5G 智慧杆系統技術規範

－第 1 部：一般要求

5G Smart pole system technical specification

- Part 1: General requirements

中 華 民 國 1 1 1 年 9 月

目錄

節次 頁次

前言 2

0. 簡介 3

1. 適用範圍 3

2. 引用標準 3

3. 用語及定義 3

4. 5G 智慧杆系統架構 4

4.1 智慧杆系統整體架構 4

4.2 智慧杆系統細部架構 5

4.3 智慧杆迴路 5

4.4 智慧杆管理系統 7

5. 5G 智慧杆系統技術規範各部概要 7

5.1 各部涵蓋範圍 7

5.2 各部規範內容概述 8

參考資料 10

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole) 現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT) 設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統。

本規範定義 5G 智慧杆系統框架，規定系統構成元件及其基本功能，並說明本系列規範系其他各部規範內容概要。

2. 引用標準

無。

3. 用語及定義

下列用語及定義適用於本規範。

3.1 網際網路(Internet)

不同電腦資訊網路間串連而形成超大型網路系統，包含私人、學術界、企業界及政府網路，透過電氣信號、無線及光纖等不同技術互相聯繫。接取至網路之設備皆使用標準網路協定相連，並發展出各種不同應用服務(例：電子郵件、語音通話及視訊串流等)。

3.2 智慧杆(smart pole)

建構智慧城市之關鍵基礎設施之一，採固定式杆狀結構(可參考一般路燈燈杆設計)，具備電源供應及網路通訊能力，可安裝或掛載各種不同設備(例：照明燈具、電信設備、資通訊設備及物聯網裝置等)之多用途載體。可提供各種智慧化應用服務 (例：高效率節能照明、行動通訊、智慧交通、資訊發布、安全監控、充電樁等)，並可透過資訊管理系統對其進行遠端監控及操作。

3.3 智慧杆迴路(smart pole cluster)

由 1 具迴路控制箱及 1 支以上智慧杆組成之群組。智慧杆及迴路控制箱透過電力電纜及通訊纜線互相連接，並經由通訊設備連接網際網路/電信網路。

備考：國內路燈施工及管理單位習慣稱呼使用相同電力饋線來源、以並連方式連接之路燈群組為〝迴路〞。

3.4 智慧杆迴路控制箱(smart pole cluster terminal box, 簡稱迴路控制箱)

固定式封閉箱體，具有框架及門板，且裝有電力設備、資訊設備及通訊設備。由迴路控制箱延伸出電力電纜及通訊纜線，連結智慧杆迴路內所有智慧杆，提供智慧杆電力供應及網路連線服務。

3.5 智慧杆系統(smart pole system)

智慧杆系統由智慧杆管理系統及不固定數量之智慧杆迴路構成，智慧杆管理系統包含營運管理平臺、應用業務平臺及資料服務平臺等不同資訊系統，智慧杆管理系統與智慧杆迴路間透過高速網路連接，並能搭配安裝於智慧杆迴路之附掛設備，提供各種應用服務。

3.6 電信網路(telecommunication network)

提供電信網路接取設備 (例：微型基地臺) 連結介面、管理資訊交換分配之電信網路基礎設施，由連結不同網路系統之骨幹網路及交換器設備組成。

4. 5G 智慧杆系統架構

4.1 智慧杆系統整體架構

智慧杆系統整體架構如圖 1 所示。

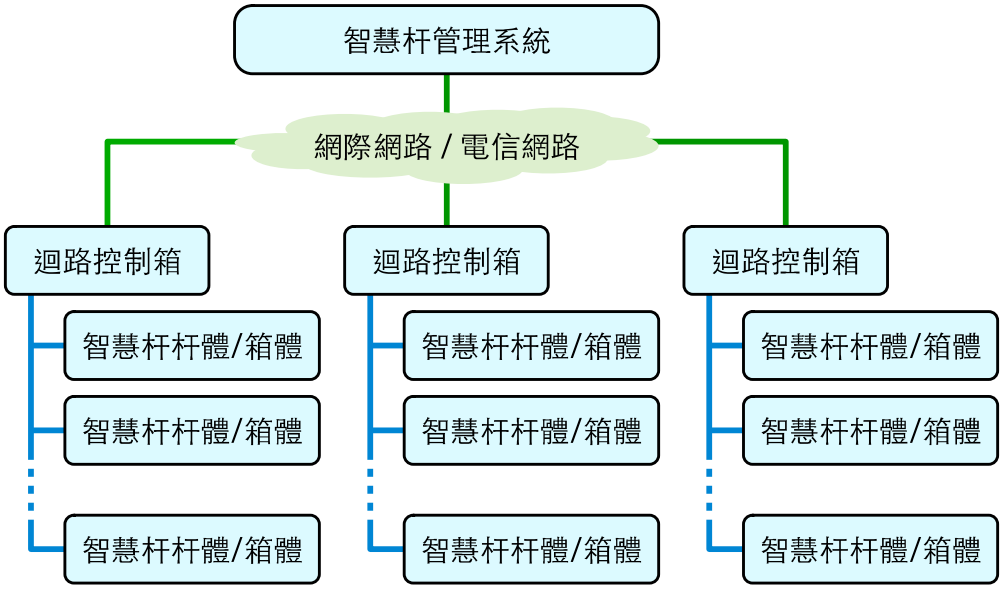


圖 1 智慧杆系統整體架構示意圖

智慧杆系統由智慧杆管理系統及不限數量之智慧杆迴路構成。智慧杆管理系統包含不同功能之資訊系統，可遠端監控、管理及操作智慧杆及附掛設備。智慧杆管理系統與智慧杆迴路間透過網際網路及電信網路相連，網路可為固接式網路、無線網路或其他足以承載智慧杆應用資訊流量之高速通訊網路基礎設施。

4.2 智慧杆系統細部架構

智慧杆管理系統及智慧杆迴路之細部架構如圖 2 所示。

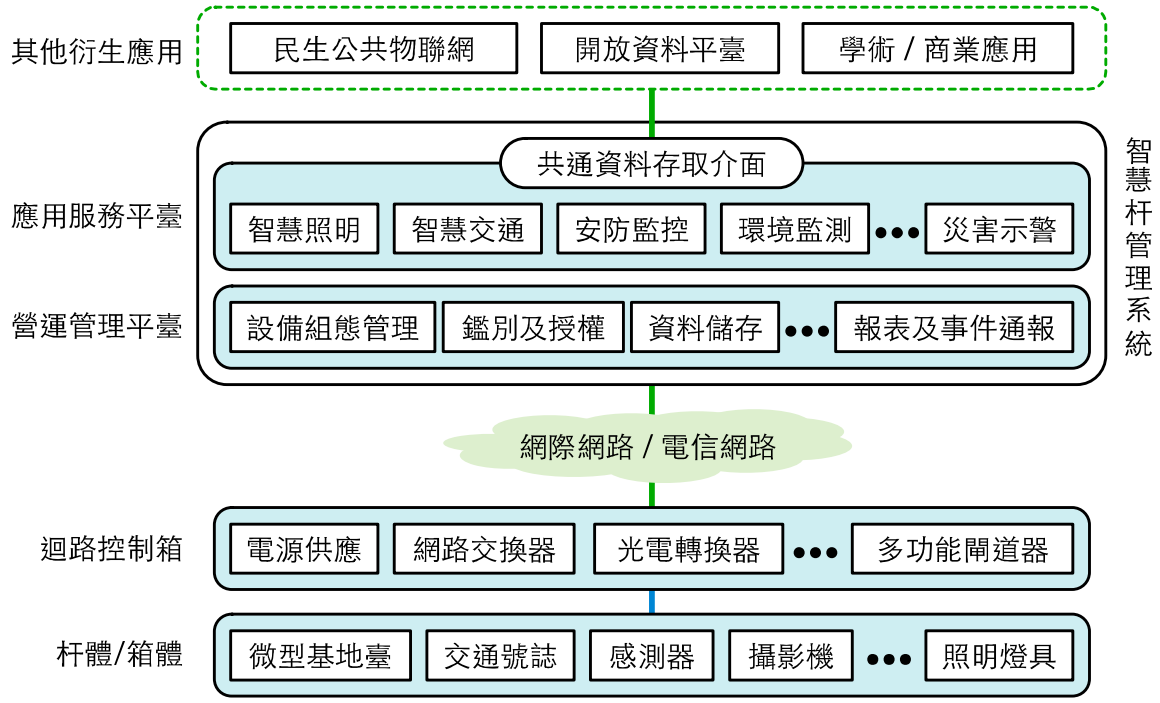


圖 2 智慧杆管理系統及智慧杆迴路之細部架構

智慧杆迴路包含迴路控制箱及智慧杆杆體/箱體，依據實際功能需求安裝不同設備，包含提供智慧杆迴路基本運作環境之基礎設施及提供應用服務之附掛設備。詳細說明參照 4.3。

智慧杆管理系統依功能及職責，細分為營運管理平臺及應用服務平臺。各平臺由不固定數量之電腦主機/電信設備組成，各自執行不同軟體/韌體程式以負責不同功能運作。並能透過應用服務平臺提供之資料共通存取介面，整合其他資料共享平臺，衍生不同應用服務。各平臺細部說明參照 4.4。

備考 1： 應用服務平臺及營運管理平臺可設置於不同地點，並利用網際網路互相連通。其網路拓樸及資訊流設計無上下層級關係。

4.3 智慧杆迴路

4.3.1 迴路控制箱

每 1 智慧杆迴路設置 1 具迴路控制箱，迴路控制箱及智慧杆之配置及連接方式和傳統路燈配線方式相近。迴路控制箱內依實際需求，安裝維持智慧杆迴路基本運作之基礎設施，包含：電力供應設備(例：供電端計費表、配電盤及不斷電系統等)及網路通訊設備(例：網路接線/跳線箱、光電轉換器、網路交換器及遠端管理設備等)，以及部分附掛設備(例：多功能閘道器、視訊監控主機等)。

迴路控制箱外型可由實作自行決定，但其結構安全、環境耐受度、電氣安全及基礎設施功能需求等相關設計，應符合本系列規範各部要求及實際場域建置需求。本系列規範各部內容參照第 5 節說明。

4.3.2 智慧杆杆體/箱體

智慧杆可用於路燈、交通號誌、各式標誌、視訊監視、車流監測、環境監測、資訊看板等多

用途，因應不同用途可採用不同型式設計，實施例如圖 3 所示。

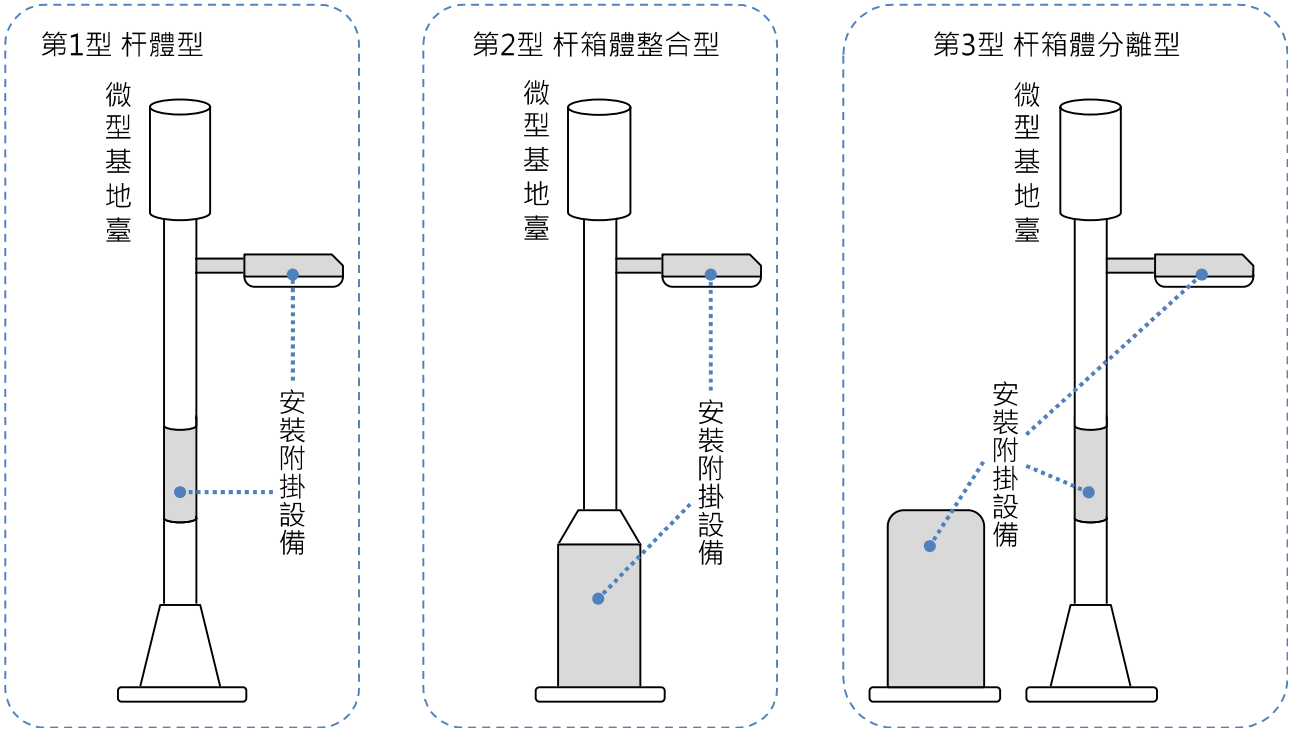


圖 3 智慧杆杆體/箱體常見實施例

杆體及箱體實施例可分為 3 型：

(a) 第 1 型(杆體型)：由杆體單獨構成，於杆體內部預留空間，可供附掛設備安裝。採用此型設計之實作應預留足夠擴充空間，或於後續改裝成杆箱體分離型，以容納額外之附掛設備。

(b) 第 2 型(杆箱體整合型)：由杆體及一具較大內部空間之箱體組成，可容納更多附掛設備。杆體和箱體採一體式設計，減少占用人行道空間。

(c) 第 3 型(杆箱體分離型)：杆體內空間不足、無法容納必要硬體元件(例：附掛設備之電源供應器等)時，可採此型設計。若因場域需要，亦可採單一分離式箱體對應多組智慧杆。

備考： 附掛設備依其用途及特性，採用各型配置時，可將部分硬體裝置以外掛方式安裝於杆體外部(例：照明燈具之燈頭部分、攝影鏡頭等)。

智慧杆杆體及箱體外型依實作而定，但其結構安全、環境耐受度、設備安裝位置及電氣安全等規格應能符合本系列規範各部要求及實際場域建置需求。本系列規範各部內容參照第 5 節說明。

設置於公有道路之智慧杆，其設置地點、施工、流程等，應依交通部市區道路及附屬工程設計規範[1]、交通工程規範[2]及各地方政府發布之路燈設置規範[3][4][5][6][7]。

4.3.3 附掛設備

智慧杆迴路內可依實際應用需求，安裝或掛載附掛設備(例：通訊設備、智慧照明燈具、交通號誌、資訊看板、網路視訊攝影機等)。附掛設備可安裝於智慧杆杆體/箱體或迴路控制箱內，附掛設備之安裝位置、種類及數量，皆依實作而定。

所有附掛設備之功能、性能、電源供應、電磁相容性、資訊互運性及資訊安全等，應能滿足其他相關法規(例：低功率射頻器材規範[8])、本系列規範各部內容及實際應用需求。本系列規

範各部內容參照第 5 節說明。

4.4 智慧杆管理系統

4.4.1 營運管理平臺

負責管理智慧杆及附掛設備之資訊系統，由 1 台以上電腦主機構成，用於收集及監控智慧杆及附掛設備相關資訊，並將各類事件訊息派送給指定管理者或營運者，以進行必要操作或處置。營運管理平臺負責附掛設備之組態管理功能，包含鑑別、註冊、監控設備運作狀況及授權使用網路資源。營運管理平臺同時具備其他維持正常運作之必要輔助功能(例：報表列印、事件通報、資料保存及人機管理介面等)。

營運管理平臺之硬體設備組成方式、實際建置位置、管理範圍及輔助功能設計，皆依實作而定。

4.4.2 應用服務平臺

由管理機關(構)、團體、企業或個人所建構之資訊系統，搭配安裝於智慧杆上之附掛設備，以共同達成應用服務功能(例: 接收監控視訊、接收環境感測資料、進行遠端操控、提供廣播資訊、進行互動服務等)。應用服務平臺同時具備其他維持正常運作之必要輔助功能(例：紀錄保存、紀錄調閱及人機管理介面等)。

應用服務平臺之硬體設備組成方式、實際建置位置、應用功能設計及輔助功能設計，皆依實作而定。

4.4.3 其他衍生應用

應用服務平臺得依實際需求或行政命令規定，透過共通資料存取介面，提供資料至其他資料共享平臺(例：民生公共物聯網)，供管理機關(構)、團體、企業或個人使用。所有資料皆由應用服務平臺負責蒐集、彙整、轉換，並以指定方式提供存取介面。資料保存方式、存取權限、申請程序等，皆依實作而定，本規範不予以規定。

5. 5G 智慧杆系統技術規範各部概要

5.1 各部涵蓋範圍

各部涵蓋範圍對應智慧杆系統細部架構如表 1 所示：

表 1. 5G 智慧杆技術各部涵蓋範圍對應智慧杆系統細部架構表

	杆體／箱體	迴路控制箱	電源供應設備	附掛設備	通訊設備	營運管理平臺	應用服務平臺
第 2-1 部：資訊互運性及通訊介面要求				○	○	○	○
第 2-2 部：資訊互運性及通訊介面測試要求				○	○	○	○
第 3 部：安裝與結構相關安全要求及試驗法	○						
第 4 部：環境可靠度要求		○		○	○		
第 5 部：電氣安全要求	○	○	○	○	○		
第 6 部：電磁相容要求	○	○	○	○	○		
第 7-1 部：資訊安全要求					○	○	○
第 7-2 部：資訊安全測試要求					○	○	○
第 8 部：電源供應系統要求		○	○	○	○		
第 9 部：性能要求				○			
第 10-1 部：5G 微型基地臺一般要求				○	○		
第 10-2 部：5G 微型基地臺性能測試要求				○	○		

5.2 各部規範內容概述

5.2.1 第 1 部：一般要求

智慧杆系統基本架構、名詞定義、涵蓋範圍及其他各部規範內容概述。

5.2.2 第 2-1 部：資訊互運性及通訊介面要求

規範智慧杆附掛設備、網路交換器、迴路設備管理、營運管理平臺及應用業務平臺之資訊網路通訊介面規格、通訊協定、資料格式及設備管理流程。

5.2.3 第 2-2 部：資訊互運性及通訊介面測試要求

規範對第 2-1 部各項規定之試驗法，包含測試環境、測試工具、測試步驟、通過條件等細部流程說明。

5.2.4 第 3 部：安裝與結構相關安全要求及試驗法

規範智慧杆設備安裝、模組及其零配件結構安全，以及測試要求，使產品在長期使用下能維持其結構安全性。

5.2.5 第 4 部：環境可靠度要求

規範智慧杆附掛設備之溫溼度、防塵防水、震動、耐候性等要求，使產品在戶外長期使用仍能維持正常運作。

5.2.6 第 5 部：電氣安全要求

規範絕緣、雷擊及感電災害預防等要求，確保產品電氣安全及避免衍生其他危險事件。

5.2.7 第 6 部：電磁相容要求

規範 5G 智慧杆在其使用環境中符合電磁相容要求及相關法規 (例：低功率射頻器材規範[8])。

5.2.8 第 7-1 部：資訊安全要求

規範智慧杆管理系統及網路通訊設備之資訊安全相關規定。

5.2.9 第 7-2 部：資訊安全測試要求

規範第 7-1 部要求之試驗法，包含智慧杆系統之設計、實作及營運管理等。

5.2.10 第 8 部：電源供應系統要求

規範智慧杆系統之電源架構系統相關要求。

5.2.11 第 9 部：性能要求

規範附掛設備之基本性能要求及試驗法，確保智慧杆系統整體運作功能完整。

5.2.12 第 10-1 部：5G 微型基地臺一般要求

規範 5G 微型基地臺操作頻段、基地臺類型、通訊介面要求、硬體、射頻、安規、電磁相容、基地臺審驗及行動通信網路性能要求。

5.2.13 第 10-2 部：5G 微型基地臺性能測試要求

規範第 10-1 部要求之試驗法，包含一致性測試、互運性測試、資訊安全測試等規定。

參考資料

[1] 市區道路及附屬工程設計規範，民國 101 年，內政部

[2] 交通工程規範，民國 110 年，交通部

[3] 桃園市政府工務局公有路燈管理要點，民國 106 年，桃園市政府

[4] 臺中市市區道路行道樹及路燈設計規範，民國 102 年，臺中市政府

[5] 臺南市道路路燈設置及管理要點，民國 101 年，臺南市政府

[6] 彰化縣路燈設置管理辦法，民國 108 年，彰化縣政府

[7] 臺東縣臺東市公有路燈管理辦法，民國 97 年，臺東縣政府

[8] 低功率射頻器材技術規範，民國 109 年，國家通訊傳播委員會

5G 智慧杆系統技術規範

－第 2-1 部：資訊互運性及通訊介面要求

5G Smart pole system technical specification

- Part 2-1: Requirements for information interoperability and communication interfaces

中 華 民 國 111 年 9 月

目錄

節次 頁次

前言 3

0. 簡介 4

1. 適用範圍 4

2. 引用標準 4

3. 用語及定義 5

4. 縮寫 9

5. 概述 10

5.1 智慧杆系統架構 10

5.2 互運性要求 11

6. 存取介面互運性 11

6.1 概述 11

6.2 資料傳輸共同要求事項 12

6.3 通訊協定共同要求事項 12

7. 網路設備 14

7.1 概述 14

7.2 區域網路介面要求事項 14

7.3 網際網路通訊介面要求事項 14

7.4 網路設備功能要求事項 14

8. 代理伺服器 15

8.1 概述 15

8.2 通訊介面要求事項 15

8.3 功能要求事項 16

8.4 引導登錄存取介面要求事項 17

9. 物聯網設備 18

9.1 概述 18

9.2 通訊介面要求事項 19

9.3 物聯網設備功能要求事項 20

9.4 引導登錄存取介面要求事項 22

9.5 設備登錄存取介面要求事項 23

9.6 狀態回報存取介面要求事項 24

10. 組態伺服器 24

10.1 概述 24

10.2 組態伺服器功能要求事項 24

10.3 設備登錄存取介面要求事項 25

10.4 設備授權存取介面要求事項 26

10.5 狀態回報存取介面要求事項 27

11. 應用伺服器 28
11.1 概述 28
11.2 設備授權存取介面要求事項 28
11.3 共同資料存取介面要求事項 29
附錄 A （規定）物聯網設備登錄及狀態回報 32
附錄 B （規定）設備授權申請及確認 35
附錄 C （規定）共同資料存取介面補充資料 38
附錄 D （參考）參數對照表及其他常用資料列表 39
參考資料 44

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole)現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT)設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統。

本規範規定 5G 智慧杆系統中，不同設備間之通訊介面實體層規格、資料鏈路層至應用層通訊協定，以及軟體執行流程。本規範涵蓋物聯網應用相關設備之功能及規格，包含物聯網設備、網路通訊設備及伺服器。

備考： 本規範未包含依法規或其他規範建置之系統(例：交通號誌、公眾無線網路及 5G 行動通訊網路子系統等，參照 D.1)。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 7648	資料元件及交換格式－資訊交換－日期及時間表示法
CNS 14649	資訊技術－廣用多八位元組編碼字元集(UCS)
ITU-T X.509:2019	Public-key and attribute certificate frameworks (ISO/IEC 9594-8:2020)
IETF/RFC 768	User Datagram Protocol
IETF/RFC 791	Internet Protocol version 4
IETF/RFC 793	Transmission Control Protocol
IETF/RFC 1035	Domain names - implementation and specification
IETF/RFC 2131	Dynamic Host Configuration Protocol

IETF/RFC 2616	Hypertext Transfer Protocol
IETF/RFC 2818	HTTP over TLS
IETF/RFC 3596	DNS Extensions to Support IP Version 6
IETF/RFC 3986	Uniform Resource Identifier (URI): Generic Syntax
IETF/RFC 4122	Universally Unique Identifier
IETF/RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
IETF/RFC 5905	Network Time Protocol (NTP)
IETF/RFC 6762	Multicast DNS
IETF/RFC 7159	The JavaScript Object Notation (JSON) Data Interchange Format
IETF/RFC 7519	JSON Web Token (JWT)
IETF/RFC 7617	The 'Basic' HTTP Authentication Scheme
IETF/RFC 8200	Internet Protocol, Version 6 (IPv6) Specification
IETF/RFC 8415	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

3. 用語及定義

本規範適用〝5G 智慧杆系統技術規範－第 1 部：一般要求〞之用語及定義，以及下列用語及定義適用於本規範。

3.1 8P8C (8 position 8 contact)

連接導電纜線乙太網路時通用之連接端子型式，包含 8 組凹槽及 8 組導電接點。

備考： 此一型式接頭俗稱〝RJ45〞。

3.2 代理伺服器(agent server)

安裝於迴路控制箱內，負責管理智慧杆迴路內所有物聯網設備網路組態之伺服器主機，其通訊介面及功能要求參照第 8 節。

3.3 應用伺服器(application server)

智慧杆管理系統伺服器之一，提供應用服務平臺之主要功能(參照本系列規範第 1 部第 5 節)，負責營運各項應用服務、進行物聯網設備鑑別及授權，以及透過共同資料存取介面提供應用服務相關資訊，供管理機關(構)或其他資料共享平臺(例：民生公共物聯網)使用。其通訊介面及功能要求參照第 11 節。

3.4 引導登錄(bootstraping)

物聯網設備使用特定通訊協定及通訊方法，以自動化方式取得互運性存取介面之網路組態相關資訊，不需人工介入或預先設定。

3.5 憑證(certificate)

表示使用者身分之資訊，通常使用密碼學演算法計算產生，以避免偽造。憑證具有多種型式，目前用於一般網際網路加密傳輸協定(例：TLS)之憑證皆依 ITU-X.509:2019 標準，憑證內包含識別符、公開金鑰及數位簽章。用於其他不同場合之憑證可為任何型式(例：自定格式之符記)。

3.6 組態伺服器(configuration server)

智慧杆管理系統伺服器之一，提供營運管理平臺之主要功能(參照〝5G 智慧杆系統技術規範－第 1 部：一般要求〞第 5 節)，負責管理安裝於各智慧杆迴路上之物聯網設備，包含物聯網設備鑑別、登錄、運作狀態監控等功能。其通訊介面及功能要求參照第 10 節。

3.7 閘道控制器(control gateway)

構成物聯網設備之硬體元件，於物聯網設備中負責控制周邊裝置，並執行本規範規定之系統功

能。閘道控制器可同時控制多種周邊裝置(例：感測器、繼電器等)，以提供不同應用服務。

3.8 域名(domain name)

網路上用於辨識單一主機或主機群組之識別符，由文字、數字、符號構成，並以字符〝.〞分隔階層。於一般英文橫式表示式中，位於最右側(字串末端)之階層為頂級域(例：〝.tw〞)，頂級域左側之階層為二級域(例：〝.com〞)，依此類推。

3.9 域名系統(domain name system, DNS)

於資訊網路上提供域名登錄、查詢、轉換為 IP 位址之分散式資料庫系統，通訊協定及資料格式依 IETF/RFC 1035 及 IETF/RFC 3596 規定。

3.10 域名伺服器(domain name server)

於資訊網路上提供域名查詢服務之伺服器主機。個別主機僅包含特定域名階層資訊，進行域名查詢時，查詢者需依域名層級分別至不同域名伺服器進行查詢，以取得次階層域名之相關資訊。

3.11 動態主機組態協定(dynamic host configuration protocol, DHCP)

於一區域網路中自動配發 IP 位址及各項連線參數至主機之通訊協定。於區域網路中設置一伺服器負責探詢新加入該網路之主機，並將相關設定資訊配發予該主機。DHCP 依網路介面使用 IPv4 或 IPv6 分為不同版本，IPv4 版本依 IETF/RFC 2123 規定，簡稱〝DHCPv4〞。IPv6 版本依 IETF/RFC 8415 規定，簡稱〝DHCPv6〞。

3.12 乙太網路(Ethernet)

一種透過導電纜線傳遞電氣信號，或透過光纖纜線傳遞光學信號，藉以進行設備間互相通訊之傳輸技術。乙太網路技術標準由 IEEE 組織 802.3 工作小組制定，其下依傳輸介質及傳輸速率差異分為許多不同版本。

3.13 防火牆(firewall)

在 2 個互連網路間進行網路封包轉發、過濾及阻擋等存取控制之網路設備。於一般網路規劃中，防火牆可用於劃分資訊安全區域之邊界，並設定網路封包來源、目的地、通訊埠等規則，以判斷是否允許資料通訊。防火牆通常為一專屬網路設備，或作為其他網路設備之附屬功能，例：使用內含上述功能之路由器，或由一般通用型伺服器安裝應用程式等方式實作。

3.14 完整域名(full qualified domain name, FQDN)

足以代表單一主機之域名，應完整包含上層域名、專屬域名及主機名等階層。通常專屬域名應由公開網域管理機構登錄為三級域名，上層域名應包含頂級域名及二級域名。

備考 1. 於極少數使用例中，專屬域名可登錄為二級域名或頂級域名。

備考 2. 主機名由依實作而定，實作亦可依實際需求再細分為更多階層。

3.15 超文字傳輸安全協定(hypertext transfer protocol secure, HTTPS)

符合 IETF/RFC 2818 規定之網際網路傳輸協定，為存取網際網路資源之常用方式。連線客戶端指定資源位置(亦即請求標的之 URI)及存取方法，連線主機端則負責對指定資源進行讀取、寫入、變更、刪除等處理，並將結果回傳至連線端。連線方式多為暫時無狀態連線，於執行結束後即中斷連線。該傳輸協定使用傳送層安全(TLS)協定進行加密處理，以保障資料傳輸過程不會遭竊聽、劫持、竄改等資安攻擊。傳送層安全協定亦可確保連線客戶端/伺服器端之身分，以避免偽裝、域名挾持等資安攻擊。

3.16 入向/出向(inbound/outbound)

於網路通訊中，入向代表遠端主機發送封包至防火牆防護範圍內部主機。出向代表防火牆防護範圍內部主機發送封包至遠端主機。

3.17 物聯網(Internet of things, IoT)

一種將資訊設備相互關聯的網路系統。設備間可透過網路通訊以交換各種資料，並執行各種自動化作業，不需人工介入。

3.18 物聯網設備(IoT equipment)

具有網際網路通訊介面，提供各種物聯網應用服務之設備。通常安裝於智慧杆迴路。物聯網設備之型式、外觀及功能皆依實際需求而定(例：環境感測器、智慧看板及邊緣運算裝置等)。

備考： 實作可依物聯網設備特性，將設備安裝於迴路控制箱內、智慧杆杆體/箱體內或智慧杆外部。物聯網設備之通訊介面及要求參照第 9 節。

3.19 網際網路協定(Internet protocol, IP)

於資訊網路中傳送及接收資料之通訊協定。通訊時，於數位資料區段前後添加來源主機、目的地主機等額外資訊，成為封包(packet)，並將封包透過網路發送至指定目的地主機。網際網路協定可分為第 4 版(IETF/RFC 791，簡稱〝IPv4〞)及第 6 版(IETF/RFC 8200，簡稱〝IPv6〞)。IPv6 與 IPv4 彼此不互通，資訊設備通訊介面通常支援其中一種，部分具較高運算能力之設備可同時支援 IPv6 及 IPv4 雙介面並存，稱為〝雙重堆疊〞(dual stack)架構。

3.20 網際網路位址(Internet protocol address)

於資訊網路中辨識單一主機之識別符，格式及編碼方式依網際網路協定規定。網際網路協定第 4 版(IPv4)及第 6 版(IPv6)位址編碼長度不同。

3.21 網際網路協定套組(Internet protocol suite)

泛用於一般資訊網路通訊之基礎通訊架構。該架構將通訊系統劃分為數個抽象階層。依一般網路工程慣例：乙太網路屬第 1 及第 2 層，網際網路協定屬第 3 層，傳輸控制協定屬第 4 層。

3.22 IPv6 路由器告示(IPv6 router advertisement, IPv6 RA)

於使用 IPv6 之區域網路中，路由器定期發送廣播封包，將路由路徑位置告知網路中所有主機。

3.23 JSON(JavaScript object notation)

一種結構化資料表示方式，使用純文字描述具有巢狀層級之資料，其文法結構源自 JavaScript 程式語言。詳細格式參照 IETF/RFC 7159 規定。

3.24 JSON 網頁符記(JSON web token, JWT)

一種用於鑑別網路連線客戶端並記錄授權相關資訊之資料格式，包含客戶端識別符、授權者、授權期限及密碼學數位簽章等資訊。詳細格式參照 IETF/RFC 7519 規定。

3.25 區域網路(local area network)

於侷限範圍內以實體纜線或無線方式連接多組設備，使設備與設備間可互相通訊之網路連接方式。區域網路可藉由第 3 層網路交換器(或路由器)設備與其他網路連接。

於本規範中，區域網路專指於智慧杆迴路內由網路設備、物聯網設備及代理伺服器所構成之網路，設備間連線之介質及連線方式應符合設備之通訊介面要求。

3.26 網路交換器(network switch)

用於網路通訊之硬體設備，可於資訊網路中連結各種不同通訊介質及裝置，負責接收及轉發資

料封包。一般常見之網路交換器依其涵蓋之網際網路協定套組階層，分為第 2 層網路交換器(簡稱〝L2 交換器〞)及具備基礎選徑功能之第 3 層網路交換器(簡稱〝L3 交換器〞)。部分進階式交換器具備網路傳送層以上處理能力，可進行封包過濾及流量控管等網路管理功能。

3.27 網路設備(network equipment)

安裝於智慧杆杆體/箱體及迴路控制箱內，負責連接區域網路及網際網路之設備，包含 L2 交換器、路由器、L3 交換器及防火牆等。網路設備之通訊介面及功能要求參照第 7 節。

3.28 網路周邊裝置(network peripheral device)

具備乙太網路連線能力之周邊裝置，不具備本規範規定之互運性介面存取功能，需透過區域網路連接閘道控制器，方可提供完整應用服務。

3.29 物件實例(object instance)

具有特定格式、特定用途之資料集(dataset)，該資料集由個別設備存放於記憶體或儲存體上，並可透過通訊協定進行讀取或寫入等操作。

3.30 周邊裝置(peripheral device)

安裝於智慧杆迴路，提供物聯網應用必要功能之硬體元件(例：感測器及繼電器等)。此硬體元件不具備乙太網路連線能力，或者不具備本規範規定之互運性介面存取功能，無法進行網際網路通訊，需搭配閘道控制器方可提供完整應用服務。

3.31 通訊埠(port)

電腦通訊網路中傳送層協定之服務端點。通常用數字代號標示，數字範圍為 0～65535。

3.32 接線埠(port)

網路交換器/路由器硬體設備中，用於連接實體網路線之硬體介面。其形狀、格式、信號種類等有多種不同型式(例：同軸電纜埠、光纖埠、雙絞線埠等)。

3.33 遠端使用者撥入鑑別服務(remote authentication dial-in user service, RADIUS)

一種使用者鑑別服務，由一臺伺服器主機集中管理使用者身分及權限。遠端使用者撥入鑑別服務同時亦代表執行上述鑑別之通訊協定；於該協定中，客戶端為提供終端使用者服務之網路設備，該網路設備提供終端使用者各項服務前，可透過 IEEE 802.1X[4]擴展鑑別協定(extensible authentication protocol, EAP)向該伺服器主機鑑別終端使用者身分，藉以決定應提供何種服務。

3.34 路由器(router)

用於網路通訊之硬體設備，負責接收封包，並依其網際網路協定套組第 3 層資訊(亦即 IP 位址)轉發資料封包至對應接線埠。路由器具備較高之運算能力，可由人工輸入或自動探索等方式，計算目的地 IP 位址對應最佳路徑。相較於第 3 層交換器，路由器可支援更多網路管理功能。

3.35 服務探索(service discovery)

為網路設備自動組態技術之一環，網路設備於加入一區域網路後，可不須個別設定便藉由廣播或多播封包，取得網路內各項服務資訊，及個別服務對應之主機 IP 位址等訊息。

3.36 傳輸控制協定(transmission control protcol, TCP)

運作於網際網路之核心協定之一，係一種以連接導向的資料串流傳送層協定。封包格式及通訊方式參照 IETF/RFC 793 規定。

3.37 傳送層安全(transport layer security, TLS)協定

運作於 TCP 之資訊傳輸安全協定。於連線時使用符合 ITU-T X.509:2019 規定之憑證及加密演算

法，鑑別連線標的並協商加密金鑰，再使用加密金鑰對後續資料封包進行加密。TLS 通用版本為 IETF/RFC 5246(version 1.2)或更新版，舊版(SSL、TLS version 1.1 或更早版本)存在安全漏洞，應避免使用。

3.38 UTF-8(8-bit Unicode transformation format)

一種 UCS(Universal Character Set)可變長度字元編碼，每一字符使用 1～4 位元組編碼。此種編碼方式多用於儲存或傳輸具多國語言之文字。

3.39 使用者資料包協定(user datagram protocol, UDP)

運作於網際網路之核心協定之一，係一種以免接式資料封包傳送層協定。封包格式及通訊方式參照 IETF/RFC 768 規定。

3.40 統一資源指示符(uniform resource indicator, URI)

用於標示存取某一特定資源或執行特定操作之網路位置資訊，其格式應符合 IETF/RFC 3986 規定。內容應至少包含通訊協定、完整域名及路徑，可依實際需要包含通訊埠及查詢字串(query string)等資訊。

3.41 通用唯一識別碼(universally unique identifier, UUID)

資訊系統中用於識別之 128 位元代號。編碼方法及表示格式參照 IETF/RFC 4122 規定。

4. 縮寫

DHCP	動態主機組態協定(dynamic host configuration protocol)
DHCPv4	適用於網際網路通訊協定版本 4 的動態主機組態協定(DHCP for IPv4)
DHCPv6	適用於網際網路通訊協定版本 6 的動態主機組態協定(DHCP for IPv6)
DNS	域名系統(domain name system)
EAP	擴展鑑別協定(extensible authentication protocol)
EAPOL	經由區域網路的擴展鑑別協定(extensible authentication protocol over local area network)
FQDN	完整域名(fully qualified domain name)
HMAC	雜湊訊息鑑別碼(hash-based message authentication code)
HTTP	超文字傳輸協定(hypertext transfer protocol)
HTTPS	超文字傳輸安全協定(hypertext transfer protocol secure)
ICMP	網際網路控制訊息協定(Internet control message protocol)
IP	網際網路協定(Internet protocol)
IPv4	網際網路協定版本 4(Internet protocol version 4)
IPv6	網際網路協定版本 6(Internet protocol version 6)
IPsec	網際網路安全協定(Internet protocol security)
JWT	JSON 網頁符記(JSON web token)
NTP	網路時間協定(network time protocol)
mDNS	多播域名系統(multicast DNS)
RADIUS	遠端使用者撥入鑑別服務(remote authentication dial-in user service)
RA	路由器告示(router advertisement)
SHA	安全雜湊演算法(Secure Hash Algorithm)
TCP	傳輸控制協定(transmission control protocol)

TLS　　傳送層安全(transport layer security)協定

UDP　　使用者資料包協定(user datagram protocol)

URI　　統一資源指示符(uniform resource indicator)

UUID　　通用唯一識別碼(universally unique identifier)

5. 概述

5.1 智慧杆系統架構

智慧杆系統(參照〝5G 智慧杆系統技術規範－第 1 部：一般要求〞)由智慧杆管理系統及一個或多個智慧杆迴路構成。智慧杆迴路由 1 具迴路控制箱及 1 支以上智慧杆組成，並經由網路連接至智慧杆管理系統。智慧杆管理系統依功能及特性，分為營運管理平臺及應用服務平臺。

智慧杆系統可提供多種不同功能，其中物聯網相關應用之系統架構如圖 1 所示。

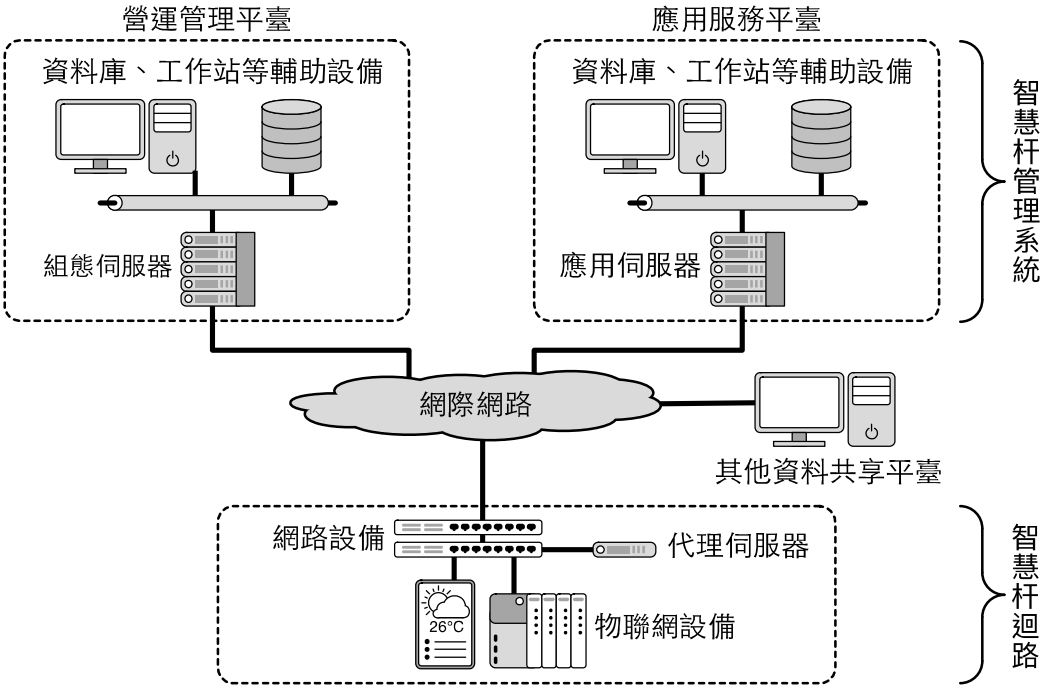


圖 1　智慧杆系統中物聯網相關應用之系統架構

智慧杆與迴路控制箱間以實體纜線及/或無線鏈路連接，形成區域網路。物聯網設備(參照第 9 節)及負責管理區域網路組態之〝代理伺服器〞(參照第 8 節)透過實體纜線連接至網路設備(參照第 7 節)，再由網路設備連接至網際網路。

營運管理平臺包含負責管理物聯網設備之〝組態伺服器〞(參照第 10 節)，以及資料庫、工作站等輔助設備。組態伺服器直接連接至網際網路，以接收物聯網設備連線。

應用服務平臺包含負責執行設備授權及共同資料存取介面等功能之〝應用伺服器〞(參照第 11 節)，以及資料庫、工作站等輔助設備。應用伺服器透過網際網路接收物聯網設備連線。

備考 1.　本規範涵蓋安裝於智慧杆迴路，提供物聯網相關應用服務之設備。此類設備之應用服務功能、型式、硬體元件組成及安裝位置等，皆依實際需求而定，包含：安裝於迴路控制箱內、智慧杆箱體內及附掛於智慧杆杆體。本規範通稱此類設備為〝物聯網設備〞。

備考 2.　於智慧杆系統中，智慧杆迴路、營運管理平臺及應用服務平臺之數量及構成方式皆依實際需求而定。智慧杆系統之設計宜具備擴充性，例：智慧杆迴路可依其所在位置分

配至不同營運管理平臺、應用服務可依其性質建構不同應用服務平臺，以及後續可建置新應用服務平臺以擴充不同應用服務等。

5.2 互運性要求

本規範涵蓋智慧杆系統中各子系統間透過網際網路協定(IP)進行通訊之功能性要求，包含：通訊介面規格、通訊協定種類、資料格式及資料交換方式等。物聯網設備、網路設備、代理伺服器、組態伺服器及應用伺服器應依本規範規定實作，以確保各子系統符合互運性之要求，包含：

(a) 物聯網設備可接入智慧杆迴路區域網路並取得網路存取權限。所有過程以自動化方式執行，不需預先設定網路組態(例：設備 IP 位址及組態伺服器位址等)。

(b) 組態伺服器可取得物聯網設備詮釋資料、進行鑑別、取得網路存取之授權範圍，以及監控物聯網設備運作狀態。所有過程以自動化方式執行為原則。

(c) 組態伺服器及應用伺服器可採分散式設計，並依實際需求擴充，不需由單一中央管理系統容納所有設備及應用服務。

(d) 管理機關(構)及其他資料共享平臺可依需求，取得物聯網設備細部管理資訊及應用服務相關資料。

備考： 本規範未包含網際網路協定以外之通訊方法(例：序列埠、匯流排、低速無線協定、類比訊號等)。使用此類通訊方法設備應搭配轉換器，將設備之存取及操作介面轉換為網際網路協定。轉換裝置型式及轉換方法依實作而定(例：參考 CNS 15652-3[1])。

6. 存取介面互運性

6.1 概述

本規範包含下列互運性存取介面，存取介面之關聯性如圖 2 所示。

(a) 引導登錄存取介面：物聯網設備藉由此介面向代理伺服器取得組態伺服器相關資訊，包含組態伺服器之 URI 及鑑別資訊。此存取介面採單向 HTTPS 協定，物聯網設備應實作客戶端，代理伺服器應實作伺服器端，請求封包內應包含物聯網系統管理機關(構)核發之鑑別資訊。

(b) 設備登錄存取介面：物聯網設備藉由此介面向組態管理伺服器提交設備登錄資訊(例：設備型號、供應者、應用服務描述等)。此存取介面採單向 HTTPS 協定，物聯網設備應實作客戶端，組態伺服器應實作伺服器端，請求封包內應包含代理伺服器提供之鑑別資訊。

(c) 狀態回報存取介面：物聯網設備藉由此介面定時向組態管理伺服器彙報即時運作狀態。此存取介面採單向 HTTPS 協定，物聯網設備應實作客戶端，組態伺服器應實作伺服器端，請求封包內應包含代理伺服器提供之鑑別資訊。

(d) 設備授權存取介面：組態伺服器藉由此介面要求應用伺服器提供授權，允許物聯網設備使用網際網路。此存取介面採雙向 HTTPS 協定，組態伺服器及應用伺服器應實作伺服器端及客戶端。進行設備授權時，應由組態伺服器向應用伺服器提出設備授權申請，請求封包內應包含物聯網設備提供之鑑別資訊。應用伺服器端應於接收申請後進行評估，並發送設備授權確認至組態伺服器，封包內應包含組態伺服器設備提供之鑑別資訊

(e) 共同資料存取介面：應用伺服器藉由此介面向管理機關(構)、對此介面具有存取權限之外部使用者或其他資料共享平臺(例：民生公共物聯網)提供各項應用服務資料。此存取介面採 HTTPS 協定，應用伺服器應實作伺服器端，應由管理機關(構)、外部使用者或其他資料

共享平臺主動向應用伺服器發起連線。鑑別方式及權限控管依實作而定。

(f) 應用服務專屬存取介面：應使用網際網路通訊之常用技術進行資料交換，包含 TCP、UDP、IPsec 及 ICMP 等。本規範未規定其連線標的、連線方法、資料交換方法、連線方向及鑑別方法等。

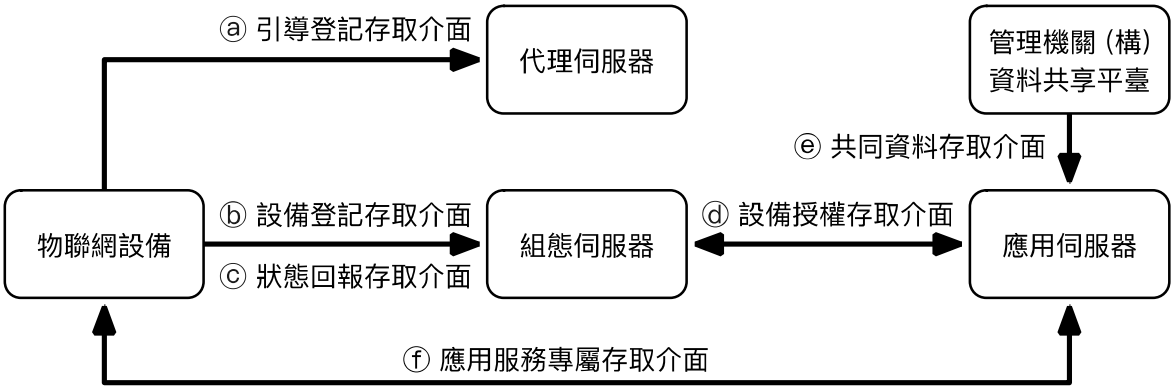


圖 2　互運性存取介面關聯性示意圖(箭頭代表連線方向)

6.2 資料傳輸共同要求事項

6.2.1 資料格式

經互運性存取介面傳輸之資料，除另有規定外，應使用符合 IETF/RFC 7159 規定之 JSON 格式。

6.2.2 文字編碼格式

所有字元應符合 CNS 14649 之字元集，並採用 UTF-8 編碼。

6.2.3 統一資源指示符

URI 編碼格式應符合 IETF/RFC 3986 規定，可包含通訊埠號。保留字元應使用百分號編碼(percentage encoding)，非保留字元(含中文)應直接使用 UTF-8 編碼。

