果對外公開。

全球行動通訊系統協會(GSMA)管理、制定並定期修訂整個網路設備安全保證方案(NESAS)規範，這項規範包含了設備製造商的開發與產品生命週期之認證、測試實驗室之認證、網路設備之安全性測試評估。並指派多個審計組織組成專家小組(Independent Audit Teams, IAT)負責針對流程進行審核(26)，設備製造商則從中挑選一個組織，作為審核旗下銷售發展與產品生命週期程序的組織，依照網路設備安全保證方案(NESAS)規範進行審議，並將結果記錄在審計報告中。檢驗結束後，網路設備安全檢測實驗室會發布一份評估報告，並宣稱網路設備符合 5G 網路安全標準。對於網路設備製造商來

說，其提供了一個可以證明自身產品與能力符合國際標準的平台，形成完整 5G 產業安全防護網。

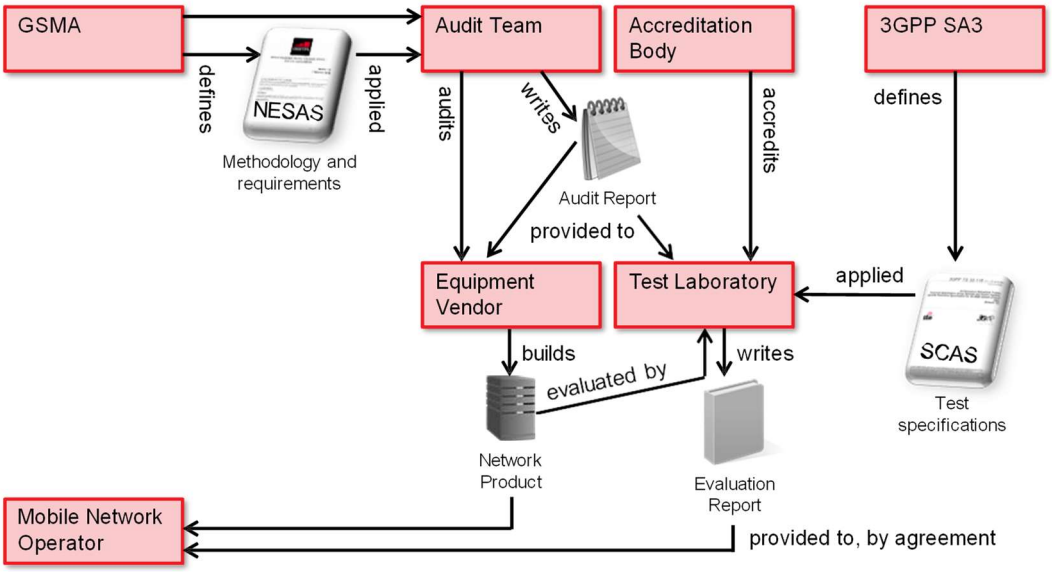

圖 13 NESAS 流程概述(24)

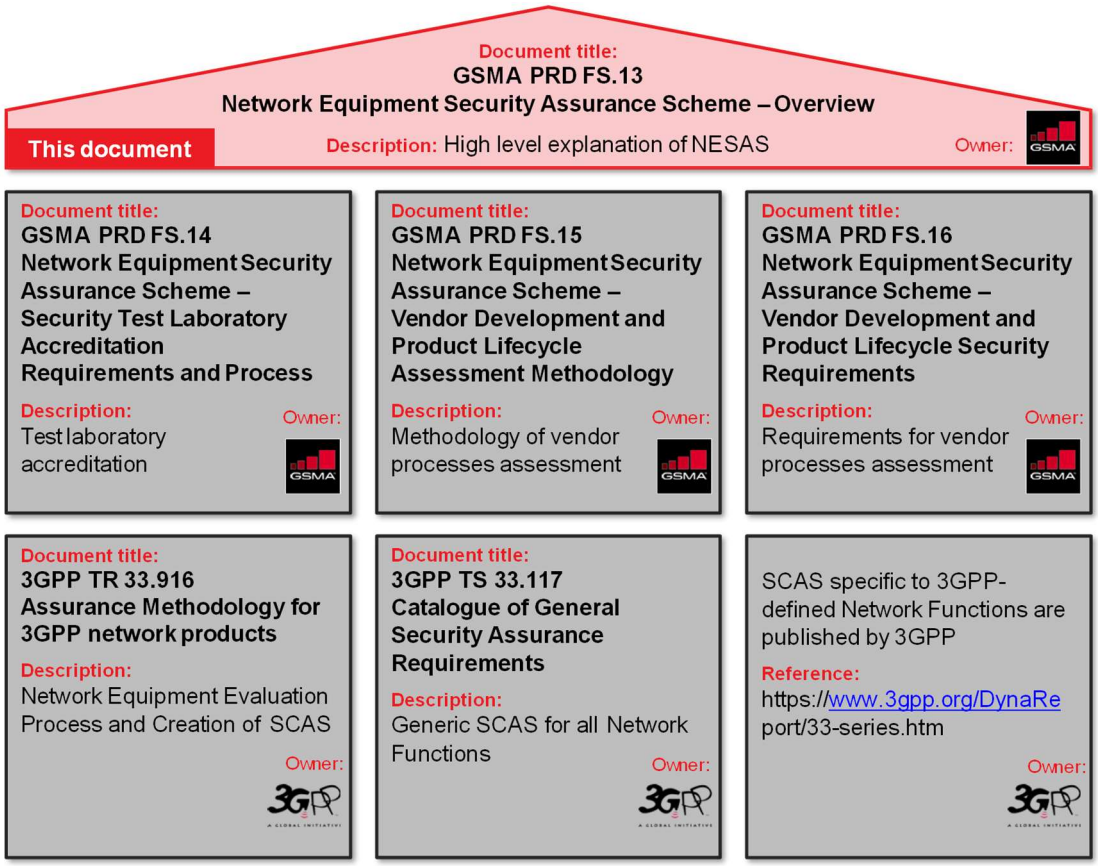

圖 14 NESAS 測試框架(24)

6.2 3GPP 基地站的安全確保機制

隨著行動通訊應用的普及，多樣化用戶裝置及小型基地臺將快速成長及佈建，所帶來的資安威脅亦隨之快速增加，過去國內雖初步建立軟體弱點檢測安全技術，然而主要聚焦於已知弱點掃描檢測、企業資安稽核解決方案等。美國聯邦交易委員會(Federal Trade Committee, FTC)已開始要求廠商進行第三方資安檢測，資通訊產品之資訊安全已經受到國際重視，歐洲、中國也已相繼要求供貨產品需出具資安檢測報告並通過電信商的資安檢測與驗證。

行動通訊標準制定重要組織第三代合作夥伴計畫(3GPP)針行動通訊產品的資安議題，在 2013 年底規劃了行動通訊裝置未來生產製造上所需要符合的資安評估標準方法論資安評估標準方法論(Security Assurance Methodology, SECAM)，依據 3GPP TR 33.805 資安評估標準方法論研究報告(27)，其主要架構說明如下圖：