6.2.4 通用唯一識別碼

UUID 之表示方式應符合 IETF/RFC 4122 規定，採 8-4-4-4-12 排列方式，數字應使用十六進制表示，英文字符(a～f)應小寫。

6.2.5 數字

應使用十進制表示(包含整數及浮點數)，不使用科學記數法及千位分隔符，不前置補 0。

6.2.6 日期

應使用符合 CNS 7648 規定之編碼格式，應包含時區，精確度應包含至秒。

6.2.7 地理座標

應符合世界大地測量系統(World Geodetic System) WGS84[14]規定，標記格式為十進制浮點數，單位為〝度〞，精確應達小數後 5 位。

6.3 通訊協定共同要求事項

6.3.1 HTTPS 伺服器端

(a) HTTPS 伺服器端應使用符合 IETF/RFC 5246 規定之 TLS 1.2 或更新版本進行傳輸加密。若客戶端使用未加密連線時，則應禁止存取。

(b) 應使用憑證機構(certificate authority, CA)核發，且未超出期限之有效憑證，存取介面 URI 之域名應能符合憑證登錄項目。

(c) 應對所有連線進行鑑別，未通過鑑別之連線應禁止存取。鑑別方法依後續各節規定。

(d) 通訊協定版本應使用符合 IETF/RFC 2616 規定之 HTTP/1.1 或更新版本，若客戶端使用舊版本連線(1.0 或更早版本)，則應回應狀態碼 426 (〝upgrade required〞)。

(e) 若請求封包標頭內容不符合存取介面 URI 之域名或路徑，則應回應狀態碼 404 (〝not found〞)。

(f) 其他未指定之錯誤依一般預設方式處理(例：503〝service unavailable〞)。

備考： HTTPS 客戶端宜具備惡意攻擊偵測能力。若同一 HTTPS 客戶端連續發生相同錯誤，宜限制該客戶端之後續連線。

6.3.2 HTTPS 客戶端：發送請求

(a) HTTPS 客戶端應使用符合 IETF/RFC 5246 規定之 TLS 1.2 或更新版本進行傳輸加密。

(b) 所有連線應包含鑑別資訊，鑑別資訊之格式、內容及鑑別方法，依後續各節規定。

(c) 通訊協定版本應使用 IETF/RFC 2616 規定之 HTTP/1.1 或更新版本，〝Host〞標頭欄位應包含連線標的 URI 之域名。

(d) 連線應為非持續性，〝Connection〞標頭欄位內容應為〝close〞。

(e) 若請求方法為〝POST〞，則請求封包應包含請求本體(body)，內容格式及編碼方式應符合 6.2 規定。封包內應包含〝Content-Type〞標頭欄位，內容應為〝application/json; charset=utf-8〞，並使用〝Content-Length〞標頭欄位以標記資料長度。

6.3.3 HTTPS 客戶端：異常及回應處理

(a) HTTPS 客戶端於發送請求封包後，應等候伺服器端回應。若連線逾時、伺服器端逾時未回應或回應不完整，則應重新發送請求封包至相同 URI。逾時時間依實作而定。

(b) 若回應狀態碼為 429 (〝too many requests〞)、500 (〝internal server error〞)、502 (〝bad gateway〞)、503 (〝service unavailable〞)或 504 (〝gateway timeout〞)，則應重新發送請求封包至相同 URI。

(c) 若回應狀態碼為 307 (〝temporary redirect〞)，則應重新發送請求封包至〝Location〞標頭欄位內容指示之 URI。

(d) 其他回應狀態碼之處理方式依後續各節規定，未指定處理方式之狀態碼應視為異常。發生異常時，應停止重新發送請求，後續處理方式依各依後續各節規定。

(e) 重新發送 HTTPS 請求時，應先等候一段時間，再發送包含相同內容之請求封包。若回應封包內包含〝Retry-After〞標頭欄位，則等候時間應符合〝Retry-After〞標頭欄位內容指示。若未收到回應封包或回應封包內未設定〝Retry-After〞標頭欄位，則可由實作自定等候時間，不宜低於 5 秒。

(f) 重新發送 HTTPS 請求時，若連續發生相同錯誤達一定次數時，則應視為異常。重試次數上限可由實作自定。

備考 1. 除另有規定外，HTTPS 客戶端不處理回應狀態碼 300 至 305 及 308 之重新導向指示。

備考 2. 發生異常時，實作宜能顯示或記錄該次異常，以利後續除錯作業。

7. 網路設備

7.1 概述

智慧杆迴路應設置防火牆、路由器及 L2 交換器等硬體設備。硬體設備之數量、型式、及安裝位置等細部設計，皆依實作而定。可使用具有多重功能之整合式硬體設備(例：包含防火牆功能之路由器)或由多組硬體設備組成。

網路設備應能以堆疊或鏈路等方式進行擴充。擴充網路設備時，其拓樸型式、纜線規格及傳輸信號型式等，皆依實作而定(例：實體纜線、無線鏈路或混合多種通訊方式)。

備考： 區域網路規模較大時，可將區域網路劃分成為多個子網域，並於子網域與子網域間設置 L3 交換器進行封包轉發，以簡化管理。

7.2 區域網路介面要求事項

網路設備應提供乙太網路介面，供物聯網設備接取區域網路，介面數量依實作而定。乙太網路介面可使用電氣信號或光學信號，規定如下：

(a) 電氣信號：應符合或相容於 100BASE-TX (IEEE 802.3u-1995[6])或 1000BASE-T (IEEE 802.3ab-1999[5])規範，可支援更高傳輸速率，連接埠型式應為 8P8C。

(b) 光學信號：應符合或相容於 100BASE-FX (IEEE 802.3u-1995[6])或 1000BASE-SX (IEEE 802.3z-1998[7])規範，可支援更高傳輸速率，連接埠型式依實作而定。

7.3 網際網路通訊介面要求事項

網路設備應具備至少 1 組可介接網際網路之通訊介面。該介面之型式、介質種類及網路拓樸結構不規定，實作可使用實體纜線、無線資料鏈路或混合使用多種通訊介質。

7.4 網路設備功能要求事項

7.4.1 接線埠存取控制

L2 交換器應支援 IEEE 802.1X-2004[4]擴展鑑別協定，並能對個別接線埠獨立設定存取控制。

L2 交換器應扮演擴展鑑別協定鑑別者(authenticator)之角色，組態伺服器應扮演鑑別伺服器之角色。物聯網設備及周邊裝置接入 L2 交換器時，應扮演擴展鑑別協定申請者(supplicant)之角色。802.1X[4]角色關係如圖 3 所示。

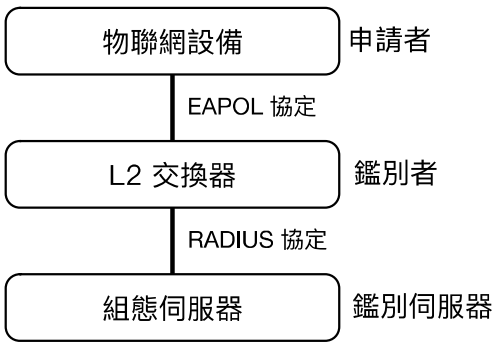


圖 3　802.1X 角色關係示意圖

物聯網設備及周邊裝置接入 L2 交換器時，L2 交換器及鑑別伺服器應對其執行鑑別。鑑別未通過時，應限制該接線埠之通訊能力。乙太網路連接中斷時，L2 交換器應重設該接線埠狀態。

L2 交換器或 RADIUS 伺服器宜設定閒置計時器(idle timer)，逾時時間依實作而定，不宜少於 24 小時。

RADIUS 伺服器不可設置於智慧杆迴路(包含迴路控制箱及智慧杆杆體/箱體內)，若網路設備內建本地端 RADIUS 伺服器功能，則應關閉該項功能。

備考 1. 網路設備間透過鏈路串接時，802.1X[4]存取控制組態應設定於個別 L2 交換器之一般接線埠，並非設定於鏈路埠。實作可使用其他技術(例：IEEE 802.1AE-2018[2])以強化 L2 交換器間資訊安全。

備考 2. 除物聯網設備及周邊裝置外之其他資訊設備(例：代理伺服器)連接至 L2 交換器時，其存取控制方式依實作而定(例：使用硬體位址作為存取控制)。

7.4.2 封包轉發

網路設備應能支援 IPv6 及 IPv4 封包於區域網路與網際網路間轉發，可選項的支援 IPv4 網路位址轉譯(network address translation, NAT)及 IPv4 通訊埠轉發(port forwarding)等功能。

7.4.3 預設選徑

網路設備應提供 IPv6 路由器告示(IPv6 RA)功能，並正確設定預設選徑資訊。

7.4.4 防火牆

網路設備應於區域網路介接網際網路介面處設定防火牆(firewall)，防火牆應能支援白名單功能。白名單功能宜預設為啟用，僅限白名單包含之標的、來源或通訊方法可允許通訊。組態伺服器及其他常用服務宜列入預設白名單(例：參照 D.2)。除上述規定外，實作得依實際需求或智慧杆系統管理機關(構)規定，自行設定其他預設規則。

備考： 防火牆預設規則依實作而定，部分重要服務之網域，諸如代理伺服器中 HTTPS 伺服器安裝 X.509 憑證之憑證撤銷清單(certificate revocation list)、線上憑證狀態協定(online certificate status protocol)等，宜加入預設規則。

7.4.5 虛擬區域網路

網路設備可選項的支援虛擬區域網路(virtual local area network, VLAN)功能，以簡化管理及強化智慧杆迴路之資訊安全防護。若網路設備支援虛擬區域網路功能，則應符合 IEEE 802.1Q-2014[3]規定。

8. 代理伺服器

8.1 概述

代理伺服器為直接連接至智慧杆迴路區域網路之伺服器主機，負責管理迴路內所有智慧杆系統物聯網設備之網路連線組態設定，包含網路位址配發、服務探索、網路校時、啟動引導登錄(bootstrapping)及其他實作自訂之管理功能。代理伺服器之硬體設備數量、型式及實際建置位置等，皆依實作而定，可使用單一獨立設備或由多組硬體設備組成。

8.2 通訊介面要求事項

8.2.1 硬體規格

代理伺服器應提供至少 1 組乙太網路介面，可使用電氣或光學信號，規定如下：

(a) 電氣信號：應符合或相容於 100BASE-TX (IEEE 802.3u-1995[6])或 1000BASE-T (IEEE 802.3ab-1999[5])規範，可支援更高傳輸速率，連接埠型式應為 8P8C。

(b) 光學信號：應符合或相容於 100BASE-FX (IEEE 802.3u-1995[6])或 1000BASE-SX (IEEE 802.3z-1998[7])規範，可支援更高傳輸速率，連接埠型式依實作而定。

8.2.2 網路層

代理伺服器應支援 IPv6 及 IPv4 雙重堆疊架構，並依智慧杆迴路設計選擇使用 IPv6 或 IPv4。代理伺服器之 IP 位址、存取控制及其他網路組態等，皆依實作而定。

8.3 功能要求事項

8.3.1 必備服務

代理伺服器應能支援以下通訊協定及服務：

(a) 動態主機組態協定(DHCP)服務。

(b) 域名查詢服務(DNS)。

(c) 多播域名服務(mDNS)。

(d) 網路校時協定服務(NTP)。

(e) 引導登錄服務(bootstrapping)。

各項服務之實作方式，包含作業系統版本、軟體框架、服務實例(instance)數量、組態及對應之網路通訊介面等，皆依實作而定。

8.3.2 校時服務

代理伺服器應提供符合 IETF/RFC 5905 規定之網路校時協定伺服器。代理伺服器本身應使用公開校時伺服器(例：參照 D.4)進行同步校時。

8.3.3 自動組態設定

代理伺服器應提供符合 IETF/RFC 8415 規定之 DHCPv6 伺服器，以及符合 IETF/RFC 2131 規定之 DHCPv4 伺服器，並依智慧杆迴路設計選擇使用 DHCPv6 或 DHCPv4，IP 位址配發規則依實作而定。

DHCP 租約期限宜設定為 24 小時以上。實作應確保 IP 位置配發具一致性(例：預先設定保留位址或將動態租約轉為保留位址)，應能避免因突發故障(例：電源中斷、替換記憶儲存元件等)導致同一設備取得不同 IP 位址。

自動配發 IP 位址時應指定搜尋域名(search domain)及域名伺服器，可選項的指定網路校時協定伺服器。搜尋域名應使用經註冊且有效之公開域名，並能符合引導登錄存取介面之 URI。域名伺服器應使用代理伺服器之 IP 位址。

備考：DHCPv6 設定搜尋域名及域名伺服器之相關參數可參照 IETF/RFC 3646[9]。

8.3.4 域名伺服器

代理伺服器應提供域名查詢服務，應依智慧杆迴路設計，使用符合 IETF/RFC 1035 (IPv4)或 IETF/RFC 3596 (IPv6)規定之介面。實作可使用域遞迴解析(recursive resolving)或轉送器(forwarder)以提供本項服務，使用轉送器時，上層域名伺服器依實作而定。

域名伺服器應能解析 mDNS 查詢結果(參照 8.3.5)，並依智慧杆迴路設計，提供 IPv6 或 IPv4 對應位址。

8.3.5 服務探索

代理伺服器應提供符合 IETF/RFC 6762 規定之域名多播域名服務(mDNS)功能，所有發布項目皆應預先設定。代理伺服器應發布之必要服務項目包含：

(a) _ntp._udp

(b) _bootstrap._sub._http._tcp

各項目應至少包含 1 組紀錄，可依實際需求登錄多組紀錄(例：作為備援)。登錄多組紀錄時，應指定不同實例(instance)名稱，實例名稱依實作而定，應由英文字符、數字及底線構成，不宜使用空白字符或其他符號。

所有紀錄之域名皆應符合 DHCP 指定之搜尋域名(search domain，參照 8.3.3)，詮釋資料(〝TXT〞紀錄)部分依實作而定(例：參照 D.3)。

除上述必要項目外，實作可依實際需求設計其他不同型式之服務。

備考：實作時應注意，域名不分英文大小寫，但 URI 之路徑(path)區分英文大小寫。

8.4 引導登錄存取介面要求事項

8.4.1 存取介面

代理伺服器之引導登錄存取介面應提供 HTTPS 伺服器功能，相關規定參照 6.3.1。

引導登錄存取介面之 URI 應為固定值，並包含完整域名(FQDN)。其完整域名應符合 mDNS 查詢結果(參照 8.3.5)。URI 之路徑應符合查詢結果〝TXT〞紀錄之〝PATH〞參數(參照 D.3)，未設定〝PATH〞參數時，路徑應為根目錄〝/〞。代理伺服器於設定後需變更 URI 時，應更新 mDNS 紀錄，不可使用重新導向。

代理伺服器可選項的提供多組存取介面作為備援，提供多組存取介面時，個別存取介面應對應至 1 組 mDNS 紀錄，其 URI 之域名及路徑皆應符合本節規定。

備考：實作可使用通配憑證(wildcard certificate)以簡化管理，不宜重複使用相同主機名。

8.4.2 代理伺服器識別符

代理伺服器應具備識別符，於同一智慧杆系統內不可重複使用。代理伺服器識別符將用於識別智慧杆迴路及計算鑑別資訊(參照 A.2)，其格式、編碼、申請及配發方式應依智慧杆系統管理機關(構)規定。管理機關(構)未規定時，應使用 UUID。

8.4.3 接收引導登錄請求

引導登錄存取介面接收 HTTPS 請求時，應依 6.3.1 及以下規定處理：

(a) 若請求方法不為〝GET〞，則應回應狀態碼 405 (〝method not allowed〞)。

(b) 查詢字串應包含參數〝id〞，則該參數應包含物聯網設備識別符。若查詢字串未包含該參數或參數內容為空字串，則應回應狀態碼 400 (〝bad request〞)。

(c) 應包含 HTTP 基本鑑別(〝Basic〞 authentication)，格式應符合 IETF/RFC 7617 規定。若未包含鑑別資訊、格式不符合規定或鑑別未通過時，則應回應狀態碼 401 (〝unauthorized〞)。

(d) 若代理伺服器因內部問題而無法處理請求時，則應回應狀態碼 500 (〝internal server error〞)或 503 (〝server unavailable〞)。

(e) 若未發生上述錯誤時，則應發送引導登錄回應至物聯網設備。狀態碼應為 200 (〝OK〞)，回應主體應為 JSON 物件，內容格式應參照 A.1，編碼格式應依 6.2 規定。

備考 1. 引導登錄回應主體 JSON 物件中〝credCfg〞鑑別資訊之計算方式依實作而定，可於代理伺服器預先配置雜湊金鑰，並由代理伺服器於本機端計算，或者透過網際網路由其他遠端伺服器取得。

備考 2. 客戶端鑑別資訊之申請、管理及鑑別方式依實作而定(例：目錄服務、資料庫等)。進行鑑別時，宜同時檢查鑑別資訊與物聯網設備識別符之關聯性。

9. 物聯網設備

9.1 概述

9.1.1 物聯網設備

物聯網設備為具備乙太網路介面、支援網際網路協定且具備本規範規定功能之硬體設備。其網路通訊介面、網際網路協定堆疊(Internet protocol stack)，以及提供應用服務之軟體程式及周邊裝置(例：內建感測器、外接周邊裝置等)共同視為單一物聯網設備，如圖 4 所示。

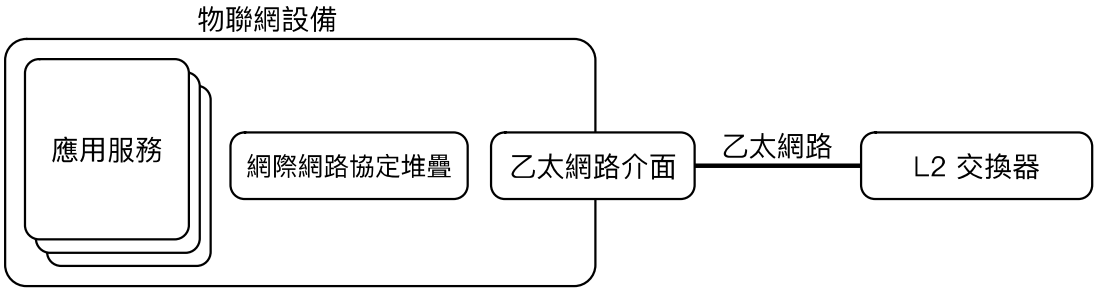


圖 4　物聯網設備示意圖

若硬體設備不具備乙太網路連線功能(例：IEC 62386[8]可控式照明器具)、不支援網際網路通訊協定或不具備本規範規定之互運性介面存取功能，則應搭配閘道控制器共同使用(參照 9.1.2)。物聯網設備之型式、外觀、硬體元件組成、軟體執行環境及安裝位置等，依實作而定。物聯網設備之其他特性(例：電源供應及環境可靠度等)，應依相關法規及本系列標準其他部規定。

9.1.2 應用服務

物聯網設備應提供 1 或多組應用服務。應用服務應依實際需求設計，可為純軟體程式或軟硬體之組合。應用服務使用之軟體程式及周邊裝置視為物聯網設備之一部分。所有應用服務皆應具備識別符，格式及編碼方式依實作而定，但於同一物聯網設備內不可重複使用。

具多組應用服務之物聯網設備實例如圖 5 所示。

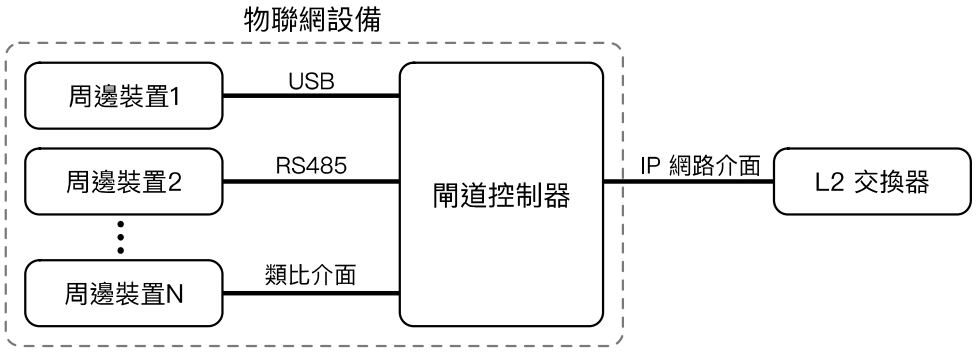


圖 5　具多組應用服務之物聯網設備實例

具多組應用服務之物聯網設備可由 1 具閘道控制器及 1 或多個周邊裝置組成。閘道控制器及其他周邊裝置可安裝於同一位置，或安裝於不同杆體或箱體內，並透過實作自定之控制介面進行控制。控制介面之型式及規格依實作而定，可使用硬體擴充介面(例：串列埠、類比信號、數位匯流排及無線通訊介面等)或透過智慧杆迴路區域網路建立網路連線。

9.1.3 網路周邊裝置

若硬體設備具備乙太網路介面且支援網際網路協定，但不具備本規範規定之互運性介面存取

功能時，則其網路存取能力時將受防火牆限制。此硬體設備可透過區域網路連接閘道控制器，以提供完整應用服務，如圖 6 實例。

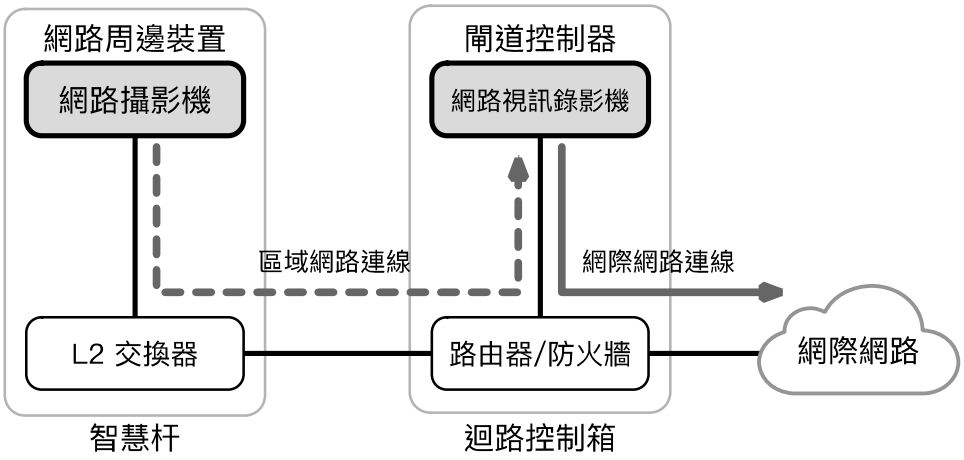


圖 6　網路周邊裝置透過區域網路連接閘道控制器之實例

於此實例中，網路周邊裝置(例：網路攝影機)透過閘道控制器(例：網路視訊錄影機或多功能閘道器等)提供遠端資料存取、遠端管理及維護等功能。

9.2　通訊介面要求事項

9.2.1　硬體規格

物聯網設備及網路周邊裝置應具備 1 組乙太網路介面，可使用電氣或光學信號，規定如下：

(a)　電氣信號：應符合或相容於 100BASE-TX (IEEE 802.3u-1995[6])或 1000BASE-T (IEEE 802.3ab-1999[5])規範，可支援更高傳輸速率，連接埠型式應為 8P8C。

(b)　光學信號：應符合或相容於 100BASE-FX (IEEE 802.3u-1995[6])或 1000BASE-SX (IEEE 802.3z-1998[7])規範，可支援更高傳輸速率，連接埠型式依實作而定。

備考：　若硬體設備包含 2 組以上乙太網路介面，則應使用其中 1 組作為主要介面，其他介面應關閉或設定為備援介面。

9.2.2　資料鏈路層至網路層

物聯網設備及網路周邊裝置應具備以下功能：

(a)　IEEE 802.1X-2004[4]擴展鑑別協定(EAP)之申請者(supplicant)角色。

(b)　支援 IPv6 及 IPv4。

(c)　符合 IETF/RFC 8415 及 IETF/RFC 2131 規定之 DHCPv6 / DHCPv4 客戶端。

9.2.3　網際網路連線

物聯網設備應支援網際網路通訊功能。物聯網設備使用網際網路進行通訊前，應先完成所有組態登錄過程(參照 9.3)，方可進行通訊。

9.2.4　區域網路內連線

物聯網設備與網路周邊裝置可依實際需求，透過區域網路互相連接。物聯網設備與網路周邊裝置間進行配對及服務探索等細部設計，依管理機關(構)相關規定辦理(例：指定 IP 位址、使用廣播或登錄 mDNS 服務紀錄等)。

備考：　區域網路可依實際需求劃分為不同廣播域(broadcast domain)，實作使用自行設計之廣播封包進行服務探索時，應先確認網路交換器之相關設定。

9.3 物聯網設備功能要求事項

9.3.1 啟用網路服務

9.3.1.1 執行步驟

物聯網設備及網路周邊裝置於首次安裝於智慧杆迴路時，應先啟用網路服務，步驟如圖 7 所示。物聯網設備應主動開始執行第 1 階段及第 2 階段之所有步驟，網路周邊裝置(例：圖 6 實例之網路攝影機)應主動執行第 1 階段之步驟。

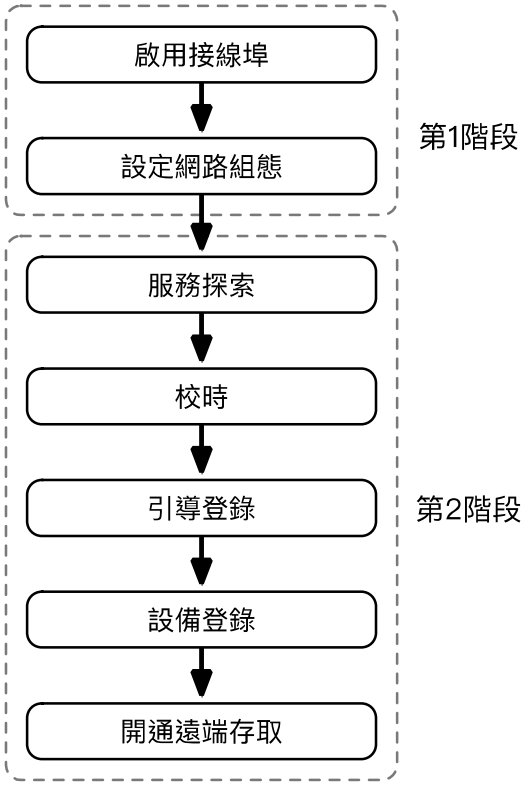


圖 7　啟用網路服務之步驟

備考： 設備登錄及開通遠端存取步驟僅需執行 1 次，其他步驟視實際運作狀況執行(例：連線鑑別資訊過期時應重新執行引導登錄步驟，設備重新啟動時應重新執行第 1 階段步驟等，依此類推)。

9.3.1.2 預設定組態

物聯網設備應預先設定以下組態：

(a)　物聯網識別符，於同一智慧杆系統中，識別符不可重複使用。

(b)　802.1X[4]鑑別資訊(參照 9.3.1.3)。

(c)　引導登錄鑑別資訊(參照 9.3.1.7)，應包含帳號及密碼

網路周邊裝置應預先設定 802.1X[4]鑑別資訊。

備考 1. 所有預設定組態之申請、管理及配發方法，應依智慧杆系統管理機關(構)規定。若管理機關(構)未規定識別符之編碼格式，則應使用 UUID。

備考 2. 802.1X[4]鑑別資訊格式應依鑑別方法(參照 D.5)而定。

9.3.1.3 啟用接線埠

物聯網設備及網路周邊裝置應支援至少 1 種常用鑑別方法(參照 D.5)。接入 L2 交換器時，物聯網設備應扮演 802.1X[4]申請者角色，並開始執行鑑別過程(EAPOL-Start)。

若物聯網設備及周邊裝置因故障或閒置逾時等因素，導致接入接線埠狀態被重設時，則應於恢復正常運作後重新執行 802.1X[4]鑑別。

9.3.1.4 設定網路組態

物聯網設備及網路周邊裝置應支援動態網路組態設定(DHCP)及人工設定網路組態。動態網路組態設定之要求包含：

(a) 設定 IP 位址、搜尋域名(search domain)及域名伺服器。

(b) 參照 IPv6 RA 或 DHCPv4 回應設定預設選徑。

(c) 定時更新 DHCP 租約。

物聯網設備應依智慧杆迴路設計，以自動判斷或人工設定方式，選擇使用 DHCPv4 或 DHCPv6 取得網路組態。若物聯網設備及周邊裝置未能設定正確網路組態(例：DHCP 無回應、多重 DHCP 回應或發生 IP 位址衝突)，則應停止運作。

備考： 物聯網設備及網路周邊裝置應優先使用 DHCP，但智慧杆系統管理機關(構)另有規定時，從其規定。

9.3.1.5 服務探索

物聯網設備完成網路組態設定後，應使用符合 IETF/RFC 6762 規定之 mDNS 查詢引導登錄存取介面資訊，其具名服務之服務型式應為：〝_bootstrap._sub._http._tcp〞。

物聯網設備應依查詢結果取得引導登錄存取介面 URI。URI 之域名應符合查詢結果之完整域名(FQDN)紀錄，路徑應符合〝TXT〞紀錄之〝PATH〞參數(參照 D.3)。若查詢結果未包含〝TXT〞紀錄或未設定〝PATH〞參數，則 URI 之路徑應為根目錄。

若 mDNS 回應包含多組不同服務實例(instance)，則物聯網設備應任意選擇 1 組服務實例作為查詢結果。

若物聯網設備未能取得引導登錄存取介面相關資訊，則應重新執行 mDNS 查詢，重新執行 mDNS 查詢之等候時間依實作而定。

9.3.1.6 校時

物聯網設備應使用網路校時服務校正作業系統時間。可選項的使用公開網路校時伺服器(例：參照 D.4)，或使用服務探索查詢代理伺服器提供之網路校時服務 URI。

使用使用服務探索查詢時，應使用符合 IETF/RFC 6762 規定之 mDNS 進行查詢，其具名服務應為：〝_ntp._udp〞。

9.3.1.7 引導登錄

物聯網設備取得引導登錄存取介面 URI 後，應向該存取介面之 URI 要求設備登錄存取介面之相關資訊，執行方式參照 9.4。

9.3.1.8 設備登錄

物聯網設備取得設備登錄存取介面相關資訊後，應向該存取介面之 URI 進行設備登錄。設備登錄執行方式參照 9.5。

9.3.1.9 開通遠端存取

物聯網設備完成設備登錄後，應等候防火牆規則完成設定，方可進行網際網路通訊。實作宜設計等候機制(例：定期探詢網路連線狀況、被動等候入向連線等)。

9.3.2 設備管理及維護

9.3.2.1 定期回報運作狀態

物聯網設備完成 9.3.1.8 設備登錄步驟後，無論防火牆規則是否已設定完成，皆應依固定週期，或者於異常狀況發生時，向組態伺服器回報目前運作狀態，執行方式參照 9.6。

狀態回報之週期應不大於設備登錄請求之〝heartbeat〞參數(參照 A.3)。該參數值應依應用服務特性或管理機關(構)要求設定。若因設備故障、網路中斷或其他因素影響，無法於指定時間內回報，則應於故障排除後重新恢復狀態回報。

狀態回報應包含個別應用服務之運作狀態診斷。物聯網設備包含多應用服務時，應包含閘道控制器本身，以及所有應用服務軟硬體元件(包含周邊裝置)之診斷結果。物聯網設備(或個別應用服務)不具備診斷之能力時，仍應定期回報，但自我診斷結果應為〝未知〞(參照 A.6)。

9.3.2.2 設備移除及刪除登錄

物聯網設備因硬體故障或其他因素需要移除時，應由智慧杆系統管理機關(構)負責執行。物聯網設備不可以任何方式主動要求刪除登錄。

物聯網設備因硬體故障而需替換閘道控制器時，原物聯網設備登錄資訊應刪除。新替換之設備應視為新增物聯網設備，並重新執行啟用網路服務之所有步驟。

9.4 引導登錄存取介面要求事項

9.4.1 發送引導登錄請求

執行引導登錄步驟時，物聯網設備應向引導登錄存取介面發送 HTTPS 請求。發送請求時，應依 6.3.2 及以下規定執行：

(a) 請求方法應為〝GET〞。

(b) URI 應符合服務探索結果(參照 9.3.1.5)。

(c) 查詢字串應包含參數〝id〞，內容應為物聯網設備識別符。

(d) 應包含 HTTP 基本鑑別(〝Basic〞 authentication)，格式應符合 IETF/RFC 7617 規定。鑑別資訊應由管理機關(構)核發。

備考：鑑別資訊之申請、管理及核發方式依實作而定。

9.4.2 接收引導登錄回應

物聯網設備接收 HTTPS 回應時，應依 6.3.3 及以下規定執行：

(a) 若回應狀態碼為 200 (〝OK〞)，則應檢查回應主體。若回應主體編碼格式符合 6.2 規定且內容符合 A.1 規定，則應視為設備登錄成功。若回應主體之格式或內容不符合上述規定，則應視為異常。

(b) 除回應狀態碼 200 及 6.3.3 列舉之回應狀態碼外，其他回應狀態碼皆視為異常。

(c) 發生異常時，若服務探索結果包含多組紀錄，則應使用不同紀錄之 URI 重新發送引導登記請求。若服務探詢結果僅包含單一紀錄，或者所有紀錄之 URI 皆發生異常，則應等候一段時間，重新執行服務探索，再重新發送引導登記請求。等候時間依實作而定，宜設定為 5 分鐘以上。

(d) 若重新嘗試次數或經過時間達上限，則應停止運作。重試次數或時間上限依實作而定，宜設定為 24 小時以上。

9.4.3 後續處理

引導登錄執行成功後，物聯網設備應依回應內容(參照 A.1)更新鑑別資訊、設備登錄存取介面 URI 及狀態回報存取介面 URI。

9.5 設備登錄存取介面要求事項

9.5.1 發送設備登錄請求

執行設備登錄步驟時，物聯網設備應向設備登錄存取介面發出 HTTPS 請求。發送請求時，應依 6.3.2 及下列規定執行：

(a) 請求方法應為〝POST〞。

(b) URI 應符合引導登錄回應封包之〝registrator〞參數內容(參照 A.1)。

(c) 請求標頭應包含〝Authorization〞欄位，型式應為〝Bearer〞，鑑別資訊應使用引導登錄回應封包之〝credCfg〞參數內容。

(d) 請求主體應包含 JSON 物件，內容格式參照 A.3，編碼格式應依 6.2 規定。

(e) JSON 物件之〝credAuthReq〞參數內容可依實際需求指定，物聯網設備與應用伺服器應使用相同之資料格式及計算方式。計算時宜使用密碼學演算法，並加入單次隨機數(nonce)，不宜使用固定之鑑別資訊。

備考 1. 實作宜使用〝jti〞參數作為單次隨機數(例：參考 D.6 實例)。組態伺服器發出之設備授權申請資訊將包含該參數(參照 B.1)，實作不需額外設計帶外(out-of-band)資料通道。

備考 2. 〝jti〞參數記錄於引導登錄回應封包之〝credCfg〞參數中，實作可依 IETF/RFC 7519 規定解析〝credCfg〞參數中未加密酬載部分(參照 A.2)，便可取得〝jti〞參數。

9.5.2 接收設備登錄回應

物聯網設備發送 HTTPS 請求後，應接收組態伺服器發出之回應。處理回應時，應依 6.3.3 及下列規定執行：

(a) 若回應狀態碼為 403 (〝forbidden〞)，則應停止運作。

(b) 若回應狀態碼為 201 (〝created〞)，則應視為設備登錄成功。

(c) 除 6.3.3 及以上列舉之回應狀態碼外，其他回應狀態碼皆視為異常。

(d) 發生異常時，應於等候一段時間後，重新進行引導登錄步驟(參照 9.4)。等候時間依實作而定，宜設定為 5 分鐘以上。

(e) 若重新嘗試次數或經過時間達上限，則應停止運作。重試次數或時間上限依實作而定，宜設定為 24 小時以上。

9.5.3 後續處理

物聯網設備完成設備登錄後，應定期回報運作狀態(參照 9.6)。於首次進行設備登錄時，物聯網設備應等候智慧杆迴路防火牆完成設定，方可進行網際網路通訊。

備考：實作宜設計等候機制(例：主動定時檢查對外連線狀態或被動等候入向連線等)。

9.5.4 變更設備登錄

物聯網設備因變更服務內容(例：變更應用伺服器 IP 位址)或變更應用服務等因素，導致組態內容變更時，應重新執行設備登錄。重新登錄時，請求封包之〝updateTime〞參數應更新。

9.6 狀態回報存取介面要求事項

9.6.1 發送狀態回報請求

執行狀態回報步驟時，物聯網設備應向狀態回報存取介面發出 HTTPS 請求。發送請求時應依 6.3.2 及以下規定處理：

(a) 方法應為〝POST〞。

(b) URI 應符合引導登錄回應封包之〝watchdog〞參數(參照 A.1)。

(c) 請求標頭應包含〝Authorization〞欄位，型式應為〝Bearer〞，鑑別資訊應使用引導登錄回應封包之〝credCfg〞參數內容。

(d) 請求主體應包含 JSON 不具名陣列，陣列內容應包含所有應用服務之運作狀態。陣列元素應為 JSON 物件，內容格式應參照 A.5，編碼格式應依 6.2 規定。

9.6.2 接收狀態回報回應

物聯網設備發送 HTTPS 請求後，應接收組態伺服器發出之回應。處理回應時，應依 6.3.3 及下列規定執行：

(a) 若回應狀態碼為 201 (〝created〞)則不做任何處理，後續應依原週期執行狀態回報。

(b) 若回應狀態碼為 308 (〝permanent redirect〞)、401 (〝unauthorized〞)或 404 (〝not found〞)，則應停止狀態回報，並重新執行引導登錄步驟(參照 9.4)。完成引導登錄步驟後，應恢復狀態回報。

(c) 若回應狀態碼為 403 (〝forbidden〞)，則應停止狀態回報，並重新執行設備登錄步驟(參照 9.5)。完成設備登錄步驟後，應恢復狀態回報。

(d) 除 6.3.3 及以上列舉之回應狀態碼外，其他回應狀態碼皆視為異常。

(e) 發生異常時，應捨棄該次回報，後續應依原週期執行狀態回報。

備考： 物聯網設備應使用引導登錄更新狀態回報存取介面 URI，不使用包含回應狀態碼 308 (〝permanent redirect〞)之〝Location〞標頭欄位重新導向[11]。

10. 組態伺服器

10.1 概述

組態伺服器負責執行物聯網設備登錄，記錄設備資訊(包含物聯網設備之型號、序號、供應商及可提供之應用服務等)，並持續監控物聯網設備運作狀態。

組態伺服器之主機數量、組成方式、硬體規格、作業系統、軟體框架等，皆依實際需求而定。

10.2 組態伺服器功能要求事項

組態伺服器應具備以下功能及存取介面：

(a) 應具備 RADIUS 伺服器之功能，並支援 IEEE 802.1X-2004[4]擴展鑑別協定(EAP)。RADIUS 伺服器應支援常用鑑別方法(參照 D.5)。

(b) 應提供設備登錄存取介面(參照 10.3)，接收物聯網設備發送之設備登錄請求，並記錄請求封包之物聯網設備組態資訊。

(c) 應提供設備授權存取介面(參照 10.4)，使用物聯網設備組態資訊，向應用伺服器取得授權及防火牆規則，以解除物聯網設備之網際網路存取限制。

(d) 應提供狀態回報存取介面(參照 10.5)，接收物聯網設備發送之狀態回報請求，並偵測物聯網設備是否發生異常。

(e) 應能刪除物聯網設備之登錄資訊及其相關設定。此功能應限制僅能由人員操作執行。

組態伺服器其他輔助功能(例：鑑別資訊管理、人機介面、報表列印、事件通知及操作人員權限管理等)，皆依實作而定。

10.3 設備登錄存取介面要求事項

10.3.1 存取介面

組態伺服器之設備登錄存取介面應支援 IPv6 及 IPv4，IP 位址及其他網路組態依實作而定，但物聯網設備(包含 IPv4 及 IPv6)應能透過網際網路連線至該存取介面。存取介面之 URI 應與引導登錄回應封包之〝registrator〞參數一致(參照 A.1)，域名應由公開域名管理機構登錄。

備考： 需變更設備登錄存取介面 URI 時，應更新代理伺服器之引導登錄設定，不宜使用狀態碼 308 (〝permanent redirect〞)導向。

10.3.2 接收設備登錄請求

設備登錄存取介面接收 HTTPS 請求時，應依 6.3.1 及以下規定處理：

(a) 若請求方法不為〝POST〞，則應回應狀態碼 405 (〝method not allowed〞)。

(b) 請求標頭應包含〝Authorization〞欄位，型式應為〝Bearer〞，格式應符合 IETF/REF 7519 規定，內容參照 A.2。若請求未包含鑑別資訊，格式不符規定或鑑別未成功時，則應回應狀態碼 401 (〝unauthorized〞)。

(c) 組態伺服器應檢查設備登錄請求資訊，辨別是否接受該物聯網設備登錄。若不允許該物聯網設備登錄(參照 10.3.3)，則應回應狀態碼 403 (〝forbidden〞)。

(d) 請求主體應包含 JSON 物件，內容格式應符合 A.3 規定，編碼格式應依 6.2 規定。若不符合上述規定，則應回應狀態碼 400 (〝bad request〞)。

(e) 若未發生上述錯誤狀況，則應依物聯網設備登錄資訊建立相關紀錄，並回應狀態碼 201 (〝created〞)，回應封包不含主體。組態伺服器應隨即依 10.3.3 規定進行後續處理。

備考： JWT 鑑別資訊包含物聯網設備及其所屬智慧杆迴路之識別符，組態伺服器可藉此進行鑑別。狀態回報存取介面亦使用相同方式處理。

10.3.3 後續處理

組態伺服器接收設備登錄請求時，應由請求封包取得設備登錄資訊，並依以下規定處理：

(a) 若物聯網設備先前未登錄，則應記錄設備登錄資訊，並執行設備授權步驟(參照 10.4)。

(b) 若物聯網設備先前已登錄，但未完成設備授權，則應更新設備登錄資訊，並執行設備授權步驟。

(c) 若物聯網設備先前已登錄，但授權結果為拒絕授權時(參照 10.4.5)，則應拒絕該物聯網設備重新申請登錄。

(d) 若物聯網設備已完成授權，但設備登錄請求包含資料更新，則應更新設備登錄資訊，並重新執行設備授權步驟。

(e) 若物聯網設備已完成授權，且設備登錄請求未包含資料更新，則不作任何後續處理。

備考： 除以上規定外，實作可選項的設計其他條件檢查(例：白名單)以決定是否允許設備登錄。條件檢查可為自動執行或以人工進行評估，其規則及管理辦法依實作而定。

10.4 設備授權存取介面要求事項

10.4.1 存取介面

組態伺服器及應用伺服器雙方皆應提供 HTTPS 伺服器端及 HTTPS 客戶端功能。設備授權存取介面之執行過程包含 2 步驟，如圖 8 所示：

(1) 執行設備授權時，應用伺服器為 HTTPS 伺服器端，組態伺服器為 HTTPS 客戶端。組態伺服器應向應用伺服器發送 HTTPS 請求，請求封包內包含設備授權申請資訊。

(2) 應用伺服器應依申請內容進行評估，完成評估後，應發送設備授權確認至組態伺服器。發送時組態伺服器為 HTTPS 伺服器端，應用伺服器為 HTTPS 客戶端。應用伺服器應向組態伺服器發送 HTTPS 請求，請求封包內包含設備授權確認資訊。

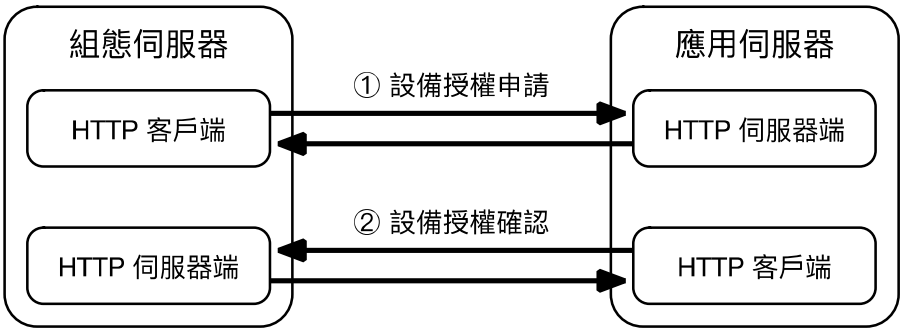


圖 8　設備授權存取介面及執行步驟示意圖

組態伺服器之設備授權存取介面應支援 IPv6 及 IPv4，IP 位址應使用網際網路公開位址。存取介面之 URI 應與設備授權申請資訊封包內容一致(參照 B.1)，域名應使用經公開域名管理機構登錄之完整域名(FQDN)。

備考： 若需變更設備授權存取介面 URI，則應重新發送設備授權申請，不宜使用狀態碼 308 (〝permanent redirect〞)導向。

10.4.2 發送設備授權申請

組態伺服器發送設備授權申請之 HTTPS 請求時，應依 6.3.2 及以下規定處理：

(a) 方法應為〝POST〞。

(b) URI 應符合設備登錄請求封包之〝authorizer〞參數內容(參照 A.3)。

(c) 應包含〝Authorization〞標頭欄位，型式應為〝Bearer〞，鑑別資訊應使用設備登錄請求封包之〝credAuthReq〞參數內容。

(d) 請求主體應包含 JSON 物件，內容格式應參照 B.1，編碼格式應依 6.2 規定。

備考： 組態伺服器可選項的指定防火牆管理政策，包含可設定之防火牆規則數量上限，以及是否允許設定 IPsec[10]。

10.4.3 接收設備授權申請之回應

組態伺服器發送 HTTPS 請求後，應等候應用伺服器發送回應。處理回應時，應依 6.3.3 及以下規定執行：

(a) 若回應狀態碼為 308 (〝permanent redirect〞)，則應依〝Location〞標頭欄位指示，更新應用伺服器之設備授權存取介面 URI，並向更新後之 URI 重新發送請求。

(b) 除回應狀態碼 308 及 6.3.3 列舉之回應狀態碼外，其他狀態碼皆不做任何處理，物聯網設

備之防火牆規則應維持不變。

10.4.4 接收設備授權確認

組態伺服器於發送設備授權申請後，應準備接收應用伺服器發送之設備授權確認 HTTPS 請求。接收 HTTPS 請求時，應依 6.3.1 及以下規定處理：

(a) 若請求方法不為〝POST〞，則應回應狀態碼 405 (〝method not allowed〞)。

(b) 請求標頭應包含〝Authorization〞欄位，型式應為〝Bearer〞，格式應符合 IETF/REF 7519。鑑別資訊應包含有效之數位簽章，〝exp〞欄位內容應在有效期限內，〝iss〞欄位內容應符合上述 HTTPS 伺服器端 URI，〝jti〞欄位內容應與請求主體之〝id〞參數一致。若不符以上規定，則應回應狀態碼 401 (〝unauthorized〞)。

(c) 請求主體應包含 JSON 物件，內容格式應參照 B.4，編碼格式應依 6.2 規定。若不符合上述規定，則應回應狀態碼 400 (〝bad request〞)。

(d) 請求主體之〝id〞應包含有效物聯網設備識別符，該物聯網設備應已完成設備登錄且尚未完成設備授權。若不符合以上規定，則應回應狀態碼 409 (〝Conflict〞)。

(e) 若未發生上述錯誤狀況，則回應狀態碼 202 (〝accepted〞)，並進行設備授權後續處理。

10.4.5 後續處理

組態伺服器進行設備授權後續處理時，應依以下規定執行：

(a) 若設備授權結果為〝DENY〞(拒絕)，則應拒絕此物聯網設備發出之設備登錄及狀態回報請求，與此物聯網設備相關之防火牆規則應視為失效。後續管理方式依實作而定(例：取消該設備接入區域網路之權限、將該設備識別符列入黑名單或拆除該設備)。

(b) 若設備授權結果為〝GRANT〞(允許)，則應檢視設備授權確認封包之防火牆規則，並調整此物聯網設備所在智慧杆迴路之入向及出向規則。

備考：變更防火牆設定時，可使用人工或自動方式處理。系統或操作人員宜保留相關紀錄。

10.5 狀態回報存取介面要求事項

10.5.1 存取介面

組態伺服器之狀態回報存取介面應支援 IPv6 及 IPv4，IP 位址及其他網路組態依實作而定，但物聯網設備(包含 IPv4 及 IPv6)應能透過網際網路連線至該存取介面。存取介面之 URI 應與引導登錄回應封包內容一致(參照 A.1)，域名應由公開域名管理機構登錄。

備考： 需變更狀態回報存取介面 URI 時，應更新代理伺服器之引導登錄設定，不宜使用狀態碼 308 (〝permanent redirect〞)。

10.5.2 接收狀態回報請求

狀態回報存取介面接收 HTTPS 請求時，應依 6.3.1 及以下規定處理：

(a) 應包含〝Authorization〞標頭欄位，型式應為〝Bearer〞，內容格式應符合 IETF/REF 7519，內容參照 A.2。若請求封包未包含鑑別資訊，格式不符規定或鑑別未成功，則應回應狀態碼 401 (〝unauthorized〞)。

(b) 若請求方法不為〝POST〞，則應回應狀態碼 405 (〝method not allowed〞)。

(c) 請求主體應為 JSON 不具名陣列，陣列元素內容應參照 A.5，編碼格式應依 6.2 規定。若不符合上述規定，則應回應狀態碼 400 (〝bad request〞)。

(d) 檢視物聯網設備識別符。若該物聯網設備尚未登錄或拒絕存取(參照 10.3.3)，則應回應狀

態碼 403 (〝forbidden〞)。

(e) 若未發生上述錯誤狀況時，則應記錄狀態回報內容，並回應狀態碼 201 (〝created〞)。回應不含主體。

10.5.3 後續處理

組態伺服器應提供狀態回報紀錄保存及檢閱功能，資料保存時間或容量等限制依實作而定。

組態伺服器應能辨識物聯網設備故障(例：依狀態回報診斷結果，或者狀態回報連續未送達次數超過預設上限等)，於物聯網設備發生故障時，宜通知相關人員處理。

11. 應用伺服器

11.1 概述

應用伺服器為智慧杆系統應用服務平臺之主要伺服器主機，提供以下功能：

(a) 提供應用服務必要功能，例：收集物聯網設備回傳之環境感測資訊、取得視訊串流等。

(b) 設備授權存取介面：物聯網設備完成設備登錄後，組態伺服器將發送物聯網設備授權申請之 HTTPS 請求至應用伺服器，應用伺服器應告知組態伺服器是否允許該物聯網設備加入運作，並提供應用服務所需之防火牆入向/出向規則。

(c) 共同資料存取介面：可取得物聯網設備詮釋資料及應用服務相關資料，提供管理機關(構)、授權使用者或其他資料共享平臺使用(例：民生公共物聯網)。

應用伺服器之系統軟硬體架構、主機數量、組成方式、硬體規格、作業系統、安裝軟體程式、系統管理及資料備份等，皆依實作而定。

11.2 設備授權存取介面要求事項

11.2.1 存取介面

應用伺服器之設備授權存取介面應提供 HTTPS 伺服器端及 HTTPS 客戶端功能，執行步驟及連線方向參照 10.4.1 說明。

應用伺服器之設備授權存取介面應支援 IPv6 及 IPv4，IP 位址應使用網際網路公開位址。存取介面 URI 應與設備登錄請求封包之〝authorizer〞參數一致(參照 A.3)，域名應使用經公開域名管理機構登錄之完整域名(FQDN)。

11.2.2 接收設備授權申請

應用伺服器接收設備授權申請之 HTTPS 請求時，應依 6.3.1 及以下規定處理：

(a) 若請求方法不為〝POST〞，則應回應狀態碼 405 (〝method not allowed〞)。

(b) 請求標頭應包含〝Authorization〞欄位，型式應為〝Bearer〞，鑑別資訊內容依實作而定，物聯網設備與應用伺服器應使用相同之資料格式及計算方式。若請求封包內未包含鑑別資訊、格式錯誤或鑑別未成功，則應回應狀態碼 401 (〝unauthorized〞)。

(c) 請求主體應包含 JSON 物件，內容格式應參照 B.1，編碼格式應依 6.2 規定。若請求主體不符合上述規定，則應回應狀態碼 400 (〝bad request〞)。

(d) 若未發生上述錯誤狀況，則應回應狀態碼 202 (〝accepted〞)，回應不包含主體，後續應依 11.2.3 規定，發送設備授權確認之 HTTPS 請求至組態伺服器。

備考： 物聯網設備於啟用網路服務過程中將取得 1 組單次隨機數(〝jti〞參數，參照 A.2)，該參數與設備授權請求封包之〝nonce〞參數內容為一致。實作宜使用該參數作為單次隨機數計算鑑別資訊(例：參考 D.6 實例)，避免使用固定預設鑑別資訊。

11.2.3 發送設備授權確認

應用伺服器應檢視請求設備授權申請資訊(參照 B.1)，評估是否允許物聯網設備加入運作。應用伺服器應依 IETF/RFC 7519 規定，解析設備授權申請資訊中〝credAuthCfm〞參數之未加密酬載部分(參照 B.3)，並於〝exp〞參數指定之期限內完成評估。評估方式依實作而定。

若應用伺服器允許物聯網設備加入運作，則應依物聯網設備之應用服務建立詮釋資料相關紀錄，格式應符合 11.3 規定。所有應用服務之詮釋資料相關紀錄皆應指派 URI，並能透過共同資料存取介面進行存取。若應用伺服器無法於期限內完成，則應至少建立主要應用服務(參照 B.1)之詮釋資料相關紀錄。

應用伺服器完成評估後，應發送設備授權確認之 HTTPS 請求至組態伺服器，發送時應依以下規定執行：

(a) 方法應為〝POST〞。

(b) URI 應符合設備授權申請之〝replyto〞參數內容(參照 B.1)。

(c) 請求標頭應包含〝Authorization〞欄位，型式應為〝Bearer〞，鑑別資訊應使用設備授權申請之〝credAuthCfm〞參數內容。

(d) 請求主體應包含 JSON 物件，內容格式應參照 B.4，編碼格式應依 6.2 規定。

(e) 若應用伺服器允許物聯網設備加入運作，則請求主體應包含應用服務所需之防火牆規則，且〝Thing〞參數應包含上述詮釋資料相關紀錄之 URI。

11.2.4 後續處理

應用伺服器發送設備授權確認 HTTPS 請求至應用伺服器後，應等候組態伺服器發送回應。處理回應時，應依 6.3.3 及下列規定執行：

(a) 若回應狀態碼為 202 (〝accepted〞)，則應等候組態伺服器完成防火牆設定，實作宜設計等候機制(例：主動定時探索或被動等候入向連線等方式)。

(c) 若回應狀態碼為 308 (〝permanent redirect〞)，則應依〝Location〞標頭欄位指示，向更新後之 URI 重新發送請求。

(b) 除 6.3.3 及以上列舉之回應狀態碼外，其他狀態碼皆視為異常。後續處理方式依實作而定。實作宜檢視錯誤發生原因，並嘗試重新發送。

11.3 共同資料存取介面要求事項

11.3.1 存取介面

應用伺服器之共同資料存取介面應支援 IPv6 或 IPv4，IP 位址應使用網際網路公開位址。

共同資料存取介面應提供 HTTPS 伺服器端功能，並應支援 OGC SensorThings v1.0[12]規定之應用程式介面(application programming interface, API)。共同資料存取介面應完整支援〝GET〞存取方法，其存取控制、其他存取方法(例：〝PATCH〞、〝DELETE〞等)、鑑別方式及權限管理等，皆依實作而定。

11.3.2 Thing 物件實例

應用伺服器應依物聯網設備之應用服務，提供〝Thing〞物件實例及其他附屬物件。〝Thing〞物件實例內容應符合依 OGC SensorThings v1.0[12]規定。〝Thing〞物件實例之〝properties〞參數內容格式應符合 C.1 規定。

〝Thing〞物件實例數量應與物聯網設備應用服務匹配，包含設備授權申請封包中〝priApp〞

及〝extApp〞參數列舉之所有應用服務，皆應個別對應至 1 組〝Thing〞物件實例。不同物聯網設備或不同應用服務不可重複對應至同一〝Thing〞物件實例。

11.3.3 補充詮釋資料

共同資料存取介面除 OGC SensorThings v1.0[12]規定之物件實例 URI 以外，應額外提供包含細部管理資訊之補充詮釋資料。所有應用服務皆應提供對應之補充詮釋資訊，不同物聯網設備或不同應用服務不可重複對應至同一補充詮釋資料。

補充詮釋資料之內容格式應符合 C.2 規定，編碼方式應符合 6.2 規定。補充詮釋資料之 URI 路徑依實作而定，但應與上述〝properties〞參數中〝profile〞參數內容一致。補充詮釋資料之存取方法應與其他 SensorThings[12]物件實例相同，但可使用不同之存取權限控管設定。

11.3.4 Location 物件實例

應用伺服器應提供 1 組以上之〝Locations〞物件實例，包含該應用服務之實際安裝位置座標。〝Locations〞物件實例所有內容皆依 OGC SensorThings v1.0[12]規定，並正確關聯至〝Thing〞物件實例。

11.3.5 Datastream 及 Observation 物件實例

11.3.5.1 共同要求

〝Datastream〞物件實例之數量及型式及內容可依實際需求自行設計，〝Thing〞物件實例可關聯至不限定數量之〝Datastream〞物件實例，但不同〝Thing〞物件實例不可關聯至相同之〝Datastream〞物件實例。〝Datastream〞物件實例內容宜與應用服務型式(參照 A.7)一致。

〝Observation〞物件實例之內容應配合〝Datastream〞物件實例型式。

不同應用服務型式對應〝Datastream〞及〝Observation〞物件實例之內容可參考 11.3.5.2、11.3.5.3 及 11.3.5.4。

11.3.5.2 感測型式應用服務

量測物理量資訊並回傳之應用服務，其〝Datastream〞物件實例宜代表包含經轉換、計算或統計後、符合觀測標的物理量量測單位之數值(例：降雨事件應累加計算並轉換為時雨量或日雨量)。

〝Datastream〞物件實例之〝unitOfMeasurement〞參數應依 SensorThing[12]規定，優先使用計量單位統一代碼 (Unified Code for Units of Measure)表示。常見物理量及其對應參數內容可參照 D.7。

11.3.5.3 媒體紀錄型式應用服務

記錄視訊、音訊等媒體資訊之應用服務，其〝Datastream〞物件實例依實際需求而定(例：攝影機或麥克風之原始資料串流，或者由不同視訊軌及音軌混合之事件紀錄)。

〝Datastream〞物件實例之〝unitOfMeasurement〞參數內容宜使用足以說明該媒體紀錄性質之資訊(例：D.7 之〝媒體串流〞項次)。〝observationType〞參數宜使用〝OM_Observation〞型式之對應 URI (參照 OGC SensorThing v1.0[12]規範文件之表 12)。

〝Observation〞物件實例之〝result〞參數內容宜為與媒體紀錄相關之 URI(例：原始串流資料、經轉換過之影片、圖片或音訊檔案、可存取該應用服務之控制介面或存取方式之說明文件等)。該 URI 存取介面之域名、存取控制、權限管理及通訊協定等，皆依媒體資源型式而定[例：FTP、HTTP、HLS (HTTP live streaming)、DASH (dynamic adaptive streaming over

HTTP)、RTMP (real-time messaging protocol)、RTSP (real-time streaming protocol)、WebRTC (real-time communication)或其他客制化應用程式之專屬 URI]。

11.3.5.4 其他型式應用服務

非屬感測器及媒體串流型式之應用服務，〝Datastream〞物件實例數量不規定。內容格式可提供系統維護紀錄(例：參照 D.8)或自行設計。自行設計之物件實例應符合 SensorThings[12]規定。

〝Observation〞物件實例之內容格式宜提供系統維護紀錄(例：參照 D.9)或自行設計。自行設計之物件實例應符合 OGC SensorThings v1.0[12]規定。

11.3.6 其他物件實例

其他物件實例，包含〝HistoricalLocation〞、〝Sensor〞、〝ObservationProperty〞及〝FeatureOfInterest〞，皆應依 OGC SensorThing v1.0[12]規定建置，並正確設定對應關係。

附錄A

(規定)

物聯網設備登錄及狀態回報

A.1. 引導登錄回應

參數	必備/選項	格式	內容說明
version	M	字串	應為〝5G 智慧杆技術規範 V1.0〞。
registrator	M	字串	組態伺服器設備登錄存取介面之 URI。
watchdog	M	字串	組態伺服器狀態回報存取介面之 URI。
credCfg	M	字串	物聯網設備連線至組態伺服器使用之鑑別資訊，格式應為符合 IETF/RFC 7519 規定之 JWT，數位簽章演算法應使用符合 FIPS 180-2:2002 規定之 HMAC-SHA256 (〝HS256〞)，標頭及酬載之輸入內容參照 A.2。

備考：〝M〞代表〝必備(Mandatory)〞，〝O〞代表〝選項(Optional)〞，下同。

A.2. JWT 輸入參數

位置	參數	必備/選項	格式	內容說明
Header	alg	M	字串	應為〝HS256〞。
	type	M	字串	應為〝JWT〞。
Payload	iss	M	字串	代理伺服器識別符。
	iat	M	整數	產生鑑別資訊之時間，格式為 UNIX 時戳，單位為秒。
	exp	O	整數	符記預計逾期時間，格式為 UNIX 時戳，單位為秒。若未設定本參數，則代表此符記為永久有效。
	aud	O	字串	組態伺服器可識別之代碼，格式及內容依實作而定(例：組態伺服器設備登錄介面之域名)。
	sub	M	字串	物聯網設備識別符。
	hcra	M	字串	連線至引導登記存取介面之 HTTPS 客戶端 IP 位址，可為 IPv4 或 IPv6，應使用完整表示式，IPv6 位址空值欄位不可省略。
	jti	M	字串	代理伺服器隨機產生之 UUID，可供物聯網設備及應用伺服器作為計算鑑別資訊之單次隨機數(nonce)。

備考：〝hcra〞為自定義 JWT 參數，代表〝HTTP client remote address〞。

A.3. 設備登錄請求

參數	必備/選項	格式	內容說明
name	M	字串	物聯網設備名稱。
model	O	字串	物聯網設備型號。
serial	O	字串	物聯網設備序號。
vender	M	字串	物聯網設備供應者。
contact	O	字串	物聯網設備維護/營運聯絡窗口。
ip	M	字串	物聯網設備之 IP 位址，可為 IPv4 或 IPv6，應使用完整表示式，IPv6 位址空值欄位不可省略。
inbound	O	數字	物聯網設備預計使用之入向通訊埠數量，不區分 TCP 或 UDP。若物聯網設備使用 IPv6，則可省略本參數。

參數	必備/選項	格式	內容說明
authorizer	M	字串	應用伺服器之設備授權存取介面 URI。此 URI 應由物聯網設備供應者指定。
credAuthReq	M	字串	實作自訂之承載符記(bearer token)鑑別資訊，組態伺服器連線至應用伺服器執行設備授權申請時，將包含本參數。 例：參考 D.6 之 JWT 實例。
heartbeat	M	整數	物聯網設備發送狀態回報之最大週期，單位秒。
updateTime	M	字串	物聯網設備登錄資訊之最後更新時間(非本次請求時間)，格式應符合 CNS 7648 規定，應包含時區，精確度至秒。
priApp	M	JSON 物件	物聯網設備主要應用服務，格式為 JSON 物件，參照 A.4。 若物聯網設備僅具備單一應用服務，則應包含該服務之說明。 若物聯網設備具多應用服務，則應包含對閘道控制器之說明(參照 9.1.2)。
extApp	O	陣列	JSON 物件陣列，格式參照 A.4。 若物聯網設備僅具備單一應用服務，則可省略本參數。 若物聯網設備具多應用服務，則應包含除閘道控制器外其他所有應用服務之說明，順序依實作而定。

A.4. 應用服務說明

參數	必備/選項	格式	內容說明
id	M	字串	實作自訂之應用服務識別符，於同一物聯網設備內應為唯一。
name	M	字串	實作自訂之應用服務名稱。
type	M	字串	應用服務主要型式，參照 A.7。
ip	O	字串	若該應用服務對應至網路周邊裝置，則可選項的填入該裝置之區域網路 IP 位址。IP 位址可為 IPv4 或 IPv6，應使用完整表示式，IPv6 位址空值欄位不可省略
port	O	陣列	包含應用服務所需之入向通訊埠號。
vender	O	字串	應為應用服務供應者名稱。
desc	O	字串	實作自訂之額外說明訊息。

A.5. 狀態回報請求(陣列元素)

參數	必備/選項	格式	內容說明
id	M	字串	實作自訂之應用服務識別符，應符合物聯網設備登錄請求之應用服務說明內容(參照 A.4)。
state	M	整數	設備運作狀態，參照 A.6。
error	O	字串	實作自訂之錯誤訊息。
temp	O	浮點數	設備溫度(單位：°C)。
watt	O	浮點數	設備耗能(單位：watt)。
cpu	O	浮點數	CPU 整體使用率。
storage	O	浮點數	儲存空間整體使用率。
dataflow	O	浮點數	資料流量(單位：mebibyte/sec)。
time	M	字串	產生本項紀錄之時間，格式為 CNS 7648 含時區，精確度至秒。

A.6. 自我診斷異常代號表

代號(十進制)	定義	備註
≤ -2	保留	
-1	未知	尚未進行診斷或周邊裝置不支援診斷功能。
0	正常	
1	暫時性異常	可自動復原修正之錯誤。
2	應用程式異常終止	
3	系統服務異常終止	無法重新啟用必要之系統服務。
4	外部服務存取異常	外部資源無法取得或鑑別未成功。
5	系統資源不足	運作效能受限制，需人工介入調整。
6	設備內部溫度過高	運作效能受限制，需人工介入調整。
7	內部硬體元件故障	無法於本機端儲存檔案或資料。
8	外部硬體元件故障	感測器或內部通訊介面故障。
9	子系統無反應	不明原因停止運作，且未回應診斷或修復請求。
10	區域網路通訊異常	無法連線至區域網路內其他物聯網設備/周邊裝置，或連線不穩定。
11	網際網路通訊異常	無法存取部分網際網路服務，或連線不穩定。
12～100	保留	
101	資安事件：阻斷攻擊	遭受分散式阻斷式攻擊或其他阻斷式攻擊。
102	資安事件：非法存取	未授權者嘗試進行操作或越權存取機敏內容。
103	資安事件：軟體完整性異常	作業系統完整性遭破壞、檔案被置換或發現異常檔案。
104	資安事件：硬體完整性異常	硬體元件異常或設備外殼不正常開啟。
105～200	保留	
201	環境災害：斷電	系統使用備援電源或不斷電系統運作。
202	環境災害：浸水	
203	環境災害：異常高溫	系統外部溫度感測器感應環境溫度超過設備正常運作範圍。
204	環境災害：線路中斷	區域網路或網際網路連線異常，切換至備援線路。
≥ 205	保留	

A.7. 應用服務型式

代號(全大寫)	內容說明
GATEWAY	多應用服務物聯網設備(參照 9.1.2)之閘道控制器。
SENSOR	該應用服務使用感測器讀取物理量(例：溫度、開路/閉路、氣體濃度及耗能等)之量測值，並上傳至指定伺服器。
MEDIA	該應用服務記錄視訊/音訊，並將原始或經處理之視訊、音訊或截圖上傳至指定伺服器。
OTHER	該應用服務非屬上述任何型式。

附錄B

(規定)

設備授權申請及確認

B.1. 設備授權申請

參數名	必備/選項	格式	內容說明
id	M	字串	物聯網設備識別符。
cluster	M	字串	物聯網設備所屬智慧杆迴路之代理伺服器識別符。
nonce	M	字串	設備登錄請求中 JWT 鑑別資訊之〝jti〞參數內容(參照 A.2)，可供物聯網設備及應用伺服器單次隨機數(nonce)以計算。
serial	O	字串	物聯網設備登錄請求之〝serial〞參數內容。
model	O	字串	物聯網設備登錄請求之〝model〞參數內容。
ip	M	字串	物聯網設備 IP 位址，應使用外部 IPv4 或 IPv6 位址，格式應採完整表示式，IPv6 空值欄位不可省略。
policy	O	JSON 物件	智慧杆迴路設定防火牆規則之基本政策，內容參照 B.2。本參數可省略。
replyto	M	字串	組態伺服器設備授權存取介面之 URI。
credAuthCfm	M	字串	應用伺服器發送設備授權確認時，應包含本參數內容之鑑別資訊。格式應為符合 IETF/RFC 7519 規定之 JWT，內容細部規定參照 B.3。
updateTime	M	整數	包含設備登錄請求之〝updateTime〞參數內容。
priApp	M	陣列	包含設備登錄請求(參照 A.3)之〝priApp〞參數內容。
extApp	O	陣列	包含設備登錄請求(參照 A.3)之〝extApp〞參數內容。若設備登錄請求未包含〝extApp〞參數，則可省略本參數。

B.2. 防火牆政策內容

參數名	必備/選項	格式	內容說明
forward	O	陣列	整數陣列，智慧杆迴路使用 IPv4 通訊埠號對映(port forwarding)時，可使用之外部通訊埠號範圍。陣列應包含 2 項元素，代表起始通訊埠號及終止通訊埠號。若未使用 IPv4 通訊埠號對映時，則可省略本參數。
maxIB	O	整數	最大可設定之防火牆入向規則數。組態伺服器將忽略陣列索引值大於該值之規則。
maxOB	O	整數	最大可設定之防火牆出向規則數。組態伺服器將忽略陣列索引值大於該值之規則。
ipsec	O	布林	是否允許設定 IPsec 規則，若內容為 false 或省略本參數，則表示不允許設定 IPsec 規則。

B.3. JWT 輸入參數

位置	參數	必備/選項	格式	內容說明
Header	alg	M	字串	應為〝HS256〞。
	type	M	字串	應為〝JWT〞。
Payload	iss	M	字串	組態伺服器設備授權存取介面之域名。
	sub	M	字串	應用伺服器設備授權存取介面之域名。

位置	參數	必備/選項	格式	內容說明
	exp	M	整數	預計失效時間，格式為 UNIX 時戳，單位為秒，實作宜設定合理數值。
	iat	M	整數	產生該符記之時間，格式為 UNIX 時戳，單位為秒。
	jti	M	字串	物聯網設備識別符。

B.4. 設備授權確認

參數名	必備/選項	格式	內容說明
id	M	字串	物聯網設備識別符。
result	M	字串	設備授權結果，應為以下結果之一(全大寫)： ● 〝GRANT〞：允許 ● 〝DENY〞：拒絕
contact	M	字串	應用服務提供者聯絡資訊，用於接收防火牆規則啟用通知，宜使用電子郵件位址，可使用一般網頁 URI 或文字描述。
inbound	O	陣列	若授權結果為〝DENY〞，則可省略本參數。 若授權結果為〝GRANT〞，則應包含由遠端連入該物聯網設備之規則列表，每項規則限定單一 IP 或單一 IP 區段，可包含多項規則，規則數量上限由智慧杆管理機關(構)規定。陣列內容格式參照 B.5。若物聯網設備不使用入向連線規則，本參數可省略。
outbound	O	陣列	若授權結果為〝DENY〞，則可省略本參數。 授權結果為〝GRANT〞，則應包含該物聯網設備連線至遠端之規則列表，每項規則限定單一 IP 或單一 IP 區段，可包含多項規則，規則數量上限由智慧杆管理機關(構)規定。陣列內容格式參照 B.6。若物聯網設備不使用出向連線規則，本參數可省略。
ipsec	O	字串	若授權結果為〝DENY〞或未使用 IPsec，則可省略本參數。 授權結果為〝GRANT〞時，則可選項的填入 IPsec 之目的地 IP 位址。
things	O	陣列	若授權結果為〝DENY〞，則可省略本參數。 授權結果為〝GRANT〞，則應包含物聯網應用服務於共同資料存取介面之對應 URI，詳細規定參照 11.2.3。格式參照 B.7，順序依實作而定。

B.5. inbound 存取規則陣列內容

參數名	必備/選項	格式	內容說明
protocol	M	字串	應為〝TCP〞或〝UDP〞。
srcIP	M	字串	連線來源 IP 位址，應使用完整表示式，IPv6 位址空值欄位不可省略。可為單一 IP 位址或 IP 區段，IP 區段應使用遮罩位元數表示。
dstPort	M	數字陣列	物聯網設備外部 IP 位址之通訊埠號範圍，陣列應包含 2 元素，代表起始通訊埠號及終止通訊埠號。若兩者相同，則代表僅設定單一通訊埠號。 若需啟用之通訊埠不連續，則應設定多組 ibound 存取規則。
forward	O	數字陣列	使用 IPv4 通訊埠對映時，物聯網設備內部 IP 位址使用之通訊埠號，範圍應與 dstPort 參數一致。若未使用 IPv4 通訊埠對映，則可省略本參數。

B.6. outbound 存取規則陣列內容

參數名	必備/選項	格式	內容說明
protocol	M	字串	應為〝TCP〞、〝UDP〞或〝ICMP〞。
dstIP	M	字串	連線目的地 IPv4 或 IPv6 位址，應使用完整表示式，IPv6 位址空值欄位不可省略。可為單一 IP 位址或 IP 區段，IP 區段應使用遮罩位元數表示。
dstPort	O	數字陣列	連線目的地之通訊埠號範圍，陣列應包含 2 元素，代表起始通訊埠號及終止通訊埠號，若兩者相同，則代表僅設定單一通訊埠號。 若協定型式為〝ICMP〞或使用所有通訊埠，則可省略本參數。

B.7. things 共同資料存取介面陣列內容

參數名	必備/選項	格式	內容說明
id	M	字串	實作自訂之應用服務識別符，應符合設備登錄請求之應用服務描述內容(參照 A.4)。
uri	M	字串	符合 OGC SensorThings v1.0[12]規定之 Things 物件 URI。

附錄C

(規定)

共同資料存取介面補充資料

C.1. properties 參數內容

參數名	必備/選項	格式	內容說明
standard	M	字串	應為〝5G 智慧杆技術規範 V1.0〞。
district	M	字串	應用服務所在行政區。
position	O	字串	應用服務所在位置說明(例：街道或地標等)。
profile	M	字串	指向該應用服務補充詮釋資料之 URI(參照 11.3.3)。

C.2. 應用服務補充詮釋資料(規定)

參數名	必備/選項	格式	內容說明
things	M	字串	對應該筆詮釋資料之 Things 物件實例 URI。
id	M	字串	應用服務所屬物聯網設備之物聯網設備識別符。
cluster	M	字串	應用服務所屬迴路之代理伺服器識別符。
app	M	字串	應用服務識別符。
pole	O	字串	應用服務所在之智慧杆(或箱體)編號。
authority	M	字串	負責該應用服務建置及管理之主管機關(構)。
vender	M	字串	負責實際營運管理該應用服務之供應者名稱。
contact	O	字串	負責實際營運管理該應用服務之供應者聯絡方式(例：電話號碼、電子郵件或網址)。
model	O	字串	應用服務對應硬體裝置之型號(例：感測器型號)。
serial	O	字串	應用服務對應硬體裝置之序號(例：感測器序號)。
platform	M	字串	目前執行之作業系統(或硬體/韌體平臺)名稱及完整版本更新編號，開源系統(如 Linux)應包含完整發行名稱。
patch	O	字串	應包含作業系統最後更新日期時間(格式應符合 CNS 7648)，或最後一次安裝之更新項目編號(應符合作業系統廠商更新公告)。 未曾進行更新時，本參數可省略。
framework	M	陣列	應包含應用服務使用之軟體框架名稱及完整版本更新編號(例：.NET、Java、Python、Node.js 等)。 若未使用任何軟體框架，則本參數應為空陣列。
version	M	字串	應用服務軟體/韌體程式版本編號。
type	M	字串	應用服務主要型式，參照 A.7。
services	O	陣列	若應用服務型式為閘道控制器(〝GATEWAY〞)，則應包含該設備上所有應用服務對應 Things 物件實例之 URI。 若應用服務為其他型式，則可省略本參數。

附錄D

(參考)

參數對照表及其他常用資料列表

D.1. 適用法規及其他標準(或規範)之應用服務

分類	項目	對應標準(或規範)
交通號誌	燈號設備	5G 智慧杆技術規範－第 9 部：性能要求
	通訊介面型式及通訊協定	中華民國交通部〝交通號誌控制器產業標準草案〞
公眾無線網路	無線射頻規格	國家通訊委員會〝低功率射頻電機技術規範〞
	建置及管理辦法	智慧杆系統主管機關(構)發布之行政命令[例：〝行政院及所屬機關(構)辦理無線上網服務永續發展作業原則〞，以及〝臺北市政府公共無線上網服務管理要點〞等]
5G 行動通訊	硬體設備及通訊介面	5G 智慧杆技術規範－第 10 部：5G 微型基地臺要求

D.2. 防火牆常用白名單清單

服務	協定	域名或 IP 位址
公開 DNS	DNS DNS-over-HTTPS	2001:4860:4860::8888 2001:4860:4860::8844 2606:4700:4700::64 2606:4700:4700::6400 8.8.8.8 8.8.4.4 1.1.1.1
公開網路校時	NTP	*.tw.pool.ntp.org *.stdtime.gov.tw
Windows 系統更新	HTTP/HTTPS	download.microsoft.com go.microsoft.com dl.delivery.mp.microsoft.com ntservicepack.microsoft.com windowsupdate.microsoft.com *.windowsupdate.microsoft.com *.update.microsoft.com wustat.windows.com *.windowsupdate.com download.windowsupdate.com *.download.windowsupdate.com
Linux 套件更新	HTTP/HTTPS	tw.archive.ubuntu.com security.ubuntu.com archive.canonical.com deb.debian.org ftp.debian.org ftp.tw.debian.org
Docker 套件更新	HTTP/HTTPS	hub.docker.com *.hub.docker.com
Android 系統更新	HTTPS, TCP 5228-5230	accounts.google.com accounts.google.tw android.clients.google.com clients1.google.com clients2.google.com

服務	協定	域名或 IP 位址
		clients3.google.com clients4.google.com clients5.google.com clients6.google.com dl.google.com dl-ssl.google.com m.google.com play.google.com pki.google.com *.googleapis.com android.com google-analytics.com googleusercontent.com *.ggpht.com *.gstatic.com *.gvt1.com *.gvt2.com *.gvt3.com
Android 事件推送服務	HTTPS, TCP 5228-5236	fcm.googleapis.com fcm-xmpp.googleapis.com

D.3. mDNS 之 TXT 紀錄

服務	鍵(Key)	值(Value)	必備/選項	備註
NTP	TXTVERS	1	O	〝TXTVERS〞為英文大寫字串。
HTTP	TXTVERS	1	O	〝TXTVERS〞為英文大寫字串。
HTTP	PATH	自定路徑	O	引導登錄存取介面 URI 路徑，應包含起始根目錄路徑字元〝/〞，不含通訊協定前綴及域名。〝PATH〞為英文大寫字串，URI 路徑大小寫依實作而定。若未設定本項紀錄，則 URI 路徑應為根目錄。

D.4. 公開網路校時伺服器

網址	提供者	種類
time.stdtime.gov.tw	國家時間與頻率標準實驗室	IPv4/IPv6
2.tw.pool.ntp.org	NTP Pool 公開服務(台灣地區)	IPv4/IPv6

D.5. 802.1X 常用鑑別方法

鑑別方法	相關標準
EAP-MD5	IETF/RFC 3748
PEAPv0/EAP-MSCHAPv2	IETF draft-kamath-pppext-peapv0 / RFC 2759
PEAPv1/EAP-GTC	IETF draft-josefsson-pppext-eap-tls-eap / RFC 3748
EAP-TLS	IETF/RFC 2716

D.6. 使用 JWT 作為自訂承載符記之實例(參考)

位置	參數	必備/選項	格式	內容說明
Header	alg	M	字串	應為〝HS256〞。
	type	M	字串	應為〝JWT〞。
Payload	iss	M	字串	物聯網設備之識別符。
	iat	M	整數	產生該符記之時間，格式為 UNIX 時戳，單位為秒。
	sub	M	字串	組態伺服器設備登錄存取介面之域名。
	nonce	M	字串	應為引導登錄回應中〝regCfg〞參數之〝jti〞參數內容。

D.7. 常見物理量與 unitOfMeasurement 參數對照清單

物理量	〝name〞	〝symbol〞	〝definition〞
長度	metre	m	https://ucum.org/ucum.html#para-28
高度	metre	m	https://ucum.org/ucum.html#para-28
距離	kilometre	km	https://ucum.org/ucum.html#para-28
重量	kilogram	kg	https://ucum.org/ucum.html#para-28
攝氏溫度	celsius	°C	https://ucum.org/ucum.html#para-30
加速度	meter per second squared	m/s2	https://qudt.org/vocab/unit/M-PER-SEC2.html
時速	kilometre per hour	km/h	https://qudt.org/vocab/unit/KiloM-PER-HR.html
秒速	metre per second	m/s	https://qudt.org/vocab/unit/M-PER-SEC.html
時刻	datetime		https://www.iso.org/iso-8601-date-and-time-format.html
10 分鐘雨量	millimetre	mm	https://ucum.org/ucum.html#para-28
時雨量	millimetre	mm	https://ucum.org/ucum.html#para-28
日累積雨量	millimetre	mm	https://ucum.org/ucum.html#para-28
露點	celsius	°C	https://ucum.org/ucum.html#para-30
相對濕度	percentage	%	https://ucum.org/ucum.html#para-29
能見度	kilometre	km	https://ucum.org/ucum.html#para-28
日照量	watt per square metre	W/m2	https://qudt.org/vocab/unit/W-PER-M2.html
日照時數	hour	hr	https://ucum.org/ucum.html#para-31
紫外線指數	index		https://www.who.int/health-topics/ultraviolet-radiation
光照度	lux	lx	https://ucum.org/ucum.html#para-30
風向	degree	º	https://ucum.org/ucum.html#para-31
風速	metre per second	m/s	https://qudt.org/vocab/unit/M-PER-SEC.html
空氣品質	AQI		https://airtw.epa.gov.tw/cht/Information/Standard/AirQualityIndicator.aspx
氣體濃度	parts per billion	ppb	https://ucum.org/ucum.html#para-29
氣體濃度	parts per million	ppm	https://ucum.org/ucum.html#para-29
PM2.5	micrograms per cubic metre	ug/m3	https://qudt.org/vocab/unit/MicroGM-PER-M3-HR.html
音量	decibel	dB	https://qudt.org/vocab/unit/DeciB.html
水位	metre	m	https://ucum.org/ucum.html#para-28

物理量	〝name〞	〝symbol〞	〝definition〞
淹水深度	centimetre	cm	https://ucum.org/ucum.html#para-28
瞬間流量	cubic metre per second	m3/s	https://qudt.org/vocab/unit/M3-PER-SEC.html
累計流量	cubic metre	m3	https://qudt.org/vocab/unit/M3.html
氣壓	pascal	Pa	https://ucum.org/ucum.html#para-30
水壓	kilo pascal	kPa	https://ucum.org/ucum.html#para-30
管壓	kilogram per square centimetre	kg/cm2	https://qudt.org/vocab/unit/KiloGM-PER-CentiM2.html
酸鹼值	potential of hydrogen	pH	https://ucum.org/ucum.html#para-45
電壓	volt	V	https://ucum.org/ucum.html#para-30
電壓	kilovolt	kV	https://ucum.org/ucum.html#para-30
電流	ampere	A	https://ucum.org/ucum.html#para-30
頻率	hertz	Hz	https://ucum.org/ucum.html#para-30
功率	watt	W	https://ucum.org/ucum.html#para-30
功率	kilowatt	kW	https://ucum.org/ucum.html#para-30
視在功率	volt-amper	VA	https://qudt.org/vocab/unit/V-A.html
視在功率	kilovolt-amper	kVA	https://qudt.org/vocab/unit/V-A.html
功率因數	percentage	%	https://ucum.org/ucum.html#para-29
耗電量	kilowatt-hour	kWh	https://qudt.org/vocab/unit/KiloW-HR.html
振幅	millimetre	mm	https://ucum.org/ucum.html#para-28
媒體串流	stream media		https://en.wikipedia.org/wiki/Streaming_media

備考 1. 本表為〝unitOfMeasurement〞參數內容參考，並非定義度量衡單位。本表使用單位及符記依 OGC SensorThings V1.0[12]規定，以 UCUM (Unified Code for Units of Measure)字彙為主。

備考 2. 本表中特殊字元〝º〞(度)為 Unicode〝Degree Sign〞(U+00B0)，UTF-8 編碼為〝0xC2 0xB0〞，不可使用中文編碼全形符號。

D.8. 其他型式應用服務 Datastream 物件實例參數

參數	內容
observationType	http://www.opengis.net/def/observationType/OGC-OM/2.0/OM_Observation
unitOfMeasurement.name	maintenance log
unitOfMeasurement.symbol	(空字元)
unitOfMeasurement.definition	(暫訂)〝5G 智慧杆技術規範 V1.0〞

D.9. 其他型式應用服務 Observation 觀測結果定義

數值	定義
≤ 99	保留(不使用)
100	應用服務正常運作
101～199	保留(不使用)

數值	定義
200	異常發生
201～299	保留(不使用)
300	異常維修開始
301～398	保留(不使用)
399	異常維修結束
400～499	保留(不使用)
500	系統維護開始
501～598	保留(不使用)
599	系統維護結束
600～998	保留(不使用)
999	應用服務結束運作
≥ 1000	保留(不使用)

參考資料

[1] CNS 15652-3-2013, 智慧照明系統－第 3 部：場域網路介面

[2] IEEE 802.1AE-2018, Media Access Control (MAC) Security

[3] IEEE 802.1Q-2014, Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks

[4] IEEE 802.1X-2004, Port-Based Network Access Control

[5] IEEE 802.3ab-1999, Physical Layer Parameters and Specifications for 1000 Mb/s Operation over 4 pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T

[6] IEEE 802.3u-1995, Media Access Control (MAC) Parameters Physical Layer, Medium Attachment Units, and Repeater for 100Mb/s Operation, Type 100BASE-T

[7] IEEE 802.3z-1998, Media Access Control Parameters, Physical Layers, Repeater and Management Parameters for 1,000 Mb/s Operation

[8] IEC 62386:2017, Digital addressable lighting interface (DALI)

[9] IETF/RFC 3646, DNS Configuration options for Dynamic Host Configuration Protocol for IPv6

[10] IETF/RFC 4301, Security Architecture for the Internet Protocol

[11] IETF/RFC 7238, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)

[12] NIST FIPS 180-2:2002, Secure Hash Standard (SHS)

[13] SensorThings:2015, Open Geospatial Consortium 15-078r6, SensorThings API Part I - Sensing

[14] WGS84:2004, World Geodetic System

5G 智慧杆系統技術規範
－第 2-2 部：資訊互運性及通訊介面測試要求

5G Smart pole system technical specification - Part 2-2: Requirements of test for information interoperability and communication interface

中 華 民 國 111 年 9 月

目錄

節次 頁次

前言 3

0. 簡介 4

1. 適用範圍 4

2. 引用標準 4

3. 用語及定義 4

4. 縮寫 5

5. 符合性測試 6

5.1 概要 6

5.2 符合性測試內容 6

5.3 可執行符合性測試之條件 6

5.4 符合性測試通過準則 6

6. 測試案例執行方法 7

6.1 待測標的 7

6.2 測試平臺 7

6.3 測試案例 8

7. 網路設備符合性測試 8

7.1 概述 8

7.2 待測標的 8

7.3 測試內容 9

7.4 符合性評估 9

8. 代理伺服器符合性測試 10

8.1 概述 10

8.2 待測標的 10

8.3 測試方法 10

8.4 符合性評估 11

8.5 合規性測試 11

9. 物聯網設備符合性測試 16

9.1 概述 16

9.2 待測標的 17

9.3 測試方法 17

9.4 產品符合性評估 18

9.5 產品合規性測試 19

10. 網路周邊裝置符合性測試 24

10.1 概述 24

10.2 待測標的 25

10.3 測試內容 25

10.4 符合性評估 25
10.5 合規性測試 26
11. 組態伺服器符合性測試 26
11.1 概述 26
11.2 待測標的 26
11.3 測試內容 26
11.4 符合性評估 28
11.5 合規性測試 29
12. 應用伺服器符合性測試 33
12.1 概述 33
12.2 待測標的 33
12.3 測試內容 33
12.4 符合性評估 34
12.5 合規性測試 36
附錄 A （規定）符合性測試清單 41
附錄 B （參考）測試報告範本 48
參考資料 50

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole)現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT)設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統。

本規範為〝5G 智慧杆技術規範－第 2-1 部：資訊互運性及通訊介面要求〞之符合性測試，包含執行測試之規定及測試程序，以確保網路設備、物聯網設備、代理伺服器、組態伺服器及應用伺服器間之通訊介面、通訊協定及通訊程序符合本系列規範第 2-1 部規定。

2. 引用標準

本規範適用本系列規範第 2-1 部之引用標準。

3. 用語及定義

本規範適用本系列規範第 2-1 部之用語及定義，以及下列用語及定義適用於本規範。

3.1 模擬器(emulator)

一種用於程式開發及除錯之程式，可讀取另一標的軟體之執行檔，並模擬其硬體執行環境，使標的軟體可於不相容之硬體平臺上執行(例：於個人電腦上執行智慧型手機程式)。標的軟體之執行碼係經模擬器轉譯，並非直接使用硬體平臺之微處理器執行，其實際功能與原生硬體平臺上執行時可能有差異。

3.2 介面模擬器(interface emulator)

一種硬體設備，於測試平臺中透過區域網路與待測標的之互運性存取介面介接，進行資料交換。介面模擬器應依本規範規定之測試案例逐一執行測試程序，並檢視待測標的反應，藉以判斷待

測標的是否符合本系列規範第 2-1 部規定。於測試過程中，介面模擬器應依測試案例之特性變更組態(例：提供 HTTPS 客戶端存取介面以測試待測標的之 HTTPS 伺服器功能，或者提供 HTTPS 伺服器存取介面以測試 HTTPS 客戶端功能)。

3.3 支援工具(support tool)

針對測試標的進行組態設定及觀察執行狀況之軟硬體設備。支援工具可藉由硬體通訊介面(例：序列埠)或區域網路連接待測標的，以進行操作或觀察。於測試過程中，支援工具可用於操作待測標的以執行測試案例，但不可協助或干擾執行程序。

3.4 測試平臺(test platform)

為執行測試所建置之測試環境，包含測試場地、電源供應、網路設備及介面模擬器。執行測試時，待測標的應設置於測試平臺所在場地中，並連接測試平臺之網路設備。

3.5 虛擬機(virtual machine)

一種軟體系統，可於提供抽象之硬體存取層，使不同作業系統可同時於同一硬體設備上運作，不會互相干擾。虛擬機與模擬器不同，模擬器讀取標的程式之執行碼後需進行轉譯，並由模擬器之軟體行程負責執行。虛擬機之軟體行程僅提供一抽象存取介面，於虛擬機內運作之作業系統仍由硬體平臺之微處理器直接執行。虛擬機可有效利用硬體資源，亦具備軟體執行緒監控及即時故障備援等進階輔助功能，於實務上多用於伺服器叢集管理。

4. 縮寫

DHCP	動態主機組態協定(dynamic host configuration protocol)
DHCPv4	適用於網際網路通訊協定版本 4 的動態主機組態協定(DHCP for IPv4)
DHCPv6	適用於網際網路通訊協定版本 6 的動態主機組態協定(DHCP for IPv6)
DNS	域名系統(domain name system)
EAP	擴展鑑別協定(extensible authentication protocol)
EAPOL	經由區域網路的擴展鑑別協定(extensible authentication protocol over local area network)
FQDN	完整域名(fully qualified domain name)
HTTP	超文字傳輸協定(hypertext transfer protocol)
HTTPS	超文字傳輸安全協定(hypertext transfer protocol secure)
ICMP	網際網路控制訊息協定(Internet control message protocol)
IP	網際網路協定(Internet protocol)
IPv4	網際網路協定版本 4(Internet protocol version 4)
IPv6	網際網路協定版本 6(Internet protocol version 6)
IPsec	網際網路安全協定(Internet protocol security)
JWT	JSON 網頁符記(JSON web token)
NTP	網路時間協定(network time protocol)
mDNS	多播域名系統(multicast DNS)
RADIUS	遠端使用者撥入鑑別服務(remote authentication dial-in user service)
RA	路由器告示(router advertisement)
TCP	傳輸控制協定(transmission control protocol)
TLS	傳送層安全(transport layer security)協定

UDP　使用者資料包協定(user datagram protocol)

URI　統一資源指示符(uniform resource indicator)

UUID　通用唯一識別碼(universally unique identifier)

VLAN　虛擬區域網路(virtual local area network)

5. 符合性測試

5.1 概要

本規範規定之符合性測試適用於依本系列規範第 2-1 部設計、製造、建置之資通訊產品或系統。

待測標的之型式依本系列規範第 2-1 部定義可分為：

(a) 網路交換器。

(b) 代理伺服器。

(c) 物聯網設備。

(d) 網路周邊設備。

(e) 組態伺服器。

(f) 應用伺服器。

執行符合性測試時，應針對待測標的單獨進行測試。

5.2 符合性測試內容

5.2.1 符合性評估

符合性評估將檢視待測標的之規格、型式及功能等是否符合本系列規範第 2-1 部要求，實施方法包含書面資料審查、目測或實地示範演練等。

5.2.2 合規性測試

合規性測試將檢視待測標的之功能及存取介面是否符合本系列規範第 2-1 部要求，執行測試時，應對待測標的實施一系列測試案例。測試範圍包含通訊協定、通訊方法、資料格式及異常處理等，但不包含硬體平臺品牌型號、電氣規格、作業系統種類及版本、執行時期環境、資料儲存媒體形式、開發程式語言、使用者互動介面或資料備援機制等。

合規性測試之目的為確保待測標的符合本系列規範第 2-1 部要求，而非協助受測試單位進行設備開發及除錯(debug)作業。執行合規性測試前，受測試單位應確認待測標的可依本系列規範第 2-1 部要求運作。

5.3 可執行符合性測試之條件

測試單位與受測單位不可為同一組織或屬同一企業，亦不可互相有隸屬關係。

於進行測試前，受測單位應向測試單位提出申請，並提供以下資訊：

(a) 受測單位名稱。

(b) 待測標的名稱或型號。

(c) 待測標的型式(參照 5.1)。

(d) 待測標的組態(例：構成待測標的之硬體、作業系統及軟體版本等)。

(e) 其他有關待測標的之細部說明。

測試單位應依申請資訊，評估待測標的是否適用於本規範。

5.4 符合性測試通過準則

待測標的應滿足以下條件，方可認定為通過符合性測試：

(a) 依本測試要求之符合性評估案例逐一執行評估，所有必備(mandatory)之符合性評估案例皆能出具佐證資料，證明其規格或功能符合本系列規範第 2-1 部要求。

(b) 依本測試要求之合規性測試案例逐一執行測試，所有必備之合規性測試案例皆已執行、所有測試程序皆符合通過條件、且未發生錯誤或故障情況。

6. 測試案例執行方法

6.1 待測標的

待測標的應為實體設備，軟體程式應安裝於硬體設備上，並完成組態設定。其軟體執行環境(包含虛擬機、作業系統及主要軟體框架等)應與實際使用時一致或完全相容，不可使用模擬器(emulator)或其他具相似功能之軟體程式模擬硬體平臺。

所有測試案例皆應針對同一待測標的進行測試。若待測標的於測試過程中受損，則應使用與原始待測標的軟硬體規格完全相同之替代品。若於測試過程中需變更待測標的之部分硬軟體元件，則測試單位可依實際執行狀況評估是否允許其繼續進行測試，或者將其視為不同測試標的，並要求受測試單位重新提出申請。

6.2 測試平臺

6.2.1 場地及環境

測試平臺之地理位置與空間大小無特殊規定，宜選擇空間大小適當、無強烈電磁波干擾、能接收全球定位系統(GPS)信號之場所，並準備必要之工具及設施。

備考：本系列規範第 2-1 部並未規定 GPS 定位功能，但部分設備可能需 GPS 校時信號方能正常運作。

6.2.2 電源供應

測試平臺應提供符合單相三線系統、額定電壓 220V、60Hz 交流電。插座形式與線材額定電流，應符合 CNS 690:2019[1]之直插平刃 2 極接地型 20A-250V(俗稱〝T 型插頭〞)。

受測單位應自行準備延長線等支援器材。若待測標的需使用不同供電規格，則應自行準備電源供應器、電源轉換器或備用電源。

6.2.3 網路連線

測試平臺應提供乙太網路及光纖網路連線，可使用電氣信號或光學信號，規定如下：

(a) 電氣信號：應符合或相容於 100BASE-TX (IEEE 802.3u-1995[5])及 1000BASE-T (IEEE 802.3ab-1999[4])規範，可支援更高傳輸速率。乙太網路纜線應滿足 ANSI/TIA-568 CAT.6 規範，纜線長度不規定。連接端子型式應為 8P8C，內部接線方式應符合 ANSI/TIA-568 之 TIA-568-A 或 TIA-568-B 規範。

(b) 光學信號：應符合或相容於 100BASE-FX (IEEE 802.3u-1995[5])及 1000BASE-SX (IEEE 802.3z-1998[6])規範，可支援更高傳輸速率。測試單位應提供可支援雙股單模(single-mode)及雙股多模(multi-mode)之模組，其他必要耗材(例：光纖纜線及連接頭等)應由受測單位及測試單位預先協議。

區域網路環境及網際網路連線應能支援 IPv4 及 IPv6 雙架構，並能存取網際網路。網際網路連線應設定適當安全防護，並依測試所需調整防火牆之入向/出向規則。

測試單位應管制可接入區域網路之設備。受測單位應預先說明待測標的之網路介面型式及數量，若其他支援工具需使用區域網路，應預先申請。

6.2.4 測試工具

執行合規性測試時，測試單位應設置測試工具，包含網路設備及介面模擬器，如圖 1 所示。介面模擬器之硬體設備、執行環境及軟體程式等，皆依實作而定。

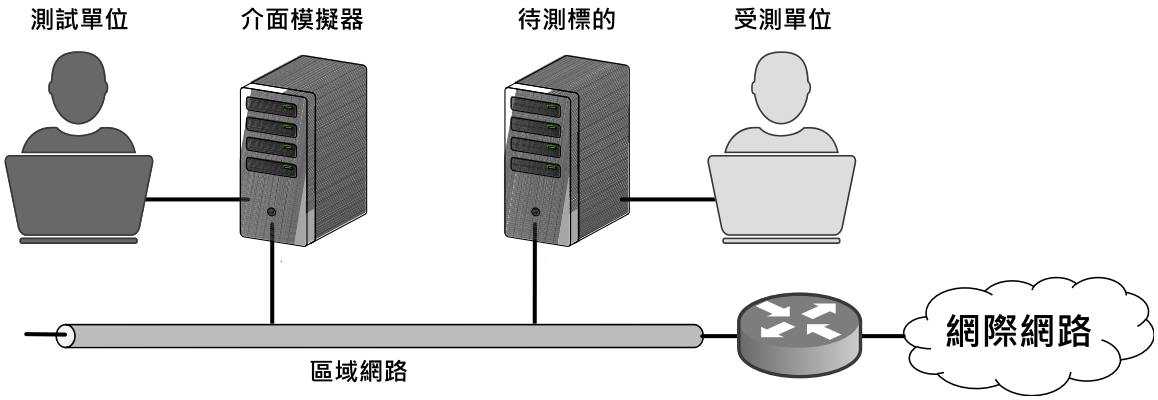


圖 1　測試布局示意圖

6.3 測試案例

執行合規性測試時，測試單位應依待測標的型式逐一執行對應之測試案例，並依測試結果填寫測試結果報告。執行測試時，標示為〝選項〞之測試案例可由受測單位決定是否執行測試，標示為〝有條件必備〞且符合測試案例規定條件之測試案例可略過，其他測試案例宜依各節所列之順序執行。測試單位可依自定順序進行測試，但測試案例應滿足其先決條件，方可執行。