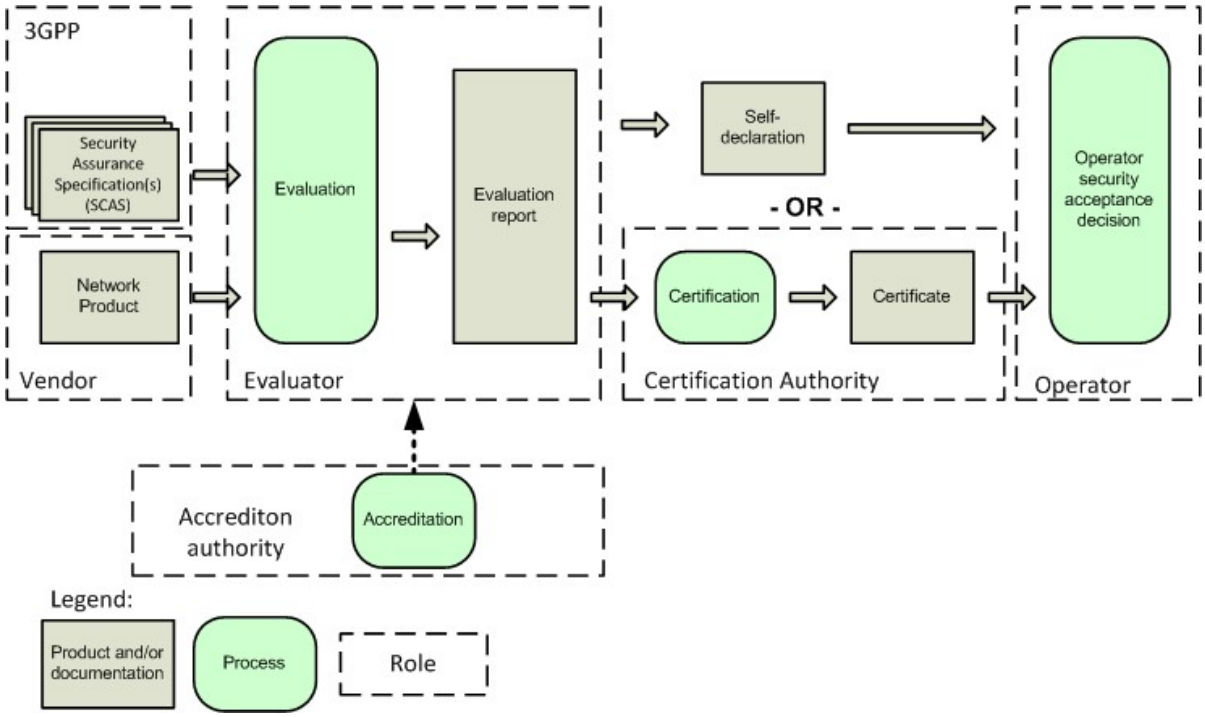

圖 15 資安評估標準方法論 SECAM 檢測流程(27)

針對 5G 基地臺(gNB)資安風險議題，未來在生產製造的過程中將會依據資安評估準則(Security Assurance Specification, SCAS)進行合規檢測，並由資安實驗室針對設備的弱點進行規範檢測及防駭漏洞檢測等兩階段測試。

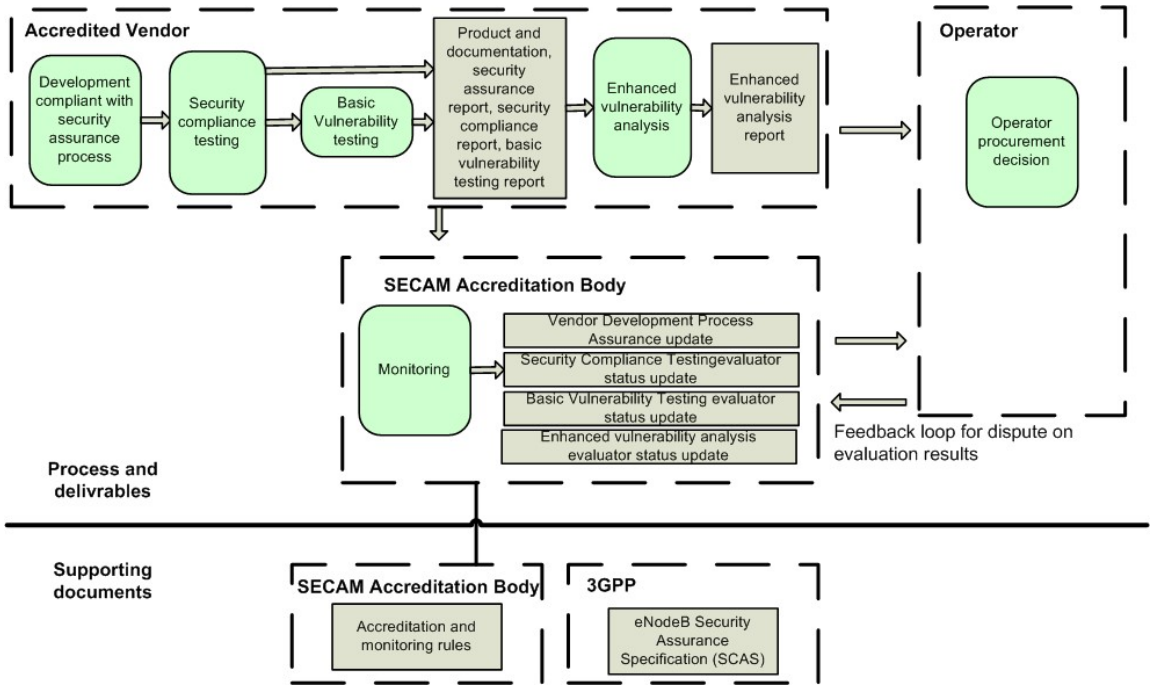

圖 16 5G 資安檢測流程(28)

隨著第三代合作夥伴計劃(3G Partnership Project, 3GPP)第一版本的第五代行動通訊資安評估準則(SCAS)標準於 2019 年底定，涵蓋第五代行動通訊(5G)基地臺的七大資安威脅面向與相關資安測試案例，將有助於電信應運商進行第五代行動通訊設備的資安檢測，作為建立第三方資安檢測資安檢測實驗室的基礎設施。同時亦提升第五代行動通訊的安全性，以保障消費者權益。依據 3GPP TS 33.511 5G 基地臺產品類別的安全保證規範[8]與 3GPP TS 33.117 通用安全保證規範[9]，其安全測試項目如表 11 與表 12 所示。

表 11 3GPP TS 33.511 之資安測試規範

標準章節	測試項目
4.2.2.1.1	無線資源控制信令的完整性保護
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	無線資源控制信令加密
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	無線資源控制信令重播攻擊保護
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

標準章節	測試項目
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	gNB 存取層加密和完整性演算法優先順序
4.2.2.1.13	gNB 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 gNB 金鑰更新

表 12 3GPP TS 33.511/TS 33.117 之資安測試規範

分類		標準章節	測試項目
保護數據和資訊		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	至少透過一個身分驗證屬性保護帳戶
		4.2.3.4.2.2	預設帳戶應刪除或禁用
		4.2.3.4.2.3	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
	特定身分驗證案例	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