執行測試案例時，標示為〝選項〞且符合各測試案例規定條件之測試程序可省略，其他測試程序應依測試案例列舉之順序執行，不可自定執行順序。每一測試程序應檢視其結果，並依以下規定彙整測試結果：

(a) 若所有測試程序皆符合測試案例之通過條件，則應記錄該測試案例為〝通過〞，並允許繼續執行與該測試案例相關之其他測試案例。

(b) 若測試案例中任何測試程序不符合測試案例之通過條件，則應記錄該測試案例為〝未通過〞。與該測試案例相關之其他測試案例皆不可執行。

(c) 若測試案例未執行，無論其原因，測試單位皆應記錄該測試案例為〝未執行〞。

測試單位可依實際狀況判斷，允許受測單位當場調整待測標的設定，並重新測試同一測試案例。重新測試時，應由該測試案例之測試程序(1)重新開始，不可單獨重複執行特定測試程序。

若故障排除需修改原始程式或重新編譯，則所有已完成之測試案例應視為無效，並重新執行所有測試案例。

7. 網路設備符合性測試

7.1 概述

本節說明網路設備符合性測試之執行方法，僅包含符合性評估，不執行合規性測試。

備考：本節列舉之案例編號中，〝NWE-E〞代表〝network equipment - evaluation〞。

7.2 待測標的

待測標的為構成智慧杆迴路區域網路所有設備之組合，包含設備之品牌、型號及軟硬體版本。

若設備組合中任意項目變更(例：更換不同品牌之 L2 交換器)，則應視為不同待測標的。

7.3 測試內容

進行符合性評估時，可採書面審查或實際操作待測標的以展示組態資訊。測試單位與受測單位應就評估方法達成共識。

7.4 符合性評估

7.4.1 網路設備建置方式

項目編號	NWE-E001	必備/選項	必備
評估標的	網路設備建置方式		
評估方式	● 展示場域建置設計圖，說明設備間堆疊實作方式。 ● 審查產品型錄、說明書、設計規格書或使用設備管理工具展示設備組態資訊。		
通過條件	● 具備至少 1 組可介接網際網路之通訊介面。 ● 具備至少 1 組可介接區域網路之通訊介面。 ● 區域網路介面應為乙太網路，規格應符合本系列規範第 2-1 部 7.2 規定。		
備註	無。		

7.4.2 接線埠存取控制

項目編號	NWE-E002	必備/選項	必備
評估標的	接線埠存取控制		
評估方式	審查產品型錄、說明書、設計規格書或使用設備管理工具展示該設備組態資訊。		
通過條件	● 待測標的應支援接線埠存取控制，鑑別方式應符合本系列規範第 2-1 部 7.4.1 要求。 ● 待測標的應關閉 RADIUS 伺服器功能。		
備註	若待測標的本身不具備 RADIUS 伺服器功能，則視為符合通過條件。		

7.4.3 封包轉發及選徑

項目編號	NWE-E003	必備/選項	必備
評估標的	封包轉發及選徑		
評估方式	審查產品型錄、說明書、設計規格書或使用設備管理工具展示該設備組態資訊。		
通過條件	● 待測標的應具備封包轉發功能，功能規格應符合本系列規範第 2-1 部 7.4.2 規定。 ● 待測標的備應提供 IPv6 路由器告示(IPv6 RA)功能，功能規格應符合本系列規範第 2-1 部 7.4.3 規定。		
備註	無。		

7.4.4 防火牆

項目編號	NWE-E004	必備/選項	必備
評估標的	防火牆		
評估方式	審查產品型錄、說明書、設計規格書或使用設備管理工具展示該設備組態資訊。		
通過條件	待測標的具備防火牆功能，功能規格應符合本系列規範第 2-1 部 7.4.4 規定。		
備註	無。		

7.4.5 虛擬區域網路

項目編號	NWE-E005	必備/選項	有條件必備
評估標的	虛擬區域網路		
評估方式	審查產品型錄、說明書、設計規格書或使用設備管理工具展示該設備組態資訊。		
通過條件	待測標的之虛擬區域網路相關功能應支援 IEEE 802.1Q-2014[2]。		
備註	若待測標的不支援虛擬區域網路功能，則本評估案例可省略。		

8. 代理伺服器符合性測試

8.1 概述

本節說明代理伺服器符合性測試之執行方法，包含符合性評估及合規性測試。

備考： 本節列舉之案例編號中，〝AGS-E〞代表〝agent server - evaluation〞，〝AGS-T〞，代表〝agent server - test〞。

8.2 待測標的

待測標的應為具備代理伺服器功能及互運性存取介面之實體設備，該實體設備之硬體規格及執行環境應與實際產品相同或完全相容。

構成待測標的之硬體元件數量及組合方式不限制，但不可透過網際網路連線將待測功能分散於遠端伺服器。與互運性介面非直接相關之支援功能，可使用簡化方式處理(例：可將鑑別伺服器安裝於支援工具中)。

受測單位應說明於該實體設備上運作之軟體名稱或來源(例：自行開發、使用開源軟體專案或作業系統內建功能)、版本及執行環境。執行環境相關資訊應包含作業系統主要發行版本及其對應之 CPU 指令集架構，以及軟體框架主要發行版本(例：〝Python 3〞或〝Node.js v18〞)。若軟體為不同來源、不同版本，或者軟體框架使用不同主要發行版本，則應視為不同待測標的。

備考： CPU 指令集架構宜使用通用、中立且未指定特定廠牌之名稱(例：〝AMD64〞宜記錄為〝X86-64〞、〝ARMv8-A〞宜記錄為〝AArch64〞)。

8.3 測試方法

8.3.1 測試平臺

執行代理伺服器符合性測試時，應將待測標的設置於測試平臺，並完成組態設定。介面模擬器應模擬物聯網設備，向待測標的發送 DHCP 請求、DNS 查詢請求、mDNS 服務探索及引導登記請求，並檢視其回應。

執行測試時，受測單位可使用支援工具監測運作狀況、設定組態及重設待測標的，但不可協助待測標的執行測試案例。支援工具可連接至待測標的之硬體介面(例：序列埠)或區域網路。

測試單位應調整網路連線環境，使待測標的及支援工具可不受限制存取網際網路 NTP 及 DNS 服務，但不可存取其他網際網路服務。若待測標的或支援工具需使用其他網際網路服務，則應預先說明並取得測試單位同意。

8.3.2 測試平臺組態設定

執行測試前，受測單位應提供組態資訊予測試單位，以設定測試平臺之組態，包含：

(a) 構成待測標的之硬體元件及其功能描述。

(b) 網路介面數量。

(c) (選項)引導登錄存取介面私有憑證之根憑證。

(d) (選項)支援工具介面型式及網際網路連線相關需求。

8.3.3 待測標的組態設定

執行測試前，測試單位應提供組態資訊予受測單位，以設定待測標的之組態，包含：

(a) IPv4 固定位址、子網路遮罩、預設選徑及 DHCPv4 配發網址區段。

(b) IPv6 固定位址、前綴(prefix)位址、預設選徑及 DHCPv6 配發網址區段。

(c) (選項)介面模擬器網路卡硬體位址。

(d) 測試用代理伺服器識別符。

(e) 測試用設備登錄存取介面 URI。

(f) 測試用狀態回報存取介面 URI。

(g) 測試用 HMAC-SHA256 密鑰。

(h) 測試用物聯網設備之鑑別資訊。

備考：IPv4/IPv6 位址數量應符合網路介面數量。

8.3.4 其他應注意事項

若待測標的具備惡意攻擊偵測功能，將連續發生相同錯誤之 HTTPS 客戶端認定為惡意攻擊並限制其連線能力，則該項功能應先關閉。

8.4 符合性評估

8.4.1 TLS 版本

項目編號	AGS-E001	必備/選項	必備
評估標的	TLS 版本		
評估方式	審查產品型錄、說明書、設計規格書或展示該設備組態資訊，或是使用 TLS 客戶端工具測試。		
通過條件	HTTPS 加密連線使用之 TLS 版本應為 1.2 或更新版本。		
備註	無。		

8.5 合規性測試

8.5.1 NTP 自動校時測試

項目編號	AGS-T001	必備/選項	必備
測試名稱	NTP 自動校時測試		
先決條件	無。		
前置作業	待測標的上層 NTP 組態設定為〝time.stdtime.gov.tw〞		
測試程序	(1) 待測標的應依指示完成 IPv6 位址及其他參數設定。 (2) 待測標的應接入測試平臺。 (3) 操作待測標的，執行自動校時。		
通過條件	● 測試程序(2)：確認 L2 交換器網路介面已連線。 ● 測試程序(3)：待測標的之內建時鐘與真實時間差應在 1 秒以內。		
備註	本測試案例應全程使用 IPv6。		

8.5.2 DHCPv6 組態測試

項目編號	AGS-T002	必備/選項	必備
測試名稱	DHCPv6 組態測試		
先決條件	無。		
前置作業	● 待測標的應依指示完成網路參數設定。 ● 待測標的應接入測試平臺，確認網路介面已連線並完成組態設定。 ● 待測標的應完成時間校正，與實際時間差應在 1 秒以內。		
測試程序	(1) 介面模擬器使用 DHCPv6 向待測標的取得網路組態設定。 (2) 檢視介面模擬器接收之 IP 位址設定。 (3) 檢視介面模擬器接收之 DNS 位址設定。 (4) 檢視介面模擬器接收之搜尋域名(search domain)設定。 (5) (選項)檢視介面模擬器接收之 NTP 位址設定。		
通過條件	● 測試程序(2)：配發之 IP 位址應符合待測標的預先設定組態。 ● 測試程序(3)：預設選徑位址應符合待測標的預先設定組態。 ● 測試程序(4)：搜尋域名應包含 FQDN 之頂級域及二級域，其中頂級域可為任意自訂字串。 ● 測試程序(5)：若 DHCP 回應包含 NTP 參數，則該參數應包含待測標的網路介面之 IP 位址。		
備註	● 本測試案例應全程使用 IPv6。 ● 若 DHCP 回應未包含 NTP 參數，則測試程序(5)可省略。 ● 若待測標的具有多組網路介面，則 DNS 參數及 NTP 參數可為待測標的中任意網路介面位址。 ● 應記錄測試程序(4)取得之搜尋域名，以備後續測試使用。		

8.5.3 DNS 查詢測試

項目編號	AGS-T003	必備/選項	必備
測試名稱	DNS 查詢測試		
先決條件	● 應完成測試案例 AGS-T002。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T002。		
前置作業	● 待測標的應清除所有 DNS 暫存紀錄。 ● 確認測試平臺可存取常用公開 DNS 伺服器，包含標準 DNS 查詢協定(TCP/UDP 埠 53)及 DNS-over-HTTPS 服務(TCP 埠 443)，連線目的地位址及網域不限。		
測試程序	(1) 使用介面模擬器，向測試 AGS-T002 中取得之 DNS 伺服器位址發送符合 IETF/RFC 1035 規範之域名解析請求，傳輸協定為 UDP 埠 53，域名解析標的為〝time.stdtime.gov.tw.〞，查詢種類包含〝A〞及〝AAAA〞。 (2) 檢視 DNS 查詢之回應。 (3) 介面模擬器同時向常用公開 DNS 伺服器發送相同查詢，並等候回應。 (4) 比對測試程序(2)與測試程序(3)之回應。		
通過條件	● 測試程序(2)：待測標的應回應包含最終域名解析結果之紀錄。 ● 測試程序(2)與測試程序(3)回應之最終域名解析結果應一致。		
備註	● 本測試案例應全程使用 IPv6。 ● 常用公開 DNS 位址可參考本系列規範第 2-1 部 D.2。		

8.5.4 mDNS 服務探詢測試(一)

項目編號	AGS-T004	必備/選項	必備
測試名稱	mDNS 服務探詢測試(一)		

先決條件	● 應完成測試案例 AGS-T003。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T002。
前置作業	無。
測試程序	(1) 使用介面模擬器發送 mDNS 查詢，查詢標的為〝_ntp._udp〞服務。 (2) 接收 mDNS 回應並檢視回應內容。 (3) 使用測試程序(2)回應內容之 FQDN，向測試 AGS-T002 取得之 DNS 伺服器位址發送域名解析查詢請求。 (4) 檢視域名解析查詢結果。
通過條件	● 測試程序(2)：回應內容應包含 FQDN，域名應符合 AGS-T002 取得之搜尋域名。 ● 測試程序(4)：域名解析查詢結果應符合待測標的之網路介面 IP 位址。
備註	● 本測試案例應全程使用 IPv6。 ● 應記錄測試程序(4)取得之 IP 位址，以備後續測試使用。

8.5.5 mDNS 服務探詢測試(二)

項目編號	AGS-T005	必備/選項	必備
測試名稱	mDNS 服務探詢測試(二)		
先決條件	● 應完成測試案例 AGS-T003。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T002。		
前置作業	無。		
測試程序	(1) 使用介面模擬器發送 mDNS 查詢，查詢標的為〝_bootstrap._sub._http._tcp〞服務。 (2) 接收 mDNS 回應並檢視回應內容。 (3) 使用測試程序(2)回應內容之 FQDN，向測試 AGS-T002 取得之 DNS 伺服器位址發送域名解析查詢請求。 (4) 檢視域名解析查詢結果。		
通過條件	● 測試程序(2)：回應內容應包含 FQDN，域名應符合 AGS-T002 取得之搜尋域名。 ● 測試程序(4)：域名解析查詢結果應符合待測標的之網路介面 IP 位址。		
備註	● 本測試案例應全程使用 IPv6。 ● 應記錄測試程序(2)回應內容之〝TXT〞紀錄及 FQDN，以備後續測試使用。		

8.5.6 NTP 伺服器測試

項目編號	AGS-T006	必備/選項	必備
測試名稱	NTP 伺服器測試		
先決條件	● 應完成測試案例 AGS-T004。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T002。		
前置作業	測試單位應另行準備一組 NTP 客戶端工具作為對照組，直接由公開 NTP 伺服器校時。		
測試程序	(1) 介面模擬器執行 NTP 客戶端工具發送校時請求，目的地位址為 AGS-T004 測試程序(3)取得之位址。 (2) 檢視回應，比對介面模擬器及對照組時間差。		
通過條件	● 測試程序(2)：顯示回應與對照組時間差應為合理數值，於網際網路連線速度正常時，顯示回應與對照組時間差應在 1 秒以內。		
備註	● 本測試案例應全程使用 IPv6。 ● 公開 NTP 伺服器應使用〝time.stdtime.gov.tw〞或〝2.tw.pool.ntp.org〞。		

8.5.7 引導登錄測試

項目編號	AGS-T007	必備/選項	必備
測試名稱	引導登錄測試		
先決條件	● 應完成測試案例 AGS-T005。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T002。		
前置作業	確認待測標的已完成組態設定，包含：組態伺服器 URI、鑑別資訊及 HMAC-SHA256 密鑰。		
測試程序	(1) 介面模擬器依規定正常程序發送引導登錄請求，標的 URI 應由 AGS-T005 執行程序(2) mDNS 服務探詢回應之紀錄內容產生。 (2) 介面模擬器檢視待測標的回應。 (3) 使用預先設定之 HMAC-SHA256 密鑰查證回應本體中〝credCfg〞參數之數位簽章。 (4) 等候 1 分鐘，重新執行測試程序(1)～(3)。		
通過條件	● 測試程序(2)：回應狀態碼應為 200，回應本體之內容格式應符合本系列規範第 2-1 部 8.4.3 規定，回應本體內容之參數應符合如下規定： ♦ 〝registrator〞參數：應符合預先設定組態之設備登錄存取介面 URI。 ♦ 〝watchdog〞參數：應符合預先設定組態之狀態回報存取介面 URI。 ♦ 〝credCfg〞參數：依 IETF/RFC 7519 規定進行解碼，標頭及酬載參數應符合本系列規範第 2-1 部 A.2 格式，物聯網設備識別符及代理伺服器識別符應符合預先設定之組態。 ● 測試程序(3)：數位簽章應通過 HMAC-SHA256 密鑰查證。 ● 測試程序(4)：重新執行時各測試程序之通過條件相同，但〝credCfg〞參數標頭之〝iat〞參數及數位簽章應不同。		
備註	● 本測試案例應全程使用 IPv6。 ● URI 應使用 mDNS 回應之 FQDN 作為域名，以及〝TXT〞記錄作為路徑，參照本系列標準第 2-1 部 9.3.1.5。 ● 若 AGS-T005 回應包含多筆紀錄，則應挑選第 1 筆回應之紀錄執行本測試。		

8.5.8 多重引導登錄存取介面測試

項目編號	AGS-T008	必備/選項	選項
測試名稱	多重引導登錄存取介面測試		
先決條件	● 應完成測試案例 AGS-T007。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T002。		
前置作業	無。		
測試程序	(1) 重複執行 AGS-T007 測試程序(1)～(3)，但標的 URI 選取 mDNS 服務探詢回應之第 2 筆紀錄進行測試。 (2) 重複測試程序(1)，每次選取 mDNS 服務探詢回應之下一筆紀錄進行測試，直到 mDNS 服務探詢回應之所有紀錄皆完成測試。		
通過條件	與測試案例 AGS-T007 相同。		
備註	● 僅具備單一網路介面之待測標的不執行本測試案例。 ● 具多網路介面之待測標的可選項的執行本測試案例。 ● 本測試案例應全程使用 IPv6。 ● 執行本測試案例時，應調整待測標的，使其回應多筆 mDNS 查詢結果紀錄。		

8.5.9 引導登錄異常測試

項目編號	AGS-T009	必備/選項	必備
測試名稱	引導登錄異常測試		
先決條件	● 應完成測試案例 AGS-T007。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T002。		
前置作業	無。		
測試程序	(1) 介面模擬器對待測標的發送引導登錄請求，但使用非加密 HTTP 連線，連線標的通訊埠為 80。 (2) 介面模擬器對待測標的發送引導登錄請求，但使用 HTTP 版本為 HTTP/1.0。 (3) 介面模擬器對待測標的發送引導登錄請求，但使用方法為〝POST〞。 (4) 介面模擬器對待測標的發送引導登錄請求，但使用方法為〝PUT〞。 (5) 介面模擬器對待測標的發送引導登錄請求，但使用方法為〝PATCH〞。 (6) 介面模擬器對待測標的發送引導登錄請求，但使用方法為〝DELETE〞。 (7) 介面模擬器對待測標的發送引導登錄請求，但 URI 路徑為隨機路徑。 (8) (有條件必備)介面模擬器對待測標的發送引導登錄請求，但擷取完整路徑之上層目錄及根目錄作為 URI。 (9) 介面模擬器對待測標的發送引導登錄請求，但〝Host〞標頭欄位使用 IP 位址。 (10) 介面模擬器對待測標的發送引導登錄請求，但不使用請求字串。 (11) 介面模擬器對待測標的發送引導登錄請求，但請求字串之〝id〞參數為空字串。 (12) 介面模擬器對待測標的發送引導登錄請求，但不包含鑑別資訊。 (13) 介面模擬器對待測標的發送引導登錄請求，但使用錯誤鑑別資訊。 (14) 介面模擬器對待測標的發送引導登錄請求，但鑑別型式為〝Bearer〞，鑑別資訊為隨機數。		
通過條件	● 測試程序(1)：應拒絕連線。 ● 測試程序(2)：應回應狀態碼 426。 ● 測試程序(3)～(6)：應回應狀態碼 405。 ● 測試程序(7)及(8)：應回應狀態碼 404。 ● 測試程序(9)：應拒絕連線、顯示 TLS 連線異常或回應狀態碼 404。 ● 測試程序(10)及(11)：應回應狀態碼 400。 ● 測試程序(12)～(14)：應回應狀態碼 401。		
備註	● 本測試案例應全程使用 IPv6。 ● 若引導登錄存取介面 URI 路徑為根目錄，則測試程序(8)可省略。		

8.5.10 DHCP 一致性測試

項目編號	AGS-T010	必備/選項	有條件必備
測試名稱	DHCP 一致性測試		
先決條件	應完成測試案例 AGS-T002。		
前置作業	應準備另一具備乙太網路之電腦，該電腦應未接入測試平臺		
測試程序	(1) 介面模擬器中斷乙太網路連線，清除 IP 設定及快取資料。 (2) 停止待測標的電源供應，等候直到待測標的完全停止運作。 (3) 重新恢復電源供應待測標的，等候直到待測標的恢復運作。 (4) 將另一電腦接入測試平臺乙太網路，並透過 DHCP 取得 IP 位址。 (5) 等候 1 分鐘。 (6) 介面模擬器重新接入測試平臺乙太網路並透過 DHCP 取得 IP。 (7) 檢視介面模擬器取得之 IP 位址。		
通過條件	測試程序(7)：介面模擬器重新取得 IP 位址應與 AGS-T002 結果相同。		

備註	● 若待測標的應預先登錄介面模擬器網路卡硬體位址(MAC Address)，則本測試案例可省略。 ● 本測試案例應全程使用 IPv6。

8.5.11 DHCPv4 組態測試

項目編號	AGS-T011	必備/選項	必備
測試名稱	DHCPv4 組態測試		
先決條件	應完成測試案例 AGS-T002。		
前置作業	待測標的應完成所有 IPv4 相關設定。		
測試程序	(1) 介面模擬器使用 DHCPv4 向待測標的取得網路組態設定。 (2) 檢視介面模擬器接收之 IP 位址設定。 (3) 檢視介面模擬器接收之預設閘道器位址設定。 (4) 檢視介面模擬器接收之 DNS 位址設定。 (5) 檢視介面模擬器接收之搜尋域名設定。 (6) (選項)檢視介面模擬器接收之 NTP 位址設定。		
通過條件	● 測試程序(2)：配發之 IP 位址應符合待測標的預先設定組態。 ● 測試程序(3)：預設選徑位址應符合待測標的預先設定組態。 ● 測試程序(4)：DNS 位址應符合待測標的預先設定組態。 ● 測試程序(5)：搜尋域名應包含 FQDN 之頂級域及二級域，其中頂級域可為任意自訂字串。 ● 測試程序(6)：若 DHCP 回應包含 NTP 參數，則該參數應包含待測標的網路介面之 IP 位址。		
備註	● 本測試案例應全程使用 IPv4。 ● 若 DHCP 回應未包含 NTP 參數，則測試程序(6)可省略。		

8.5.12 IPv4 相容性測試

項目編號	AGS-T012	必備/選項	必備
測試名稱	IPv4 相容性測試		
先決條件	● 應完成測試案例 AGS-T011。 ● 若介面模擬器取得之 DHCP 組態已逾時，則應重新執行 AGS-T0011。		
前置作業	與 AGS-T003、AGS-T004、AGS-T005、AGS-T006 及 AGS-T007 之前置作業相同。		
測試程序	(1) 執行測試 AGS-T003，但使用 IPv4。 (2) 執行測試 AGS-T004，但使用 IPv4。 (3) 執行測試 AGS-T005，但使用 IPv4。 (4) 執行測試 AGS-T006，但使用 IPv4。 (5) 執行測試 AGS-T007，但使用 IPv4。		
通過條件	與 AGS-T003、AGS-T004、AGS-T005、AGS-T006 及 AGS-T007 之通過條件相同。		
備註	● 本測試案例應全程使用 IPv4。 ● 介面模擬器應使用 DNS 查詢結果之 IPv4 位址相關紀錄。		

9. 物聯網設備符合性測試

9.1 概述

本節說明代理伺服器符合性測試之執行方法，包含符合性評估及合規性測試。

備考： 本節列舉之案例編號中，〝ITE-E〞代表〝IoT equipment - evaluation〞，〝ITE-T〞，代

表〝IoT equipment - test〞。

9.2 待測標的

待測標的應為具備物聯網設備互運性存取介面之實體設備，該實體設備之硬體規格及執行環境應與實際產品相同或完全相容。

構成待測標的之硬體元件數量及組合方式不限制，但不可透過網際網路連線將待測功能分散於遠端伺服器。

受測單位應說明於該實體設備上運作之軟體名稱或來源(例：自行開發、開源軟體專案或作業系統內建功能)、版本及執行環境。執行環境應提供之資訊依以下規定：

(a) 若硬體未使用作業系統或僅使用實時作業系統(real-time operating system, RTOS)，則應提供其硬體之型號及版本。

(b) 若硬體包含作業系統，則應提供其作業系統主要發行版本及其對應之 CPU 指令集架構，以及軟體框架主要發行版本(例：〝Python 3〞或〝Node.js v18〞)。

若軟體程式為不同來源、不同版本，或者執行環境不同，則應視為不同待測標的。

9.3 測試方法

9.3.1 測試平臺

執行物聯網設備符合性測試時，應將待測標的設置於測試平臺，並完成組態設定。介面模擬器應模擬代理伺服器及組態伺服器，回應待測標的發送之 802.1X[3]鑑別請求、DHCP 請求、DNS 查詢請求、mDNS 服務探索請求、引導登錄請求、設備登錄請求及狀態回報請求，並檢視其回應。模擬代理伺服器與模擬組態伺服器應使用不同 IP 位址。

測試平臺之區域網路應設定接線埠存取控制。待測標的接入測試平臺之區域網路時，應先通過 802.1X[3]鑑別後，方可啟用接線埠。

執行測試時，受測單位可使用支援工具監測運作狀況、設定組態及重設待測標的，但不可協助待測標的執行測試案例。支援工具可連接至待測標的之硬體介面(例：序列埠)或區域網路，接入區域網路時，其接線埠不需設定存取控制。

測試單位應調整網路設備，使待測標的及支援工具可不受限制存取網際網路 NTP 及 DNS 服務，但不可存取其他網際網路服務。若待測標的或支援工具需使用其他網際網路服務，則應預先說明並取得測試單位同意。

9.3.2 測試平臺組態設定

執行測試前，測試單位應提供組態資訊予受測單位，以設定待測標的之組態，包含：

(a) 構成待測標的之硬體元件及其功能描述。

(b) (選項)支援工具介面型式及網路連線相關需求。

(c) 802.1X[3]支援鑑別方式(EAP-MD5、EAP-TTLS、PEAPv0 或其他方式)。

9.3.3 待測標的組態設定

執行測試前，測試單位應提供組態資訊予受測單位，以設定待測標的之組態，包含：

(a) 設備識別符。

(b) 802.1X[3]鑑別資訊(憑證或帳號及通行碼)。

(c) 引導登錄鑑別資料(帳號及通行碼)。

9.3.4 時間相關之組態設定

受測單位應說明待測標的之時間相關組態，包含：

(a) 服務探詢及引導登錄重試(retry)等候時間。

(b) 引導登錄重試次數或時間上限。

(c) HTTPS 重送(resend)等候時間。

(d) HTTPS 重送次數上限。

(e) 設備登錄之重試等候時間。

(f) 設備登錄之重試次數或時間上限。

(g) 執行測試程序之最長等候時間。

執行測試時，所有測試程序之等候時間、重送次數上限、重試次數或時間上限等，應符合以上組態資訊，可容許誤差±5 秒以內。若待測標的超過以上組態資訊中最長之等候時間但仍未開始執行下一測試程序，則應視為測試案例未通過。

備考 1. 為加速測試進行，受測單位宜調整待測標的之時間相關組態如下：

(a) 狀態回報週期(設備登錄請求之〝heartbeat〞參數)：1 分鐘。

(b) HTTPS 重送等候時間：5 秒。

(c) HTTPS 重送次數上限：3 次。

(d) 服務探詢、引導登錄及設備登錄重試等候時間：1 分鐘。

(e) 引導登錄及設備登錄重試次數或時間上限：10 次(或 10 分鐘)。

備考 2. 受測單位可調整待測標的(例：變更作業系統組態或重新編譯程式)以設定時間相關組態，但應向測試單位說明調整範圍。

9.4 產品符合性評估

9.4.1 人工設定網路組態

項目編號	ITE-E001	必備/選項	必備
評估標的	人工設定網路組態		
評估方式	審查產品型錄、說明書、設計規格書或展示該設備組態資訊。		
通過條件	確認待測標的具備人工設定網路組態之功能		
備註	無。		

9.4.2 TLS 版本

項目編號	ITE-E002	必備/選項	必備
評估標的	TLS 版本		
評估方式	審查產品型錄、說明書、設計規格書或展示該設備組態資訊，或使用 TLS 客戶端工具測試。		
通過條件	HTTPS 加密連線使用之 TLS 版本應為 1.2 或更新版本。		
備註	無。		

9.5 產品合規性測試

9.5.1 異常程序測試(一)

項目編號	ITE-T001	必備/選項	必備
測試名稱	異常程序測試(一)：HTTP 客戶端及引導登錄異常		
先決條件	無。		
前置作業	● 確認測試平臺已正確設定所有組態。 ● 確認待測標的已正確設定，包含 802.1X[3]及引導登錄之鑑別資訊。		
測試程序	(1) 啟動或重設待測標的，並接入測試平臺乙太網路介面。 (2) 等候待測標的發送 mDNS 查詢，介面模擬器不回應。 (3) 介面模擬器等等候待測標的發送 mDNS 查詢，並依正常程序回應，查詢結果包含單一引導登錄存取介面相關資訊。 (4) 介面模擬器等等候待測標的發送引導登錄請求，介面模擬器回應狀態碼 500。 (5) 重複執行測試程序(4)，直到待測標的停止重送 HTTPS 請求。 (6) 重複執行測試程序(3)。 (7) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (8) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 401。 (9) 介面模擬器等候待測標的發送引導登錄請求，並回應狀態碼 401。 (10) 重複執行測試程序(3)。 (11) 重複測試程序(9)及測試程序(10)，直到待測標的停止發送引導登錄請求。 (12) 檢視待測標的之系統時間，受測單位可使用支援工具展示待測標的系統時間，或者檢視 HTTP 請求標頭之〝Date〞欄位。		
通過條件	● 待測標的發出之引導登錄請求封包應符合本系列規範第 2-1 部 9.4.1 規定。 ● 待測標的發出之設備登錄請求封包應符合本系列規範第 2-1 部 9.5.1 規定。 ● 測試程序(1)：應檢視網路設備或 RADIUS 紀錄，若待測標的未成功接入，則應視為測試案例未通過。 ● 測試程序(2)：mDNS 查詢之具名服務應為〝_bootstrap._sub._http._tcp〞。 ● 測試程序(5)：待測標的達 HTTP 重送次數上限後，應停止重送。 ● 測試程序(7)：引導登錄請求之 URL 應與 mDNS 查詢結果一致。 ● 測試程序(8)：設備登錄請求之 URL 應與引導登記回應封包內容一致。 ● 測試程序(9)：引導登錄請求之 URL 應與 mDNS 查詢結果一致。 ● 測試程序(11)：待測標的達重試次數或時間上限後，應停止後續運作。 ● 測試程序(12)：系統時間與實際時間差異應為合理值，直接展示系統時間時，時間差應在 1 秒內。若 HTTP 請求標頭內包含〝Date〞欄位時，則該欄位內容與介面模擬器接收該次請求之時間差應在 3 秒內。		
備註	● 本測試案例應全程使用 IPv6。 ● HTTP 請求標頭之〝Date〞欄位為非必備欄位，若待測標的發送之 HTTP 請求標頭未包含〝Date〞欄位，則受測單位使用支援工具以顯示系統時間。		

9.5.2 異常程序測試(二)

項目編號	ITE-T002	必備/選項	必備
測試名稱	異常程序測試(二)：HTTP 客戶端及設備登錄異常		
先決條件	應完成測試案例 ITE-T001。		
前置作業	重設待測標的之啟用網路服務程序，或完全重設待測標的。		
測試程序	(1) 重新執行待測標的之引導登錄程序，或完全重設待測標的並重新接入區域網路。 (2) 介面模擬器等候待測標的發送 mDNS 查詢，並依正常程序回應，查詢結果包含單一引導登錄存取介面相關資訊。 (3) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。		

	(4) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 503，〝Retry-After〞標頭欄位指定等候時間為 10 秒。 (5) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 307，〝Location〞標頭欄位應填入不同之任意 URI。 (6) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 404。 (7) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (8) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 401。 (9) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (10) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 403。 (11) 檢視待測標的狀態。
通過條件	● 待測標的發出之引導登錄請求封包應符合本系列規範第 2-1 部 9.4.1 規定。 ● 待測標的發出之設備登錄請求封包應符合本系列規範第 2-1 部 9.5.1 規定。 ● 測試程序(4)及(5)：待測標的應等候 10 秒再重送相同請求。 ● 測試程序(6)：請求封包之 URI 應符合測試程序(5)回應之〝Location〞標頭欄位內容。 ● 測試程序(8)：請求封包之 URI 應符合 mDNS 查詢結果。 ● 測試程序(11)：待測標的應停止執行啟用網路服務程序。
備註	本測試案例應全程使用 IPv6。

9.5.3 設備登錄程序測試

項目編號	ITE-T003	必備/選項	必備
測試名稱	設備登錄程序測試		
先決條件	應完成測試案例 ITE-T002。		
前置作業	清除待測標的啟用網路服務程序，或完全重設待測標的。		
測試程序	(1) 重新執行 ITE-T002 測試程序(1)及(2)。 (2) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (3) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 201。 (4) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 201。 (5) 重複測試程序(4)，共 20 次。 (6) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 418。 (7) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 201。		
通過條件	● 待測標的發出之引導登錄請求封包應符合本系列規範第 2-1 部 9.4.1 規定。 ● 待測標的發出之設備登錄請求封包應符合本系列規範第 2-1 部 9.5.1 規定。 ● 待測標的發出之狀態回報請求封包應符合本系列規範第 2-1 部 9.6.1 規定。 ● 測試程序(4)～(7)：狀態回報請求封包之陣列內容(包含陣列大小及各元素內容之〝id〞參數)應與測試程序(3)設備登錄請求之應用服務(包含〝priApp〞及〝extApp〞參數)一致。 ● 測試程序(5)：狀態回報週期(period)應不大於測試程序(3)設備登錄請求之〝heartbeat〞參數內容，可容許誤差為 5 秒以內。 ● 測試程序(6)與測試程序(7)：間隔時間應不大於測試程序(3)設備登錄請求之〝heartbeat〞參數內容，可容許誤差為 5 秒以內。		
備註	本測試案例應全程使用 IPv6。		

9.5.4 組態變更測試

項目編號	ITE-T004	必備/選項	有條件必備
測試名稱	組態變更測試		
先決條件	應完成測試案例 ITE-T003。		

前置作業	若完成 ITE-T003 後，待測標的曾重設、重新啟動或中斷乙太網路連線，則應重新執行 ITE-T003 測試程序(1)～(3)。
測試程序	(1) 操作待測標的，執行組態變更。 (2) 介面模擬器等候待測標的發送設備登錄請求，並依正常程序發送回應狀態碼 201。
通過條件	● 待測標的發出之設備登錄請求封包應符合本系列規範第 2-1 部 9.5.1 規定。 ● 測試程序(2)：設備登錄請求之〝updateTime〞參數應與 ITE-T005 不同。
備註	● 若待測標的具備多應用服務，且應用服務可於部署後調整，則應執行本測試案例。 ● 若待測標的僅具備單一應用服務，或者應用服務皆為固定不可變更，則可選項的執行本測試案例。 ● 本測試案例應全程使用 IPv6。 ● 受測單位可使用支援工具操作待測標的以進行本測試案例(例：變更應用服務、變更設備授權存取介面 URI 等)。

9.5.5 異常程序測試(三)

項目編號	ITE-T005	必備/選項	必備
測試名稱	異常程序測試(三)：HTTP 客戶端及狀態回報異常		
先決條件	應完成測試案例 ITE-T003。		
前置作業	若完成 ITE-T003 後，待測標的曾重設、重新啟動或中斷乙太網路連線，則應重新執行 ITE-T003 測試程序(1)～(3)。		
測試程序	(1) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 500。 (2) 重複執行測試程序(1)，直到待測標的停止重發。 (3) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 502。 (4) 重複執行測試程序(3)，直到待測標的停止重發。 (5) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 504。 (6) 重複執行測試程序(5)，直到待測標的停止重發。 (7) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 429，〝Retry-After〞標頭欄位指定等候時間為 5 秒。 (8) 重複執行測試程序(7)，直到待測標的停止重發。 (9) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 503，〝Retry-After〞標頭欄位指定時間為 10 秒。 (10) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 201。		
通過條件	● 待測標的發出之狀態回報請求封包應符合本系列規範第 2-1 部 9.6.1 規定，其內容應保持一致。 ● 測試程序(2)：HTTPS 重送時間間隔及重送次數應符合時間相關組態設定。 ● 測試程序(2)與(3)：時間間隔應不大於 ITE-T003 設備登錄請求之〝heartbeat〞參數內容，可容許誤差為 5 秒以內。 ● 測試程序(3)：狀態回報請求封包不可與測試程序(1)中介面模擬器接收之封包完全相同。 ● 測試程序(4)：HTTPS 重送時間間隔及重送次數應符合時間相關組態設定。 ● 測試程序(4)與(5)：時間間隔應不大於 ITE-T003 設備登錄請求之〝heartbeat〞參數內容，可容許誤差為 5 秒以內。 ● 測試程序(5)：狀態回報請求封包不可與測試程序(3)中介面模擬器接收之封包完全相同。 ● 測試程序(6)：HTTPS 重送時間間隔及重送次數應符合時間相關組態設定。 ● 測試程序(6)與(7)：時間間隔應不大於 ITE-T003 設備登錄請求之〝heartbeat〞參數內容，可容許誤差為 5 秒以內。 ● 測試程序(7)：狀態回報請求封包不可與測試程序(5)中介面模擬器接收之封包完全		

	相同。 ● 測試程序(7)與(8)：HTTPS 重送時間間隔應為 5 秒，重送次數應符合時間相關組態設定。 ● 測試程序(8)與(9)：時間間隔應不大於 ITE-T003 設備登錄請求之〝heartbeat〞參數內容，可容許誤差為 5 秒以內。 ● 測試程序(9)：狀態回報請求封包不可與測試程序(7)中介面模擬器接收之封包完全相同。 ● 測試程序(9)與(10)：HTTPS 重送時間間隔應為 10 秒，。 ● 測試程序(10)：請求內容應與測試程序(9)相同。
備註	本測試案例應全程使用 IPv6。

9.5.6 異常程序測試(四)

項目編號	ITE-T006	必備/選項	必備
測試名稱	異常程序測試(四)：狀態回報異常		
先決條件	應完成測試案例 ITE-T003。		
前置作業	若完成 ITE-T003 後，待測標的曾重設、重新啟動或中斷乙太網路連線，則應重新執行 ITE-T003 測試程序(1)～(3)。		
測試程序	(1) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 307，〝Location〞標頭欄位應填入不同之任意 URI，〝Retry-After〞標頭欄位指定等候時間為 10 秒。 (2) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 401。 (3) 介面模擬器等候待測標的發送引導登錄請求，並回應狀態碼 418。 (4) 重複測試程序(3)，直到經過時間大於回報週期。 (5) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (6) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 308，〝Location〞標頭欄位應填入不同之任意 URI。 (7) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (8) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 404。 (9) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (10) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 201。		
通過條件	● 待測標的發出之引導登錄請求封包應符合本系列規範第 2-1 部 9.4.1 規定。 ● 待測標的發出之狀態回報請求封包應符合本系列規範第 2-1 部 9.6.1 規定，其請求內容應保持一致。 ● 測試程序(1)與測試程序(2)：時間間隔應符合〝Retry-After〞標頭欄位指定時間。 ● 測試程序(2)：請求封包之 URI 應符合測試程序(1)回應之〝Location〞標頭欄位。 ● 測試程序(4)：待測標的於執行引導登錄期間，不可發送狀態回報請求。 ● 測試程序(7)：待測標的發送之封包應為引導登錄請求，不可發送狀態回報請求。		
備註	● 本測試案例應全程使用 IPv6。 ● 物聯網設備不使用狀態碼 308 回應之〝Location〞標頭欄位進行重新導向，參照第 2-1 部 9.6.2 規定。		

9.5.7 異常程序測試(五)

項目編號	ITE-T007	必備/選項	必備
測試名稱	異常程序測試(五)：狀態回報異常及設備登錄		
先決條件	應完成測試案例 ITE-T003。		
前置作業	若完成 ITE-T003 後，待測標的曾重設、重新啟動或中斷乙太網路連線，則應重新執行 ITE-T003 測試程序(1)～(3)。		
測試程序	(1) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 403。		

	(2) (選項)等候待測標的發送引導登錄請求，介面模擬器依正常程序發送引導登錄回應。 (3) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 201。 (4) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 201。
通過條件	● 待測標的發出之引導登錄請求封包應符合本系列規範第 2-1 部 9.4.1 規定。 ● 待測標的發出之設備登錄請求封包應符合本系列規範第 2-1 部 9.5.1 規定。 ● 待測標的發出之狀態回報請求封包應符合本系列規範第 2-1 部 9.6.1 規定，其陣列內容(包含陣列大小及各元素內容之〝id〞參數)應與設備登錄請求之應用服務(包含〝priApp〞及〝extApp〞參數)一致。
備註	● 本測試案例應全程使用 IPv6。 ● 待測標的可跳過測試程序(2)，直接執行測試程序(3)。

9.5.8 重新啟用交換器接線埠測試

項目編號	ITE-T008	必備/選項	必備
測試名稱	重新啟用交換器接線埠測試		
先決條件	應完成測試案例 ITE-T003。		
前置作業	若完成 ITE-T003 後，待測標的曾重設、重新啟動或中斷乙太網路連線，則應重新執行 ITE-T003 測試程序(1)～(3)。		
測試程序	(1) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 201。 (2) 移除待測標的乙太網路連線。 (3) 設定測試平臺，重設交換器接線埠存取控制。 (4) 重新接入待測標的。 (5) 介面模擬器等候待測標的發送狀態回報請求，並回應狀態碼 201。		
通過條件	待測標的發出之狀態回報請求封包應符合本系列規範第 2-1 部 9.6.1 規定。		
備註	● 本測試案例應全程使用 IPv6。 ● 介面模擬器於測試期間應維持 DHCP 一致性，配發相同 IP 位址。		

9.5.9 多重引導登錄存取介面測試

項目編號	ITE-T009	必備/選項	必備
測試名稱	多重引導登錄存取介面測試。		
先決條件	應完成測試案例 ITE-T001。		
前置作業	重設待測標的之啟用網路服務程序，或完全重設待測標的。		
測試程序	(1) 重新執行待測標的之引導登錄程序，或完全重設待測標的並重新接入區域網路。 (2) 介面模擬器等候待測標的發送 mDNS 查詢，並依正常程序回應，查詢結果包含 3 組紀錄，各自對應不同 URI。 (3) 介面模擬器等候待測標的發送引導登錄請求，並回應狀態碼 429。 (4) 重複測試程序(3)，直到待測標的停止重新發送。 (5) 介面模擬器等候待測標的發送引導登錄請求，並回應狀態碼 502。 (6) 重複測試程序(5)，直到待測標的停止重新發送。 (7) 介面模擬器等候待測標的發送引導登錄請求，並依正常程序發送引導登錄回應。 (8) 介面模擬器等候待測標的發送設備登錄請求，並回應狀態碼 403。 (9) 檢視待測標的狀態。		
通過條件	● 測試程序(3)：請求封包之 URI 應符合測試程序(2)回應，可為任意順序。 ● 測試程序(5)：請求封包之 URI 應與測試程序(3)不同，URI 應符合測試程序(2)回應，可為任意順序。 ● 測試程序(7)：請求封包之 URI 應與測試程序(3)及(5)不同，URI 應符合測試程序		

	(2)回應，可為任意順序。 ● 測試程序(8)：設備登錄請求之 URI 應與測試程序(7)引導登錄回應封包內容一致。 ● 測試程序(9)：待測標的應停止執行啟用網路服務程序。
備註	● 本測試案例應全程使用 IPv6。 ● 待測標的可選項的使用多執行緒實作，並同步執行測試程序(3)、(5)及(7)。介面模擬器宜實作工作佇列(task queue)或類似機制，於首次及第 2 次接收請求時回應異常狀態碼，並於第 3 次接收請求時依正常程序執行。

9.5.10 異常程序測試(六)

項目編號	ITE-T010	必備/選項	必備
測試名稱	異常程序測試(六)：多重介面異常測試		
先決條件	應完成 ITE-T009。		
前置作業	重設待測標的之啟用網路服務程序，或完全重設待測標的。		
測試程序	(1) 重新執行待測標的之引導登錄程序，或完全重設待測標的並重新接入區域網路。 (2) 介面模擬器等候待測標的發送 mDNS 查詢，並依正常程序回應，查詢結果包含 3 組紀錄，各自對應不同 URI。 (3) 介面模擬器等候待測標的發送引導登錄請求，並回應狀態碼 418。 (4) 介面模擬器等候待測標的發送引導登錄請求，並回應狀態碼 418。 (5) 介面模擬器等候待測標的發送引導登錄請求，並回應狀態碼 418。 (6) 重複測試程序(2)～(5)，直到待測標的停止引導登錄請求封包。 (7) 檢視待測標的狀態。		
通過條件	● 測試程序(3)：請求封包之 URI 應符合測試程序(2)回應，可為任意順序。 ● 測試程序(4)：請求封包之 URI 應與測試程序(3)不同，URI 應符合測試程序(2)回應，可為任意順序。 ● 測試程序(5)：請求封包之 URI 應與測試程序(3)及(5)不同，URI 應符合測試程序(2)回應，可為任意順序。 ● 測試程序(7)：待測標的應停止執行啟用網路服務程序。		
備註	● 本測試案例應全程使用 IPv6。 ● 待測標的可選項的使用多執行緒實作，並同步執行測試程序(2)、3 及 4，介面模擬器應具處理同步發送請求之能力。		

9.5.11 IPv4 相容性測試

項目編號	ITE-T011	必備/選項	必備
測試名稱	IPv4 相容性測試		
先決條件	應完成測試案例 ITE-T003。		
前置作業	重設待測標的之啟用網路服務程序，或完全重設待測標的。完全重設待測標的，改為使用 IPv4。		
測試程序	重新執行 ITE-T003，但使用 IPv4。		
通過條件	與 ITE-T003 之通過條件相同。		
備註	本測試案例應全程使用 IPv4。		

10. 網路周邊裝置符合性測試

10.1 概述

本節說明代理伺服器符合性測試之執行方法，包含符合性評估及合規性測試。

備考： 本節列舉之案例編號中，〝NWP-E〞代表〝network peripheral - evaluation〞，〝NWP-T〞，代表〝network peripheral - test〞。

10.2 待測標的

待測標的應為實體設備，並具備存取乙太網路介面及網際網路協定之功能。

構成待測標的之硬體元件數量及組合方式不限制。但不可透過網際網路連線將部分功能分散於遠端伺服器。

受測單位應說明待測標的之品牌、型號及版本。不同品牌、型號及版本應視為不同待測標的。

10.3 測試內容

10.3.1 測試平臺

執行網路周邊裝置符合性測試時，應將待測標的設置於測試平臺，並完成組態設定。介面模擬器應模擬 RADIUS 伺服器及代理伺服器，負責執行鑑別及 DHCP 設定。

測試平臺之區域網路應設定接線埠存取控制。待測標的接入測試平臺之區域網路時，應先通過 802.1X[3]鑑別後，方可啟用接線埠。

執行測試時，受測單位可使用支援工具監測運作狀況、設定組態及重設待測標的，但不可協助待測標的執行測試案例。支援工具可連接至待測標的之硬體介面(例：序列埠)或區域網路，接入區域網路時，其接線埠不需設定存取控制。

測試單位應調整網路設備，使待測標的及支援工具可不受限制存取網際網路 NTP 及 DNS 服務，但不可存取其他網際網路服務。若待測標的或支援工具需使用其他網際網路服務，則應預先說明並取得測試單位同意。

10.3.2 測試平臺組態設定

執行測試前，受測單位應提供組態資訊予測試單位，以設定測試平臺之組態，包含：

(a) 構成待測標的之硬體元件及其功能描述。

(b) (選項)支援工具介面型式及網路連線相關需求。

(c) 待測標的可支援之 802.1X[3]鑑別方式。

10.3.3 待測標的組態設定

執行測試前，測試單位應提供 802.1X[3]鑑別資訊(憑證或帳號及通行碼)予受測單位，受測單位應將鑑別資訊設定於待測標的。

10.4 符合性評估

10.4.1 具備人工設定網路組態功能

項目編號	NWP-E001	必備/選項	必備
評估標的	具備人工設定網路組態功能		
評估方式	審查產品型錄、說明書、設計規格書或展示該設備組態資訊。		
通過條件	確認待測標的具備人工設定網路組態之功能。		
備註	無。		

10.4.2 IPv4 支援能力

項目編號	NWP-E002	必備/選項	必備
評估標的	IPv4 支援能力		

評估方式	審查產品型錄、說明書、設計規格書或展示該設備組態資訊。
通過條件	待測標的可支援 IPv4。
備註	無。

10.5 合規性測試

10.5.1 接入區域網路測試

項目編號	NWP-T001	必備/選項	必備
測試名稱	接入區域網路測試		
先決條件	無。		
前置作業	確認待測標的已正確設定 802.1X[3]鑑別資訊。		
測試程序	(1) 啟動或重設待測標的，並接入測試平臺之區域網路。 (2) 檢視待測標的網路組態設定。 (3) 移除待測標的乙太網路連線、關閉電源或重設待測標的。 (4) 設定測試平臺，重設交換器接線埠存取控制狀態。 (5) 待測標的重新接入區域網路。 (6) 檢視待測標的網路組態設定。		
通過條件	● 測試程序(1)，檢視網路設備或 RADIUS 紀錄，若成功接入區域網路，則視為通過。若逾時仍未成功接入，則本測試案例應視為未通過。 ● 測試程序(2)及(6)，受測單位應使用測試工具展示包含 IP 位址及 DNS 伺服器位址。		
備註	於測試程序(3)，受測單位得選擇模擬連線障礙之方法。		