分類		標準章節	測試項目
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	僅允許經過身分驗證的特權升級
	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

分類		標準章節	測試項目
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
		4.2.6.2.4	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	流量分割
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

6.3 O-RAN 對於 Open RAN 基地臺的安全確保機制

開放式無線接取網路聯盟(O-RAN Alliance)為了加速 O-RAN 集中單元(O-CU)與 O-RAN 分散單元(O-DU)及 O-RAN 無線電單元(O-RU)間的整合與測試，在 2019 年 6 月成立測試與整合焦點小組(Test and Integration Focus Group, TIFG)，訂定各介面之測試項目規格書、制定 O-RAN 測試實驗室的標準與指南，並推廣 O-RAN 測試規範，以利各項設備的垂直整合，並於 2019 年 9 月成立開放測試與整合中心(Open Testing and Integration Centre, OTIC)。

關於 Open RAN 架構的資安問題部分，開放式無線接取網路聯盟(O-RAN Alliance)於 2021 年成立安全焦點小組(Security Focus Group, SFG)，專注於制定 Open RAN 安全架構與框架、開放測試與整合中心(OTIC)安全驗證、開源安全準則與開放介面安全準則四大方向，並積極推廣 3GPP 資安確保標準(Security Assurance Specification, SCAS)測試成果，並將資安確保標準(SCAS)測試系統的技術延伸並融合在 Open RAN 架構中，確保 Open RAN 架構不論在控制平面或用戶平面可以擁有網路設備安全保證方案(NESAS)同等級之安全防護能力。

依據無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(SFG)所訂之資安測試標準(Security Test Specification)規格文件 [10] 所規定之資安測試工具與資安測試案例如下表 13 與表 14 所示。

表 13 Open RAN 資安測試工具[10]

測試工具	工具描述
商用終端或模擬器	商用終端(UE)需要預先配置一個使用者身分模組(Subscriber Identity Module, SIM)卡進行連線測試，而終端模擬器(UE emulator)可以模擬一個或同時模擬多個真實終端進行連線測試。在實驗室環境中，終端(UE)可以透過射頻電纜(RF cables)或透過空中(over the air, OTA)連線測試中的系統(System Under Test, SUT)；終端(UE)應放置在電磁波隔離箱(RF Shielding Box)或電磁波隔離室(RF Shielding Room)內，以避免受到外部信號的干擾。透過連接到終端(UE)的日誌工具捕獲測量和 KPI 日誌以進行測試驗證和報告。
商用 4G/5G 核心網路或模擬器	4G/5G 核心網路或模擬器用於無線存取網路(RAN)之測試中系統(SUT)所需的核心網路程序，並支援處理 4G/5G 的非存取層(Non-Access Stratum, NAS)會話，其必須支持應用伺服器和商用終端或模擬器間的端到端連接和數據傳輸。
商用網際網路協多媒體子系統(IMS)或模擬器	商用網際網路協多媒體子系統(IP Multimedia System, IMS)或模擬器用於支援使用會談初始協定(Session Initiation Protocol, SIP)和即時傳輸協定(Real-time Transport Protocol, RTP)等的語音和視訊服務，如長期演進語音承載服務(Voice over LTE, VoLTE)、長期演進視訊承載服務(Video over LTE, ViLTE)、新無線語音承載服務(Voice over NR, VoNR)、新無線視訊承載服務(Video over NR, ViNR)和向後支援演進版分封系統服務(Evolved Packet System Fallback, EPS Fallback)，其應該能與 4G/5G 核心網路或模擬器介接，以建立支援語音和視訊服務的專用承載。
應用(流量)伺服器	應用(流量)伺服器(application(traffic)server)用於生成商用終端(UE)真實的各種數服務據流量，且應該盡可能靠近商用 4G/5G 核心網路或模擬器。
網路減損模擬器	網路減損模擬器(network impairment emulator)用於需要在前傳介面(Open Front-Haul)數據封包延遲(delay)或信號跳動(jitter)的減損測試。
射頻衰減器與衰落產生器	射頻衰減器(RF attenuators)用於需要無線電信號衰減的測試。衰落產生器(Fading generators)可用於模擬特定的無線電信道條件，例如城市、農村與高速列車。

測試工具	工具描述
封包產生器工具/阻斷服務攻擊模擬器	封包產生器工具/阻斷服務(DoS)攻擊模擬器用於阻斷服務(DoS)的資安測試流量。該工具必須支援產生網路 2 至 7 層的協定流量，包含以太網協議(Ethernet Protocol)、網際網路協定(Internet protocol, IP)與傳輸控制協定(Transmission Control Protocol, TCP)及用戶資料元協定(User Datagram Protocol, UDP)、精確時間協定(Precision Time Protocol, PTP)、演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)、傳送層安全協定(Transport Layer Security protocol, TLS)、超文件傳輸協定(Hypertext transfer protocol, HTTP)與超文件傳輸協定第 2 版(HTTP/2)。該工具根據測試需求布署在各個通信網段中。
封包擷取工具	封包擷取工具(packet capture tool)用於擷取流量數據樣本以進行驗證、分析和故障排除，也可以用於合法擷取流量數據，作為模糊攻擊資安測試的樣板。該工具必須支援網路 2 至 7 層的協定，包含以太網協議(Ethernet Protocol)、網際網路協定(Internet protocol, IP)與傳輸控制協定(Transmission Control Protocol, TCP)及用戶資料元協定(User Datagram Protocol, UDP)、精確時間協定(Precision Time Protocol, PTP)、演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)、傳送層安全協定(Transport Layer Security protocol, TLS)、超文件傳輸協定(Hypertext transfer protocol, HTTP)與超文件傳輸協定第 2 版(HTTP/2)。該工具根據測試需求布署在各個通信網段中。
網路流量分流器	網路流量分流器是一種硬體或軟體設備，提供對計算機網路上的數據流量的存取性和可見性。
模糊測試工具	協定模糊測試(protocol fuzzing tool)用於生成非預期的輸入協定之資安測試。該工具必須支援重播變異之網路 2 至 7 層的協定流量，包含以太網協議(Ethernet Protocol)、網際網路協定(Internet protocol, IP)與傳輸控制協定(Transmission Control Protocol, TCP)及用戶資料元協定(User Datagram Protocol, UDP)、精確時間協定(Precision Time Protocol, PTP)、演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)、傳送層安全協定(Transport Layer Security protocol, TLS)、超文件傳輸協定(Hypertext transfer protocol, HTTP)與超文件傳輸協定第 2 版(HTTP/2)。該工具根據測試需求布署在各個通信網段中。
弱點掃描工具	弱點掃描工具(vulnerability scanning tool)用於在資安測試中搜尋已知漏洞。該工具依賴周期性更新已知的常見漏洞披露(Common Vulnerabilities and Exposures, CVE)的資料庫，並支援掃描運行網路通訊協定(Transmission Control Protocol/Internet Protocol, TCP/IP)的網路服務。該工具根據測試需求布署在各個通信網段中。