11. 組態伺服器符合性測試

11.1 概述

本節說明組態伺服器符合性測試之執行方法，包含符合性評估及合規性測試。

備考： 本節列舉之案例編號中，〝CFS-E〞代表〝configuration server - evaluation〞，〝CFS-T〞，代表〝configuration server - test〞。

11.2 待測標的

待測標的應為具備組態伺服器功能及互運性存取介面之實體設備，該實體設備之硬體規格及執行環境應與實際產品相同或完全相容。

構成待測標的之硬體元件數量及組合方式不限制，但不可透過網際網路連線將待測功能分散於遠端伺服器。與互運性介面非直接相關之支援功能，可使用簡化方式處理(例：可將資料庫安裝於支援工具中)。

受測單位應說明於該實體設備上運作之軟體名稱或來源(例：自行開發、開源軟體專案或作業系統內建功能)、版本及執行環境。執行環境相關資訊應包含軟體框架主要發行版本(例：〝Java SE 18〞)，若未使用軟體框架，則應提供作業系統主要發行版本及其對應之 CPU 指令集架構。

若軟體為不同來源、不同版本，或者軟體框架使用不同主要發行版本，則應視為不同待測標的。

11.3 測試內容

11.3.1 測試平臺

執行組態伺服器符合性測試時，應將待測標的設置於測試平臺，並完成組態設定。介面模擬器應模擬物聯網設備及應用伺服器，向待測標發送設備登錄請求，並回應設備授權請求。模

擬物聯網設備與模擬應用伺服器應使用不同 IP 位址。

測試單位及受測單位應預先約定測試平臺之域名查詢相關組態(例：設定區域網路 DNS 伺服器或變更〝hosts〞檔案)，使介面模擬器及待測標的能正確解析存取介面之完整域名。若待測標的於測試期間需使用私有域名及私有憑證，則應預先向測試單位提出說明，並提供域名及憑證等組態資訊。

執行測試時，受測單位可直接於待測標的本機操作或使用支援工具。測試單位應調整網路連線環境，使待測標的及支援工具可不受限制存取 DNS 及 NTP，但不可存取其他網際網路服務。待測標的或支援工具需使用其他網際網路服務，則應預先說明並取得測試單位同意。

11.3.2 測試平臺組態設定

執行測試前，受測單位應提供組態資訊予測試單位，以設定測試平臺之組態，包含：

(a) 構成待測標的之硬體元件及其功能描述。

(b) 網路介面數量。

(c) (選項)支援工具介面型式及網路連線相關需求。

(d) 設備登錄存取介面 URI 及對應之網路介面。

(e) 狀態回報存取介面 URI 及對應之網路介面。

(f) 設備授權存取介面 URI 及對應之網路介面。

備考：待測標的可預先設定測試用資料，以產生對應之存取介面。

11.3.3 待測標的組態設定

執行測試前，測試單位應提供組態資訊予受測單位，以設定待測標的之組態，包含：

(a) IPv6 及 IPv4 固定位址。

(b) DNS 伺服器位址(包含 IPv6 及 IPv4)。

(c) 測試用物聯網設備識別符。

(d) 測試用代理伺服器識別符。

(e) 測試用 HMAC-SHA256 密鑰。

11.3.4 時間相關之組態設定

受測單位應說明待測標的之時間相關組態，包含：

(a) HTTPS 重送等候時間。

(b) HTTPS 重送次數上限。

(c) 狀態回報封包漏失之次數(或時間)上限。

(d) 運作狀態異常之判定次數。

執行測試時，所有測試程序之重送等候時間、重送次數上限、判定次數或時間上限等，應符合以上組態資訊，可容許誤差±5 秒以內。

備考 1. 為加速測試進行，受測單位宜調整待測標的之時間相關組態如下：

(a) HTTPS 重送等候時間：5 秒。

(b) HTTPS 重送次數上限：3 次。

(c) 狀態回報封包漏失之次數：5 次。

(d) 運作狀態異常之故障判定次數：3 次。

備考 2. 受測單位可調整待測標的(例：變更作業系統組態或重新編譯程式)以設定時間相關組

態，但應向測試單位說明調整範圍。

11.3.5 其他應注意事項

若待測標的具備惡意攻擊偵測功能，將連續發生相同錯誤之 HTTPS 客戶端認定為惡意攻擊並限制其連線能力，則該項功能應先關閉。

11.4 符合性評估

11.4.1 TLS 版本

項目編號	CFS-E001	必備/選項	必備
評估標的	TLS 版本		
評估方式	審查產品型錄、說明書、設計規格書或展示系統組態資訊，或使用 TLS 客戶端工具測試。		
通過條件	HTTPS 加密連線使用之 TLS 版本應為 1.2 或更新版本。		
備註	無。		

11.4.2 服務存取介面 URI

項目編號	CFS-E002	必備/選項	必備
評估標的	服務存取介面 URI		
評估方式	說明書、設計規格書或展示系統組態資訊。		
通過條件	● 待測標的之 HTTPS 伺服器端可設定 URI 相關組態。 ● 展示待測標的目前使用之 FQDN，或說明如何取得公開 FQDN。		
備註	無。		

11.4.3 RADIUS 支援能力

項目編號	CFS-E003	必備/選項	必備
評估標的	RADIUS 支援能力		
評估方式	審查產品型錄、說明書、設計規格書或展示系統組態資訊。		
通過條件	RADIUS 伺服器應能支援第 2-1 部 D.4 列舉之鑑別型式。		
備註	無。		

11.4.4 設備登錄資訊管理

項目編號	CFS-E004	必備/選項	必備
評估標的	設備登錄資訊管理		
評估方式	實機展示、輸出表單或操作畫面截圖。		
通過條件	● 待測標的應記錄包含第 2-1 部 A.3 及 A.4 之設備登錄資訊。 ● 待測標的應提供設備登錄刪除功能。		
備註	受測單位可預先設定測試用資料。		

11.4.5 防火牆組態管理

項目編號	CFS-E005	必備/選項	必備
評估標的	防火牆組態管理		
評估方式	設計規格書、實機展示、輸出表單或操作畫面截圖。		

通過條件	待測標的可使用自動化方式變更防火牆組態，或者以輸出表單或其他方式通知相關人員進行處理。
備註	無。

11.4.6 運作狀態紀錄管理

項目編號	CFS-E006	必備/選項	必備
評估標的	運作狀態紀錄管理		
評估方式	設計規格書、實機展示、輸出表單或操作畫面截圖		
通過條件	● 待測標的應記錄包含第 2-1 部 A.6 之所有運作狀態資訊。 ● 待測標的應提供異常偵測功能，可由物聯網設備之狀態回報，偵測設備發生異常。 ● (選項)說明物聯網設備發生故障後之處理程序。		
備註	待測標的可預先設定測試用資料。		

11.5 合規性測試

11.5.1 異常程序測試(一)

項目編號	CFS-T001	必備/選項	必備
測試名稱	異常程序測試(一)：HTTPS 伺服器端異常處理		
先決條件	無。		
前置作業	● 確認測試平臺已正確設定所有組態。 ● 確認待測標的已正確設定所有組態，成功接入測試平臺並能使用網路介面。		
測試程序	(1) 介面模擬器向待測標的發送設備登錄請求，連線標的為設備登錄存取介面，但使用未加密 HTTP 連線，連線標的通訊埠為 80。 (2) 介面模擬器向待測標的發送設備登錄請求，但請求封包之 URI 路徑部分為隨機路徑。 (3) (選項)重複執行測試程序(1)，但擷取設備登錄存取介面 URI 之完整路徑之上層目錄作為 URI 之路徑，直到根目錄。 (4) 介面模擬器向待測標的發送設備登錄請求，但請求封包之 URI 域名部分為 IP 位址。 (5) 介面模擬器向待測標的發送設備登錄請求，但不包含鑑別資訊。 (6) 介面模擬器向待測標的發送設備登錄請求，但鑑別資訊為隨機數。 (7) 介面模擬器向待測標的發送設備登錄請求，但使用 HTTP 基本鑑別(〝Basic〞 authentication)。 (8) 介面模擬器向待測標的發送設備登錄請求，但使用 HTTP 版本為 HTTP/1.0。 (9) 介面模擬器向待測標的發送設備登錄請求，但使用方法為〝GET〞。 (10) 介面模擬器向待測標的發送設備登錄請求，但使用方法為〝PUT〞。 (11) 介面模擬器向待測標的發送設備登錄請求，但使用方法為〝PATCH〞。 (12) 介面模擬器向待測標的發送設備登錄請求，但使用方法為〝DELETE〞。 (13) 介面模擬器向待測標的發送設備登錄請求，但請求本體為空白 JSON 物件。 (14) 重複執行測試程序(3)～(13)，但發送狀態回報請求封包，連線標的亦改為狀態回報存取介面。 (15) 重複執行測試程序(3)～(13)，但發送設備授權確認之請求封包，連線標的亦改為設備授權存取介面。		
通過條件	● 測試程序(1)：應拒絕連線。 ● 測試程序(2)及(3)：應回應狀態碼 404。 ● 測試程序(4)：應拒絕連線、發生 TLS 連線異常或回應狀態碼 404。		

	● 測試程序(5)～(7)：應回應狀態碼 401。 ● 測試程序(8)：應回應狀態碼 426。 ● 測試程序(9)～(12)：應回應狀態碼 405。 ● 測試程序(13)：應回應狀態碼 400。 ● 測試程序(14)之通過條件與測試程序(3)～(13)之通過條件相同。 ● 測試程序(15)之通過條件與測試程序(3)～(13)之通過條件相同。
備註	● 本測試案例應全程使用 IPv6。 ● 若存取介面 URI 路徑為根目錄，則測試程序(3)可省略。 ● 若設備登錄存取介面、狀態回報存取介面與設備授權存取介面之 URI 使用相同域名，則測試程序(2)～(4)可省略。

11.5.2 異常程序測試(二)

項目編號	CFS-T002	必備/選項	必備
測試名稱	異常程序測試(二)：HTTPS 客戶端異常處理		
先決條件	應完成測試案例 CFS-T001。		
前置作業	待測標的應清除所有設備登錄資訊。		
測試程序	(1) 介面模擬器依正常程序向待測標的發送設備登錄請求，鑑別資訊應由介面模擬器使用預設組態之 HMAC-SHA256 密鑰計算數位簽章，請求內容〝credAuthReq〞參數由介面模擬器隨機產生，〝hearbeat〞參數應設定為 60 秒。 (2) 介面模擬器等候待測標的發送設備授權請求，回應狀態碼 500。 (3) 介面模擬器持續等候接收，直到停止待測標的停止重發。 (4) 重複執行測試程序(1)。 (5) 介面模擬器等候待測標的發送設備授權申請之 HTTPS 請求，回應狀態碼 308，〝Location〞標頭欄位應填入不同之任意 URI。 (6) 介面模擬器等候待測標的發送設備授權申請之 HTTPS 請求，回應狀態碼 502。 (7) 重複執行測試程序(6)，直到停止待測標的停止重發設備授權請求。 (8) 重複執行測試程序(1)～(3)，回應狀態碼改為 504。 (9) 重複執行測試程序(1)～(3)，回應狀態碼改為 429，〝Retry-After〞標頭欄位指定等候時間為 5 秒。 (10) 重複執行測試程序(1)～(3)，回應狀態碼改為 503，〝Retry-After〞標頭欄位指定等候時間為 10 秒。 (11) 重複執行測試程序(1)及(2)，回應狀態碼改為 307，〝Location〞標頭欄位應填入不同之任意 URI，〝Retry-After〞標頭欄位指定等候時間為 30 秒。 (12) 介面模擬器等候待測標的發送設備授權申請之 HTTPS 請求，回應狀態碼 418。 (13) 檢視待測標的狀態。		
通過條件	● 設備授權申請之請求封包與設備登錄請求封包比對： ♦ 設備授權申請之 URI 應符合設備登錄請求之〝authorizer〞參數 ♦ 設備授權申請之〝credAuthReq〞參數應符合設備登錄請求之鑑別資訊 ♦ 設備授權申請之〝nonce〞參數應符合設備登錄請求中鑑別資訊之〝jti〞參數。 ● 測試程序(1)：待測標的應發送回應狀態碼 202，回應封包不包含本體(body)。 ● 測試程序(2)及(3)：所有請求封包之內容應相同，重發次數應符合待測標的預設組態。 ● 測試程序(4)：待測標的應發送回應狀態碼 202，回應封包不包含本體。 ● 測試程序(6)及(7)：請求封包標的 URI 應符合測試程序(2)回應之〝Location〞標頭欄位內容。 ● 測試程序(9)：HTTPS 重送時間間隔應為 5 秒。 ● 測試程序(10)，HTTPS 重送時間間隔應為 10 秒。		

	● 測試程序(12)：待測標的不可發送設備授權請求。 ● 測試程序(12)：請求封包標的 URI 應符合測試程序(12)回應之〝Location〞標頭欄位內容。 ● 測試程序(13)：待測標的應停止發送 HTTPS 請求。
備註	本測試案例應全程使用 IPv6。

11.5.3 設備登錄及設備授權測試

項目編號	CFS-T003	必備/選項	必備
測試名稱	設備登錄及設備授權測試		
先決條件	應完成測試案例 CFS-T002。		
前置作業	● 待測標的應清除所有設備登錄資訊。 ● 待測標的應暫時停用防火牆自動管理功能。		
測試程序	(1) 介面模擬器依正常程序向待測標的發送設備登錄請求，鑑別資訊應由介面模擬器使用預設組態之 HMAC-SHA256 密鑰計算數位簽章，請求內容〝credAuthReq〞參數由介面模擬器隨機產生，〝hearbeat〞參數應設定為 60 秒。 (2) 介面模擬器等候待測標的發送設備授權申請之 HTTPS 請求，回應狀態碼 202。 (3) 介面模擬器發送設備授權確認之 HTTPS 請求至待測標的，授權結果為〝GRANT〞，〝inbound〞及〝outbound〞參數可填入任意防火牆存取規則。 (4) 檢視待測標的之防火牆規則異動紀錄。		
通過條件	● 測試程序(1)：待測標的應發送回應狀態碼 202，回應封包不包含本體(body)。 ● 測試程序(2)：設備授權申請之 HTTPS 請求封包與設備登錄請求封包比對： ◆ 設備授權申請之 URI 應符合設備登錄之〝authorizer〞參數。 ◆ 設備授權申請之〝credAuthReq〞參數應符合設備登錄請求之鑑別資訊。 ◆ 設備授權申請之〝nonce〞參數應符合設備登錄請求中鑑別資訊之〝jti〞參數。 ● 測試程序(3)：待測標的應回應狀態碼 202。 ● 測試程序(4)：防火牆規則異動紀錄應符合測試程序(3)發送之防火牆存取規則。		
備註	● 本測試案例應全程使用 IPv6。 ● 受測試單位可操作待測標的，使設備登錄請求通過條件檢查，以觸發待測標的執行測試程序(2)。 ● 本測試案例不測試待測標的是否能自動調整防火牆規則，但應展示規則異動之相關資訊(例：資料庫或日誌等)。 ● 若受測單位於執行本測試案例時，調整待測標的之防火牆自動管理功能，則受測單位應說明調整範圍。		

11.5.4 物聯網設備異常偵測測試

項目編號	CFS-T004	必備/選項	必備
測試名稱	物聯網設備異常偵測測試		
先決條件	應完成測試案例 CFS-T003。		
前置作業	若執行 CFS-T003 後待測標的經重設，或者測試資料已清除，則應重新執行 CFS-T003 測試程序(1)～(3)。		
測試程序	(1) 介面模擬器向待測標的發送狀態回報請求封包，所有設備狀態皆為正常。 (2) 重複執行測試程序(1)，共 5 次，間隔時間應符合 CFS-T002 測試程序(1)發送設備登錄請求封包之〝hearbeat〞參數。 (3) 介面模擬器停止發送任何封包，直到待測標的顯示該物聯網設備出現異常。 (4) 重複執行測試程序(1)，但狀態回報之〝state〞參數應為 5(〝系統資源不足〞)。 (5) 重複執行測試程序(4)，間隔時間應符合 CFS-T002 測試程序(1)發送設備登錄請求		

	封包之〝hearbeat〞參數，直到待測標的顯示該物聯網設備出現異常。
通過條件	● 測試程序(1)及(2)：待測標的應回應狀態碼 201。 ● 測試程序(3)：待測標的應於經過一定時間後顯示該物聯網設備出現異常狀況。經過時間應符合受測單位預先提供之時間相關組態資訊。 ● 測試程序(4)：待測標的應回應狀態碼 201。 ● 測試程序(5)：待測標的應於經過一定時間後顯示該物聯網設備出現異常狀況。經過時間應符合受測單位預先提供之時間相關組態資訊。
備註	● 本測試案例應全程使用 IPv6。 ● 受測單位應操作待測標的以展示物聯網設備之異常紀錄(例：資料庫或日誌等)。

11.5.5 變更設備登錄測試

項目編號	CFS-T005	必備/選項	必備
測試名稱	變更設備登錄測試		
先決條件	應完成測試案例 CFS-T004。		
前置作業	● 若執行 CFS-T004 後待測標的經重設，或者測試資料已清除，則應先重新執行 CFS-T003 測試程序(1)～(3)，再執行本測試案例。 ● 待測標的應暫時停用防火牆自動管理功能。		
測試程序	(1) 執行 CFS-T003 測試程序(1)，設備登錄請求之〝updateTime〞參數更新至執行本測試案例之時間。 (2) 執行 CFS-T003 測試程序(2)。 (3) 執行 CFS-T003 測試程序(3)，設備授權確認之授權結果為〝GRANT〞，防火牆入向及出向規則內容應與 CFS-T003 不同。 (4) 檢視待測標的之防火牆規則異動紀錄。		
通過條件	與 CFS-T003 之通過條件相同。		
備註	● 本測試案例應全程使用 IPv6。 ● 本測試案例不測試待測標的是否能自動調整防火牆規則，但應展示規則異動之相關資訊(例：資料庫或日誌等)。 ● 若受測單位於執行本測試案例時，調整待測標的之防火牆自動管理功能，則受測單位應說明調整範圍。		

11.5.6 拒絕授權測試

項目編號	CFS-T006	必備/選項	必備
測試名稱	拒絕授權測試		
先決條件	應完成測試案例 CFS-T005。		
前置作業	● 若執行 CFS-T005 後待測標的經重設，或者測試資料已清除，則應先重新執行 CFS-T003 測試程序(1)～(3)，再執行本測試案例。 ● 待測標的應暫時停用防火牆自動管理功能。		
測試程序	(1) 執行 CFS-T003 測試程序(1)，設備登錄請求之〝updateTime〞參數更新至執行本測試案例之時間。 (2) 執行 CFS-T003 測試程序(2)。 (3) 執行 CFS-T003 測試程序(3)，設備授權確認之授權結果為〝DENY〞，防火牆入向及出向規則可省略。 (4) 介面模擬器向待測標之狀態回報介面發送狀態回報請求封包，執行狀態可由實作自定。 (5) 介面模擬器向待測標之狀態回報介面發送設備登錄請求封包，請求封包內容應與 CFS-T005 測試程序(1)之請求封包一致。 (6) 檢視待測標的之防火牆規則異動紀錄。		

通過條件	● 測試程序(1)～(3)：與 CFS-T003 測試程序(1)～(3)之通過條件相同。 ● 測試程序(4)及(5)：待測標的應回應狀態碼 403。 ● 測試程序(5)：所有與該物聯網設備相關之防火牆紀錄應刪除，或者標示為待刪除。
備註	● 本測試案例應全程使用 IPv6。 ● 本測試案例不測試待測標的是否能自動調整防火牆規則，但應展示規則異動之相關資訊(例：資料庫或日誌等)。 ● 若受測單位於執行本測試案例時，調整待測標的之防火牆自動管理功能，則受測單位應說明調整範圍。

11.5.7 IPv4 相容性測試

項目編號	CFS-T007	必備/選項	必備
測試名稱	IPv4 相容性測試		
先決條件	應完成測試案例 CFS-T003。		
前置作業	● 待測標的應清除所有設備登錄資訊。 ● 待測標的應暫時停用防火牆自動管理功能。		
測試程序	重新執行 CFS-T003 測試程序(1)～(3)，但使用 IPv4。		
通過條件	與 CFS-T003 之通過條件相同。		
備註	本測試案例應全程使用 IPv4。		

12. 應用伺服器符合性測試

12.1 概述

本節說明組態伺服器符合性測試之執行方法，包含符合性評估及合規性測試。

備考： 本節列舉之案例編號中，〝APS-E〞代表〝application server - evaluation〞，〝APS-T〞，代表〝application server - test〞。

12.2 待測標的

待測標的應為具備應用伺服器功能及互運性存取介面之實體設備，該實體設備之硬體規格及執行環境應與實際產品相同或完全相容。

構成待測標的之硬體元件數量及組合方式不限制，但不可透過網際網路連線將待測功能分散於遠端伺服器。與互運性介面非直接相關之支援功能，可使用簡化方式處理(例：可將資料庫安裝於支援工具中)。

受測單位應說明於該實體設備上運作之軟體名稱或來源(例：自行開發、開源軟體專案或作業系統內建功能)、版本及執行環境。執行環境相關資訊應包含軟體框架主要發行版本(例：〝Java SE 18〞)，若未使用軟體框架，則應提供作業系統主要發行版本及其對應之 CPU 指令集架構。

若軟體為不同來源、不同版本，或者軟體框架使用不同主要發行版本，則應視為不同待測標的。

12.3 測試內容

12.3.1 測試平臺

執行應用伺服器符合性測試時，應將待測標的設置於測試平臺，並完成組態設定。介面模擬器應模擬組態伺服器，向待測標發送設備授權申請，接收設備授權確認，並透過共同資料存取介面取得物聯網設備相關資訊。

測試單位及受測單位應預先約定測試平臺之域名查詢相關組態(例：設定區域網路 DNS 伺服器

或變更〝hosts〞檔案)，使介面模擬器及待測標的能正確解析存取介面之完整域名。若待測標的於測試期間需使用私有域名及私有憑證，則應預先向測試單位提出說明，並提供域名及憑證等組態資訊。

執行測試時，受測單位可直接於待測標的本機操作或使用支援工具。測試單位應調整網路連線環境，使待測標的及支援工具可不受限制存取 DNS 及 NTP，但不可存取其他網際網路服務。待測標的或支援工具需使用其他網際網路服務，則應預先說明並取得測試單位同意。

12.3.2 測試平臺組態設定

執行測試前，受測單位應提供組態資訊予測試單位，以設定測試平臺之組態，包含：

(a) 構成待測標的之硬體元件及其功能。

(b) 網路介面數量。

(c) (選項)支援工具介面型式及網路連線相關需求。

(d) 設備登錄存取介面 URI 及對應之網路介面及鑑別資訊。

(e) 測試用物聯網設備之設備登錄資訊。

(f) (選項)共同資料存取介面之鑑別方法及鑑別資訊。

12.3.3 待測標的組態設定

執行測試前，測試單位應提供組態資訊予受測單位，以設定待測標的之組態，包含：

(a) IPv6 及 IPv4 固定位址。

(b) DNS 伺服器位址(包含 IPv6 及 IPv4)。

除以上組態資訊外，受測單位應於待測標的設定測試用資料，包含授權資訊及〝Thing〞物件實例。測試用資料內容可由受測單位自行設計。

12.3.4 時間相關之組態設定

受測單位應說明待測標的之時間相關組態，包含：

(a) HTTPS 重送等候時間。

(b) HTTPS 重送次數上限。

執行測試時，所有測試程序之 HTTPS 重送等候時間及重送次數上限，應符合以上組態資訊，可容許誤差±5 秒以內。

備考 1. 為加速測試進行，受測單位宜調整待測標的之時間相關組態如下：

(a) HTTPS 重送等候時間：5 秒。

(b) HTTPS 重送次數上限：3 次。

備考 2. 受測單位可調整待測標的(例：變更作業系統組態或重新編譯程式)，以設定時間相關組態，但應向測試單位說明調整範圍。

12.4 符合性評估

12.4.1 TLS 版本

項目編號	APS-E001	必備/選項	必備
評估標的	TLS 版本		
評估方式	審查產品型錄、說明書、設計規格書或展示系統組態資訊，或使用 TLS 客戶端工具測試。		
通過條件	HTTPS 加密連線使用之 TLS 版本應為 1.2 或更新版本。		

備註	無。

12.4.2 OGC SensorThings API v1.0 符合性評估(一)

項目編號	APS-E002	必備/選項	選項
評估標的	OGC SensorThings API v1.0[7]符合性評估(一)：全系統自行建置		
評估方式	展示 OGC SensorThings API v1.0[7]合規性測試證明。		
通過條件	提出 OGC 組織核發之測試報告。		
備註	● 受測單位可自行決定是否執行本評估案例。 ● 適用本評估案例之先決條件：受測單位已於網際網路實際提供共同資料存取介面之相關服務，且存取介面由測試單位負責管理，包含網域及系統平臺。若共同資料存取介面為外部服務供應者之軟體租借服務(PaaS/SaaS)，則不適用本評估案例。		

備考： OGC 公布之測試項目為〝SensorThings API (STA) 1.0 Conformance Test Suite〞，參考網址：http://cite.opengeospatial.org/teamengine/about/sta10/1.0/site/

12.4.3 OGC SensorThings API v1.0 符合性評估(二)

項目編號	APS-E003	必備/選項	選項
評估標的	OGC SensorThings API v1.0[7]符合性評估(二)：租用外部服務		
評估方式	● 展示外部服務供應者提供之 OGC SensorThings API v1.0[7]符合性聲明。 ● 展示受測單位委託外部服務供應者提供之服務之契約、購買證明、授權證明、帳號授權狀態或其他等效文件。		
通過條件	● 外部服務供應者提出之符合性聲明為 OGC 組織核發之有效證明或報告。 ● 服務契約等文件若具有效時限，效期應能涵蓋待測標的執行符合性評估之整個期程。		
備註	● 受測單位可自行決定是否執行本評估案例。 ● 適用本評估案例之先決條件：受測單位使用外部服務供應者之軟體租借服務(PaaS/SaaS)提供共同資料存取介面相關服務。		

12.4.4 OGC SensorThings API v1.0 資料模型符合性評估(一)

項目編號	APS-E004	必備/選項	選項
評估標的	OGC SensorThings API v1.0[7]資料模型符合性評估(一)：感測器型式應用		
評估方式	展示感測器型式應用服務測試資料之任意 Datastream 及 Observation 物件。		
通過條件	Datastream 及 Observation 物件符合本系列規範第 2-1 部 11.3.5.2 規定。		
備註	● 受測單位可自行決定是否執行本評估案例。 ● 適用本評估案例之先決條件：待測標的包含感測器型式應用服務。		

12.4.5 OGC SensorThings API v1.0 資料模型符合性評估(二)

項目編號	APS-E005	必備/選項	選項
評估標的	OGC SensorThings API v1.0[7]資料模型符合性評估(二)：媒體紀錄型式應用		
評估方式	展示感測器型式應用服務測試資料之任意 Datastream 及 Observation 物件。		
通過條件	Datastream 及 Observation 物件符合本系列規範第 2-1 部 11.3.5.3 規定。		
備註	● 受測單位可自行決定是否執行本評估案例。 ● 適用本評估案例之先決條件：待測標的包含媒體紀錄型式應用服務。		

12.5 合規性測試

12.5.1 異常程序測試（一）

項目編號	APS-T001	必備/選項	必備
測試名稱	異常程序測試（一）：HTTP 伺服器異常處理		
先決條件	無。		
前置作業	確認待測已正確設定所有組態，並已完成測試資料匯入。		
測試程序	(1) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但請求封包之 URI 路徑部分為隨機路徑。 (2) (有條件必備) 重複測試程序(1)，但擷取設備登錄申請之 HTTPS 存取介面 URI 之完整路徑之上層目錄作為 URI 之路徑，直到根目錄。 (3) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但請求封包之 URI 域名部分為 IP 位址。 (4) 介面模擬器向待測標的發送設備登錄申請之 HTTP 請求，使用未加密連線，連線標的通訊埠為 80。 (5) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但使用 HTTP 版本為 HTTP/1.0。 (6) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但使用方法為〝PUT〞。 (7) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但使用方法為〝PATCH〞。 (8) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但使用方法為〝DELETE〞。 (9) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但使用方法為〝GET〞。 (10) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但不包含鑑別資訊。 (11) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但鑑別資訊為隨機數。 (12) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但使用 HTTP 基本鑑別(〝Basic〞authentication)，帳號及通行碼為隨機數。 (13) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，但請求本體應為空白 JSON 物件。 (14) 重複測試程序(1)～(8)，但連線標的改為共同資料存取介面，請求 URI 為測試用物聯網資訊對應〝things〞物件實例。 (15) 介面模擬器向待測標的發送 HTTPS 請求，請求 URI 為測試用物聯網資訊對應〝things〞物件實例，但使用方法為〝POST〞。		
通過條件	● 測試程序(1)及(2)：應回應狀態碼 404。 ● 測試程序(3)：應拒絕連線、發生 TLS 連線異常或回應狀態碼 404。 ● 測試程序(4)：應拒絕連線。 ● 測試程序(5)：應回應狀態碼 426。 ● 測試程序(6)～(9)：應回應狀態碼 405。 ● 測試程序(10)～(12)：應回應狀態碼 401。 ● 測試程序(13)：應回應狀態碼 400。 ● 測試程序(14)：參照測試程序(1)～(7)之通過條件。 ● 測試程序(15)：應回應狀態碼 426。		
備註	● 本測試案例應全程使用 IPv6。 ● 若設備登錄存取介面 URI 路徑為根目錄，則測試程序(8)可省略。 ● 若設備授權存取介面及共同資料存取介面使用相同域名，則不需重複執行測試程序(1)～(3)。		

12.5.2 異常程序測試（二）

項目編號	APS-T002	必備/選項	必備
測試名稱	異常程序測試(二)：HTTPS 客戶端異常處理		
先決條件	應完成測試 APS-T001。		
前置作業	待測標的應清除所有設備登錄資訊。		
測試程序	(1) (選項)介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，〝id〞參數為隨機數。 (2) 操作待測標的使其執行授權評估及確認程序。 (3) 介面模擬器等候待測標的發送設備登錄確認之 HTTPS 請求，回應狀態碼 500。 (4) 介面模擬器持續等候接收，直到停止待測標的停止重發設備授權請求。 (5) 重複執行測試程序(1)。 (6) 介面模擬器等候待測標的發送設備登錄確認之 HTTPS 請求，回應狀態碼 308，〝Location〞標頭欄位應填入不同之任意 URI。 (7) 介面模擬器等候待測標的發送設備登錄確認之 HTTPS 請求，回應狀態碼 502。 (8) 重複執行測試程序(7)，直到停止待測標的停止重發。 (9) 重複執行測試程序(1)～(4)，回應狀態碼改為 504。 (10) 重複執行測試程序(1)～(4)，回應狀態碼改為 429，〝Retry-After〞標頭欄位指定等候時間為 5 秒。 (11) 重複執行測試程序(1)～(4)，回應狀態碼改為 503，〝Retry-After〞標頭欄位指定等候時間為 10 秒。 (12) 重複執行測試程序(1)～(3)，回應狀態碼改為 307，〝Location〞標頭欄位應填入不同之任意 URI，〝Retry-After〞標頭欄位指定等候時間為 30 秒。 (13) 介面模擬器等候待測標的發送設備登錄確認之 HTTPS 請求，回應狀態碼 202。		
通過條件	● 設備授權確認之請求封包應符合本系列標準第 2-1 部 11.2.3。 ● 設備授權確認之請求封包與設備授權申請之請求封包比對： ♦ 設備授權確認之 URI 應符合設備授權申請之〝replyto〞參數。 ♦ 設備授權確認之鑑別資訊參數應符合設備授權申請之〝credAuthCfm〞參數。 ♦ 設備授權確認之〝id〞參數應符合設備授權申請中鑑別資訊之〝id〞參數。 ● 設備授權確認請求封包中，授權結果應為〝DENY〞。 ● 測試程序(2)：待測標的應發送回應狀態碼 202，回應封包不包含本體(body)。 ● 測試程序(3)及(4)：所有請求封包之內容應相同，重發次數應符合待測標的預設組態。 ● 測試程序(5)：待測標的應發送回應狀態碼 202，回應封包不包含本體。 ● 測試程序(7)及(8)：請求封包標的 URI 應符合測試程序(6)回應之〝Location〞標頭欄位內容。 ● 測試程序(10)：HTTPS 重送時間間隔應為 5 秒。 ● 測試程序(11)，HTTPS 重送時間間隔應為 10 秒。 ● 測試程序(13)：請求封包標的 URI 應符合測試程序(12)回應之〝Location〞標頭欄位內容。		
備註	● 本測試案例應全程使用 IPv6。 ● 測試程序(1)可省略。 ● 待測標的停止重發後，可視實際需求將待測標的重設或清除異常狀態。		

12.5.3 設備授權確認測試

項目編號	APS-T003	必備/選項	必備
測試名稱	設備授權確認測試		
先決條件	應完成測試 APS-T002。		

前置作業	待測標的應清除所有設備登錄資訊。
測試程序	(1) 介面模擬器向待測標的發送設備登錄申請之 HTTPS 請求，所有設備登錄資訊皆使用受測標的預先提供之組態。 (2) 操作待測標的使其執行授權評估及確認程序，授權結果為〝GRANT〞。 (3) 介面模擬器等候待測標的發送設備登錄確認之 HTTPS 請求，回應狀態碼 202。
通過條件	● 設備授權確認之請求封包應符合本系列標準第 2-1 部 11.2.3。 ● 設備授權確認之請求封包中，〝inbound〞、〝outbound〞參數內容應符合一般 IP 通訊規則 ● 設備授權確認之請求封包中，〝things〞參數應為陣列，陣列元素應包含至少 1 組符合 OGC SensorThings API v1.0[7]規定之〝Thing〞物件實例 URI。
備註	本測試案例應全程使用 IPv6。

12.5.4 OGC SensorThings API v1.0 資料關聯性測試

項目編號	APS-T004	必備/選項	有條件必備
測試名稱	OGC SensorThings API v1.0[7]資料關聯性測試		
先決條件	● 應完成測試 APS-T003。 ● 若受待測標的已通過 APS-E002 或 APS-E003 評估，則不需執行本測試案例。		
前置作業	若待測標的經過重設或執行狀態已清除，則應重新執行 APS-T003。		
測試程序	(1) 介面模擬器向 APS-T003 測試中取得之〝Thing〞物件實例 URI 發送 HTTPS 請求，並檢視回應內容。 (2) (選項)介面模擬器向測試程序(1)中〝Datastream〞關聯資料之 URI 發送 HTTPS 請求，並檢視回應內容。 (3) (選項)介面模擬器向測試程序(2)中〝Observation〞關聯資料之 URI 發送 HTTPS 請求，並檢視回應內容。		
通過條件	● 所有 HTTPS 請求回應狀態碼皆應為 200(OK)。若取得回應狀態碼為其他錯誤，測試單位得視實際情況調整網路連線、延後測試或要求受測單位當場檢查。 ● 〝Thing〞、〝Datastream〞及〝Observation〞物件實例格式應符合 OGC SensorThings API v1.0[7]規定。 ● 測試程序(1)：〝Thing〞物件實例內應包含 1 組〝Location〞關聯資料，可選項的包含〝HistoricalLocation〞及〝Datastream〞關聯資料。 ● 測試程序(2)：〝Datastream〞物件實例內應包含 1 組〝ObservedProperty〞及 1 組〝Sensor〞關聯資料，可選項的包含〝Observatoin〞關聯資料。 ● 測試程序(3)：〝Observation〞物件實例內應包含 1 組〝FeatureOfInterest〞關聯資料。		
備註	● 若待測標的已完成 APS-E002 或 APS-E003，則可省略本測試案例。 ● 若〝Thing〞物件實例未包含〝Datastream〞關聯資料，則測試程序(2)及(3)可省略。 ● 若〝Datastream〞物件實例未包含〝Observation〞關聯資料，則測試程序(3)可省略。 ● HTTPS 請求之鑑別方法及鑑別資料應符合受測單位預先提供之組態。 ● HTTPS 請求發生異常時，若受測單位無法當場調整修復，則視為本測試案例未通過。		

12.5.5 詮釋資料存取測試

項目編號	APS-T005	必備/選項	必備
測試名稱	詮釋資料存取測試		
先決條件	應完成測試 APS-T003。		

前置作業	若待測標的經過重設或執行狀態已清除，則應重新執行 APS-T003。
測試程序	(1) 介面模擬器向 APS-T003 測試中取得之〝Thing〞物件實例 URI 發送 HTTPS 請求，並檢視回應內容。 (2) 解析測試程序(1)取得之回應內容，檢視〝properties〞內容。 (3) 介面模擬器向測試程序(2)〝properties〞內容之〝profile〞參數發送 HTTPS 請求，檢視回應內容，並解析回應內容中〝services〞陣列。 (4) (有條件必備)介面模擬器使用測試程序(3)〝services〞陣列內所有元素之 URI，發送 HTTPS 請求。
通過條件	● 所有 HTTPS 請求回應狀態碼皆應為 200(OK)。若取得回應狀態碼為其他錯誤，測試單位得視實際情況調整網路連線、延後測試或要求受測單位當場檢查。 ● 測試程序(2)，〝Thing〞物件實例格式之〝property〞參數內容應符合本系列規範第 2-1 部 11.3.2 規定。 ● 測試程序(3)，回應內容應符合本系列規範第 2-1 部 11.3.3 規定。 ● 測試程序(4)，所有請求皆應回應符合 OGC SensorThings API v1.0 規定之〝Thing〞物件實例。
備註	● 若〝services〞陣列未包含任何元素，則省略測試程序(4)。 ● HTTPS 請求之鑑別方法及鑑別資料應符合受測單位預先提供之組態。 ● HTTPS 請求發生異常時，若受測單位無法當場調整修復，則視為本測試案例未通過。

12.5.6 IPv4 相容性測試

項目編號	APS-T006	必備/選項	必備
測試名稱	IPv4 相容性測試		
先決條件	應完成測試 APS-T003 及 APS-T005。		
前置作業	若待測標的經過重設或執行狀態被清除，則應重新執行 APS-T003。		
測試程序	(1) 重新執行 APS-T003，但使用 IPv4。 (2) 重新執行 APS-T005，但使用 IPv4。		
通過條件	與測試 APS-T003 及 APS-T005 相同。		
備註	本測試案例應全程使用 IPv4。		

附錄A

(規定)

符合性測試清單

A.1. 網路交換器

第 2-1 部對應節次	評估/測試案例	必備/選項	備註
第 6 節			本節不適用於網路交換器之符合性測試。
7.1			本節無規定事項。
7.2	NWE-E001	M	
7.3	NWE-E001	M	
7.4.1	NWE-E002	M	
7.4.2	NWE-E003	M	
7.4.3	NWE-E003	M	
7.4.4	NWE-E004	M	
7.4.5	NWE-E005	C1	執行本評估案例之條件詳後述。

上表必備/選項條件說明如下：

- C1：使用 VLAN 之設備，應執行本評估案例。未使用 VLAN 之設備，本評估案例可省略。

備考： 必備/選項之〝M〞代表〝必備(mandatory)〞，〝O〞代表〝選項(optional)〞，〝C〞代表有〝條件必備(conditional mandatory)〞下同。

A.2. 代理伺服器

第 2-1 部對應節次	評估/測試案例	必備/選項	備註
6.1			本節無規定事項。
6.2	AGS-T007	M	本節為資料格式共同要求。
6.3.1	AGS-E001	M	本節為存取介面共同要求。
	AGS-T007	M	
	AGS-T009	M	
6.3.2			本節不適用於代理伺服器之符合性測試。
6.3.3			本節不適用於代理伺服器之符合性測試。
8.1			本節無規定事項。
8.2.1	AGS-T001	M	
8.2.2	AGS-T001	M	
	AGS-T011	M	
	AGS-T012	M	
8.3.1	AGS-T001	M	
	AGS-T002	M	
	AGS-T003	M	
	AGS-T004	M	
	AGS-T007	M	
8.3.2	AGS-T001	M	
	AGS-T006	M	
8.3.3	AGS-T002	M	
	AGS-T010	M	
	AGS-T011	M	
8.3.4	AGS-T003	M	
	AGS-T004	M	
	AGS-T005	M	
8.3.5	AGS-T004	M	
	AGS-T005	M	
	AGS-T008	C1	執行本測試案例之條件詳後述。
8.4.1	AGS-T007	M	
	AGS-T008	C1	執行本測試案例之條件詳後述。
8.4.2	AGS-T007	M	
8.4.3	AGS-T007	M	
	AGS-T009	M	

上表必備/選項條件說明如下：

- C1： 若待測標的僅具單一網路介面，則不適用本測試案例。若待測標的具多重網路介面，可選項的執行本測試案例。

A.3. 物聯網設備

第 2-1 部對應節次	評估/測試案例	必備/選項	備註
6.1			本節無規定事項。
6.2	ITE-T001	M	本節為資料格式共同要求。
	ITE-T005	M	
6.3.1			本節不適用於物聯網設備之符合性測試。
6.3.2	ITE-E002	M	本節為存取介面共同要求。
	ITE-T001	M	
6.3.3	ITE-T001	M	本節為存取介面共同要求。
	ITE-T002	M	
	ITE-T005	M	
9.1			本節無規定事項。
9.2.1	ITE-T001	M	
9.2.2	ITE-T001	M	
	ITE-T011	M	
9.2.3	ITE-T001	M	
9.2.4			本節無規定事項。
9.3.1.1	ITE-T001	M	
9.3.1.2	ITE-T001	M	
9.3.1.3	ITE-T001	M	
	ITE-T008	M	
9.3.1.4	ITE-E001	M	
	ITE-T001	M	
9.3.1.5	ITE-T001	M	
	ITE-T009	M	
9.3.1.6	ITE-T001	M	
9.3.1.7	ITE-T001	M	
9.3.1.8	ITE-T001	M	
9.3.1.9			本節無規定事項。
9.3.2.1	ITE-T003	M	
9.3.2.2			本節無規定事項。
9.4.1	ITE-T001	M	
9.4.2	ITE-T001	M	
	ITE-T009	M	
	ITE-T010	M	
9.4.3	ITE-T001	M	
9.5.1	ITE-T001	M	

第 2-1 部對應節次	評估/測試案例	必備/選項	備註
9.5.2	ITE-T001	M	
	ITE-T002	M	
	ITE-T003	M	
9.5.3	ITE-T003	M	
9.5.4	ITE-T004	C1	執行本測試案例之條件詳後述。
9.6.1	ITE-T003	M	
9.6.2	ITE-T003	M	
	ITE-T005	M	
	ITE-T006	M	
	ITE-T007	M	

上表必備/選項條件說明如下：

- C1： 若待測標的具備多應用服務，且應用服務可於佈建後調整，則應執行本測試案例。若待測標的僅具備單一應用服務，或者應用服務皆為固定不可變更，則可選項的執行本測試案例。

A.4. 網路周邊裝置

第 2-1 部對應節次	評估/測試案例	必備/選項	備註
第 6 節			本節不適用於網路周邊裝置之符合性測試。
9.1			本節無規定事項。
9.2.1	NWP-T001	M	
9.2.2	NWP-E002	M	
	NWP-T001	M	
9.2.3			本節不適用於網路周邊裝置之符合性測試。
9.2.4			本節無規定事項。
9.3.1.1	NWP-T001	M	
9.3.1.2	NWP-T001	M	
9.3.1.3	NWP-T001	M	
9.3.1.4	NWP-E001	M	
	NWP-T001	M	
9.3.1.5			本節不適用於網路周邊裝置之符合性測試。
9.3.1.6			本節不適用於網路周邊裝置之符合性測試。
9.3.1.7			本節不適用於網路周邊裝置之符合性測試。
9.3.1.8			本節不適用於網路周邊裝置之符合性測試。
9.3.1.9			本節無規定事項。
9.3.2.1			本節不適用於網路周邊裝置之符合性測試。
9.3.2.2			本節無規定事項。
9.4			本節不適用於網路周邊裝置之符合性測試。
9.5			本節不適用於網路周邊裝置之符合性測試。
9.6			本節不適用於網路周邊裝置之符合性測試。

A.5. 組態伺服器

第 2-1 部對應節次	評估/測試案例	必備/選項	備註
6.1			本節無規定事項。
6.3.1	CFS-E001	M	
	CFS-T001	M	
6.3.2	CFS-T002	M	
6.3.3	CFS-T002	M	
10.1			本節無規定事項。
10.2	CFS-E003	M	
	CFS-E004	M	
10.3.1	CFS-E002	M	
	CFS-T001	M	
	CFS-T007	M	
10.3.2	CFS-T001	M	
	CFS-T002	M	
	CFS-T006	M	
10.3.3	CFS-E004	M	
	CFS-T002	M	
	CFS-T003	M	
	CFS-T005	M	
10.4.1	CFS-E002	M	
	CFS-T001	M	
10.4.2	CFS-T001	M	
	CFS-T002	M	
10.4.3	CFS-T002	M	
	CFS-T003	M	
10.4.4	CFS-T006	M	
10.4.5	CFS-E005	M	
	CFS-T003	M	
	CFS-T005	M	
	CFS-T006	M	
10.5.1	CFS-E002	M	
	CFS-T001	M	
	CFS-T007	M	
10.5.2	CFS-E006	M	
	CFS-T001	M	
	CFS-T004	M	
	CFS-T006	M	
10.5.3	CFS-T004	M	

A.6. 應用伺服器

第 2-1 部對應節次	評估/測試案例	必備/選項	備註
6.1			本節無規定事項。
6.3.1	APS-E001	M	
	APS-T001	M	
6.3.2	APS-T002	M	
6.3.3	APS-T002	M	
11.1			本節無規定事項。
11.2.1	APS-T001	M	
	APS-T005	M	
11.2.2	APS-T001	M	
11.2.3	APS-T002	M	
	APS-T003	M	
11.2.4	APS-T002	M	
11.3.1	APS-E002	C1	執行本測試案例之條件詳後述。
	APS-E003	C1	執行本測試案例之條件詳後述。
	APS-T004	C1	執行本測試案例之條件詳後述。
11.3.2	APS-T004	M	
11.3.3	APS-T005	M	
11.3.4	APS-T004	M	
11.3.5.1	APS-T004	C1	執行本測試案例之條件詳後述。
11.3.5.2	APS-E004	C2	執行本測試案例之條件詳後述。
11.3.5.3	APS-E005	C3	執行本測試案例之條件詳後述。
11.3.5.4			本節無規定事項。

上表必備/選項條件說明如下：

- C1： APS-E002、APS-E003 及 APS-T004，3 項測試/評估案例中應至少執行 1 項。
- C2： 若待測標的包含感測器型式服務應用，則可選項的執行本測試案例。
- C3： 若待測標的包含媒體紀錄型式服務應用，則可選項的執行本測試案例。

附錄B

(參考)

測試報告範本

待測標的資訊			測試案號：IOT-2022-TPI-00001
產品名稱	◇◇◇牌代理伺服器		
產品型號	TEST-AGS-001	產品種類	代理伺服器
硬體版本	R◇berryP◇ v4 Model B (2022)	軟體版本	1.0.0rc
執行環境	處理器指令集架構：AArch64 作業系統：Arch Linux ARM (2022/01) 軟體來源：作業系統內建、Avahi v0.8 (mDNS)、自行開發 (bootstrap) 主要軟體框架：Python 3		
製造廠商	中文：◇◇◇科技股份有限公司 英文：◇◇◇ Inc, co. ltd.		
聯絡方式	◇◇市◇◇路◇◇號◇樓		

檢測單位資訊	
檢測單位	○○科技股份有限公司
檢測場所	○○市○○路○○號○樓
檢測時間	2023/○○/01～2023/○○/04
檢測人員	李○○、林○○

測試個案紀錄

測試/評估案例	適用本次測試	測試時間	檢測人員	結果
AGS-E001	適用	2023/○○/01 09:00	李○○、林○○	通過
AGS-T001	適用	2023/○○/01 09:05	李○○、林○○	通過
AGS-T002	適用	2023/○○/01 09:10	李○○、林○○	通過
AGS-T003	適用	2023/○○/01 09:20	李○○、林○○	通過
AGS-T004	適用	2023/○○/01 09:35	李○○、林○○	通過
AGS-T005	適用	2023/○○/01 10:30	李○○、林○○	通過
AGS-T006	適用	2023/○○/01 11:20	李○○	通過
AGS-T007	適用	2023/○○/02 14:10	林○○	通過
AGS-T008	不適用	-	未測試	未測試
AGS-T009	適用	2023/○○/02 14:45	林○○	通過
AGS-T010	適用	2023/○○/02 15:30	林○○	通過
AGS-T011	適用	2023/○○/03 09:30	李○○、林○○	通過
AGS-T012	適用	2023/○○/03 09:40	李○○、林○○	通過

檢測執行人員簽名：

李○○ 2022/○○/03

林○○ 2022/○○/03

備註：

- 受測單位使用 1 台筆記型電腦作為支援工具，安裝 LDAP、Wireshark 及 PuTTY 等軟體。
- 待測標的僅具備單一網路介面，不適用 AGS-T008 測試條件

符合性檢測彙整報告				
規範章節	測試個案	必備/選項	檢測結果	備註
6.2	AGS-T007	必備	通過	
6.3.1	AGS-E001	必備	通過	
	AGS-T007	必備	通過	
	AGS-T009	必備	通過	
8.2.1	AGS-T001	必備	通過	
8.2.2	AGS-T001	必備	通過	
	AGS-T011	必備	通過	
	AGS-T012	必備	通過	
8.3.1	AGS-T001	必備	通過	
	AGS-T002	必備	通過	
	AGS-T003	必備	通過	
	AGS-T004	必備	通過	
	AGS-T007	必備	通過	
8.3.2	AGS-T001	必備	通過	
	AGS-T006	必備	通過	
8.3.3	AGS-T002	必備	通過	
	AGS-T010	必備	通過	
	AGS-T011	必備	通過	
8.3.4	AGS-T003	必備	通過	
	AGS-T004	必備	通過	
	AGS-T005	必備	通過	
8.3.5	AGS-T004	必備	通過	
	AGS-T005	必備	通過	
	AGS-T008	不適用	未測試	
8.4.1	AGS-T007	必備	通過	
	AGS-T008	不適用	未測試	
8.4.2	AGS-T007	必備	通過	
8.4.3	AGS-T007	必備	通過	
	AGS-T009	必備	通過	