測試工具	工具描述
網路功能虛擬化(NFV)評量基準與資源耗竭工具	網路功能虛擬化(NFV)工具用於雲平台(O-Cloud)系統性能評量和生成資源耗竭型阻斷服務(DoS)攻擊的資安測試。該工具應該能夠布署於公共或私有類型的雲平台(O-Cloud)環境上用以測試虛擬網路功能(Virtualized Network Function, VNF)或容器網路功能化(Container Network Function, CNF)的支援度。
安全外殼協定審計工具	安全外殼協定(SSH)審計工具用於驗證服務器和用戶端配置的安全外殼協定(SSH)軟體的協議版本、密碼套件和已知漏洞等。
傳送層安全協定(TLS)掃描工具	傳送層安全協定(Transport Layer Security protocol, TLS)掃描工具用於驗證傳送層安全協定(TLS)軟體伺服器的協定版本、安全套件與已知弱點等資訊。
資料包傳送層安全協定(DTLS)掃描工具	資料包傳送層安全協定(Datagram Transport Layer Security protocol, DTLS)掃描工具用於驗證資料包傳送層安全協定(DTLS)軟體伺服器的協定版本、安全套件與已知弱點等資訊。
網際網路金鑰交換(IKE)掃描工具	網際網路金鑰交換(Internet key exchange, IKE)掃描工具用於驗證網際網路安全協定(Internet Protocol Security, IPSec)軟體伺服器的協定版本、安全套件與已知弱點等資訊。

表 14 Open RAN 資安測試案例[10]

案例編號	測試案例	案例描述
STC-Chapter 4-001	安全外殼協定(SSH)的伺服器與用戶端	安全外殼協定(Secure Shell, SSH)需要使用足夠強大加密協定套件。
STC-Chapter 4-002	傳送層安全協定(TLS)	支援適當配置的傳送層安全協定(Transport Layer Security protocol, TLS)1.2 版或 1.3 版。
STC-Chapter 4-003	資料包傳送層安全協定(DTLS)	支援適當配置的資料包傳送層安全協定(Datagram Transport Layer Security protocol, DTLS)1.2 版。
STC-Chapter 4-004	網際網路安全協定(IPSec)	驗證網際網路安全協定(Internet Protocol Security, IPSec)是否正確設定通信安全協議。
STC-Chapter 5-5.2-001	網路服務列舉(Service Enumeration)	不允許未註冊的網路服務。
STC-Chapter 5-5.3-001	暴力破解(Brute Forcing)	不允許未經授權存取管理平面。

案例編號	測試案例	案例描述
STC-Chapter 5-5.3-002	未經授權的密碼重置 (Unauthorized Password Reset)	確認沒有任何未經授權規避、停用或重置管理員(Admin)密碼的機制。
STC-Chapter 5-5.3-003	強制密碼政策 (Password Policy Enforcement)	確認會強制執行密碼政策(Password Policy)。
STC-Chapter 5-5.4	模糊測試(Fuzzing)	測試 O-RAN 系統中使用之串流控制傳輸協定(Stream Control Transmission Protocol, SCTP)、網際網路協定(Internet protocol, IP)、傳輸控制協定(Transmission Control Protocol, TCP)、用戶資料元協定(User Datagram Protocol, UDP)、安全外殼協定模糊測試(SSH protocol)、超文件傳輸協定(Hypertext transfer protocol, HTTP)與超文件傳輸協定第 2 版(HTTP/2)、網路設定協定(NETCONF)、E1 應用協定(E1AP)、E2 應用協定(E2AP)、A1 協定、協同傳輸介面(Cooperative Transport Interface, CTI)、演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)以及精確時間協定(Precision Time Protocol, PTP)模糊測試的強健性。
STC-Chapter 5-5.5-001	阻斷服務/資訊洪水 (Denial of Service / Message Flooding	O-RAN 系統和主要介面需要具備足夠的強健性來抵抗分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊。
STC-Chapter 6-6.2-001	系統弱點掃描(System Vulnerability Scanning)	透果對 O-RAN 系統進行弱點掃描(Vulnerability Scanning)以確保 O-RAN 元件的作業系統(Operating System, OS)及應用程式(applications)無已知弱點。
STC-Chapter 7-7.2-001	開源軟體元件分析 (Open-Source Software Component Analysis)	N/A
STC-Chapter 7-7.3-001	二元碼靜態分析 (Binary Static Analysis)	N/A
STC-Chapter 8-8.2-001	機器學習資料毒害(ML Data Poisoning)	N/A

6.4 Open RAN 基地臺測試案例的彙整分析

彙整前述的 3GPP 基地站安全確保機制以及 O-RAN 安全確保機制，對於 5G Open RAN 基地臺的每個元件之測試案例分別敘述於下列各節，5G Open RAN 基地臺的製造商可先行依據下列各節的測試案例於研發階段先行驗證產品的安全性。

6.4.1 非即時無線接取網路智能控制的測試案例

非即時無線接取網路智能控制(Non-Real Time Radio Access Network Intelligent Controller, Non-RT RIC)位於服務管理與編排(Service Management and Orchestration, SMO)內，功能包括資料分析、訓練機器學習(Machine Learning, ML)模型、提供額外資訊(Enrichment Information)、設定方針(Policy)。依據開放式無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(SFG)的資安測試標準(Security Test Specification)規格文件[10]，Open RAN 集中單元-控制平面(CU-CP)的測試案例如表 15 所示。

表 15 Open RAN 非即時無線接取網路智能控制(Non-RT RIC)測試案例

標準章節	測試項目
STC-Chapter 4-002	傳送層安全協定(TLS)
STC-Chapter 5-5.2-001	網路服務列舉(Service Enumeration)
STC-Chapter 5-5.2-001	暴力破解(Brute Forcing)
STC-Chapter 5-5.3-002	未經授權的密碼重置(Unauthorized Password Reset)
STC-Chapter 5-5.3-003	強制密碼政策(Password Policy Enforcement)
STC-Chapter 5-5.4	模糊測試(Fuzzing)
STC-Chapter 5-5.5-001	阻斷服務/資訊洪水(Denial of Service / Message Flooding
STC-Chapter 8-001	機器學習資料毒害(ML Data Poisoning)

6.4.2 近即時無線接取網路智能控制的測試案例

近即時無線接取網路智能控制(Near Real Time Radio Access Network Intelligent Controller, Near-RT RIC)位於無線接取網路(Radio Access Network, RAN)內，接收與分析來自無線接取網路(RAN)的即時資訊，結合非即時無線接取網路智能控制(Non-RT RIC)提供的額外資訊，監控或預測用戶連線狀況的變化。依據開放式無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(SFG)的資安測試標準(Security Test Specification)規格文件[10]，Open RAN 集中單元-控制平面(CU-CP)的測試案例如表 16 所示。