綜合評量：

應執行測試/評估案例：12 件

已執行測試/評估案例：12 件

未符合案例：0 件

符合性檢測結果：

產品「◇◇◇牌代理伺服器（TEST-AS-001）」**通過**符合性檢測

報告簽署人簽名：

何○○ 2023/○○/05

參考資料

[1] CNS 690:2019 配線用插頭及插座－型式及尺度

[2] IEEE 802.1Q-2014, Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks

[3] IEEE 802.1X-2004, Port-Based Network Access Control

[4] IEEE 802.3ab-1999, Physical Layer Parameters and Specifications for 1000 Mb/s Operation over 4 pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T

[5] IEEE 802.3u-1995, Media Access Control (MAC) Parameters Physical Layer, Medium Attachment Units, and Repeater for 100Mb/s Operation, Type 100BASE-T

[6] IEEE 802.3z-1998, Media Access Control Parameters, Physical Layers, Repeater and Management Parameters for 1,000 Mb/s Operation

[7] SensorThings:2015, Open Geospatial Consortium 15-078r6, SensorThings API Part I - Sensing

5G 智慧杆系統技術規範
－第 3 部：安裝與結構相關安全要求及試驗法

5G Smart pole system technical specification
- Part 3: Installation and structure-related safety requirements and test methods

中 華 民 國 111 年 9 月

目錄

節次 頁次
前言 3
0. 簡介 4
1. 適用範圍 4
2. 引用標準 4
3. 用語及定義 5
3.1 智慧杆結構(structure of smart pole) 5
3.2 杆體(body) 6
3.3 箱體(box) 6
3.4 底座(foundation) 7
3.5 網路通訊設備(network communication equipment) 7
3.6Wi-Fi 無線網路設備(wireless Wi-Fi equipment) 7
3.7 照明設備(illumination equipment) 7
3.8 交通號誌(traffic light) 7
3.9 視訊監控設備(video monitoring equipment) 7
3.10 智慧路側單元(smart roadside unit) 7
3.11 充電設施(charging facility) 7
3.12 物聯網設備(IoT equipment) 7
3.13 數位看板(digital billboard) 7
3.14 緊急求助設備(emergency equipment) 7
3.15 環境監測設備(environmental monitoring equipment) 7
4. 附掛設備安裝要求 7
4.1 一般 7
4.2 電信網路微型基地臺 8
4.3Wi-Fi 網路設備 8
4.4 照明設備 8
4.5 交通號誌 8
4.6 視訊監視設備 8
4.7 數位看板 8
4.8 充電設施 8
5. 結構相關安全 8
5.1 一般 8
5.2 材料要求 8
5.3 結構相關安全要求 8
5.3.1 鍍鋅要求 8
5.3.2 抗拉強度要求 8
5.3.3 溫度要求 9

5.3.4 絕緣電阻與耐電壓要求 9
5.3.5 耐蝕性要求 9
5.3.6 抗風要求 9
5.3.7 耐震要求 9
5.4 結構相關安全試驗法 9
5.4.1 鍍鋅層附著量及均勻性試驗 9
5.4.2 抗拉強度試驗 9
5.4.3 溫度試驗 9
5.4.4 絕緣電阻與耐電壓試驗 9
5.4.5 耐蝕性試驗 10
5.4.6 抗風試驗 10
5.4.7 耐震試驗 10
附錄 A（參考）智慧杆底座與接地阻抗要求 11
附錄 B（參考）智慧杆之設計示例 12
參考資料 14

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole)現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT)設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60 Hz 及 500 V 以下交流電源供電之智慧杆系統的安裝與結構相關安全要求及試驗法。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 1247	熱浸鍍鋅檢驗法
CNS 2111	金屬材料拉伸試驗法
CNS 2112	金屬材料拉伸試驗片
CNS 2473	一般結構用軋鋼料
CNS 4117	道路照明用燈杆（漸細型）
CNS 5422	漏電斷路器
CNS 6445	配管用碳鋼鋼管
CNS 8503	熱浸法鍍鋅作業方法
CNS 8886	鹽水噴霧試驗法
CNS 9118	道路照明燈具

CNS 10007	鋼鐵之熱浸鍍鋅
CNS 14165	電器外殼保護分類等級(IP 碼)
CNS 14335	燈具一般要求
CNS 14335-2-3	燈具－第 2-3 部：道路及街道照明用燈具之個別要求
CNS 14546	發光二極體交通號誌燈燈面及燈箱
CNS 14676-5	電磁相容－測試與量測技術－第 5 部：突波抗擾度測試
CNS 15176-1	風力機－第 1 部：設計要求
CNS 15598-1	影音、資訊及通訊技術設備 第 1 部:安全要求
CNS 16069	高速公路及快速道路 LED 路燈
IEC 60950-22	Information technology equipment - Safety - Part 22: Equipment to be installed outdoors
IEC 61000-4-5	Electromagnetic compatibility (EMC) Part 4-5:Testing and measurement techniques - Surge immunity test
IEC 61969-3	Mechanical structures for electrical and electronic equipment - Outdoor enclosures - Part 3: Environmental requirements, tests and safety aspects
內政部營建署	建築物耐風設計規範及解說
內政部營建署	建築物耐震設計規範及解說

3. 用語及定義

下列用語及定義適用於本規範：

3.1 智慧杆結構(structure of smart pole)

智慧杆之結構部分係指杆體、箱體及底座，如圖 1、2 所示。

備考：智慧杆定義參照第 1 部

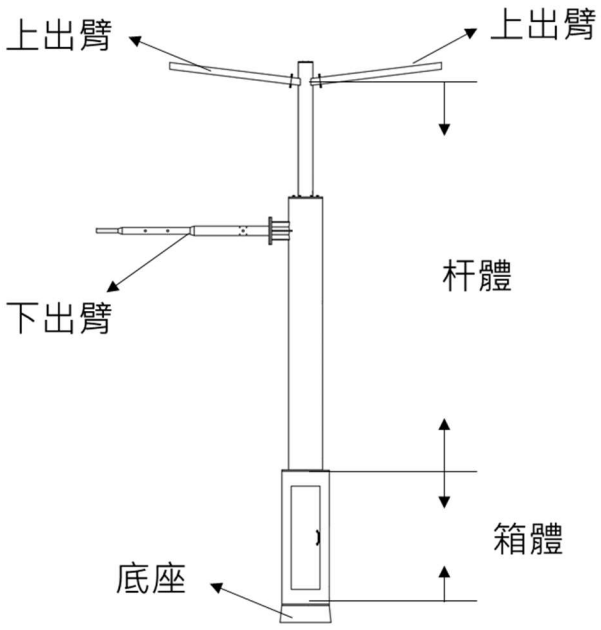


圖 1　單側式智慧杆示意圖

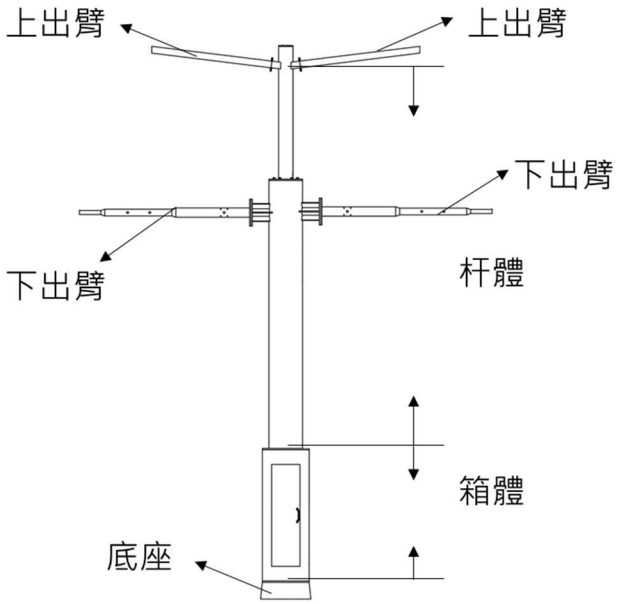


圖 2　雙側式智慧杆示意圖

3.2 杆體(body)

杆體包含主杆及上、下出臂，如圖 3 所示。

附掛設備安裝於杆體之規劃如下：

(a) 杆頂：電信網路微型基地臺。`

(b) 主杆上部：Wi-Fi 網路設備、視訊監控設備、智慧路側、數位看板、環境監測設備等。

(c) 主杆下部：互動數位看板等。

(d) 上出臂：照明設備等。

(e) 下出臂：交通號誌及路牌等。

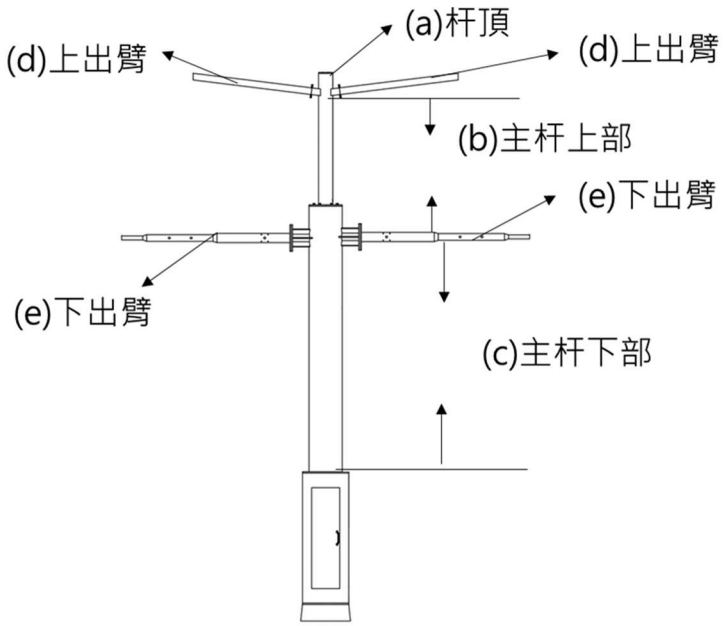


圖 3　智慧杆分層定義示意圖

3.3 箱體(box)

位於杆體下方與杆體結合之儲存空間，可用於存放電源供應、充電設施、物聯網設備、智慧杆迴路管理伺服器、緊急求助等設備，使其能避免因環境及氣候因素影響而失效。

箱體亦可與杆體整合為一體。

備考：若箱體空間不敷需求，則可於杆體附近另設附屬箱體，設置數量不限。

3.4 底座(foundation)

於智慧杆箱體底部與基礎結合之固定結構，用以穩固智慧杆之架設。底座亦可與箱體整合為一體。

3.5 網路通訊設備(network communication equipment)

用於提供智慧杆各子系統網際網路連線功能，包含網路層、傳輸層。

3.6Wi-Fi 無線網路設備(wireless Wi-Fi equipment)

將網路訊號用於提供民眾 Wi-Fi 無線網路及網際網路公眾連網服務。

3.7 照明設備(illumination equipment)

用於提供智慧杆周邊人行或車行道路照明。照明設備應能透過網路通訊設備進行資料交換，執行回報及控制等功能。

3.8 交通號誌(traffic light)

包含路口號誌、路口號誌控制器、資訊可變標誌控制器、車輛偵測控制器等。

3.9 視訊監控設備(video monitoring equipment)

可捕捉、紀錄、傳送光學視訊資訊之攝影機（含鏡頭）及數位資料處理裝置。攝影機應安裝於杆體上，並透過內建或外接之數位資料處理設備，將其捕捉之光學視訊資訊以數位化方式紀錄，並能透過網路通訊設備執行如事件回報、影像資訊傳輸等功能。

3.10 智慧路側單元(smart roadside unit)

車聯網技術搭配 5G、Wi-Fi 或短距離傳輸，提供可即時更新之道路交通號誌、狀況與路況等訊息給車輛與行人。

3.11 充電設施(charging facility)

用於提供電動車輛充電功能。

3.12 物聯網設備(IoT equipment)

具有網際網路通訊介面，並可提供各種應用服務，通常安裝於智慧杆迴路。物聯網設備之外型、外觀及功能皆依實際需求而定(例：環境感測器、智慧看板及邊緣運算裝置等)。

3.13 數位看板(digital billboard)

透過聲音與影像傳遞訊息之面板，主要作為政策宣導、緊急事件推播、資訊發布與互動式即時資訊查詢功能之設備。

3.14 緊急求助設備(emergency equipment)

透過影像與語音發出呼救功能之設備，與管理平台後台系統直接連結，由管理人員提供服務或協助。

3.15 環境監測設備(environmental monitoring equipment)

如溫度、濕度、風向、風速、雨量、紫外線、PM2.5、噪音等周遭環境感測設備。

4. 附掛設備安裝要求

4.1 一般

除智慧杆使用場域環境對附掛設備之安裝具有其他特殊需求外，應依照本規範進行附掛設備安裝。

4.2 電信網路微型基地臺

電信微型基地臺安裝於杆頂， 且應與其他具有天線或接收、發送之無線設備保持適當距離， 避免通訊設備互相干擾。微型基地臺周圍有易干擾信號之金屬物體時，應調整微型基地臺之天線方向或與干擾物體保持適當距離。固裝微型基地臺用之凸緣盤應以螺栓鎖固或焊接方式固定在杆體上。

4.3Wi-Fi 網路設備

Wi-Fi 網路設備以側面掛載方式安裝於杆體上部位置，並與微型基地臺保持適當距離，Wi-Fi 設備與杆體之固定方式，以卡箍搭配螺絲將其固定於杆體上。

4.4 照明設備

智慧杆照明設備(燈具)之安裝方式分為與杆體一體成型式燈具及整體式燈具兩種，採用一體成型式時，燈具中之光源於智慧杆設置完成後，現場安裝光源；採用整體式時，由於燈具本體無法拆卸，用螺絲將燈具直接固定安裝於上出臂，方便後續保養更換。

4.5 交通號誌

交通號誌(紅綠燈)應藉由焊接或螺絲固定等施作工法，固定於智慧杆的杆體上，方便後續保養更換。

4.6 視訊監視設備

視訊監視設備依據智慧杆應用之場域與實際使用需求，安裝於杆體上，安裝時應以鏡頭不受周圍設備或線路遮蔽為原則，使用卡箍與螺絲等進行固定。

4.7 數位看板

訊息發布使用之數位看板，安裝於杆體上，使用卡箍與螺絲固定。互動式數位看板安裝於主杆下部，設置高度以便利使用者操作之高度為原則，使用卡箍與螺絲固定。

4.8 充電設施

本節規範與智慧杆結構相關之安全要求， 以使智慧杆在布建後之使用期間， 其結構不會對使用者、行人及車輛造成危害， 並相當程度保護智慧杆內部設備及外掛設備的安全及穩定運轉。

5. 結構相關安全

5.1 一般

本節規範為智慧杆結構相關之安全要求，以使智慧杆在布建後之使用期間， 其結構不會對使用者、行人及車輛造成危害，並相當程度保護智慧杆內部設備及外掛設備的安全及穩定運轉。

5.2 材料要求

杆體、箱體及底座材質應採用 CNS 2473 之 SS400 或同等以上材質。

5.3 結構相關安全要求

5.3.1 鍍鋅要求

鍍鋅層附著量及均勻性依 CNS 4117 第 5 節之規定。

5.3.2 抗拉強度要求

智慧杆之材料抗拉強度應能夠符合負載情況下之使用安全，材料強度拉伸試驗依照 CNS 2111 求得抗拉強度、降伏強度與伸長率並符合 CNS 2473 標準之表 3 規定，拉

伸試驗所使用之金屬試片需依 CNS 2473 第 5 節之規定。

5.3.3 溫度要求

依據 CNS 15598-1 第 9.3 節標準定義金屬表面在設備工作情況下，身體接觸智慧杆外部金屬時的表面最大溫度限制，並以 9.2 節中最嚴格的熱能量源分級 TS1 作為金屬表面溫度定義。

5.3.4 絕緣電阻與耐電壓要求

依據 CNS 9118 標準規定進行絕緣電阻與耐電壓試驗，試驗結果須符合規範要求。

5.3.5 耐蝕性要求

依據 CNS 8886 中性鹽霧試驗標準，試驗後目視觀察試驗板表面應無產生腐蝕、起泡、剝離現象。

5.3.6 抗風要求

智慧杆應經過適當設計，且設計中需考慮外部條件(如：加裝之附掛設備)，以安全承受本規範所訂定抗風要求之風況。智慧杆之抗風要求，應符合 CNS 15176-1 對風力機或建築物耐風設計規範及解說中對抗風之規範，以確保當智慧杆之結構面對 17 級風之極端風況時，不發生倒塌、斷裂、傾斜、彎折等重大安全問題為設計原則。

5.3.7 耐震要求

為確保強化智慧杆之抗震能力，智慧杆應經過專業技師簽認設計，且設計中需考慮外部條件(如：加裝之附掛設備)，以安全承受所訂定耐震要求之震度。智慧杆之耐震要求，應符合 CNS 15176-1 對風力機或建築物耐震設計規範及解說之耐震基本原則訂定，智慧杆之結構體在中小度地震時保持在彈性限度內；設計地震時容許產生塑性變形，但韌性需求不得超過容許韌性容量；最大考量地震時則使用之韌性可以達規定之韌性容量，而不發生倒塌、斷裂、傾斜、彎折等重大安全問題為設計原則。以上所稱中小度地震為回歸期 50 年之地震，設計地震為回歸期 475 年之地震，最大考量地震為回歸期 2475 年之地震。

5.4 結構相關安全試驗法

5.4.1 鍍鋅層附著量及均勻性試驗

鍍鋅層附著量及均勻性試驗：

(1)鍍鋅層附著量參照 CNS 1247 之 5.2 間接法試驗。

(2)鍍鋅層均勻性參照 CNS 1247 之第 6 節試驗。

5.4.2 抗拉強度試驗

(1)拉伸試片應取自智慧杆之杆體，並參照 CNS 2473 表 3 之規定。

(2)拉伸試驗參照 CNS 2111。

5.4.3 溫度試驗

參照 CNS 15598-1 之 9.3.2 試驗。

5.4.4 絕緣電阻與耐電壓試驗

(1)絕緣電阻試驗：參照 CNS 9118 執行試驗。

(2)耐電壓試驗：參照 CNS 9118 執行試驗。

5.4.5 耐蝕性試驗

參照 CNS 8886 中性鹽霧試驗法試驗。

5.4.6 抗風試驗

製造商應提出符合本規範智慧杆(含相關附屬裝置)抗風設計，至少可抵抗最大風速 17 級風之相關證明資料(設計報告中，應詳述極端風況風速下之抗風設計值，以防止危險造成之損壞)。

試驗依下列擇 1 規定實施：

(1)製造商設計智慧杆時，應參考建築物耐風設計規範及解說中之各項抗風與設計耐風相關計算公式進行設計，試驗結果應取得結構技師認證。

(2)無法將智慧杆整體進行抗風試驗時，可透過第三方單位認可之模擬分析軟體進行試驗，將智慧杆模型與尺度等設計參數輸入模擬軟體進行抗風模擬，測試其抗風程度是否符合至少可抵抗最大風速 17 級風之要求。

5.4.7 耐震試驗

製造商應提出符合本規範智慧杆耐震設計，可抵抗至少震度 6 弱之相關證明資料(設計報告中，應詳述智慧杆之各項耐震值，以防止危險造成之損壞)

試驗依下列擇 1 規定實施：

(1)製造商設計智慧杆時，應參考建築物耐震設計規範及解說中之各項耐震與設計地震相關計算公式進行設計，試驗結果應取得結構技師認證。

(2)無法將智慧杆整體進行耐震試驗時，可透過第三方單位認可之模擬分析軟體進行試驗，將智慧杆模型與尺度等設計參數輸入模擬軟體進行地震模擬，測試其耐震程度是否符合面對震度 6 弱時不發生倒塌、斷裂等重大安全問題之要求。

附錄 A

(參考)

智慧杆底座與接地阻抗要求

A.1 智慧杆基礎底座：(僅供業者參考)

為埋入地下並用以提供智慧杆整體穩定性之部分，基礎之設計應確保在各種狀態下不會產生傾倒、翻覆、滑動，並得以土壤被動土壓、基礎反力以及結構自重，做為提供穩定性之來源。除應依據建築物基礎設計規範與解說予以妥善設計外，基礎四周土壤皆應夯壓緊實。



圖 A.1　智慧杆基礎示意圖

A.2 接地阻抗要求

為因應智慧杆內部將會裝設大量用電設備與線路，並配合智慧杆使用安全考量，杆體需配置接地保護，避免漏電造成操作者與路上用路人之危害，杆體應符合內政部營建署-通則第 16529 章廣場照明設備要求做為接地阻抗要求標準，智慧杆、開關箱等設備，施工承攬廠商應以責任施工方式作妥接地，接地電阻應在 50Ω 以下。

A.3 接地阻抗試驗要求

(a) 試驗：試驗依下列規定

量測杆體之接地端與杆體表面兩端之接地電阻，量測到之接地電阻需在 50 Ω以下，避免當接地失效時，觸碰杆體表面發生導電危險。

附錄 B

(參考)

智慧杆之設計示例

B.1 尺度要求 (僅供業者參考)

(a) 智慧杆高度至少為 8m 規格(依據微型基地臺涵蓋率)。

(b) 杆體之外接圓直徑建議至少為 500mm；箱體之外接圓直徑建議至少為 550mm。

(c) 材質: SS400(低碳鋼)。

(d) 智慧杆各部設計時之建議尺度如表 B.1 所示：

智慧杆設計時之實際尺度，用以下建議方案之規格為基礎，可針對實際使用場景、周遭環境與特殊需求等，進行綜合因素評估後，以不造成安全性問題為原則，進行細部調整。因應使用環境之不同，杆體之設計可採用圓柱形或多邊形方式設計，杆頂之外部遮罩使用非金屬材質，避免對內部的裝置產生訊號干擾或屏蔽的問題。

表 B.1　8m 智慧杆建議規格

部位		尺度	參考來源 註 1
杆體	杆體	寬 500mm × 高 8000mm × 厚 6mm	(1)
	頂部	Φ500mm × 高 500mm	-
	出臂(路燈)	長 2000mm	(1)
	出臂(號誌燈)	長 3500mm	(2)
	交通號誌	高 5500mm(距離地面)	-
	路名牌(直式)	長 900mm × 寬 450mm	(3)
	路名牌(橫式)	長 900mm × 寬 300mm	(3)
	方向指示牌	長 2400mm × 寬 900mm	(3)
	道路遵行指示牌	Φ600mm	(3)
箱體	箱體	Φ550mm × 高 2000mm × 厚 6mm	-
基礎	底座(梯形)	寬 650mm~750mm × 高 250mm	-
	埋入部分之深度	700mm	(1)

註 1 參考來源：

(1) 全臺設置 LED 路燈技術規範，104 年，經濟部能源局

(2) 號誌設計因素之探討，93 年，交通部運輸研究所

(3) 道路交通標誌標線號誌設置規則，110 年，交通部

(e) 智慧杆附掛設備與裝置之建議重量、尺度如表 B.2 所示：

實際重量與尺度規格以業者實際狀況為主。

表 B.2　重量、尺度要求建議規格

項目	重量	尺度
智慧照明	15kg	620mm╳24 mm╳70mm
Wi-Fi	1kg	230mm╳175mm╳70mm
空氣盒子	0.3kg	150mm╳110mm╳47mm
交通號誌	11.6kg	1280mm╳32mm╳27mm
光達	1.5kg	200mm╳200mm╳200mm
雷達	1kg	150mm╳100mm╳50mm
車聯網	3.2kg	300mm╳79mm╳249mm
影像監視	7kg	700mm╳250mm╳500mm

B.2 許可差

(a) 長度:杆長±0.8%。

(b) 橫截面尺度:標稱值±0.5%。

(c) 尺度長寬許可差:±2 mm。

(d) 檢修門框尺度:±5 mm。

(e) 出臂伸長度:±2%。

參考資料

[1] 全臺設置 LED 路燈技術規範，104 年，經濟部能源局

[2] 號誌設計因素之探討，93 年，交通部運輸研究所

[3] 道路交通標誌標線號誌設置規則，110 年，交通部

[4] 低功率射頻電機技術規範，107 年，國家通訊傳播委員會

[5] 建築物耐震設計規範及解說，100 年，內政部

[6] 建築物耐風設計規範及解說，103 年，內政部

[7] 市區道路及附屬工程設計規範，111 年，內政部

5G 智慧杆系統技術規範

- 第 4 部：環境可靠度要求

5G Smart pole system technical specification

- Part 4: Environmental reliability requirements

中 華 民 國 111 年 9 月

目錄

節次 頁次

前言 2

0. 簡介 3

1. 適用範圍 3

2. 引用標準 3

3. 用語及定義 4

3.1 最大操作溫度(maximum operating temperature, *Tmax*) 4

3.2 隨機振動(random vibrations) 4

3.3 加速度頻譜密度(acceleration spectral density, ASD) 4

3.4 程序 Sa 2 (procedure Sa 2) 4

4. 一般要求 4

4.1 低溫操作試驗 5

4.2 高溫操作試驗 5

4.3 濕熱試驗 5

4.4 日照試驗 6

4.5 防塵防水試驗 6

4.6 振動試驗 7

4.7 鹽水噴霧試驗 8

4.8 溫度循環試驗 9

4.9 濕熱循環試驗 10

4.10 風洞試驗 12

參考資料 13

前言

本規範係依 CNS 3689 「國家標準草案構成及格式之指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole)現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT)設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60 Hz 及 500 V 以下交流電源之多用途智慧杆系統，包含 5G 微型基地臺、自駕車路側設備、空氣品質感測器、氣象感測器、Wi-Fi 裝置、影像與語音緊急求助裝置、充電樁、迴路控制箱等附掛設備之試驗要求。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 3622	環境試驗法（電氣、電子）通則
CNS 3623	環境試驗法（電氣、電子）–濕熱（穩態）試驗
CNS 3633	環境試驗法（電氣、電子）–溫度變化試驗
CNS 3634	環境試驗方法（電氣、電子） –高溫（耐熱性）試驗方法
CNS 8886	鹽水噴霧試驗法
CNS 11233	環境試驗法（電氣、電子）–低溫(耐寒性)試驗法
CNS 12565	環境試驗方法（電氣、電子）–溫濕度循環（12＋12 小時循環）試驗方法
CNS 12874	環境試驗法（電氣、電子）–鹽霧（循環）試驗
CNS 14165	電器外殼保護分類等級(IP 碼)
CNS 15425-1	電動機車充電系統 - 第 1 部：一般要求

CNS 15481-4	道路車輛－電機電子配備環境條件與試驗－第 4 部：氣候負載
CNS 15511-1	電動車輛傳導式充電系統－第 1 部：一般要求
CNS 16069	高速公路及快速道路 LED 路燈
IEC 60068-2-64	Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance

3. 用語及定義

本規範適用「5G 智慧杆系統技術規範－第 1 部：一般要求」之用語及定義，以及下列用語及定義適用於本規範。

3.1 最大操作溫度(maximum operating temperature, *Tmax*)

系統/組件能連續操作時之最高周圍溫度。

3.2 隨機振動(random vibrations)

在任何給定的時間，其瞬間值無法預測之振動[1]。

3.3 加速度頻譜密度(acceleration spectral density, ASD)

當帶寬接近零且平均時間接近無限大時，每單位帶寬，其加速度信號通過窄帶濾波器之中心頻率均方值[1]。

3.4 程序 Sa 2 (procedure Sa 2)

提供日照試驗之試驗法 Sa 的三種試驗方式，分為程序 Sa 1：適用於熱效應評估、程序 Sa 2：適用於退化效應評估及程序 Sa 3：適用於光化學效應評估。

4. 一般要求

智慧杆附掛設備應依表 1 智慧杆附掛設備與試驗項目對照表之試驗項目進行測試。

表 1　智慧杆附掛設備與試驗項目對照表

設備試驗項目(節次)	5G 微型基地臺	自駕車路側設備	空氣品質感測器、氣象感測器、Wi-Fi 裝置	影像與語音緊急求助裝置	充電樁	迴路控制箱
低溫操作試驗 (4.1)	○	○	○	○	○	○
高溫操作試驗 (4.2)	○	○	○	○		○
濕熱試驗 (4.3)	○	○	○	○	○	○
日照試驗 (4.4)	△	△	△			
防塵防水試驗 (4.5)	○	○	○	○	○	○
振動試驗 (4.6)	○	○	○	○		
鹽水噴霧試驗 (4.7)	○	○		○		
溫度循環試驗 (4.8)	○	○				
濕熱循環試驗 (4.9)	○	○				
風洞試驗 (4.10)	○					

備考 1. 「○」智慧杆附掛設備應符合相關試驗要求。

備考 2. 「△」如有需要可選擇之試驗項目。

4.1 低溫操作試驗

4.1.1 目的

此試驗模擬智慧杆附掛設備暴露於低溫且供電之情形。為評估產品對低溫耐受之能力或動作之能力，例如於極低之周圍溫度下操作裝置，失效模式可能為低溫造成電氣故障。

4.1.2 試驗法

依 CNS 11233 及 CNS 3622 進行試驗，以溫度變化≦1℃/min 下降至-20 ℃，並維持 16 小時後回復至室溫環境。

備考：電動汽車充電相關設備依 CNS 15511-1 之 12.10 進行試驗。

4.1.3 要求

智慧杆附掛設備於試驗前後，均須進行外觀及功能確認，且試驗期間與試驗後，裝置仍可維持正常操作。

備考：電動汽車充電相關設備須符合 CNS 15511-1 之 12.10 要求。

4.2 高溫操作試驗

4.2.1 目的

此試驗模擬智慧杆附掛設備暴露於高溫且供電之情形。為評估產品對高溫耐受之能力或動作之能力，例如於極高之周圍溫度下操作裝置，失效模式可能為高溫造成電氣故障。

4.2.2 試驗法

依 CNS 3634 及 CNS 3622，以溫度變化≦1 ℃/min。

升溫至製造商所指定最大操作溫度高 10 ℃(但高 10 ℃後之試驗溫度不可低於 60 ℃)，並連續進行 96 小時試驗。未指定最大操作溫度時，則以 60 ℃條件進行試驗。

4.2.3 要求

智慧杆附掛設備於試驗前後，均須進行外觀及功能確認，且試驗期間與試驗後，裝置仍可維持正常操作。

4.3 濕熱試驗

4.3.1 目的

此試驗模擬智慧杆附掛設備在穩定之高周圍相對濕度下的使用情況。為評估產品置於定溫高濕下規定時間後的效應，失效模式為濕氣造成電氣故障。

4.3.2 試驗法

(a) **自駕車路側設備**

依 CNS 15481-4 之 5.7 進行試驗，試驗條件為溫度(40 ± 2)℃及相對濕度(85 ± 3)%，並連續進行 21 天試驗。

(b) **5G 微型基地臺、空氣品質感測器、氣象感測器、Wi-Fi 設備、影像與語音緊急求助裝置、迴路控制箱**

依 CNS 3623 及 CNS 3622 進行試驗。各附掛設備應符合溫度(40 ± 2)℃及相對濕度(93 ± 3)%，並持續 240 小時試驗。

備考：電動汽車充電相關設備依 CNS 15511-1 之 12.9 進行試驗。

4.3.3 要求

智慧杆附掛設備於試驗前後，均須進行外觀及功能確認，且試驗期間與試驗後，裝置仍可維持正常操作。

備考：電動汽車充電相關設備須符合 CNS 15511-1 之 12.9 要求。

4.4 日照試驗

4.4.1 目的

此試驗為確保智慧杆附掛設備，遭受太陽輻射之熱效應及光化效應影響，可能造成材料特性損害或影響其裝置的耐久性等，甚至影響功能。應選擇適當材質，以確保對太陽輻射之抵抗力及可承受曝露在太陽輻射下時，當產品執行動作試驗期間所受到誘發造成的熱效應而影響功能。

4.4.2 試驗法

依 IEC60068-2-5 之程序 Sa 2 進行試驗，幅照強度應為 1,090 W/m^2 ± 10 %及溫度 50 ℃下，每個日循環的總輻照強度量為 21.8 kWh/m^2，日照時間為 20 小時照射，4 小時暗黑，共執行 10 個循環試驗，日照循環試驗圖參照圖 1 [3][4]。

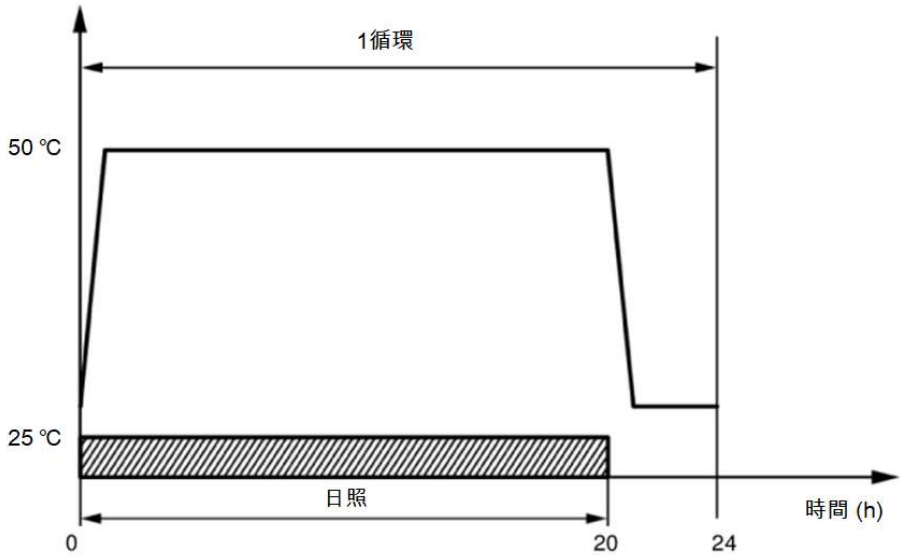


圖 1　日照循環試驗圖[3][4]

4.4.3 要求

智慧杆附掛設備執行日照試驗時，於試驗前後均須進行外觀及功能確認，且試驗期間與試驗後，裝置仍可維持正常操作。

4.5 防塵防水試驗

4.5.1 目的

此試驗為確保智慧杆附掛設備受到外來固體物或水侵入內部設備造成損害性影響之防護。

4.5.2 試驗法

依 CNS 14165 之防護等級進行試驗。

4.5.3 要求

(a) 電動汽車充電相關設備須符合 CNS 15511-1 之 12.4 要求。

(b) 電動機車充電相關設備須符合 CNS 15425-1 之 4.3.5 要求。

(c) 智慧杆杆體與箱體之防護等級，應不低於 IP55 之要求。試驗結果符合本系列規範第 3 部之 5.4.4 之防水、防塵要求時，此項可判定符合。

(d) 其他智慧杆非杆體內附掛設備之防護等級，應不低於 IP65 之要求。試驗結果符合本系列規範第 5 部之 4.2 之粉塵、固體外物及水侵入之防護要求，此項可判定符合。

4.6 振動試驗

4.6.1 目的

此試驗係檢查智慧杆附掛設備，是否因振動而產生故障與損壞，執行試驗之目的，乃在瞭解產品在運輸過程或在既定使用環境下，可能發生的機械強度不足或劣化情況，並利用試驗以確認其可耐振動傷害的程度，例如機構變形、扣件鬆脫、脫落或龜裂等現象。

4.6.2 試驗法

(a) 5G 微型基地臺

依 NEBS 環境模擬 GR-63-CORE Zone 4 等級進行試驗，其試驗條件參照表 2[5]。

表 2　振動試驗條件[5]

座標點 Coordinate Point	頻率(Hz) Frequency (Hz)	上層加速度值(g) Values for Upper Floor Acceleration (g)
1	0.3	0.2
2	0.6	2.0
3	2.0	5.0
4	5.0	5.0
5	15.0	1.6
6	50.0	1.6

(b) 自駕車路側設備、空氣品質感測器、氣象感測器、Wi-Fi 裝置、影像與語音緊急求助裝置

依 IEC 60068-2-64 之 Table A.4 Category No. 3 的振動條件以及 Spectrum A.2 Stationary installation 試驗曲線進行試驗。圖 2 為振動試驗曲線圖及表 3 為隨機振動試驗條件。試驗時使附掛設備朝 3 個相互垂直之方向(X、Y、Z)

振動，試驗頻率：10 Hz ~ 500 Hz，每個軸向振動 4 小時，共 12 小時。

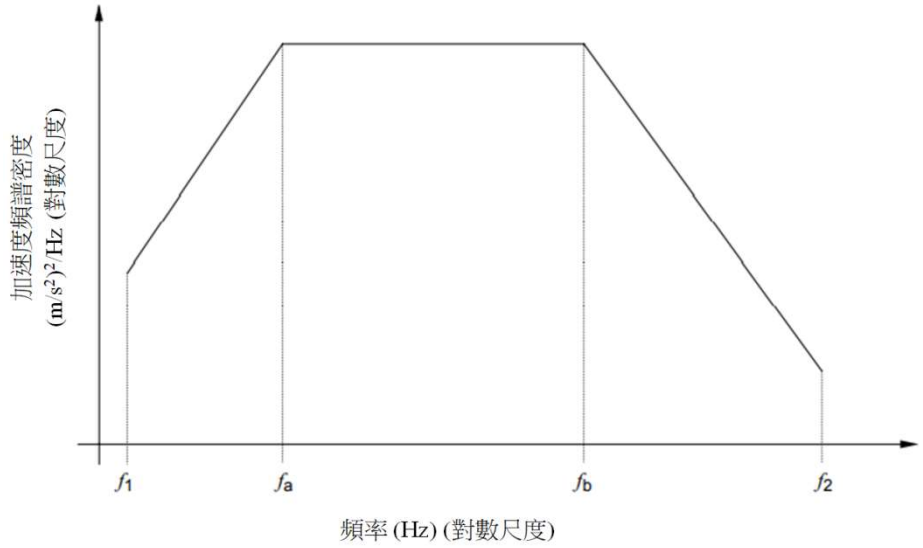


圖 2　振動試驗曲線圖

表 3　隨機振動試驗條件

頻率 (Hz)		加速度頻譜密度 $((m/s^2)^2/Hz)$
f_1	10	0.022
f_a	30	0.20
f_b	200	0.20
f_2	500	0.0052
7.0 g_{rms}		

4.6.3 要求

智慧杆附掛設備於試驗前後，均須進行外觀及功能確認，外觀檢查裝置不得有變形、鬆扣、脫落或龜裂等現象。且試驗後，裝置仍可維持正常操作。

4.7 鹽水噴霧試驗

4.7.1 目的

此試驗為模擬智慧杆附掛設備之金屬材料、合金、板材與塗層等，對於遭受到鹽霧及濕熱條件下的抵抗能力，嚴重可能因侵蝕造成結構影響或鹽害侵入造成電氣上的損壞。

4.7.2 試驗法

依 CNS 12874 及 CNS 3622 試驗 Kb 之標準方法 1 進行試驗。試驗條件為每一循環 7 天，包含執行 2 小時鹽水噴霧、6 天又 22 小時濕熱，需進行 4 個循環(共 28 天)試驗，參照圖 3。

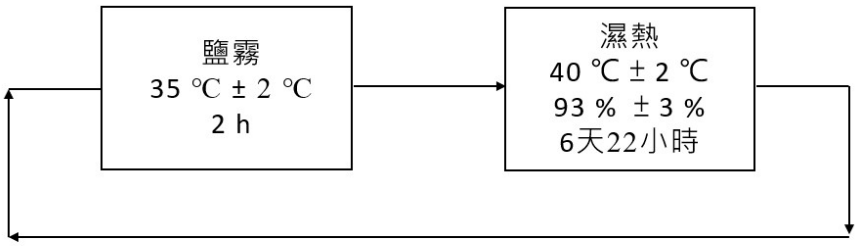


圖 3　鹽水噴霧循環試驗

4.7.3 要求

試驗後進行目視檢查，項目包含識別、外觀及表面狀態不可有腐蝕現象。

檢查方式在最合適之距離與適當光線下，以目視檢查 RN 值應在 9.3 以上，參照 CNS 8886 附錄 1 (規定)數字分級法，且試驗後裝置仍可維持正常操作。

4.8 溫度循環試驗

4.8.1 目的

此試驗模擬智慧杆附掛設備，隨溫度變化之電氣操作情況，為評估產品對周圍溫度變化之耐受程度及/或維持其正常功能之能力，例如於周圍溫度變化下操作系統/組件，用以確保在連續溫度變化下還能正常操作。失效模式為溫度變化時造成電氣故障。

4.8.2 試驗法

依 CNS 3633 及 CNS 3622 之溫度定速變化試驗(Nb 試驗)進行

溫度循環。

試驗開始溫度為 20 ℃，依規定降溫到-20 ℃並維持 90 分鐘，之後升溫至製造者所指定最大操作溫度高 10℃(但高 10℃後之試驗溫度不可低於 60℃)並維持 110 分鐘，隨後降溫至 20 ℃為 1 個循環試驗，需進行 30 次循環試驗(若未指定最大操作溫度時，則以 60 ℃條件進行試驗)。表 4 為溫度循環試驗之溫度與時間對照表，圖 4 溫度循環之指定變化率曲線。

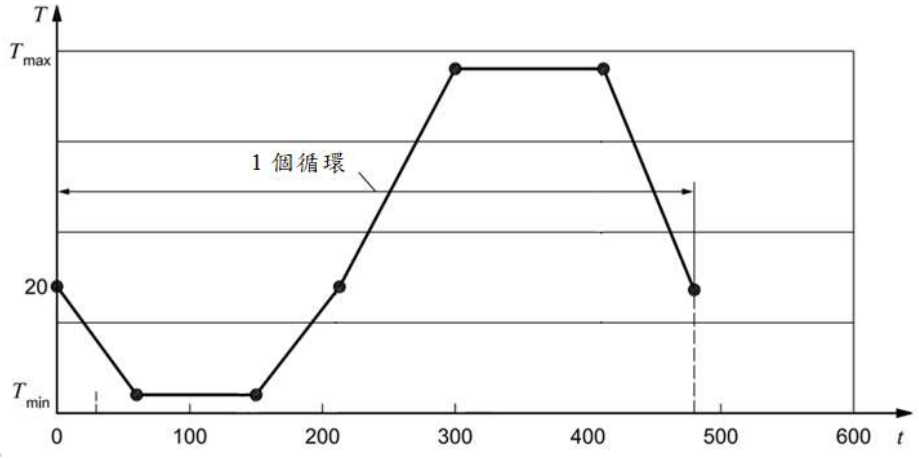


圖 4　溫度循環之指定變化率曲線

說明

T 溫度(℃)

t 時間(min)

Tmin：*-20* ℃

Tmax：製造商所指定最大操作溫度

表 4　溫度循環之溫度與時間對照表(參照圖 4)

時間 (min)	試驗溫度(℃)
0	20
60	-20
150	-20
210	20
300	*Tmax* + 10[(a)]
410	*Tmax* + 10[(a)]
480	20
註：[(a)]若未指定最大操作溫度時，則以 60 ℃條件進行試驗。 *Tmax* + 10：不可低於 60℃。	

4.8.3 要求

智慧杆附掛設備於試驗前後,均須進行外觀及功能確認,且試驗期間與試驗後，裝置仍可維持正常操作。

4.9 濕熱循環試驗

4.9.1 目的

此試驗模擬智慧杆附掛設備在高濕度之狀態下返復溫度變化時,產品之表面產生結露之條件下的耐受程度及/或維持其正常功能之能力。失效模式為濕氣侵入造成電氣故障。

4.9.2 試驗法

依 CNS 12565 及 CNS 3622 所規定之試驗 Db 的方法 1 進行試驗，試驗包括濕熱循環試驗之穩定期間及循環測試(參照圖 5 及圖 6)。上限溫度：55 ℃。循環次數：6 次。

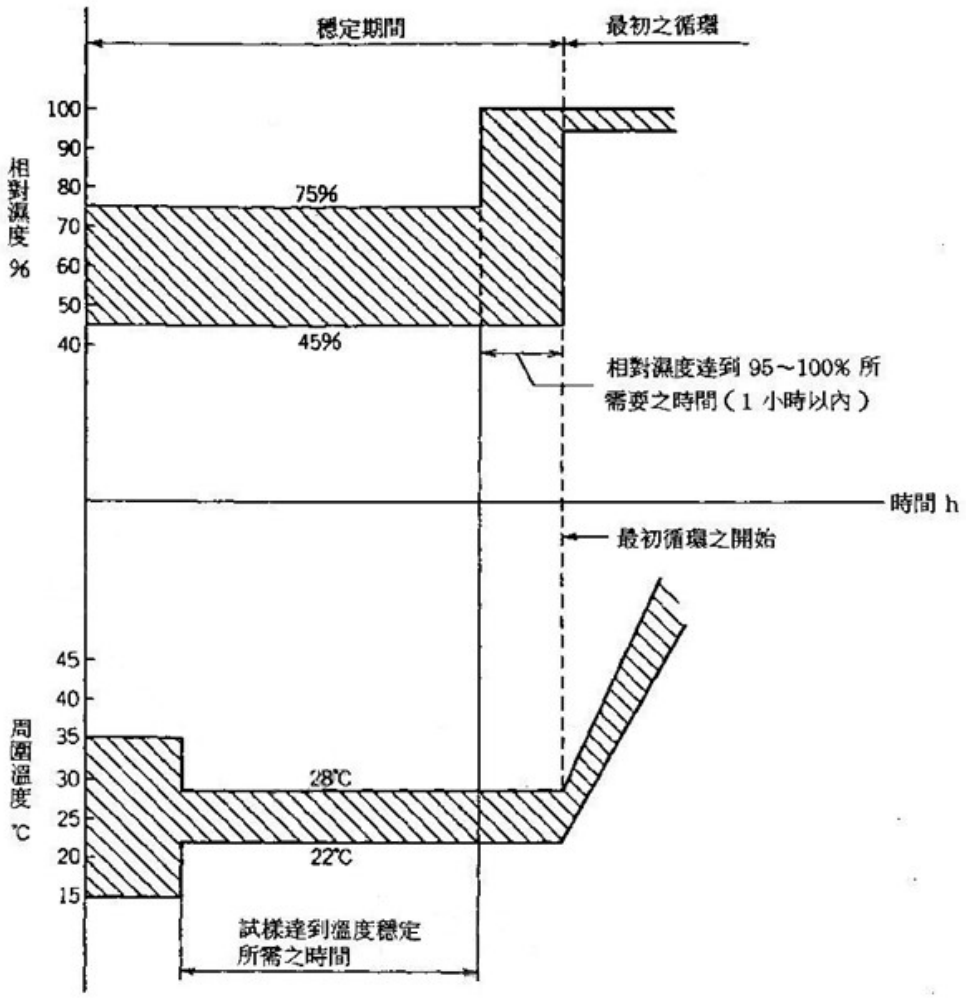


圖 5　濕熱循環試驗(穩定期間)

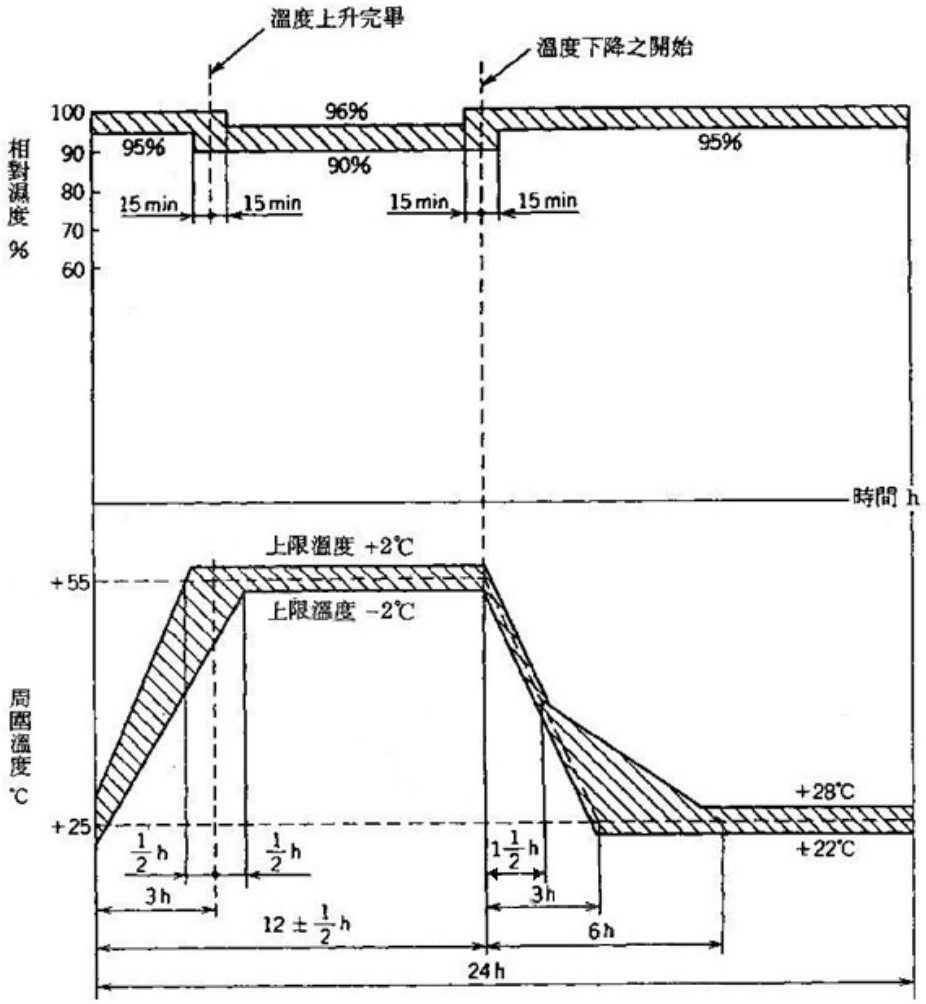


圖 6 濕熱循環試驗(方法 1)