表 16 近即時無線接取網路智能控制(Near-RT RIC)測試案例

標準章節	測試項目
STC-Chapter 4-002	傳送層安全協定(TLS)
STC-Chapter 4-003	資料包傳送層安全協定(DTLS)
STC-Chapter 4-004	網際網路安全協定(IPSec)
STC-Chapter 5-5.2-001	網路服務列舉(Service Enumeration)
STC-Chapter 5-5.2-001	暴力破解(Brute Forcing)
STC-Chapter 5-5.3-002	未經授權的密碼重置(Unauthorized Password Reset)
STC-Chapter 5-5.3-003	強制密碼政策(Password Policy Enforcement)
STC-Chapter 5-5.4	模糊測試(Fuzzing)
STC-Chapter 5-5.5-001	阻斷服務/資訊洪水(Denial of Service / Message Flooding
STC-Chapter 6-6.2-001	系統弱點掃描(System Vulnerability Scanning)
STC-Chapter 7-001	開源軟體元件分析(Open-Source Software Component Analysis)
STC-Chapter 7-002	二元碼靜態分析(Binary Static Analysis)
STC-Chapter 8-001	機器學習資料毒害(ML Data Poisoning)

6.4.3 Open RAN 基地臺集中單元-控制平面的測試案例

Open RAN 基地臺集中單元-控制平面(CU-CP)主要負責無線資源控制(Radio Resource Control, RRC)與封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)等控制平面的網路功能，涉及到用戶設備(UE)之控制平面(control plane)封包的完整性和機密性。依據第三代合作夥伴計畫(3GPP)之服務與系統第 3 工作組(Service and System Aspects#3, SA3)的 S3-211792 提案 (29) 與 S3-211793 提案 (30)，以及開放式無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(Security Focus Group, SFG)的資安測試標準(Security Test Specification)規格文件 [10] 建議，Open RAN 集中單元-控制平面(CU-CP)的測試案例如表 17 所示。

表 17 Open RAN 基地臺集中單元-控制平面(CU-CP)測試案例

標準章節	測試項目
4.2.2.1.1	無線資源控制信令的完整性保護
4.2.2.1.4	無線資源控制完整性檢查失敗
4.2.2.1.6	無線資源控制信令加密
4.2.2.1.9	無線資源控制信令重播攻擊保護
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

標準章節	測試項目
4.2.2.1.12	gNB 存取層加密和完整性演算法優先順序
4.2.2.1.13	gNB 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 及 Fn、E1 介面的機密性保護
4.2.2.1.17	控制平面資料在 N2 與 Xn 及 Fn、E1 介面的完整性保護
4.2.2.1.18	雙連線的 gNB 金鑰更新
案例編號	測試項目
STC-Chapter 4-002	傳送層安全協定(TLS)
STC-Chapter 4-003	資料包傳送層安全協定(DTLS)
STC-Chapter 4-004	網際網路安全協定(IPSec)
STC-Chapter 5-5.2-001	網路服務列舉(Service Enumeration)
STC-Chapter 5-5.3-001	暴力破解(Brute Forcing)
STC-Chapter 5-5.3-002	未經授權的密碼重置(Unauthorized Password Reset)
STC-Chapter 5-5.3-003	強制密碼政策(Password Policy Enforcement)
STC-Chapter 5-5.4	模糊測試(Fuzzing)
STC-Chapter 5-001	阻斷服務/資訊洪水(Denial of Service / Message Flooding
STC-Chapter 6-6.2-001	系統弱點掃描(System Vulnerability Scanning)
STC-Chapter 7-001	開源軟體元件分析(Open-Source Software Component Analysis)
STC-Chapter 7-002	二元碼靜態分析(Binary Static Analysis)

6.4.4 Open RAN 基地臺集中單元-用戶平面的測試案例

Open RAN 基地臺集中單元-用戶平面(CU-UP)者則負責服務數據適配協定(Service Data Adaptation Protocol, SDAP)以及封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)等用戶平面的網路功能，涉及到用戶設備(UE)之用戶平面(user plane)封包的完整性和機密性。依據第三代合作夥伴計畫(3GPP)之服務與系統第 3 工作組(SA3)的 S3-211792 提案 (29) 與 S3-211793 提案 (30)，以及開放式無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(SFG)的資安測試標準(Security Test Specification)規格文件 [10]建議，Open RAN 集中單元-控制平面(CU-CP)的測試案例如表 18 所示。

表 18 Open RAN 基地臺集中單元-用戶平面(CU-UP)測試案例

標準章節	測試項目
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
4.2.2.1.5	用戶平面完整性檢查失敗
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
4.2.2.1.10	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	gNB 存取層加密和完整性演算法優先順序
4.2.2.1.13	gNB 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 E1 介面的機密性保護
4.2.2.1.17	控制平面資料在 E1 介面的完整性保護
4.2.2.1.18	雙連線的 gNB 金鑰更新
案例編號	測試項目
STC-Chapter 4-002	傳送層安全協定(TLS)
STC-Chapter 4-003	資料包傳送層安全協定(DTLS)
STC-Chapter 4-004	網際網路安全協定(IPSec)
STC-Chapter 5-5.2-001	網路服務列舉(Service Enumeration)
STC-Chapter 5-5.3-001	暴力破解(Brute Forcing)
STC-Chapter 5-5.3-002	未經授權的密碼重置(Unauthorized Password Reset)
STC-Chapter 5-5.3-003	強制密碼政策(Password Policy Enforcement)
STC-Chapter 5-5.4	模糊測試(Fuzzing)
STC-Chapter 5-001	阻斷服務/資訊洪水(Denial of Service / Message Flooding
STC-Chapter 6-6.2-001	系統弱點掃描(System Vulnerability Scanning)
STC-Chapter 7-001	開源軟體元件分析(Open-Source Software Component Analysis)
STC-Chapter 7-002	二元碼靜態分析(Binary Static Analysis)

6.4.5 Open RAN 基地臺分散單元的測試案例

Open RAN 基地臺分散單元(DU)則負責無線鏈路控制(Radio Link Control, RLC)與媒體存取控制(Media Access Control, MAC)以及上層實體層(Upper Physical layer, PHY)等網路功能，當其遭受攻擊時仍然會影用戶設備(UE)的可用性(availability)。依據開放式無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(SFG)的資安測試標準(Security Test Specification)規格文件[10]，Open RAN 集中單元-控制平面(CU-CP)的測試案例如表 19 所示，其中紅字底線為建議增加之資安測項。

表 19 Open RAN 基地臺分散單元(DU)測試案例

標準章節	測試項目
4.2.2.1.16	控制平面資料在 Fn 介面的機密性保護
4.2.2.1.17	控制平面資料在 Fn 介面的完整性保護
案例編號	測試項目
STC-Chapter 4-001	安全外殼協定(SSH)的伺服器與用戶端
STC-Chapter 4-002	傳送層安全協定(TLS)
STC-Chapter 4-003	資料包傳送層安全協定(DTLS)
STC-Chapter 4-004	網際網路安全協定(IPSec)
STC-Chapter 5-5.2-001	網路服務列舉(Service Enumeration)
STC-Chapter 5-5.3-001	暴力破解(Brute Forcing)
STC-Chapter 5-5.3-002	未經授權的密碼重置(Unauthorized Password Reset)
STC-Chapter 5-5.3-003	強制密碼政策(Password Policy Enforcement)
STC-Chapter 5-5.4	模糊測試(Fuzzing)
STC-Chapter 5-5.5-001	阻斷服務/資訊洪水(Denial of Service / Message Flooding
STC-Chapter 6-6.2-001	系統弱點掃描(System Vulnerability Scanning)
STC-Chapter 7-001	開源軟體元件分析(Open-Source Software Component Analysis)
STC-Chapter 7-002	二元碼靜態分析(Binary Static Analysis)

6.4.6 Open RAN 基地臺無線電單元

Open RAN 基地臺無線電單元(RU)則負責下層實體層(Lower Physical layer, Lower-PHY)以及射頻(Radio Frequency, RF)信號處理等網路功能。依據開放式無線接取網路聯盟(O-RAN Alliance)之安全焦點小組(SFG)的資安測試標準(Security Test Specification)規格文件[10]，Open RAN 集中單元-控制平面(CU-CP)的測試案例如表 20 所示。

表 20 Open RAN 基地臺無線電單元(RU)測試案例

標準章節	測試項目
STC-Chapter 4-001	安全外殼協定(SSH)的伺服器與用戶端
STC-Chapter 4-002	傳送層安全協定(TLS)
STC-Chapter 5-5.2-001	網路服務列舉(Service Enumeration)
STC-Chapter 5-5.3-001	暴力破解(Brute Forcing)
STC-Chapter 5-5.3-002	未經授權的密碼重置(Unauthorized Password Reset)
STC-Chapter 5-5.3-003	強制密碼政策(Password Policy Enforcement)
STC-Chapter 5-5.4	模糊測試(Fuzzing)
STC-Chapter 5-5.5-001	防止客戶端被竊取資料的安全措施(Client Security Measures Against Interception)

標準章節	測試項目
STC-Chapter 6-6.2-001	系統弱點掃描(System Vulnerability Scanning)
STC-Chapter 7-001	開源軟體元件分析(Open-Source Software Component Analysis)
STC-Chapter 7-002	二元碼靜態分析(Binary Static Analysis)

7. 結論與建議

本研究報告探討 5G Open RAN 系統架構，參考無線接取網路聯盟(O-RAN Alliance)及第三代合作夥伴計畫(The 3rd Generation Partnership Project , 3GPP)之標準規範與技術研究報告，彙整 3GPP 基地站安全確保機制以及 O-RAN 安全確保機制；電信網路運營商在布署分散式虛擬化 5G 基地臺時，一般會同時從供應商處同時購買和布署虛擬網路功能(Virtual Network Functions, VNF)、虛擬層(virtualization layer)和硬體層(hardware layer)。而開放式無線接取網路聯盟(O-RAN Alliance)主要是基於第三代合作夥伴計畫(3GPP)的 5G 基地臺(gNB)架構，發展一個開放式無線接取網路的管理架構，制定低層分割(low layer split)架構的標準，並提供 5G 基地臺(gNB)的無線接取網路(Radio Access Network, RAN)網路功能虛擬化，同時發展重點也著重於使用開放原始碼軟體(Open Source Software)和商用產品(Commercial off the shelf, COTS)的開放硬體架構。

隨著 Open RAN 開放式架構的網通設備「白牌化」後，市場也擔心開放架構會不會造成更多的資安漏洞。依據歐盟與北約組織在 2019 年 5 月在 5G 安全會議所提出的「布拉格倡議(Prague Proposals)」(23)，可信任的 5G 網路軟硬體設備供應鏈管理將是 5G 資安管理最重要的關鍵議題。因此，5G 電信事業不僅需要可信任的網路軟硬體設備供應鏈業者，更必須有能力驗證 5G 相關網路軟硬體設備的安全性才行。因此開放式無線接取網路聯盟(Open Radio Access Network Alliance, O-RAN Alliance)成立安全焦點小組(Security Focus Group, SFG)以克服 Open RAN 的資安議題。為了確保 Open RAN 開放式架構的設備商在實作相關網路產品的安全標準規範落實度，針對安全確保機制，將採用全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)制定的網路設備安全保證方案(Network Equipment Security Assurance Scheme, NESAS)搭配第三代合作夥伴計畫(3GPP)制定的產品資安確保標準(Security Assurance Specification, SCAS)來驗證，同時針對 O-RAN 新增加的介面與架構制定相關的資安測試案例。

台灣已有工業電腦與伺服器廠商以及小型基地臺製造商積極投入 5G Open RAN 開放式架構網通設備的市場，建議 5G Open RAN 基地臺的製造商及軟硬體開發商可依據開放式無線接取網路聯盟(O-RAN Alliance)的方案，先依據全球行動通訊系統協會(GSMA)制定的網路設備安全保證方案(NESAS)，搭配第三代合作夥伴計畫(3GPP)制定的產品資安確保標準(SCAS)來驗證 5G Open RAN 基地臺產品的安全性，以降低產品於

商用時的資安修補成本。除了可以滿足潛在客戶的資安需求外，同時亦可提升產品的國際市場競爭力。

資策會資安所團隊於第三代合作夥伴計畫(3GPP)之服務與系統第 3 工作組(Service and System Aspects#3, SA3)，透過電子郵件討論向第 3 工作組(SA3)建議增訂 3GPP 分散式基地臺產品資安確保標準(SCAS)，團隊也會依據本研究報告的研究結果向國際標準組織提出修訂產品資安確保標準(SCAS)。未來當開放式無線接取網路聯盟(O-RAN Alliance)的資安測試標準規格(Security Test Specification)之資安測試項目正式定稿後，建議訂定 5G Open RAN 開放式架構網通設備的測試項目，協助台灣廠商與檢測實驗室建立 5G Open RAN 開放式架構的資安檢測能量。其中開源軟體元件分析(Open-Source Software Component Analysis)、二元碼靜態分析(Binary Static Analysis)與 5G Open RAN 相關協定的模糊測試(Fuzzing)以及機器學習資料毒害(ML Data Poisoning)等資安測試，屬於驗證 5G Open RAN 基地臺產品開發階段的強健性與安全性，台灣廠商可以依據潛在客戶的需求導入相關測試以提升產品競爭力。期望電信事業未來在營運時，能夠透過本研究報告獲得 5G Open RAN 開放式架構的基本資安防護知識，以確保 5G Open RAN 開放式架構應用服務的安全性。

附錄A
(參考)
開放式無線接取網路聯盟(O-RAN Alliance)簡介

開放式無線接取網路聯盟(O-RAN Alliance)共設立 10 個工作組(Working Group, WG)及 4 個焦點小組(Focus Group, FG)如下：

(a) 第一工作組(WG1) - 應用範例和整體架構：

第一工作組(WG1)負責 Open RAN 的應用範例和整體架構，領導分配 Open RAN 架構和應用案例給其他開放式無線接取網路聯盟工作組，並推動其他工作組完成 Open RAN 架構範圍內的工作任務。

(b) 第二工作組(WG2) - 非即時無線接取網路智能控制和 A1 介面：

第二工作組(WG2)的主要目標是發展非即時無線接取網路智能控制(Non-RT RIC)以支持無線接取網路(RAN)，提供非實時智能無線電資源管理與策略最佳化，並提供近即時無線接取網路智能控制(Near-RT RIC)所需的人工智慧(AI)和機器學習(ML)模型。