4.9.3 要求

智慧杆附掛設備於試驗前後，均須進行外觀及功能確認，且試驗期間與試驗後，裝置仍可維持正常操作。

4.10 風洞試驗

應依 4.10.1、4.10.2 及 4.10.3 實施或依「5G 智慧杆系統技術規範-第 3 部:安裝與結構相關安全要求及試驗法」5.4.6 抗風試驗替代 4.10 風洞試驗。

4.10.1 目的

此試驗模擬智慧杆 5G 微型基地臺附掛天線裝置，遭受強烈颱風等級的強風吹襲時的耐受強度而不得損壞。

4.10.2 試驗方法

依據 CNS 16069 在風速 17 級風(56.1~61.2)m/s，強烈颱風)狀態下，以 0 、90 與及 180 分別測試 20 分鐘，或依第 3 部 5.4.6 抗風試驗法實施[2]。

4.10.3 要求

智慧杆附掛設備於試驗前後，均須進行做外觀及功能確認，且試驗期間與試驗後，裝置不可有結構性的損壞。

參考資料

[1] CNS 61373 鐵路應用－鐵路車輛設備－衝擊及振動試驗

[2] CNS 16069 高速公路及快速道路 LED 路燈

[3] IEC 60068-2-5 Environmental testing–Part 2-5: Tests–Test S: Simulated solar radiation at ground level and guidance for solar radiation testing and weathering

[4] MIL-STD-810H (2019) METHOD 505 SOLAR RADIATION (SUNSHINE)

[5] GR-63-CORE NEBS Requirements Physical Protection

5G 智慧杆系統技術規範

－第 5 部：電氣安全要求

5G Smart pole system technical specification

- Part 5: Electrical safety requirements

中 華 民 國 111 年 9 月

目錄

節次 頁次
前言 3
0. 簡介 4
1. 適用範圍 4
2. 引用標準 4
3. 用語及定義 5
3.1 絕緣(insulation) 5
3.1.1 基本絕緣(basic insulation) 5
3.1.2 雙重絕緣(double insulation) 5
3.1.3 強化絕緣(reinforced insulation) 5
3.1.4 補充絕緣(supplementary insulation) 5
3.1.5 導電部件(conductive part) 5
3.1.6 外露導電部件(exposed conductive part) 5
3.1.7 危險電壓(hazardous voltage) 5
3.2 使用(use) 5
3.2.1 室內使用(indoor use) 5
3.2.2 室外使用(outdoor use) 5
3.3 一般用語(general terms) 5
3.3.1 保護性導體(protective conductor) 5
3.3.2 接觸電流(touch current) 6
4. 一般要求 6
4.1 防電擊保護 6
4.1.1 殘存電能 6
4.1.2 可觸及部位或零件不得為危險帶電 6
4.2 粉塵、固體外物及水侵入之防護 6
4.3 耐濕性 6
4.4 絕緣電阻 6
4.5 接觸電流 7
4.6 脈衝耐電壓 7
4.6.1 AC 耐電壓 7
4.6.2 脈衝耐電壓試驗(1.2 μs/50 μs) 8
4.7 溫升試驗 8
4.7.1 一般 8
4.7.2 試驗法 8
4.8 機械強度 9
4.9 異常操作試驗 9
4.9.1 過載與異常操作之保護 9

4.9.2 在異常的操作或故障後 9
4.9.3 模擬故障狀態 9
4.9.4 保護裝置 10
4.10 內部配線 10
4.11 沿面距離及空間距離 10
4.12 外殼與外部保護電路之有效接地連續性 10
4.13 輸入測試 10
4.14 標示及說明書 11
4.14.1 安裝手冊 11
4.14.2 設備標示 11
4.14.3 標示耐久性試驗 11
5. 子系統電氣安規測試 12
5.1 5G 基地臺之電氣安規測試要求 12
5.2 不斷電系統之電氣安規測試要求 12
5.3 照明設備之電氣安規測試要求 12
5.4 資訊影音及影像監控相關設備之電氣安規測試要求 12
5.5 電力設備之電氣安規測試要求 12
5.6 環境監測之電氣安規測試要求 12
5.7 充電樁之電氣安規測試要求 12
5.8 電子式電度表之電氣安規測試要求 12
參考資料 13

前言

本規範係依 CNS 3689 「國家標準草案構成及格式之指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole) 現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT) 設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於使用 60 Hz 及 500 V 以下交流低壓電源之多用途智慧杆，包含子系統領域的電機及電子設備之安全性要求及試驗法。不包括設備效能及功能特性之規定。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 9816	電器試驗用試驗指
CNS 14165	電器外殼保護分類等級
CNS 14335	燈具－第 1 部：一般要求及試驗
CNS 14843-1	不斷電系統(UPS)－ 第 1 部：使用於操作者觸及區之不斷電系統安全通則
CNS 14843-2	不斷電系統(UPS)－ 第 1 部：使用於限制觸及區之不斷電系統安全通則
CNS 15233	發光二極體道路照明燈具
CNS 15425-1	電動機車充電系統檢驗法
CNS 15425-2	電動機車充電系統－第 2 部：安全連接要求
CNS 15511-1	電動車輛傳導式充電系統－第 1 部：一般要求
CNS 15511-23	電動車輛傳導式充電系統－第 23 部：電動車輛直流充電站

CNS 15511-24	電動車輛傳導式充電系統－第 24 部：電動車輛直流充電站與電動車輛間充電控制用數位通訊
CNS 15549	接觸電流與保護導體電流之量測法
CNS 15598-1	影音、資訊及通訊技術設備
CNS 15620-1	低電壓系統下設備之絕緣協調－第 1 部：原理、要求及試驗
CNS 15772	電器外殼對外來機械衝擊之保護分類等級(IK 碼)
CNS 61347-1	光源控制裝置－第 1 部：通則及安全要求
CNS 15783-1	低電壓開關裝置及控制裝置組裝品-第 1 部：一般規則
IEC 60068-2-78	Environmental testing − Part 2-78:Tests − Test Cab: Damp heat , steady state

3. 用語及定義

本規範適用「5G 智慧杆系統技術規範－第 1 部：一般要求」之用語定義，及下列用語及定義適用於本規範。

3.1 絕緣(insulation)

3.1.1 基本絕緣(basic insulation)

對危害帶電部件提供基本保護之絕緣。

3.1.2 雙重絕緣(double insulation)

基本絕緣與補充絕緣兩者組成之絕緣。

3.1.3 強化絕緣(reinforced insulation)

提供危害帶電部件相當於雙重絕緣之電擊防護等級的絕緣。

備考：強化絕緣可包括數層，其不能依基本絕緣或補充絕緣單獨試驗。

3.1.4 補充絕緣(supplementary insulation)

針對故障保護，對基本絕緣額外施加之獨立絕緣。

3.1.5 導電部件(conductive part)

承載電流的部件。

3.1.6 外露導電部件(exposed conductive part)

電氣設備之導電部件，其可接觸且通常不帶電，但基本絕緣失效時會變成帶電。

備考：觸及已變成帶電之外露導電部件， 電氣設備之導電部件僅能變成帶電，不視為外露導電部件本身。

3.1.7 危險電壓(hazardous voltage)

指電路中超過 42.4 Vpeak 或是 60 Vd.c.的電壓， 此電路不符合限電流電路或電信網路電壓電路之要求。

3.2 使用(use)

3.2.1 室內使用(indoor use)

在建築物內之正常環境條件下操作。

3.2.2 室外使用(outdoor use)

在室外條件之特定範圍下能夠操作。

3.3 一般用語(general terms)

3.3.1 保護性導體(protective conductor)

為安全目的提供之導體，例：電擊防護。

例：保護性導體之例包括保護性搭接導體、保護性接地導體及用於電擊防護的接地導體。

3.3.2 接觸電流(touch current)

當人體觸及2個或更多可觸及部件時，或人體觸及一個可觸及部件與地時，流過人體之電流。

4. 一般要求

4.1 防電擊保護

4.1.1 殘存電能

在供電設備的電源電壓斷連後 5s 內，於其輸入電源端子處量測，電源線與保護性接地導體之間的電壓應不大於 60 Vd.c.，或殘存的電能應小於 0.2 J。

以檢驗及依 CNS 15598-1 之 5.5.2.2 查核符合性。

4.1.2 可觸及部位或零件不得為危險帶電

此外，當不連接至其他設備時，除下列情形外，端子之非可觸及接點不可為危險帶電部：

- 信號輸出端子之接點，如果因其功能上必須使其危險帶電，則接點與電源須如 4.11 有關可觸及導電零件之規定隔離。
- 作為設備至電源、插座連接及供電至其他設備之連接裝置接點。

上述決定是否為危險帶電部位之方法僅適用於危險帶電電壓未超過 1,000 Va.c.或 1,500 Vd.c.對於較高電壓者，並參照 CNS 9816 以試驗指或測試針可觸及部分與危險電壓部位間應有基本絕緣的空間距離。

4.2 粉塵、固體外物及水侵入之防護

外殼對固體異物及水之防護等級，依CNS 14165試驗查核符合性。

設備應有 CNS 14165 外殼防護 IP 等級，要求如下：

- 智慧杆杆體與箱體之防護等級應不低於IP55之要求。
- 其他智慧杆非杆體內附掛設備之防護等級應不低於IP65之要求。

4.3 耐濕性

濕度處理應於溫濕箱內或溫濕室內執行 48 h，相對濕度(93±3)%，溫度 T 維持在誤差 2 ℃內且介於 20 ℃至 30 ℃間之任何值，不發生水氣凝結。在此條件下，組件或次組件不予通電。

對於熱帶條件下，時間應為 120h，溫度(40±2)℃及相對濕度(93±3)%。

測試後，測試樣品須進行 4.6 之試驗。

備考 1.在濕度處理前，應把樣品放置在 T 與(T+4)℃之間持續 4 h。

備考 2.試驗中設備不得帶電。

4.4 絕緣電阻

以量測 500 V d.c.絕緣電阻查核其符合性。

1 min 後量測的絕緣電阻不小於表 1 給定的值，則此設備視為符合規定。

絕緣電阻施加 500 Vd.c. 電壓於所有連接在一起之輸入/輸出(包括電源)與可觸及部件之

間，量測之絕緣電阻(R)應不得超過表 1 所示之值：

－I 類設備：R > 1 MΩ

－Ⅱ類設備：R > 7 MΩ

表 1　絕緣電阻限制值

部件間之絕緣要求	絕緣電阻(MΩ)
部件之間藉由基本絕緣或補充絕緣隔離	1
部件之間藉由雙重絕緣或強化絕緣隔離	7

試驗期間，本試驗之所有超低電壓(ELV)電路應連接至可觸及部件上。施加試驗電壓持續 1 min 後，立即在(40±2)℃、相對濕度(93±3)%下，依 IEC 60068-2-78 試驗 Ca 進行濕熱連續試驗 4 天。

4.5 接觸電流

AC 供電網路任一極(pole)與相互連接之可觸及金屬部件，與使用金屬箔覆蓋部件之外部絕緣間的接觸電流，依 CNS 15549 之圖 4 進行量測且不得超過表 2 所示之值。接觸電流應在(40±2)℃、相對濕度(93±3)%下，依 IEC 60068-2-78 試驗 Ca 進行 4 天濕熱連續試驗後，於 1 h 內量測，依 CNS 15549 連接至 AC 供電網路。

試驗電壓應為最大額定電壓之 1.1 倍。設備經由隔離變壓器或以與接地隔離之方式饋入。

表 2　接觸電流限制值

	I 類	Ⅱ類
任一相與相互連接之可觸及金屬部件與金屬箔覆蓋絕緣的外部部件間	3.5 mA	0.25 mA
任一相與正常不帶電之不可觸及金屬部件間(若為雙重絕緣)	不適用	3.5 mA
相互連接之不可觸及部件及可觸及部件與金屬箔覆蓋絕緣的外部部件間(補充絕緣)	不適用	0.5 mA

4.6 脈衝耐電壓

4.6.1 AC 耐電壓

在 60 Hz 之電源頻率下，耐電壓應依下列條件執行 1 min：

(a) I 類設備。

依 CNS 15620-1 之 5.3.3.2 規定，施加(*U*n+1,200 V)(r.m.s.)於共模(所有與外露導電部件相關之電路)及差模(在每個電氣獨立電路與所有其他外露導電部件或電路之間)。

備考：Un 為中性點接地供電系統之〝線對中性點〞的標稱電壓。

(b)Ⅱ類設備。

依 CNS 15620-1 之 5.3.3.2.3 規定，施加 2 倍(*U*n+1,200 V)(r.m.s)於共模及差模。

(c)I 類及Ⅱ類交流設備與 AC 供電及超低電壓電路之間的絕緣為雙重絕緣或强化絕緣時，則應在絕緣上施加 2 倍(*U*n+1,200 V)(r.m.s.)。可使用等於 AC 峰值之 DC 電壓進行試驗。

針對本試驗，所有電氣設備應依相關規範連接，除針對較低試驗電壓設計項目，消耗電流之裝備(例：繞組、量測儀器，電壓突波抑制裝置)施加試驗電壓將導致電流流動時應予以斷連。此類裝備應在其 1 個端子處斷連，除非設計不能承受全部試驗電壓，在這種情形下，所有端子均可斷連。

備考：測試電壓須以設計之適當信號源輸入以得到，測試電壓調整致適當水準後輸出端子短路，輸出電流至少 200 mA。當輸出電流小於 100 mA，過電流裝置不可跳脫。測試電壓值量測精確度為±3%。起始時，測試電壓不超過預設測試值之一半，然後迅速調升至該預設測試值，並維持 1 min。

4.6.2 脈衝耐電壓試驗(1.2 μs/50 μs)

應依 CNS 15620-1 表 F.5 中之脈衝電壓進行電力電路之脈衝耐受試驗。

應在帶電部件與外露導電部件間施加衝擊電壓。

應依 CNS 15598-1 之使用附錄 D 合適之脈衝試驗產生器。每一極至少 3 次脈衝，各次脈衝間隔至少 1 s，施加於個別相關點之間。

使用表 D.1 中脈衝試驗產生器電路 2 產生等於交流電源暫態電壓之 1.2μs/50μs 脈衝於下述各點間：

－ 線對線。

－ 所有的火線導體導電性連接在一起與中性線。

－ 所有的火線導體導電性連接在一起與保護接地。

－ 中性線及保護接地。

設備直接連接至公共 AC 供電網路的部件，應依過電壓種類Ⅳ試驗。

永久連接設備應依過電壓種類Ⅲ試驗。

4.7 溫升試驗

4.7.1 一般

本節之規定係為避免下列情形產生。

－ 可觸及部件溫度超出限制值。

－ 零組件、部件、絕緣物及塑膠材料超出溫度限制值，於設備之合理壽命期內，其可能在正常使用下，降低電氣或機械或其他性能。

事實須考慮，長時間基礎，某些絕緣材料之電氣及機械性質可能反向影響(例：軟化劑於低於正常軟化溫度時汽化的材料)。

在試驗中，聲音放大器參照 CNS 15598-1 之附錄 E 操作。

材質與零組件的溫度不可超出 CNS 15598-1 之 5.4.1.4 表 9 及 CNS 61347-1 之附錄 L 表 L.2 之規定。

4.7.2 試驗法

高溫下操作之零組件須有效屏蔽(shielded)或隔離以避免其接觸材料或零組件。

符合性以檢驗材質資料表及藉由溫度的記錄。待測設備或待試驗的設備部分依在正常負載下運作直到溫度達到穩定。

遵守設備適用之試驗條件，則允許單獨試驗零組件及其他部件。

為固定、架設或合併於大型設備之設備，將實際或模擬廠商的安裝指引，在最不利的

狀況下試驗。

故障後會發生危險的電氣絕緣物之溫度(繞組除外)，測量其接近熱源的絕緣物表面，參照 CNS 15598-1 表 9 之規定。

試驗時：

－ 熱動斷路器及過電流保護裝置不可動作。

－ 未中止設備正常操作時，則允許恆溫器動作。

－ 限溫器可動作。

－ 封膠不可流出。

4.8 機械強度

設備外殼機械衝擊保護等級，應依 CNS 15772 IK08 等級以上進行試驗。

試驗後，樣品應符合下列要求：

－ 未損及規定之 IP 等級。

－ 無部件之移動、鬆動、分離或變形，致損及任何安全功能。

－ 試驗未造成設備不符合張力緩和要求的結果(適用時)。

－ 試驗未導致不同極性之未絕緣帶電部件、未絕緣帶電部件與可觸及不帶電或接地金屬之間的沿面距離及空間距離低於最低可接受值。

－ 試驗未導致任何其他會提高起火或電擊之風險的損害跡象。

4.9 異常操作試驗

4.9.1 過載與異常操作之保護

設備應設計為儘可能將由火或電性衝擊所造成的風險降到最低。不管此風險是由機械或電子的過負載或故障或異常操作或不小心使用所造成。

4.9.2 在異常的操作或故障後

此設備仍然要符合本規範所要求的安全範圍，不可對操作者造成傷害。但不要求此設備仍能正常操作。可使用熔線、熱阻斷器、過電流保護裝置等，以提供足夠的保護以檢驗及 4.6 之試驗檢查其符合性。在每項試驗進行之前，應先確認設備處於正常操作狀態下。設備中零組件或次組件的圍封方式使得在 4.6 中所述的短路或開路不容易做到時，在不損害此設備的情況下，允許以特殊的連接線連接到此等必要的零組件試驗。當零組件接線試驗也不可能時，整個零組件或組件看成單體，須通過 4.6 之試驗。設備之試驗條件為：任何正常使用可能發生之狀況與可預見之誤用狀態。此外，具保護外蓋之設備試驗時，外蓋仍須如正常待機狀態蓋好直到穩定狀態為止。

4.9.3 模擬故障狀態

可藉模擬下列故障狀態條件以檢查其符合性。

(a)將一次側的任何零組件加以短路或開路處理。

(b)將任何失效時，可能不利於補充絕緣或強化絕緣的零組件，加以短路或開路處理。

(c)將各相關零組件與部件分別加以短路或開路處理。

備考：過載條件為正常電流至短路最大電流之間的任何條件。

(d)將電源輸出插座以外之端子，或連接器以最不利之負載阻抗接上。此類端子或連接器之作用為提供電器設備之信號輸出。

(e)在指出的其他單一故障。

在此有些內部的電路有多端點的輸出，只要抽其中的一個輸出來做試驗即可。

一次側零組件含電源輸入，如電源線、電源插接器、EMC 濾波器、開關及其內部配線不可模擬故障狀態，須符合相關節次的規定。

4.9.4 保護裝置

保護裝置於設備中有恆溫器、限溫器、熱動斷路器或有一電容但未用熔線來保護或可能與接點並聯，皆應執行下列試驗。

恆溫器、限溫器及溫度斷路器要同時做評估，以符合要求。

電器設備應依正常操作，同時任何做溫度限制控制的地方皆要短路。電器設備有超過一個以上的恆溫器、限溫器或熱動斷路器皆要個別短路。

未發生電流過大之中斷時，則此電器設備，應該在穩定狀態已經建立時儘速的關掉，同時也應該允許去冷卻到適當的室溫。

對於僅在短時間操作的電器設備，試驗時間相當於其額定操作時間。對於電器設備是屬於短時間或間歇性的設備，不論額定操作時間或額定間歇時間為何，此電器設備要重覆地做試驗使電器設備達到穩定的使用狀況。在此等試驗情況下恆溫器、限溫器或熱動斷路器不用短路。

任何試驗時，手動重置型熱動斷路器予以動作，或在穩定狀態前造成電流的中斷，加熱時間視為已經結束。當中斷是由於本質上就比較弱的部分斷裂造成的，要再拿第二個試樣做一次。兩個試樣均要同時符合 4.6 所述之值。

4.10 內部配線

內部配線提供主電源電力至其他設備之內部配線，應至少具有 CNS 15598-1 表 G.7 規定之標稱截面積，包括註[a]之條件，以檢查其符合性 。

4.11 沿面距離及空間距離

由製造商設置之設備內的空間及沿面距離，應符合 CNS 15620-1 中表 F.4 規定之要求。

設備內直接連接至公共 AC 供電網路的部件，應依過電壓種類Ⅳ設計。

永久連接之設備至少應依過電壓種類Ⅲ設計。

除永久連接之設備外，至少應依過電壓種類Ⅱ設計。

在較高過電壓種類下使用之設備，應包括適當的過電壓保護裝置(參照 CNS 15620-1 之 4.3.3.6)。

4.12 外殼與外部保護電路之有效接地連續性

外露導電部件應連接到外部保護性導體。

除相關法規另有規定外，此試驗應依 CNS 15783-1 之 10.5.2 執行。

4.13 輸入測試

在正常負載下，設備之輸入穩態電流不得超過額定電流之 10 %。

在下述電壓及正常負載下測量其輸入電流，以檢查其符合性。

- 當其額定電壓為一或多重電壓時，於每一額定電壓下測量輸入電流。
- 當其額定電壓為一或多重電壓範圍時，於每一額定電壓範圍上、下限測量輸入電流。標示單一電流值時，則與該一電壓範圍內測得之電流取較高者作比對。標示為兩電

流值，中間以短線相連接時，則兩電流值與該一電壓範圍測得之電流作比對。

每一情況下，電流之讀值將待輸入電流穩定後記錄。在正常操作下，電流值會隨正常操作循環變化，則其穩態電流即為在一代表性的時間內、經由一記錄 r.m.s.電流表量測得之平均指示值。

4.14 標示及說明書

4.14.1 安裝手冊

設備製造商應在手冊中說明介面特性及接線說明。

具備保護裝置時，手冊應指明保護裝置之特性，敘述型式及定額。該資訊可提供於詳細的電路圖。

4.14.2 設備標示

設備製造商應提供每一設備的標籤，以耐久方式標示，並位在安裝與維護期間清晰易讀位置：

(a)設備製造商之名稱、簡稱、商標或特殊標示。

(b)型式名稱或識別編號或任一其他識別措施，可從設備製造商獲得相關資訊。

(c)限於室內使用時，標示〝限室內使用〞或相當之說明。

(d)製造日期之識別措施。

(e)電流種類。

(f)採交流電時，標示頻率及相數。

(g)額定電壓(若輸入與輸出不同)。

(h)額定電流(若輸入與輸出不同)及測定額定電流之周圍溫度。

(i)保護等級。

(j)特別宣告分類、特性及參差因數、使用之嚴酷或異常環境條件等所有需要的資訊。

以檢驗並依本規範 4.14.3 查核符合性。

4.14.3 標示耐久性試驗

藉模壓、壓製、刻印或類似方式進行標示，包括使用積層塑膠披覆之標籤，不須執行以下試驗。

本規範要求的標示應以矯正後之視力亦可清晰易讀、耐久，並於使用時可見。以檢驗及使用浸水的布摩擦標示 15 s，再用浸石油精的布再次摩擦標示 15 s，查核符合性。

備考：石油精定義為芳香烴體積含量最大 0.1 %之己烷溶劑，考利丁醇值為 29，初始沸點為 65 ℃，最終沸點為 69 ℃，密度 0.6 8g/cm^3。

試驗後，以正常或矯正後之視力在不經額外放大下，標示應清晰易讀。標示牌應不易移除且不得捲曲。

5. 子系統電氣安規測試

智慧杆相關子系統在安裝於智慧杆前，除應符合各相對應之電氣安規產品測試標準外，另須符合本規範其他部智慧杆設置測試。

5.1 5G 基地臺之電氣安規測試要求

5G 基地臺相關設備，須符合 CNS 15598-1 之電氣安規要求。

5.2 不斷電系統之電氣安規測試要求

電力相關設備，須符合 CNS 14843-1 及 CNS 14843-2 之電氣安規要求。

5.3 照明設備之電氣安規測試要求

智慧照明相關設備，須符合 CNS 14335 及 CNS 15233 之電氣安規要求。

5.4 資訊影音及影像監控相關設備之電氣安規測試要求

資訊影音及影像監控相關設備，須符合 CNS 15598-1 之電氣安規要求。

5.5 電力設備之電氣安規測試要求

電力相關設備，須符合 CNS 15598-1 之電氣安規要求。

5.6 環境監測之電氣安規測試要求

環境監測相關設備，須符合 CNS 15598-1 之電氣安規要求。

5.7 充電樁之電氣安規測試要求

電動機車充電相關設備，須符合 CNS 15425-1、CNS 15425-2 之電氣安規要求。

電動汽車充電相關設備，須符合 CNS 15511-1、CNS 15511-23、CNS 15511-24 之電氣安規要求。

5.8 電子式電度表之電氣安規測試要求

電子式電度表，須符合 IEC 61010-1 電氣安規之要求。

參考資料

[1] 全臺設置 LED 路燈技術規範，104 年，經濟部能源局

[2] CNS 14336-1 資訊技術設備－安全性－第 1 部：一般規定

[3] CNS 14408 影音及其類似電子產品－安全規定

[4] CNS 15620-4 低電壓系統下設備之絕緣協調－第 4 部：高頻電壓應力之考量

[5] CNS 15668 電擊防護－裝設及設備之一般觀念

[6] CNS 16125 電動機車定置式交流及直流傳導式供電系統－一般要求

[7] IEC 60364-5-54 Low-voltage electrical installations – Part 5-54: Selection and erection of electrical equipment – Earthing arrangements and protective conductors

[8] IEC 61000-3-11 Electromagnetic compatibility (EMC) - Part 3-11: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems - Equipment with rated current ≤ 75 A and subject to conditional connection

[9] IEC 61000-3-12 Electromagnetic compatibility (EMC) - Part 3-12: Limits - Limits for harmonic currents produced by equipment connected to public low-voltage systems with input current > 16 A and <= 75 A per phase

[10] IEC 61000-4-2 Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test

[11] IEC 61000-4-3 Electromagnetic compatibility (EMC) - Part 4-3 : Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test

[12] IEC 61000-4-4 Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test

[13] IEC 61000-4-5 Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test

[14] IEC 61000-4-6:2013,Electromagnetic compatibility (EMC) - Part 4-6:Testing and measurement techniques-Immunity to conducted disturbances, induced by radio-frequency fields

[15] ITU-T K Suppl. 10 Analysis of electromagnetic compatibility aspects and definition of requirements for 5G systems

[16] IEC 61000-4-8:2009,Electromagnetic compatibility (EMC) - Part 4-8:Testing and measurement techniques - Power frequency magnetic field immunity test

[17] IEC 61969-3 Mechanical structures for electrical and electronic equipment - Outdoor enclosures - Part 3: Environmental requirements, tests and safety aspects

[18] IEC 61851-21-2 Electric vehicle conductive charging system – Part 21-2: Electric vehicle requirements for conductive connection to an AC/DC supply – EMC requirements for off-board electric vehicle charging systems

5G 智慧杆系統技術規範

－第 6 部：電磁相容要求

5G Smart pole system technical specification

- Part 6 : Electromagnetic compatibility (EMC) requirements

中 華 民 國 111 年 9 月

目錄

節次 頁次
前言 2
0. 簡介 3
1. 適用範圍 3
2. 引用標準 3
3. 用語及定義 4
4. 子系統電磁相容性測試 7
5. 智慧杆電磁相容性測試 7
5.1 一般 7
5.2 設備分類 7
5.3 測試項目與測試條件要求 7
5.3.1 放射測試 7
5.3.2 抗擾度測試 11
5.3.3 量測不確定度 15
參考資料 16

前言

本規範係依 CNS 3689 「國家標準草案構成及格式之指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole) 現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT) 設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆。本規範定義 5G 智慧杆系統框架，規定系統構成元件及其基本功能，並說明本系列規範系其他各部規範內容概要。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 14115	電氣照明與類似設備射頻擾動特性之限制值與量測法
CNS 14674-1	電磁相容性(EMC)－一般性標準－第 1 部：住宅、商業與輕工業環境之抗擾度
CNS 14674-2	電磁相容性(EMC)－一般性標準－第 2 部：工業環境之抗擾度
CNS 14674-3	電磁相容性(EMC)－一般性標準－第 3 部：住宅、商業與輕工業區環境之放射標準
CNS 14674-4	電磁相容(EMC)－一般標準－第 4 部:工業環境之放射標準
CNS 14676-2	電磁相容－測試與量測技術－ 第 2 部：靜電放電抗擾度測試
CNS 14676-3	電磁相容－測試與量測技術－第 3 部：輻射、射頻與電磁場抗擾度測試

CNS 14676-4	電磁相容－測試與量測技術－第 4 部：電性快速暫態/叢訊的抗擾度測試
CNS 14676-5	電磁相容－測試與量測技術－第 5 部：突波抗擾度測試
CNS 14676-6	電磁相容－測試與量測技術－第 6 部：射頻場感應的傳導擾動抗擾度
CNS 14676-8	電磁相容性－測試與量測技術－第 8 部：電源頻率磁場抗擾度測試
CNS 14934-2	電磁相容－限制值－第 2 部：諧波電流發射（設備每相輸入電流在 16 A 以下）之限制值
CNS 14934-3	電磁相容－限制值－第 3 部：每相額定電流在 16 A 以下且不屬於有條件連接之設備於公共低電壓電源系統中電壓改變、電壓變動及閃爍之限制值
CNS 14934-4	電磁相容－限制值－第 4 部：額定電流大於 16 A 之設備於低電壓電源系統中諧波電流發射之限制值
CNS 14934-5	電磁相容－限制值－第 5 部：額定電流大於 16 A 之設備於低電壓電源系統中電壓變動及閃爍之限制值
CNS 15511-3	電動車輛傳導式充電系統 － 第 3 部：安全要求
CNS 15936	多媒體設備之電磁相容－放射要求
CNS 16069	高速公路及快速道路 LED 路燈
CNS 16125	電動機車定置式交流及直流傳導式供電系統－一般要求
IEC 61000-4-11:2004	Electromagnetic compatibility (EMC) - Part 4-11:Testingand measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests
NCC IS ALL	行動通信基地臺射頻設備技術規範

3. 用語及定義

下列用語及定義適用於本規範。

3.1 智慧杆（smart pole）

建構智慧城市之關鍵基礎設施之一，採固定式杆狀結構 (可參考一般路燈燈杆設計)，具備電源供應及網路通訊能力，可安裝或掛載各種不同設備 (例：照明燈具、電信設備、資通訊設備及物聯網裝置等) 之多用途載體。可提供各種智慧化應用服務 (例：高效率節能照明、行動通訊、智慧交通、資訊發布、安全監控、充電樁等)，並可透過資訊管理系統對其進行遠端監控及操作。

3.2 待測設備 (EUT)

本規範適用之範圍包含之零組件或設備。

備考:有關電磁相容及其相關現象之用語及定義，已定義於 CNS 14299。

3.3 埠（port）

一種實體介面，經由此介面，電磁能量可進入或離開待測設備。

備考：參照圖 1。

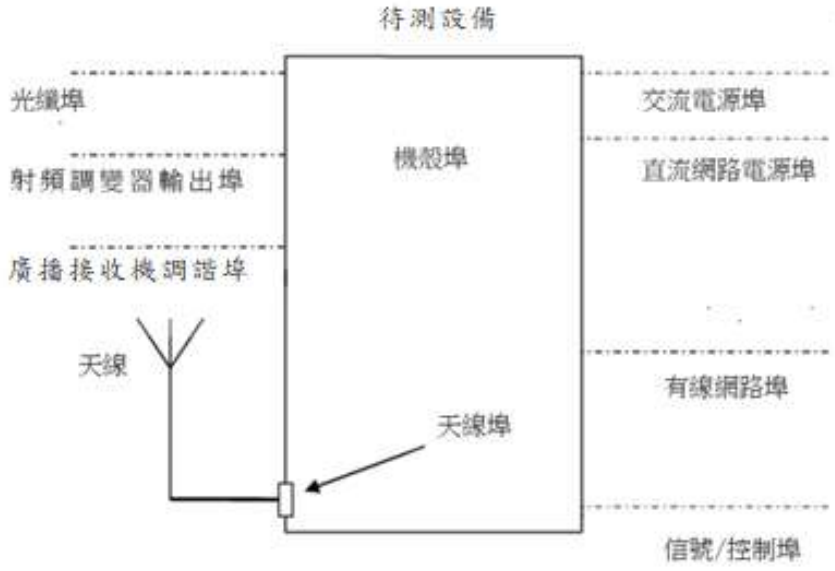


圖1　埠之範例

3.3.1 交流電源埠(AC mains power port)

用以連接交流電源網路之連接埠。

備考：具有直流電源埠之設備， 係由專屬之交流轉直流電源轉換器供電， 則定義為交流電源供電之設備。

3.3.2 直流網路電源埠(DC network power port)

非由專屬交流轉直流 (AC/DC)電源轉換器供電之埠，且不支援通訊，該埠連接直流供電網路 。

備考 1.具有直流電源埠，其由專屬 AC/DC 轉換器供電，則視為交流電源供電設備。

備考 2.直流電源埠支援通訊時，視為有線網路埠，諸如乙太網路埠包含供電乙太網路**(PowerOver Ethernet, POE)**。

3.3.3 有線網路埠 (wired network port)

用於聲音、資料及訊號轉移的連接點（埠），透過直接連接至單一用戶或多用戶的通訊網路，意圖介接至廣泛傳輸系統 。

備考 1.示例包括有線電視(CATV)、公眾交換電話網路(PSTN)、整體服務數位網路(ISDN)、各種數位使用者線路(xDSL)、區域網路(LAN)及類似網路。

備考 2.此等埠可以支援遮蔽或非遮蔽的纜線，而且可以帶有交流或直流的電源，只要他是通訊規格整體的一部分即可。

3.3.4 訊號/控制埠 (signal/control port)

意圖介接待測設備各部件的埠，或在待測設備與本地關連設備間作介接的埠，且要依相關功能性之規格使用（例：使用最大長度纜線連接至此埠等）。

備考：案例包含 RS-232、通用序列匯流排(USB)、高解析多媒體介面(HDMI) 、IEEE1394(Fire Wire)等。

3.3.5 光纖埠 (optical fibre port)

光纖連接設備之埠。

3.3.6 射頻調變器輸出埠 (RF modulator output port)

此輸出埠意圖連接至廣播接收機之調諧器埠，以便傳輸訊號至廣播接收機 。

3.3.7 廣播接收機調諧器埠 (broadcast receiver tuner port)

用於接收調變射頻訊號之埠，該訊號攜載地面傳輸、衛星/有線傳輸之聲音/影像廣播及類似之服務。

備考：調諧器埠可連至天線、有線電視分配系統、錄放影機或類似裝置。

3.3.8 天線埠(antenna port)

異於 3.3.7 廣播接收機調諧器埠，該埠連接天線，而該天線用於意圖傳輸/接收輻射之射頻能量。

3.3.9 類比/數位資料埠(analogue/digital data port)

訊號/控制埠(3.3.4)、天線埠(3.3.8)、有線網路埠(3.3.3)、廣播接收機調諧器埠(3.3.7)或具有金屬屏蔽/金屬拉伸防護功能光纖埠(3.3.5) 等。

3.3.10 機殼埠 (enclosure port)

待測設備之實體邊界，經由此埠可能輻射電磁場。

3.4 電源埠 (power port)

連接到裝置的輸入埠，其導體或電纜攜載裝置或相關設備運作所需之電力。

備考：電源埠可以是交流或直流。

3.5 配置 (arrangement)

位於某區域內，待測設備、關連設備及其他任何相關纜線等所有部件之物理布局及方位。

3.6 關連設備 (associated equipment, AE)

監測待測設備運轉之必要設備。

3.7 操作模式 (mode of operation)

於測試或量測期間，待測設備所有功能之操作組態。

3.8 子系統 (subsystem)

安裝於智慧杆且可獨立運作之裝置，例如：廣播接收機設備、音訊設備、資訊技術設備、照明設備、燈光控制設備、影像設備等裝置。

3.8.1 廣播接收機設備 (broadcast receiver equipment)

具有調諧器之設備，意圖接收廣播服務。

備考：此等廣播服務為典型電視機及收音機服務，包含地面廣播、衛星廣播/有線傳輸等。

3.8.2 音訊設備 (audio equipment)

具備任何一項（或結合多項）產生、輸入、儲存、播放、恢復、傳輸、接收、放大、處理、轉換或控制音頻訊號等主要功能之設備。

3.8.3 資訊技術設備 (information technology equipment, ITE)

設備具有資料/電信訊號之輸入、儲存、顯示、恢復、傳輸、處理、交換或控制等單個（或組合）之主要功能，此設備典型上可以配備 1 個或多個埠作為資訊之轉送。

備考：ITE 包含資料處理裝置、辦公室機器、電子商務設備及電信設備等。

3.8.4 照明設備 (lighting equipment)

以照明為目的而具有產生/散發光線為主要功能之所有照明設備，且預期連接至低電壓電源或由電池操作。

3.8.5 燈光控制設備 (lighting control equipment)

產生或處理電氣訊號的設備，用以控制燈具光線之強度、顏色、性質或方向等。

3.8.6 影像設備 (video equipment)

設備具有影像訊號之產生、輸入、儲存、顯示、播放、恢復、傳輸、接收、放大、處理、交換或控制等單一（或複合性）之主要功能。

4. 子系統電磁相容性測試

智慧杆相關子系統(3.8)在安裝於智慧杆前，除應符合各相對應之電磁相容性產品測試標準外，另須符合本規範針對智慧杆設置之環境進行相關抗擾度測試，相關要求如下。若產品申請使用於工業環境時，須符合 CNS 14674-2 及 CNS 14674-4 之要求；若產品申請使用於住宅、商業與輕工業區環境時，須符合 CNS 14674-1 及 CNS 14674-3。

無論設備位於室內或是室外，當待測設備製造商未定義待測設備預期使用的環境，則應進行最嚴格的放射和抗擾度試驗，即應採用最低放射限制值和最高抗擾度試驗位準，例：產品電磁放射符合乙類標準(住宅、商業與輕工業區環境)要求，而電磁抗擾度符合工業環境標準要求，則產品可適用於任何地方使用。

5. 智慧杆電磁相容性測試

5.1 一般

智慧杆子系統安裝於實際杆體後，電磁相容性應符合 5.3.1 及 5.3.2 要求。

5.2 設備分類

本規範定義甲類設備與乙類設備，涉及該兩類設備之最終使用環境。

乙類設備之要求為對於住宅環境之廣播服務提供適當保護，主要應用於住宅環境之設備，應符合乙類限制值，其他設備應符合甲類限制值。廣播接收機設備屬乙類設備。

備考：符合甲類要求設備，對於住宅環境之廣播服務，可能無法提供適當保護。

無論設備位於室內或是室外，當待測設備製造商未定義待測設備預期使用的環境，則應進行最嚴格的放射和抗擾度試驗，即應採用最低放射限制值和最高抗擾度試驗位準，例：產品電磁放射符合乙類標準(住宅、商業與輕工業區環境)要求，而電磁抗擾度符合工業環境標準要求，則產品可適用於任何地方使用。

5.3 測試項目與測試條件要求

智慧杆子系統安裝於實際杆體後，電磁相容性測試項目與測試條件如下。

5.3.1 放射測試

放射測試分別在智慧杆於輕載與重載條件下進行測試，量測接收機應符合 CISPR 16-1-1:2010 第 2 節之要求，檢波器及頻寬則應如附錄 A 相關表格之規定，當本規範規定使用平均值檢波器，則要使用 CISPR 16-1-1:2010 第 6 節所規定之線性

平均值檢波器。

一個單獨的放射，其位準超過任何相關限制值時，在 2min 量測時段內符合下列 2 個條件，則可不加採計:

(a)超過限制值之放射應少於 1s。

(b)在任何 15s 觀測時間內，放射值不超過限制值 1 次以上。

量測時，應小心避免量測系統過載。

5.3.1.1 傳導放射測試

(a) 電源端擾動電壓測試

頻率範圍從 150 kHz~30 MHz，甲類與乙類設備之交流電源輸入埠擾動電壓限制值如表 1 與表 2 所示，電源輸入埠擾動電壓參照 CNS 15936 等相關標準之限制值要求。

表 1　甲類設備交流電源輸入埠擾動電壓限制值

埠	頻率範圍 (MHz)	限制值 (dBμV)	檢測值	基本標準
交流電源輸入	0.15～0.5	79	準峰值	例：CNS 15936
	0.5～30	73		
	0.15～0.5	66	平均值	
	0.5～30	60		
備考:在頻率的轉折點，應採用較嚴之限制值。				

表 2　乙類設備交流電源輸入埠擾動電壓限制值

埠	頻率範圍 (MHz)	限制值 (dBμV)	檢測值	基本標準
交流電源輸入	0.15～0.5	66～56	準峰值	例：CNS 15936
	0.5～5	56		
	5～30	60		
	0.15～0.5	56～46	平均值	
	0.5～5	46		
	5～30	50		
備考:在頻率的轉折點，應採用較嚴之限制值。				

(b) 訊號與通訊埠擾動電壓測試

頻率範圍從 150 kHz～30 MHz，甲類與乙類設備之訊號與通訊埠擾動電壓限制值與電流限制值如表 3 至表 6 所示，訊號與通訊埠擾動電壓測試，參照 CNS 15936 等相關標準之限制值要求。

表 3　甲類設備訊號與通訊埠擾動電壓限制值

埠	頻率範圍 (MHz)	限制值 (dBμV)	檢測值	基本標準
有線網路	0.15～0.5	97～87	準峰值	例：CNS

與 訊號/控制	0.5～30	87		15936
	0.15～0.5	84～74	平均值	
	0.5～30	74		

備考 1.在 0.15 MHz～0.5 MHz 的頻帶中，限制值隨著頻率的對數呈線性關係遞減。

備考 2.在頻率的轉折點，應採用較嚴之限制值。

備考 3.電流與電壓的擾動限制值是使用阻抗穩定網路(ISN)檢測，ISN 對待測訊號與通訊埠所顯現的共模(異對稱模式)阻抗為 150 Ω(轉換因子為 20 log 150 / 1 = 44 dB)。

備考 4.適用於意圖連接到超過 3m 長之纜線。

表4　乙類設備訊號與通訊埠擾動電壓限制值

埠	頻率範圍 (MHz)	限制值 (dBμV)	檢測值	基本標準
有線網路 與 訊號/控制	0.15～0.5	84～74	準峰值	例：CNS 15936
	0.5～30	74		
	0.15～0.5	74～64	平均值	
	0.5～30	64		

備考 1.在 0.15 MHz～0.5 MHz 的頻帶中，限制值隨著頻率的對數呈線性關係遞減。

備考 2.在頻率的轉折點，應採用較嚴之限制值。

備考 3.電流與電壓的擾動限制值是使用阻抗穩定網路(ISN)檢測，ISN 對待測訊號與通訊埠所顯現的共模(異對稱模式)阻抗為 150 Ω(轉換因子為 20 log 150 / 1 = 44 dB)。

備考 4.適用於意圖連接到超過 3m 長之纜線。

表5　甲類設備訊號與通訊埠擾動電流限制值

埠	頻率範圍 (MHz)	限制值 (dBμA)	檢測值	基本標準
有線網路 與 訊號/控制	0.15～0.5	53～43	準峰值	例：CNS 15936
	0.5～30	43		
	0.15～0.5	40～30	平均值	
	0.5～30	30		

備考 1.在 0.15 MHz～0.5 MHz 的頻帶中，限制值隨著頻率的對數呈線性關係遞減。

備考 2.在頻率的轉折點，應採用較嚴之限制值。

備考 3.電流與電壓的擾動限制值是使用阻抗穩定網路(ISN)檢測，

ISN 對待測訊號與通訊埠所顯現的共模(異對稱模式)阻抗為 150 Ω(轉換因子為 20 log 150 / 1 = 44 dB)。 備考 4.適用於意圖連接到超過 3m 長之纜線。

表6 乙類設備訊號與通訊埠擾動電流限制值

埠	頻率範圍 (MHz)	限制值 (dBμA)	檢測值	基本標準
有線網路與訊號/控制	0.15～0.5	40～30	準峰值	例：CNS 15936
	0.5～30	30		
	0.15～0.5	30～20	平均值	
	0.5～30	20		
備考 1.在 0.15 MHz～0.5 MHz 的頻帶中，限制值隨著頻率的對數呈線性關係遞減。 備考 2.在頻率的轉折點，應採用較嚴之限制值。 備考 3.電流與電壓的擾動限制值是使用阻抗穩定網路(ISN)檢測，ISN 對待測訊號與通訊埠所顯現的共模(異對稱模式)阻抗為 150 Ω(轉換因子為 20 log 150 / 1 = 44 dB)。 備考 4.適用於意圖連接到超過 3m 長之纜線。				

5.3.1.2 輻射放射測試

頻率範圍從 30 MHz～6,000 MHz，甲類與乙類設備之輻射放射限制值如表 7 與表 8 所示，輻射放射測試所要求之最高測試頻率如表 9 所示，輻射放射測試參照 CNS 15936 等相關標準之限制值要求，對於所使用量測設施，僅於量測設施(或場地)通過驗證量測之量測距離，始可顯示符合性。

表7 甲類設備的輻射放射限制值

埠	量測頻率 (MHz)	量測距離 (m)	限制值 (dBμV/m)	檢測值	基本標準
機殼	30～230	10	40	準峰值	例：CNS 15936
	230～1,000	10	47		
	1,000～3,000	3	56	平均值	
			76	峰值	
	3,000～6,000	3	60	平均值	
			80	峰值	
備考:在頻率的轉折點，應採用較嚴之限制值。					

表 8　乙類設備的輻射放射限制值

埠	量測頻率 (MHz)	量測距離 (m)	限制值 (dBμV/m)	檢測值	基本標準
機殼	30～230	10	30	準峰值	例：CNS 15936
	230～1,000	10	37		
	1,000～3,000	3	50	平均值	
			70	峰值	
	3,000～6,000	3	54	平均值	
			74	峰值	
備考:在頻率的轉折點，應採用較嚴之限制值。					

表 9　輻射放射所要求之最高頻率

最高內部頻率 (F_x)	最高量測頻率
$F_x \leq 108$ MHz	1 GHz
108 MHz < $F_x \leq 500$ MHz	2 GHz
500 MHz < $F_x \leq 1$ GHz	5 GHz
$F_x > 1$ GHz	5× F_x，最高 6 GHz

5.3.1.3 諧波電流測試

依待測物交流輸入額定電流決定測試標準，額定電流小於 16A 時，依 CNS 14934-2 執行測試；額定電流 16A 以上時，依 CNS 14934-4 執行測試。

5.3.1.4 電壓閃爍測試

依待測物交流輸入額定電流決定測試標準，額定電流小於 16A 時，依 CNS 14934-3 執行測試；額定電流 16A 以上時，CNS 14934-5 執行測試。

備考：此項測試僅適用安裝於室內之設備。

5.3.2 抗擾度測試

本規範涵蓋所有住宅、商業、輕工業及工業環境，無論設備位於室內或室外，當待測設備製造商未定義待測設備預期使用的環境，則應進行最嚴格的抗擾度試驗。在執行抗擾度測試時，智慧杆應於正常操作模式下進行測試。

5.3.2.1 抗擾度性能準則

應用本規範所定義之測試後，使得設備變為危險或不安全時，則該設備視為測試無效。

(a) 性能準則 A:

在測試進行時或測試後,設備應繼續如所預期的操作。當設備如預期使用時，其性能劣化或功能喪失不可低於製造商所規定之性能位準。性能位準由可容許之性能喪失取代。製造商未指定最低性能位準或可容許的性能喪失時，兩者均由產品說明和文件及使用者對設備合理之期望來推算。

(b) 性能準則 B:

在測試後，設備應繼續如所預期的操作。當設備如預期使用時，其性能劣化或功能喪失不可低於製造商所規定之性能位準。性能位準由可容許之性能喪失取代。測試期間容許性能劣化但不容許實際操作狀態或儲存資料之改變。製造商未指定最低性能位準或可容許之性能喪失時，兩者均由產品說明和文件及使用者對設備合理之期望來推算。

(c) 性能準則 C:

功能可自動恢復或可由操作控制恢復，則容許功能暫時性的喪失。

備考：智慧杆系統及其子系統之性能準則，應由主管機關訂定。

5.3.2.2 靜電放電抗擾度測試

此測試依 CNS 14676-2 靜電放電抗擾度測試條件執行測試，主要目的為建立共同及可重複的原則，以做為電機、電子設備遭受靜電放電時之功能評估，此外也包括人員對重要設備鄰近物體可能發生的靜電放電。

備考：本項測試是否執行，由主管機關訂定。

表10 靜電放電抗擾度測試條件

埠	試驗規格	性能準則	基本標準
機殼	接觸放電: 4 kV 空氣放電: 8 kV	參照 5.3.2.1 備考	CNS 14676-2 CNS 14674-1 CNS 14674-2
備考 1. 接觸放電要施加到裝置上之導電且可碰觸的部位，產品內部或輸出插座內之金屬接點則不適用此要求。			

5.3.2.3 輻射電磁場抗擾度測試

依 CNS 14676-3 輻射電磁場抗擾度測試條件執行測試，主要目的為輻射相關的抗擾度測試，關係到來自任何訊號源射頻電磁場的防護，特別專注於來自數位無線電話與其他射放射裝置之射頻放射的防護。

表11 輻射電磁場抗擾度測試條件

埠	試驗規格	性能準則	基本標準
機殼	80 MHz ～1 GHz 住宅以外環境區位準: 10 V/m 住宅環境區位準:3V/m (80% AM 1 kHz)	參照 5.3.2.1 備考	CNS 14676-3 CNS 14674-1 CNS 14674-2
	1 GHz～6 GHz 3 V/m (80% AM 1 kHz)	參照 5.3.2.1 備考	CNS 14676-3 CNS 14674-1 CNS 14674-2
備考 1.規定的試驗位準是指未調變載波的 rms.值。 備考 2.針對 1 GHz～6 GHz 測試範圍，因智慧杆尺寸或規格等問題而無法依 CNS			