(c) 第三工作組(WG3) - 近即時無線接取網路智能控制和 E2 介面：

第三工作組(WG3)的重點是定義一個基於近即時無線接取網路智能控制(Near-RT RIC)的體系結構，該體系結構透過數據收集和透過 E2 介面進行的操作，可以實現無線接取網路(RAN)資源的近即時智能控制和最佳化。

(d) 第四工作組(WG4) - 開放的前傳介面：

第四工作組(WG4)的目標是提供真正開放前傳介面(Open Fronthaul Interface)，在其中可以實現多廠商 O-RAN 分散單元(O-RAN Distributed Unit, O-DU)與 O-RAN 無線電單元(O-RAN Radio Unit, O-RU)間的互通性。

(e) 第五工作組(WG5) - 開放的 F1 介面、W1 介面、E1 介面與 X2 介面及 Xn 介面：

第五工作組(WG5)的目的是為 F1 介面、W1 介面、E1 介面與 X2 介面及 Xn 介面提供完全符合第三代合作夥伴計畫(3GPP)規範，且多間廠商可配置操作的文件規範，並依實際需求增強第三代合作夥伴計畫(3GPP)現有的標準規範。

(f) 第六工作組(WG6) - 雲端化與協作平台：

第六工作組(WG6)的重點是透過雲端化(Cloudification)與協作平台(Orchestration)推動分割無線接取網路(RAN)軟體與硬體底層平台，並產出可用於布署 O-RAN 集中單元(O-RAN Central Unit, O-CU)與 O-RAN 分散單元(O-DU)的商用硬體平台技術和參考設計文件。

(g) 第七工作組(WG7) - 白盒(White Box)硬體：

第七工作組(WG7)的主要目標是推廣白牌硬體，透過指定並發布完整的參考設計，以促進軟體和硬體平台的分割，進而降低電信事業的 5G 整體建置的成本

(h) 第八工作組(WG8) - 堆疊參考設計：

第八工作組(WG8)的目的是基於開放式無線接取網路聯盟(O-RAN Alliance)和 第三代合作夥伴計畫(3GPP)規範，設計和發布計劃為 O-RAN 集中單元(O-CU)與 O-RAN 分散單元(O-DU)開發軟體架構。

(i) 第九工作組(WG9) - 負責開放式 X-haul 傳輸：

第九工作組(WG9)的主要目標是負責 Open RAN 架構中之 X-Haul 傳輸網路，以支援全面 5G 系統服務覆蓋的網路建置中，無線電接取網路(RAN)與 5G 核心網路(5G Core Network, 5GC)間高頻寬與低延遲的傳輸需求。

(j) 第十工作組(WG10) - 營運管理與維護：

第十工作組(WG10)的重點在於提供 Open RAN 架構中，非即時無線接取網路智能控制(Non-RT RIC)、近即時無線接取網路智能控制(Near-RT RIC)、O-RAN 集中單元(O-CU)與 O-RAN 分散單元(O-DU)及 O-RAN 無線電單元(O-RU)的營運管理與維護(Operations, Administration, and Maintenance, OAM)，著重在擴展開放式無線接取網路聯盟(O-RAN Alliance)與現有標準不支援的部分，發展依循第三代合作夥伴計畫(3GPP)與歐洲電信標準化協會(European Telecommunications Standards Institute, ETSI)的 O1 管理介面。

(k) 開源軟體焦點小組(OSFG)：

開源軟體焦點小組(Open Source Focus Group, OSFG)的主要目標是 Open RAN 架構中，推廣非即時無線接取網路智能控制(Non-RT RIC)、近即時無線接取網路智能控制(Near-RT RIC)、O-RAN 集中單元(O-CU)與 O-RAN 分散單元(O-DU)及 O-RAN 無線電單元(O-RU)等網路元件，使用開放原始碼軟體(Open Source Software)。

(l) 標準發展焦點小組(SDFG)：

標準發展焦點小組(Standard Development Focus Group, SDFG)的目的是協助推動開放式無線接取網路聯盟(O-RAN Alliance)的 10 個工作組(WG)及 4 個焦點小組(FG)執行標準化的工作。

(m) 測試與整合焦點小組(TIFG)：

開放式無線接取網路聯盟(O-RAN Alliance)的測試與整合焦點小組(Test and Integration Focus Group, TIFG)專注於實現端到端(End to End)操作性測試規範，並於開放測試與整合中心(Open Test and Integration Center, OTIC)釋出認證方法與 Open RAN 網路端到端的測試標準。

(n) 安全焦點小組(SFG)：

安全焦點小組(Security Focus Group, SFG)專注於制定 Open RAN 網路安全架構與框架、開放測試與整合中心(OTIC)安全驗證、開源安全準則與開放介面安全準則四大方向。

開放式無線接取網路聯盟(O-RAN Alliance)已經發布的 48 項規格如下：

表 21 開放式無線接取網路聯盟(O-RAN Alliance)標準規格

工作組/焦點小組	標準規格
第一工作組(WG1)	1) RAN Architecture Description v5.0 2) RAN Slicing Architecture v5.0 3) RAN Use Cases Analysis Report v6.0 4) O-RAN Use Cases Detailed Specification 6.0
第二工作組(WG2)	5) O-RAN AI/ML workflow description and requirements v1.03 6) O-RAN Non-RT RIC Architecture v1.0 7) O-RAN Non-RT RIC & A1 Interface: Use Cases and Requirements v4.0 8) O-RAN A1 interface: Type Definitions v2.00 9) O-RAN A1 interface: General Aspects and Principles v 2.03
第三工作組(WG3)	10) O-RAN Near-RT RIC and E2 Interface: Use Cases and Requirements v1.0 11) O-RAN E2 General Aspects and Principles(E2GAP)v2.0 12) O-RAN E2 Application Protocol(E2AP)v2.0 13) O-RAN E2 Service Model(E2SM)v2.0 14) O-RAN E2 Service Model: RAN Control(E2SM-RC)v1.0 15) O-RAN E2 Service Model: Key Performance Measurement(E2SM-KPM)v2.0
第四工作組(WG4)	16) O-RAN Open Fronthaul Management Plane Specification v7.0 17) O-RAN Fronthaul Interoperability Test Specification (IOT)v5.0 18) O-RAN Fronthaul Control, User and Synchronization Plane Specification v7.0 19) O-RAN Open Fronthaul Conformance Test Specification v4.0
第五工作組(WG5)	20) O-RAN NR C-plane profile v5.0 21) O-RAN O1 Interface specification for O-CU-UP and O-CU-CP v1.0 including Yang models 22) O-RAN O1 Interface specification for O-DU v2.0 including YANG models and AnnexD
第六工作組(WG6)	23) O-RAN Cloud Architecture and Deployment Scenarios for O-RAN Virtualized RAN v2.02 24) O-RAN Acceleration Abstraction Layer FEC Profiles v1.0 25) O-RAN Orchestration Use Cases and Requirements for O-RAN Virtualized RAN v2.01 26) O-RAN O2 General Aspects and Principles v1.01 27) O-RAN Acceleration Abstraction Layer General Aspects and Principles v1.01 28) O-RAN O2ims Interface Specification v1.0

工作組/焦點小組	標準規格
第六工作組(WG6)	29) O-RAN O-Cloud Notification API Specification for Event Consumers v1.0
第七工作組(WG7)	30) O-RAN Hardware Reference Design Specification for Indoor Picocell(FR1)with Split Architecture Option 8 v3.0 31) O-RAN Hardware Reference Design Specification for Indoor Picocell(FR1)with Split Architecture Option 7-2 v3.0 32) O-RAN Deployment Scenarios and Base Station Classes v3.0 33) O-RAN Hardware Reference Design Specification for Outdoor Microcell with Split Architecture Option 7.2 v2.0 34) O-RAN Hardware Reference Design Specification for Fronthaul Gateway v2.0 35) O-RAN Hardware Reference Design Specification for Indoor Picocell with Fronthaul Split Option 6 v2.0
第八工作組(WG8)	36) O-RAN Stack Interoperability Test Specification v2.0 37) O-RAN Base Station O-DU and O-CU Software Architecture and APIs v4.0
第九工作組(WG9)	38) O-RAN Base Station O-DU and O-CU Software Architecture and APIs v4.0 39) O-RAN Management Interface for Transport Network Elements v2.0 40) O-RAN Xhaul Transport Testing v1.01
第十工作組(WG10)	41) O-RAN Operations and Maintenance Architecture v5.0 42) O-RAN Operations and Maintenance Interface Specification v5.0
安全焦點小組(SFG)	43) O-RAN Security Protocols Specifications v2.0 44) O-RAN Security Threat Modeling and Remediation Analysis 2.0 45) O-RAN Security Requirements Specifications v1.0
測試與整合焦點小組(TIFG)	46) O-RAN Certification and Badging Processes and Procedures v2.0 include template table of records 47) O-RAN End-to-end Test Specification v2.0 48) O-RAN Criteria and Guidelines of Open Testing and Integration Centre v3.0

參考資料

(1) 3GPP TR 21.905-h00, “Vocabulary for 3GPP Specifications (Release 17)” (https://www.3gpp.org/ftp//Specs/archive/21_series/21.905/21905-h00.zip)

(2) 3GPP TS 23.501-h20, “System Architecture for the 5G System(5GS) (Release 17)” (https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-h20.zip)

(3) 3GPP TS 38.413-g70, “NG-RAN; NG Application Protocol (NGAP) (Release 16)” (https://www.3gpp.org/ftp/Specs/archive/38_series/38.413/38413-g70.zip)

(4) 3GPP TS 29.281-h10, “General Packet Radio System (GPRS)Tunnelling Protocol User Plane (GTPv1-U) (Release 17)” (https://www.3gpp.org/ftp/Specs/archive/29_series/29.281/29281-h10.zip)

(5) 3GPP TS 38.423-g70, “NG-RAN; Xn Application Protocol (XnAP) (Release 16)” (https://www.3gpp.org/ftp/Specs/archive/38_series/38.423/38423-g70.zip)

(6) 3GPP TS 38.473-g70, “NG-RAN; F1 Application Protocol(F1AP) (Release 16)” (https://www.3gpp.org/ftp/Specs/archive/38_series/38.473/38473-g70.zip)

(7) 3GPP TS 38.463-g70, “NG-RAN; E1 Application Protocol(E1AP) (Release 16)” (https://www.3gpp.org/ftp/Specs/archive/38_series/38.463/38463-g70.zip)

(8) O-RAN WG3, “O-RAN Near-Real-time RAN Intelligent Controller, E2 Application Protocol(E2AP)1.01 - July 2020” (https://www.o-ran.org/specifications)

(9) O-RAN WG2, “O-RAN A1 interface: Application Protocol 3.01 - March 2021” (https://www.o-ran.org/specifications)

(10) O-RAN WG10, “O-RAN Operations and Maintenance Interface Specification 5.0 - July 2021” (https://www.o-ran.org/specifications)

(11) O-RAN WG6, “O-RAN O2 General Aspects and Principles Specification 1.0 - July 2020” (https://www.o-ran.org/specifications)

(12) O-RAN WG4, “O-RAN Fronthaul Control, User and Synchronization Plane Specification 7.0 - July 2021” (https://www.o-ran.org/specifications)

(13) “美國總統簽署《安全可信通訊網路法》,” 科技法律研究所, 財團法人資訊工業策進會 (https://stli.iii.org.tw/article-detail.aspx?no=55&tp=5&i=180&d=8523)

(14) “美國國防部 5G 戰略,” 科技法律研究所, 財團法人資訊工業策進會 (https://stli.iii.org.tw/article-detail.aspx?no=55&tp=5&d=8498)

(15) “《2021 年國防授權法》與美軍網路戰略動向,” 財團法人國防安全研究院

(16) “中國公司試圖主導美國力挺新一代網絡開放架構,” 美國之音 (https://www.voacantonese.com/a/china-attempts-to-head-a-new-framework-of-internet-20210107/5728571.html)

(17) “美國 5G 科技加速方案（5G FAST Plan）,” 科技法律研究所, 財團法人資訊工業策進會
(https://stli.iii.org.tw/article-detail.aspx?no=16&tp=5&d=8246)

(18) “Forum on 5G Open Radio Access Networks,” FCC
(https://www.fcc.gov/news-events/events/forum-5g-virtual-radio-access-networks)

(19) “FCC Seeks Comment on Open Radio Access Networks”, Mar 18, 2021
(https://www.fcc.gov/document/fcc-seeks-comment-open-radio-access-networks-0)

(20) “Making sure that Open doesn’t open the door for new risks in 5G,” Ericson

(21) “Security Considerations of Open RAN” whitepaper, August 2020, Ericson

(22) 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)

(23) The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world, Prague 5G Security Conference

(24) GSMA FS.13, “Network Equipment Security Assurance Scheme – Overview Version 2.0”
(https://www.gsma.com/security/wp-content/uploads/2021/02/FS.13-NESAS-Overview-v2.0.pdf)

(25) ISO/IEC 17025:2017, “General requirements for the competence of testing and calibration laboratories”
(https://www.iso.org/standard/66912.html)

(26) 「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」期末報告定稿，財團法人電信技術中心
(https://www.grb.gov.tw/search/planDetail?id=13215614)

(27) 3GPP TR 33.805-c00, “Study on security assurance methodology for 3GPP network products (Release 12)”
(https://www.3gpp.org/ftp/Specs/archive/33_series/33.805/33805-c00.zip)

(28) 3GPP TR 33.916-g000, “Security Assurance Methodology (SCAS)for 3GPP network products (Release 15)”
(https://www.3gpp.org/ftp//Specs/archive/33_series/33.916/33916-g00.zip)

(29) 3GPP S3-211792, “Discussion on adding SCAS for the various split gNB cases”
(https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_103e/Docs/S3-211792.zip)

(30) 3GPP S3-211793, “Adding SCAS for the various split gNB cases”
(https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_103e/Docs/S3-211793.zip)

版本修改紀錄

版本	時間	摘要
v1.0	2022/01/06	出版