14676-3 進行配置與測試時，則使用手持無線電等射頻發射裝置替代方法執行測試。

備考 3.針對 1 GHz～6 GHz 測試範圍，亦可依通訊監理單位規定之無線通訊頻帶執行測試即可，參照 NCC IS ALL「行動通信基地臺射頻設備技術規範」，有關其他調變方式則參照 CNS 14676-3 說明。

5.3.2.4 快速暫態抗擾度測試

依 CNS 14676-4 快速暫態抗擾度測試條件執行測試，主要目的為建立一個共通且可再現的準則，評估電氣和電子設備在電源、訊號、控制和接地埠遭受電性快速暫態叢訊時的抗擾度。

表12 快速暫態抗擾度測試條件

埠	試驗規格	性能準則	基本標準
交流電源輸入	重複率: 5 kHz 住宅以外環境區位準: 2 kV 住宅環境區位準:1 kV	參照 5.3.2.1 備考	CNS 14676-4 CNS 14674-1 CNS 14674-2
外部通訊	重複率: 5 kHz 住宅以外環境區位準:1 kV 住宅環境區位準: 0.5kV	參照 5.3.2.1 備考	CNS 14676-4 CNS 14674-1 CNS 14674-2
內部訊號與電力線	重複率: 5 kHz 住宅以外環境區位準:1 kV 住宅環境區位準:0.5 kV	參照 5.3.2.1 備考	CNS 14676-4 CNS 14674-1 CNS 14674-2
備考：依製造商的功能規格，僅適用於其通訊埠電纜總長度>3m。			

5.3.2.5 突波抗擾度測試

依CNS 14676-5突波抗擾度測試條件執行測試,主要目的為建立共同的參考，以作為電氣及電子遭受突波時，評估其抗擾度。

表13 突波抗擾度測試條件

埠	試驗規格	性能準則	基本標準
交流電源輸入	1.2μs/50μs 線對地: 1.室外設備：10 kV 2.室內設備：2 kV 線對線: 1.室外設備：5 kV	參照 5.3.2.1 備考	CNS 14676-5 CNS 16069

	2.室內設備：1 kV		
外部通訊	1.2μs/50μs 線對地: 住宅以外環境區位準:1 kV 住宅環境區位準:N/A	參照 5.3.2.1 備考	CNS 14676-5 CNS 14674-1 CNS 14674-2

5.3.2.6 射頻傳導擾動抗擾度測試

依 CNS 14676-6 射頻傳導擾動抗擾度測試條件執行測試，主要目的為建立有關電機、電子設備對於由意圖發射的射頻(RF)發射機所產生之電磁擾動的傳導抗擾度要求，其頻率範圍在 150 kHz～80 MHz。

表 14 射頻傳導擾動抗擾度測試條件

埠	試驗規格	性能準則	基本標準
交流電源輸入	150 kHz ～ 80 MHz 住宅以外環境區位準:10 V 住宅環境區位準:3 V	參照 5.3.2.1 備考	CNS 14676-6 CNS 14674-1 CNS 14674-2
外部通訊	150 kHz～80 MHz 住宅以外環境區位準: 3 V 住宅環境區位準:3 V	參照 5.3.2.1 備考	CNS 14676-6 CNS 14674-1 CNS 14674-2
內部訊號與電力線	150 kHz～80 MHz 住宅以外環境區位準: 3 V 住宅環境區位準:3 V	參照 5.3.2.1 備考	CNS 14676-6 CNS 14674-1 CNS 14674-2
備考 1.該測試位準定義為進入 150Ω 負載之等效電流。 備考 2.規定的試驗位準是指未調變載波的 rms.值 備考 3.依據製造商的功能規格，僅適用於其通訊埠電纜總長度>3m。			

5.3.2.7 電源頻率磁場抗擾度測試

依 CNS 14676-8 電源頻率磁場抗擾度測試條件執行測試，主要目的為建立共通及可再現的基準，以評估住宅、商業與輕工業區環境應用的電氣及電子設備在其遭遇電源頻率為連續且短暫的持續磁場時之抗擾度。

表 15 電源頻率磁場抗擾度測試條件

埠	試驗規格	性能準則	基本標準
機殼	60 Hz 30 A/m	參照 5.3.2.1 備考	CNS 14676-8 CNS 14674-1 CNS 14674-2

5.3.2.8 電源下降與中斷抗擾度測試

依 IEC 61000-4-11 電源下降與中斷抗擾度測試條件執行測試，主要目的為建立有關電氣和電子設備在電壓暫時下降、電壓短時間中斷和電壓產生變化時的抗擾度。

表16 電源下降與中斷抗擾度測試條件

埠	試驗規格	性能準則	基本標準
交流電源輸入 (60Hz)	殘餘電壓 < 40% 住宅以外環境區，週期: 12	參照 5.3.2.1 備考	IEC 61000-4-11 CNS 14674-1 CNS 14674-2
	殘餘電壓< 70% 週期: 30	參照 5.3.2.1 備考	
	殘餘電壓 0% 住宅以外環境區，週期: 1 住宅環境區,週期:1 及 0.5	參照 5.3.2.1 備考	
	殘餘電壓 0% 週期: 300	參照 5.3.2.1 備考	

5.3.3 量測不確定度

若適用，量測儀器之不確定度應依 CISPR 16-4-2 決定。

備考 1. 對於給定之試驗法，僅於 U_{lab} 值(測試實際值)大於 Ucispr 值(CISPR 16-4-2 所規定之值)時，應將 U_{lab} 實際值記錄於試報告中。

備考 2. 本項要求依主管機關規定。

參考資料

[1] 全臺設置 LED 路燈技術規範，民國 104 年，經濟部能源局

[2] CNS 15425-2 電動機車充電系統－第 2 部：安全連接要求

[3] IEC 61000-3-11 Electromagnetic compatibility (EMC) - Part 3-11: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems - Equipment with rated current ≤ 75 A and subject to conditional connection

[4] IEC 61000-3-12 Electromagnetic compatibility (EMC) - Part 3-12: Limits - Limits for harmonic currents produced by equipment connected to public low-voltage systems with input current > 16 A and <= 75 A per phase

[5] IEC 61000-4-2 Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test

[6] IEC 61000-4-3 Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test

[7] IEC 61000-4-4 Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test

[8] IEC 61000-4-5 Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test

[9] IEC 61000-4-6:2013,Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques-Immunity to conducted disturbances, induced by radio-frequency fields

[10] ITU-T K Suppl. 10 Analysis of electromagnetic compatibility aspects and definition of requirements for 5G systems

[11] IEC 61000-4-8:2009 Electromagnetic compatibility (EMC) - Part 4-8:Testing and measurement techniques - Power frequency magnetic field immunity test

[12] IEC 61851-21-2 Electric vehicle conductive charging system – Part 21-2: Electric vehicle requirements for conductive connection to an AC/DC supply – EMC requirements for off-board electric vehicle charging systems

5G 智慧杆系統技術規範

－第 7-1 部：資訊安全要求

5G Smart pole system technical specification

- Part 7-1: Information security requirements

中 華 民 國 1 1 1 年 9 月

目錄

節次 頁次

前言 2
0. 簡介 3
1. 適用範圍 3
2. 引用標準 3
3. 用語及定義 4
3.1 資產(asset) 4
3.2 攻擊(attack) 4
3.3 防火牆(firewall) 4
3.4 完整性(integrity) 4
3.5 協定(protocol) 4
3.6 遠端存取(remote access) 4
3.7 風險(risk) 4
3.8 路由器(router) 4
3.9 伺服器(server) 4
3.10 系統(system) 4
3.11 威脅(threat) 5
4. 資訊安全要求概述 5
4.1 一般 5
4.2 資訊安全防護標的 5
4.3 資訊安全威脅模型 6
5. 資訊安全基本要求 6
5.1 概述 7
5.2 資訊安全等級 7
5.3 資訊安全基本要求彙總 7
6. 資訊安全構面要求 9
6.1 系統安全要求 9
6.2 軟體及韌體更新 9
6.3 通訊安全 10
6.4 鑑別與授權機制 10
附錄 A (參考) 補充資料 12
A.1 本規範資訊安全要求項目對應之標準 12
A.2 資訊安全利害關係人 13
參考資料 14

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole)現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網 (internet of things, IoT)設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

第 1 部：一般要求。

第 2-1 部：資訊互運性及通訊介面要求。

第 2-2 部：資訊互運性及通訊介面測試要求。

第 3 部：安裝與結構相關安全要求及試驗法。

第 4 部：環境可靠度要求。

第 5 部：電氣安全要求。

第 6 部：電磁相容要求。

第 7-1 部：資訊安全要求。

第 7-2 部：資訊安全測試要求。

第 8 部：電源供應系統要求。

第 9 部：性能要求。

第 10-1 部：5G 微型基地臺一般要求。

第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統。

本規範涵蓋 5G 智慧杆體內網路設備、迴路控制箱內網路設備及代理伺服器、5G 智慧杆管理系統之組態伺服器及應用伺服器之資訊安全要求。

本規範不適用 5G、wifi 及交通號誌系統之資訊安全要求。

備考：物聯網設備相關資訊安全管理要求由本系列規範第 2-1 部、民生公共物聯網資通安全及相關國家標準另定之。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 62443-1-1	工業通訊網路－網路及系統安全－第 1-1 部：術語、概念及模型
CNS62443-4-1	工業自動化及控制系統之安全性－第 4-1 部：產品開發生命週期之安全要求事項
IEC 62443-2-2	Security for industrial automation and control systems - Part 2-2: IACS security protection
IEC 62443-2-3	Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment
IEC 62443-3-3	Industrial communication network-Network and system security - Part 3-3: System security requirements and security levels
IEC 62443-4-2	Security for industrial automation and control systems - Part 2-2:Technical security requirements for IACS components

3. 用語及定義

本規範適用 5G 智慧杆系統技術規範-第 1 部：一般要求之用語及定義，以及下列用語及定義適用於本規範。

3.1 資產(asset)

由組織所擁有或在組織監管職責下之實體或邏輯物件，對組織具感受或實際上的價值。

[引用自 CNS 62443-1-1 之 3.2.6]

3.2 攻擊(attack)

為使用系統資源，對系統攻擊(衍生自智慧型威脅)，亦即蓄意嘗試(特別是在方法上或技術上)規避安全服務並違反系統之安全政策的智慧型行為。

[引用自 CNS 62443-1-1 之 3.3.29]

3.3 防火牆(firewall)

於 2 個互連網路間進行網路封包轉發、過濾及阻擋等存取控制之網路設備。於一般網路規畫中，防火牆可用於劃分資訊安全區域之邊界，並設置網路封包來源、目的地、通訊埠等規則，以判斷是否允許資料通訊。防火牆通常為一專屬網路設備，或作為其他網路設備之附屬功能，例：使用內含上述功能之路由器，或由一般通用型伺服器安裝應用程式等方式實作。

[引用自本系列規範第 2-1 部之 3.12]

3.4 完整性(integrity)

反映運作之系統的邏輯正確性及可靠性、實作保護機制之硬體及軟體的邏輯完備性，以及資料結構與所儲存資料之一致性的系統品質。

[引用自 CNS 62443-1-1 之 3.2.60]

3.5 協定(protocol)

用以實作並控制系統間某些相關聯形式(例：通訊)之規則集(亦即，格式與程序)。

[引用自 CNS 62443-1-1 之 3.2.80]

3.6 遠端存取(remote access)

於由不同地理位置以如同身處安全區內之權限，使用安全區周界內的系統。

[引用自 CNS 62443-1-1 之 3.2.83]

3.7 風險(risk)

預期損失，以機率表示特定威脅將利用特定脆弱性之特定後果。

[引用自 CNS 62443-1-1 之 3.2.87]

3.8 路由器(router)

用於網路通訊之硬體設備，負責接收封包，並依其網際網路協定套組第三層資訊 (亦即 IP 位址)轉發資料封包至對應連接埠。路由器具備較高之運算能力，可由人工輸入或自動探索等方式，計算目標 IP 位址對應最佳轉發路徑。相較於第三層交換器，路由器可支援更多網路管理功能。

[引用自本系列規範第 2-1 部之 3.34]

3.9 伺服器(server)

向客戶端應用程式及裝置提供資訊或服務之裝置或應用系統。

[引用自 CNS 62443-1-1 之 3.2.119]

3.10 系統(system)

由互動、相關聯或相依元件形成之複合體。

[引用自 CNS 62443-1-1 之 3.2.123]

3.11 威脅(threat)

安全違規之可能性，存在於可能出現危害安全並造成損害的情況、能力及、動作或事件時。

[引用自 CNS 62443-1-1 之 3.2.125]

4. 資訊安全要求概述

4.1 一般

5G 智慧杆因布建於戶外環境，其資訊安全要求包括資訊安全及實體安全 2 大層面，圖 1 係 5G 智慧杆系統常見之布建情境。

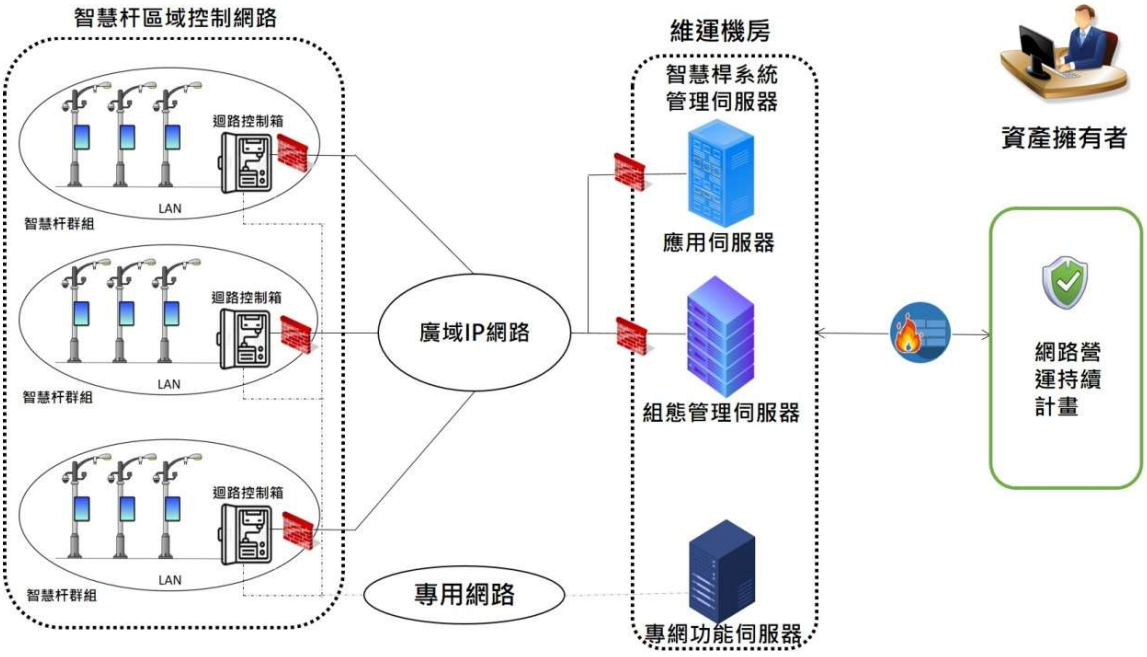


圖 1 智慧杆系統常見之布建情境

由不同地區之智慧杆群組所組成之智慧杆區域控制網路，智慧杆群組經區域網路透過廣域 IP 網路串接至維運機房，維運機房內可建置眾多伺服器(例:本系列規範第 2-1 部定義之組態伺服器及應用伺服器)智慧杆系統管理者可透過特定介面對智慧杆系統進行管理。

4.2 資訊安全防護標的

圖 2 為 5G 智慧杆系統資訊安全防護標的示意圖，本規範資安防護標的包括杆體內網路設備、迴路控制箱內網路設備與代理伺服器、組態伺服器及應用伺服器。物聯網設備相關資訊安全管理要求由本系列規範第 2-1 部、民生公共物聯網資通安全及相關國家標準另定之。

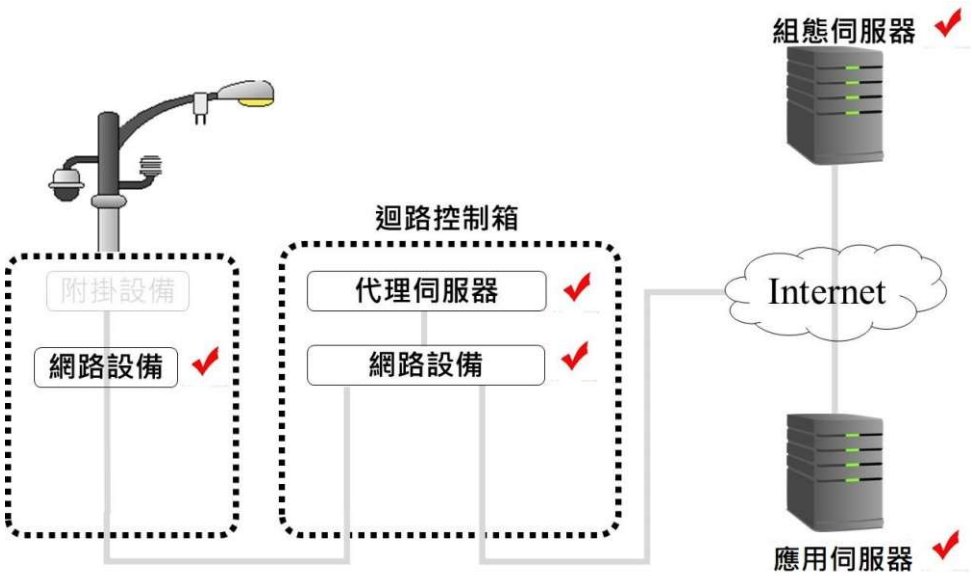


圖 2 5G 智慧杆系統資訊安全防護標的示意圖

4.3 資訊安全威脅模型

依資訊安全防護標的整理出如表 1 之資訊安全威脅模型，分別針網路設備(例:閘道器、路由器)、代理伺服器、組態伺服器及應用伺服器，進行通訊安全、資料安全及計算安全的威脅分析。通訊安全層面考量機密性、完整性及可用性；資料安全考量資料機密性及存取控制性；計算安全考量平台可信任性、軟體可信任性、資訊區隔性。

表 1　資訊安全威脅模型

核心部件 / 安全層面	組態伺服器	應用伺服器	代理伺服器	網路設備
通訊安全	竊聽 冒名 連結劫持 重播攻擊	竊聽 冒名 連結劫持 重播攻擊	竊聽 冒名 連結劫持 重播攻擊	竊聽 冒名 連結劫持 重播攻擊
資料安全	資料損壞	隱私違反 資料損壞	資料損壞	
計算安全	程式損壞	軟體遭竊 程式損壞 模型失效	程式損壞	

5. 資訊安全基本要求

5.1 概述

本規範規定系統資訊安全、軟體與韌體更新、通訊資訊安全及鑑別與授權機制等構面，以檢視杆體內部網路、網路設備與代理伺服器之資訊安全程度，如表 2 所示，說明如下：

(a) 系統資訊安全：確保網路設備、代理伺服器、組態伺服器及應用伺服器之防禦能力，包含需要資源、日誌等。

(b) 軟體與韌體更新：網路設備、代理伺服器、組態伺服器及應用伺服器之韌體版本更新服務，與代理伺服器、組態伺服器及應用伺服器之作業系統與應用程式之相關程式修補等，應具備足夠之資訊安全防護。

(c) 通訊資訊安全：杆體內物聯網設備與迴路控制箱代理伺服器通訊、迴路控制箱代理伺服器與位於網際網路之組態伺服器及應用伺服器間，通訊資料應加密或使用網路安全協定提供足夠安全之防護。

(d) 鑑別及授權機制：對每個可存取杆體內部網路設備、迴路控制箱內代理伺服器及網路設備之介面應建立識別機制、鑑別機制與授權機制及權限控管機制，包括遠端管理介面、通訊等，應具備一定防護能力，以防止人員存取未經授權之資料或進行權限外之操作。

5.2 資訊安全等級

本規範將各項資訊安全要求區分為 3 個資訊安全等級，第 1 級之效果為防止非蓄意誤操作、不成熟之攻擊行為或無足夠資源之蓄意攻擊行為；第 2 級之效果為防止蓄意且有資源之攻擊行為；第 3 級之效果為防止蓄意且有資源與中風險之攻擊行為。資訊安全等級說明如表 2；各資訊安全基本要求與其對應之安全等級如表 3，其相對應之標準項目彙整於附錄 A。

備考：中風險泛指除智慧杆系統本身尚失其預設功能外並攻擊外部網際網路營運之資訊系統。

表 2　資訊安全等級說明

資訊安全等級	說明	備註
第 1 級	防止非蓄意誤操作或不成熟之攻擊行為，或防止攻擊者無足夠資源之蓄意攻擊行為。	應滿足表 3 規範之第 1 級之資訊安全要求細項
第 2 級	防止蓄意且有資源之攻擊行為。	應滿足表 3 規範之第 2 級之資訊安全要求細項
第 3 級	防止蓄意且有資源與中風險以上之攻擊行為。	應滿足表 3 規範之第 3 級之資訊安全要求細項

5.3 資訊安全基本要求彙總

資訊安全基本要求彙整於表 3，第 1 欄為基本要求，第 2 欄為安全要求類別，第 3 欄為資訊安全要求細項，其內容參照第 6 節，第 4 欄資訊安全等級。

備考：第 2 級應包含第 1 級資訊安全要求細項，第 3 級應包含第 1、2 級資訊安全要求細項。

表 3　資訊安全基本要求彙總表

資訊安全構面	安全要求類別	資訊安全要求細項	資訊安全等級		
			第 1 級	第 2 級	第 3 級
6.1 系統安全	6.1.1 系統最基本功能	6.1.1.(a)	**V**	**V**	**V**
		6.1.1.(b)	**V**	**V**	**V**
		6.1.1.(c)	**V**	**V**	**V**
		6.1.1.(d)	**V**	**V**	**V**
	6.1.2 裝置安全強化	6.1.2.(a)	**V**	**V**	**V**
		6.1.2.(b)	**V**	**V**	**V**
		6.1.2.(c)	**V**	**V**	**V**
	6.1.3 系統日誌	6.1.3.(a)	**V**	**V**	**V**
		6.1.3.(b)	**V**	**V**	**V**
		6.1.3.(c)		**V**	**V**
		6.1.3.(d)	**V**	**V**	**V**
		6.1.3.(e)	**V**	**V**	**V**
		6.1.3.(f)			**V**
	6.1.4 作業系統與網路服務	6.1.4.(a)	**V**	**V**	**V**
		6.1.4.(b)		**V**	**V**
		6.1.4.(c)		**V**	**V**
6.2 軟體及韌體更新	6.2.1 更新安全	6.2.1.(a)	**V**	**V**	**V**
		6.2.1.(b)	**V**	**V**	**V**
		6.2.1.(c)	**V**	**V**	**V**
		6.2.1.(d)	**V**	**V**	**V**
		6.2.1.(e)		**V**	**V**
	6.2.2 版本安全	6.2.2.(a)	**V**	**V**	**V**
		6.2.2.(b)	**V**	**V**	**V**
		6.2.2.(c)	**V**	**V**	**V**
		6.2.2.(d)	**V**	**V**	**V**
6.3 通訊安全	6.3.1 資料傳輸安全	6.3.1.(a)	**V**	**V**	**V**
		6.3.1.(b)	**V**	**V**	**V**
	6.3.2 資料儲存安全	6.3.2.(a)	**V**	**V**	**V**
		6.3.2.(b)	**V**	**V**	**V**
6.4 鑑別與授權機制	6.4.1 帳戶管理	6.4.1.(a)	**V**	**V**	**V**
		6.4.1.(b)	**V**	**V**	**V**
	6.4.2 存取控制	6.4.2.(a)	**V**	**V**	**V**
		6.4.2.(b)	**V**	**V**	**V**
		6.4.2.(c)	**V**	**V**	**V**
	6.4.3 身分鑑別	6.4.3.(a)	**V**	**V**	**V**
		6.4.3.(b)		**V**	**V**
		6.4.3.(c)		**V**	**V**

		6.4.3.(d)	**V**	**V**	**V**
		6.4.3.(e)		**V**	**V**

6. 資訊安全構面要求

6.1 系統安全要求

6.1.1 系統最基本功能

(a) 系統應明確定義必要之功能。

(b) 系統日誌儲存容量應滿足保存期限所需，可參照 NIST SP 800-92[4]之建議。

(c) 系統時間應與世界協調時間(Coordinated Universal Time, UTC)同步。

(d) 系統時間參照來源應受保護，以防止未經授權更改。

6.1.2 裝置安全強化

(a) 代理伺服器、組態伺服器及應用伺服器應刪除非必要之應用程式及網路服務。

(b) 代理伺服器、組態伺服器及應用伺服器應使用最少必要之通訊協定。

(c) 代理伺服器、組態伺服器及應用伺服器不得使用已知存在脆弱性之應用程式及網路服務。

6.1.3 系統日誌

(a) 網路設備、代理伺服器、組態伺服器及應用伺服器應具安全日誌功能並記錄網路、系統及資訊安全事件。

(b) 網路設備、代理伺服器、組態伺服器及應用伺服器應防止遭修改或刪除安全日誌。

(c) 網路設備、代理伺服器、組態伺服器及應用伺服器，應能自動將安全日誌傳送到安全資訊與事件管理系統或異地紀錄伺服器儲存。

(d) 網路設備、代理伺服器、組態伺服器及應用伺服器間應具備時間同步機制。

(e) 網路設備、代理伺服器、組態伺服器及應用伺服器發生使用者異常登入安全事件時，應具備主動告警機制，將包括該設備識別符等訊息，回報相關人員。

(f) 日誌系統儲存容量到達最大容量比例臨限值前，系統應於規定之時效內對相關人員發出告警訊息。

6.1.4 作業系統及網路服務

(a) 網路設備、代理伺服器、組態伺服器及應用伺服器之作業系統與網路服務，不應存在美國國家弱點資料庫所公布及更新之常見弱點與脆弱性資料(CVE)且通用脆弱性評分系統(CVSS)最新版本之分數評比 7 分以上或高風險等級。

(b) 網路設備、代理伺服器、組態伺服器及應用伺服器應具抵禦阻絕服務 (DoS)攻擊之能力。

(c) 防火牆規則設定及維護應文件化並提供定期檢視機制。

6.2 軟體及韌體更新

6.2.1 更新安全

(a) 網路設備、代理伺服器、組態伺服器及應用伺服器應支援遠端更新功能。

(b) 網路設備、代理伺服器、組態伺服器，以及應用伺服器進行韌體更新時，即使發生更新未成功，系統應仍能回復正常運作。

(c) 網路設備、代理伺服器、組態伺服器及應用伺服器之更新路徑應通過安全通道，以確保韌體之機密性、完整性、可用性及正確性，且安全通道版本應符合 TLSV1.2[1]或 DTLS

V1.2 以上規範。

(d) 網路設備、代理伺服器、組態伺服器及應用伺服器於更新韌體前，應使用數位簽章查證韌體之完整性及來源。

(e) 網路設備、代理伺服器、組態伺服器及應用伺服器應具備定期檢查是否有可用之安全更新，並顯示產品版本更新狀態之機制。

6.2.2 版本安全

(a) 網路設備、代理伺服器、組態伺服器及應用伺服器之硬體及韌體版本應唯一。

(b) 相關服務提供者應能提供各韌體版本之加密雜湊值作為韌體版本之追溯管控。

(c) 網路設備、代理伺服器、組態伺服器及應用伺服器內各硬體模組應可獨立替換。

(d) 網路設備、代理伺服器、組態伺服器及應用伺服器之韌體簽章金鑰應妥善保管不可外洩或被輕易取得。

6.3 通訊安全

6.3.1 資料傳輸安全

(a) 機敏資料傳輸時，已確保資料之機密性、完整性、可用性及正確性，且伺服器傳輸協定應符合 TLS V1.2[1]或 DTLS V1.2 以上規範。

備考：機敏資料包括但不限於身分鑑別資訊(如使用者帳戶、通行碼)及含有使用者隱私之資料。

(b) 使用無線連接時，應提供授權、監控及限制機制。

6.3.2 資料儲存安全

(a) 代理伺服器、組態伺服器及應用伺服器儲存之機敏資料應加密儲存。

(b) 代理伺服器、組態伺服器及應用伺服器儲存之機敏資料，其加密方式應採用符合 NIST SP800-57[3]及 ISO/IEC 19790[2]同等或以上等級之加密演算法。

6.4 鑑別與授權機制

6.4.1 帳戶管理

(a) 網路設備、代理伺服器、組態伺服器及應用伺服器，不應包含預設、臨時及匿名帳戶。

(b) 僅允許經授權之特定帳戶可遠端存取代理伺服器、組態伺服器及應用伺服器。

6.4.2 存取控制

(a) 代理伺服器、組態伺服器及應用伺服器，應能限制某些主機網路服務之存取權限。

(b) 網路設備、代理伺服器、組態伺服器及應用伺服器，應提供人員使用者至少 2 層級(例:管理者及一般使用者)以上之存取權限。

(c) 代理伺服器、組態伺服器及應用伺服器應允許定義新的角色。

6.4.3 身分鑑別

(a) 使用者或伺服器經網路存取代理伺服器、組態伺服器及應用伺服器，應通過身分鑑別。

備考：網路設備及伺服器鑑別機制由本系列規範第 2 部規定。

(b) 對於身分鑑別所使用之通行碼強度應有規定，以避免被輕易破解遭不當利用。

(c) 進行遠端操控代理伺服器、組態伺服器及應用伺服器，應具防止重送攻擊之機制。

(d) 使用者身分鑑別未成功時，應中斷連接。

(e) 使用者在多次登入代理伺服器、組態伺服器及應用伺服器未成功後，代理伺服器、組態

伺服器及應用伺服器應拒絕該使用者的請求、登入次數及時間應可設定。

附錄 A

(參考)

補充資料

A.1 本規範資訊安全要求項目對應之標準

以下表 A.1 列出本規範資訊安全要求項目與對應之標準。

表 A.1　本規範資訊安全要求項目對應之標準

本規範節次	CNS/IEC62443 系列標準	其他相關規範
6.1.1.(a)	IEC 62443-3-3 SR 7.7	
6.1.1.(b)	IEC 62443-3-3 SR 2.9	NIST SP 800-92[4]
6.1.1.(c)	IEC 62443-3-3 SR 2.11	
6.1.1.(d)	IEC 62443-3-3 SR 2.11 RE2	
6.1.2.(a)	IEC 62443-3-3 SR7.7	
6.1.2.(b)	CNS 62443-4-1 SI-2	
6.1.2.(c)	IEC 62443-3-3 SR7.7	
6.1.3.(a)	IEC 62443-3-3 CR 1.12	
6.1.3.(b)	IEC 62443-3-3 SR 6.1	
6.1.3.(c)	無	
6.1.3.(d)	IEC 62443-3-3 SR 2.11 RE 1	
6.1.3.(e)	IEC 62443-3-3 SR 3.3	
6.1.3.(f)	IEC 62443-3-3 SR 2.9 RE1	
6.1.4.(a)	CNS 62443-4-1 SVV-3 CNS 62443-4-1 DM-3	
6.1.4.(b)	IEC 62443-3-3 SR 7.1 IEC 62443-4-2 CR 7.1	
6.1.4.(c)	IEC 62443-3-3 SR 7.6	
6.2.1.(a)	IEC 62443-4-2 CR 3.10 IEC 62443-4-2 EDR 3.10 IEC 62443-4-2 NDR 3.10	
6.2.1.(b)	IEC 62443-3-3 SR 7.4	
6.2.1.(c)	CNS 62443-4-1 SUM-4	
6.2.1.(d)	IEC 62443-3-3 SR 2.4 IEC 62443-4-2 EDR 3.12	
6.2.1.(e)	CNS 62443-4-1 SR-2 CNS 62443-4-1 SUM-2	
6.2.2.(a)	IEC 62443-4-2 CR 1.2	
6.2.2.(b)	CNS 62443-4-1 SUM-4	
6.2.2.(c)	IEC 62443-4-2 CR 3.10	
6.2.2.(d)	CNS 62443-4-1 SM-8 IEC 62443-4-2 EDR 3.13	
6.3.1.(a)	IEC 62443-3-3 SR 4.1	

	IEC 62443-3-3 SR 4.3	
6.3.1.(b)	IEC 62443 3-3 SR 2.2	
6.3.2.(a)	IEC 62443-4-2 CR 4.1	
6.3.2.(b)	IEC 62443-4-2 CR 1.7	
6.4.1.(a)	CNS 62443-4-1 SG-6	
6.4.1.(b)	IEC 62443-3-3 SR 2.1 RE 2	
6.4.2.(a)	IEC 62443-3-3 SR 5.2 RE 1	
6.4.2.(b)	IEC 62443-3-3 SR 2.1 IEC 62443-4-2 CR 2.1	
6.4.2.(c)	IEC 62443-3-3 SR 2.1 RE 2	
6.4.3.(a)	IEC 62443-3-3 SR 1.13 IEC 62443-4-2 NDR 1.13	
6.4.3.(b)	IEC 62443-3-3 SR 1.7 IEC 62443-4-2 CR 1.7	
6.4.3.(c)	IEC 62443-3-3 SR 3.8 IEC 62443-4-2 CR 3.8	
6.4.3.(d)	IEC 62443-3-3 SR 1.13 RE 1	
6.4.3.(e)	IEC 62443-3-3 SR 1.11 IEC 62443-4-2 CR 1.11	
備考 1. system requirement, SR 備考 2. system integrity, SI 備考 3. component requirement, CR 備考 4. requirement enhancement, RE 備考 5. embedded device requirement, EDR 備考 6. network device requirement, NDR		

A.2 資訊安全利害關係人

以下說明本規範所論及資訊安全利害關係人：

－資產擁有者(asset owner, AO)：管理者為 5G 智慧杆系統之資產擁有者，可以自建自營或委辦予營運者代管維運方式管理 5G 智慧杆系統。

－系統整合服務提供者(system integration service provider)：為 5G 智慧杆系統設計、安裝、配置、測試及調適者，可協助資產擁有者執行風險評鑑活動。

－物聯網設備產品供應者(IoT equipment product supplier)：製造 5G 智慧杆物聯網設備硬體或產品之供應者。

－物聯網服務提供者(IoT service provider)：整合 5G 智慧杆體內部物聯網設備、區域網路與迴路控制箱內部網路及主機設備。

－網路服務提供者(network service provider)：提供 5G 智慧杆系統迴路控制箱透過網際網路及後端相關管理與功能相關之主機設備與軟體應用程式。

－維護服務供應者(maintenance service supplier)：維護 5G 智慧杆系統相關硬體或軟體之服務供應者。

參考資料

[1] IETF/RFC 5246, The Transport Layer Security (TLS) Protocol V1.2

[2] ISO/IEC 19790,Information technology-Security techniques-Security requirements for cryptographic modules

[3] NIST SP800-57, Recommendation for Key Management: Part 1 – General

[4] NIST SP800-92, Guide to Computer Security Log Management

5G 智慧杆系統技術規範

－第 7-2 部：資訊安全測試要求

5G Smart pole system technical specification - Part 7-2: Testing specifications for information security requirements

中 華 民 國 111 年 9 月

目錄

節次 **頁次**

前言 2

0. 簡介 3

1. 適用範圍 3

2. 引用標準 3

3. 用語及定義 3

3.1 共同平台列舉(CPE) 3

3.2 軟體物料清單(SBOM) 3

4. 檢測通過準則 4

5. 資訊安全構面要求 4

5.1 系統安全要求 4

5.2 軟體及韌體更新 13

5.3 通訊安全 19

5.4 鑑別與授權機制 22

參考資料 29

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole)現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網 (internet of things, IoT)設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

第 1 部：一般要求。

第 2-1 部：資訊互運性及通訊介面要求。

第 2-2 部：資訊互運性及通訊介面測試要求。

第 3 部：安裝與結構相關安全要求及試驗法。

第 4 部：環境可靠度要求。

第 5 部：電氣安全要求。

第 6 部：電磁相容要求。

第 7-1 部：資訊安全要求。

第 7-2 部：資訊安全測試要求。

第 8 部：電源供應系統要求。

第 9 部：性能要求。

第 10-1 部：5G 微型基地臺一般要求。

第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統。

本規範涵蓋 5G 智慧杆體內網路設備、迴路控制箱內網路設備及代理伺服器、5G 智慧杆管理系統之組態伺服器及應用伺服器的資訊安全要求之測試規範，資訊安全要求由本系列規範第 7-1 部制定。

本規範不適用 5G、wifi 及交通號誌系統之資訊安全要求。

備考：物聯網設備相關資訊安全管理要求由本系列規範第 2-1 部、民生公共物聯網資通安全及相關國家標準另定之。

2. 引用標準

本規範適用 5G 智慧杆系統技術規範-第 7-1 部之引用標準。

3. 用語及定義

本規範適用 5G 智慧杆系統技術規範-第 7-1 部之用語及定義，以及下列用語及定義適用於本規範。

3.1 共同平台列舉(common platform enumeration, CPE)

美國國家標準與技術研究院(National Institute of Standards and Technology, NIST)所提出將脆弱性標準化之方式，用以識別應用程式、作業系統及硬體上的各種設備之資訊資產，且有版本區別。

3.2 軟體物料清單(software bill of materials, SBOM)

美國電信暨資訊管理局(National Telecommunications and Information Administration, NTIA)所提出

之正式紀錄，包含建立軟體時所有組件之細節及供應鏈關係。至少應記錄軟體名稱、識別符、版本、彼此間依賴關係、開發者等內容。

4. 檢測通過準則

(a) 前置條件

廠商應宣告代測標的應通過測試項目清單，或達成本系列規範第 7-1 部之資訊安全等級。

備考：第 2 級應包含第 1 級資訊安全要求細項，第 3 級應包含第 1、2 級資訊安全要求細項。

(b) 通過符合性檢測

待測標的應通過清單內所列之測試項目，方可認定為通過檢測。若宣告達成本系列規範第 7-1 部之資訊安全等級，則代測標的於該資安等級規範之所有測試項目，判定條件結果不可為〝不符合要求〞，方可認定為通過檢測。

5. 資訊安全構面要求

5.1 系統安全要求

5.1.1 系統最基本功能

5.1.1.1 系統應明確定義必要之功能

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.1.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的必要之資訊安全功能。

(d) 前置條件

廠商應提供書面資料，說明必要之功能、目的及預設值。

(e) 測試方法及步驟

測試人員檢視待測標的之功能及其目的。

(f) 判定條件

-符合要求

待測標的所提供之功能與書面資料記載內容一致。

-不符合要求

待測標的所提供之功能與書面資料記載內容不一致。

-不適用

本測試項目無不適用之條件。

5.1.1.2 系統日誌儲存容量應符合 NIST SP 800-92[4]之建議

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.1.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否有針對安全事件日誌檔配置之儲存容量應符合 NIST SP 800-92[4]之建議。

(d) 前置條件

廠商應提供書面資料，說明設置文件、待測標的之日誌儲存設置環境與安全事件日誌儲存容量。

(e) 測試方法及步驟

(1) 測試人員審查廠商所提供之書面資料，並依設置文件建置日誌儲存環境。

(2) 嘗試以錯誤之帳戶及通行碼登入待測標的以觸發安全事件日誌。

(f) 判定條件

-符合要求

待測標的可將安全事件日誌儲存至儲存環境，並從管理介面(例:系統之硬碟管理工具)得知目前儲存容量。

-不符合要求

待測標的不支援儲存安全事件日誌，或無法從管理介面得知儲存裝置之儲存容量。

不適用

-本測試項目無不適用之條件。

5.1.1.3 系統時間應與世界協調時間(Coordinated Universal Time, UTC)同步

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.1.(c)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的時間與 UTC 同步，且僅經授權之使用者與系統管理者可進行設定。

(d) 前置條件

待測標的應與 UTC 參照來源伺服器連接。

(e) 測試方法及步驟

(1) 測試人員以測試電腦連接至待測標的之管理介面。

(2) 以系統管理者，手動調整系統時間至錯誤之時間。再啟用時間校時功能，確認測試標的時間是否重新調整與 UTC 一致。

(f) 判定條件

-符合要求

待測標的可重新調整與 UTC 同步。

-不符合要求

待測標的無法重新調整與 UTC 同步。

-不適用

本測試項目無不適用之條件。

5.1.1.4 系統時間參照來源應受保護，以防止未經授權更改

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.1.(d)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的之時間可與外部系統時間參照來源同步，且僅經授權之使用者可者進行設定。

(d) 前置條件

(1) 待測標的可與需系統時間參照來源伺服器連接。

(2) 提供使用者角色與權限對照表。

(e) 測試方法及步驟

(1) 測試人員以測試電腦連接至測試標的之管理介面。

(2) 以經授權使用者或系統管理者，手動調整系統時間至錯誤之時間。再啟用時間校時功能，確認測試標之時間是否重新調整與時間參照來源同步。

(3) 以未經授權的使用者身分登入系統，嘗試關閉時間校時功能或調整系統時間。

(f) 判定條件

-符合要求

僅經授權使用者或系統管理者可設定系統時間參照來源。

-不符合要求

待測標的不支援設定系統時間參照來源；或未經授權使用者可設定系統時間參照來源。

-不適用

本測試項目無不適用之條件。

5.1.2 裝置安全強化

5.1.2.1 代理伺服器、組態伺服器及應用伺服器應刪除非必要之應用程式及網路服務

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.2.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的應不存在非必要之應用程式及網路服務。

(d) 前置條件

(1) 待測標的保持預設出廠資訊。

(2) 廠商應提供書面資料說明應用程式及網路服務、目的及預設值。

(3) 提供作業系統存取權限。

(e) 測試方法及步驟

(1) 測試人員使用管理者登入待測標的之作業系統，列出所有執行的應用程式及網路服務。

(2) 核對待測測標的實際執行之應用程式及網路服務是否一致。

(f) 判定條件

-符合要求

待測標的預設執行之應用程式及網路服務與書面資料一致。

-不符合要求

待測標的預設執行之應用程式及網路服務與書面資料不一致。

-不適用

本測試項目無不適用之條件。

5.1.2.2 代理伺服器、組態伺服器及應用伺服器應使用最少必要之通訊協定

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.2.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的應不存在非必要之通訊協定。

(d) 前置條件

(1) 待測標的保持預設出廠資訊。

(2) 廠商應提供書面資料說明必要通訊協定，說明功能、目的及預設值。

(3) 提供作業系統存取權限。

(e) 測試方法及步驟

(1) 測試人員以封包側錄工具側錄待測標的對外之網路連接，記錄待測標的對外連接所使用的通訊協定。

(2) 測試人員登入作業系統，列出所有執行的網路連接，記錄所有網路連接對應之應用程式，並判定所使用通訊協定。

(3) 核對待測標的實際執行之通訊協是否一致。

(f) 判定條件

-符合要求

待測標的使用的通訊協定與書面資料一致。

-不符合要求

待測標的使用的通訊協定與書面資料不一致。

-不適用

本測試項目無不適用之條件。

5.1.2.3 代理伺服器、組態伺服器及應用伺服器不得使用已知存在脆弱性之應用程式及網路服務

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.2.(c)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的所使用的應用程式及網路服務不存在已知安全脆弱性。

(d) 前置條件

廠商應提供待測標的之軟體物料清單。

(e) 測試方法及步驟

(1) 測試人員檢視待測標的之軟體物料清單。

(2) 測試人員針對每一筆軟體物料，將依版本資訊或共同平台列舉字串在美國國家弱點資料庫是否存在已知安全脆弱性。

(f) 判定條件

-符合要求

所有軟體物料皆不存在已知安全脆弱性。

-不符合要求

任一筆軟體物料存在至少 1 個已知安全脆弱性。

-不適用

本測試項目無不適用之條件。

5.1.3 系統日誌

5.1.3.1 網路設備、代理伺服器、組態伺服器及應用伺服器應具安全日誌功能並記錄完整網路、系統及資訊安全事件。

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.3.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的具備安全日誌功能，應記錄完整網路、系統及資訊安全事件。

(d) 前置條件

(1) 廠商應提供書面資料，說明設定安全日誌功能之步驟。

(2) 測試人員依書面資料，設定待測標的安全日誌功能。

(e) 測試方法及步驟

(1) 測試人員連接至待測標的之管理介面。

(2) 測試人員分別使用正確使用者帳戶通行碼與錯誤的使用者帳戶通行碼登入系統，並記錄登入時間。

(3) 測試人員依書面資料，檢視檢測標的安全日誌是否有記錄步驟(2)之登入成功與登入未成功之紀錄。

(f) 判定條件

-符合要求

待測標的具備安全日誌功能，且正確記錄使用者登入成功與未成功之紀錄。

-不符合要求

待測標的不支援安全日誌功能或無法記錄使用者登入成功與未成功之紀錄。

-不適用

本測試項目無不適用之條件。

5.1.3.2 網路設備、代理伺服器、組態伺服器及應用伺服器應防止遭修改或刪除安全日誌

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.3.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否防止任何人修改或刪除安全日誌。

(d) 前置條件

測試人員依待測標的書面資料，設定安全日誌功能。

(e) 測試方法及步驟

(1) 測試人員登入待測標的介面並瀏覽安全日誌功能頁面，記錄安全日誌功能頁面 URL。

(2) 測試人員登出待測標的管理介面，並重新瀏覽安全日誌功能頁面，確認是否可以存取安全日誌並執行修改與刪除作業。

(f) 判定條件

-符合要求

測試人員無法修改或刪除安全日誌。

-不符合要求

測試人員可修改或刪除安全日誌。

-不適用

本測試項目無不適用之條件。

5.1.3.3 網路設備、代理伺服器、組態伺服器及應用伺服器，應能自動將安全日誌傳送到安全資訊與事件管理系統或異地紀錄伺服器儲存

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.3.(c)。

(b) 適用安全等級(全文修改)

第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否支援將安全日誌傳送至日誌伺服器或其他集中管理伺服器。

(d) 前置條件

(1) 廠商應提供書面資料，說明設定安全日誌步驟。

(2) 測試人員依書面資料，設定待測標的安全日誌功能。

(3) 待測標的與日誌伺服器需能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(e) 測試方法及步驟

(1) 測試人員登入待測標的管理介面，並將安全日誌設定傳送至遠端日誌伺服器。

(2) 測試人員登出待測標的管理介面，並以錯誤使用者帳戶通行碼登入待測標的管理介面。

(3) 測試人員確認是否可以於遠端日誌伺服器查詢到剛才的登入未成功行為。

(f) 判定條件

-符合要求

測試人員可於遠端日誌伺服器檢視待測標的之安全日誌。

-不符合要求

待測標的不支援將安全日誌傳送至遠端日誌伺服器或無法從遠端日誌伺服器檢視待測標的安

全日誌內容。

-不適用

本測試項目無不適用之條件。

5.1.3.4 網路設備、代理伺服器、組態伺服器及應用伺服器間應具備時間同步機制

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.3.(d)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否支援與時間同步伺服器進行網路校時之功能。

(d) 前置條件

(1) 廠商應提供書面資料，說明設定時間同步伺服器步驟。

(2) 測試人員依書面資料，設定待測標的之時間同步伺服器。

(3) 測標的與時間同步伺服器需能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(e) 測試方法及步驟

(1) 測試人員登入管理介面，將時間設定成錯誤的日期與時間。

(2) 測試人員登出之後，重新登入管理介面，並設定時間同步伺服器網址或 IP 位址。

(3) 測試人員完成設定之後，檢視待測標的目前之日期與時間是否與時間同步伺服器一致。

(f) 判定條件

-符合要求

待測標的可連接至時間同步伺服器，且時間與時間同步伺服器一致。

-不符合要求

待測標的不支援時間同步功能，或時間校正之後與時間同步伺服器不一致。

-不適用

本測試項目無不適用之條件。

5.1.3.5 網路設備、代理伺服器、組態伺服器及應用伺服器發生使用者異常登入安全事件時，應具備主動告警機制，將包括該設備識別符等訊息，回報相關人員

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.3.(e)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

待測標的是否支援使用者異常登入安全事件主動告警機制。

(d) 前置條件

(1) 廠商應提供書面資料，說明觸發告警機制之條件與告警方式步驟。

(2) 測試人員依書面資料，確認待測標的觸發告警機制之條件與告警方式。

(e) 測試方法及步驟

(1) 測試人員嘗試連續登入未成功達待測標的所設定的告警觸發次數。

(2) 測試人員檢視是否有收到待測標的所送出的告警資訊，其內容應至少包括日期、時間及該設備之識別符。

(f) 判定條件

-符合要求

測試人員可接收到待測標的所發出之使用者異常登入安全事件告警訊息。

-不符合要求

待測標的不支援使用者異常登入安全事件告警機制，或其安全事件告警機制無主動通知功能。

-不適用

本次測試項目無不適用之情況。

5.1.3.6 日誌系統儲存容量到達最大容量比例臨限值前，系統應於規定之時限內對相關人員發出告警訊息

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.3.(f)。

(b) 適用安全等級

第 3 級。

(c) 測試目的

查證待測標的是否具備日誌儲存容量告警功能。

(d) 前置條件

(1) 廠商應提供書面資料，說明觸發告警機制之條件與告警方式步驟。

(2) 測試人員依書面資料，確認待測標的觸發告警機制之條件與告警方式。

(e) 測試方法及步驟

(1) 測試人員依書面資料，檢視待測標的是否有日誌儲存容量告警機制。

(2) 測試人員利用工具將大量模擬之日誌或大型檔案，傳送至日誌系統並到達容量臨限值。

(f) 判定條件

-符合要求

待測標的本身支援日誌儲存容量告警機制並發出告警訊息。

-不符合要求

待測標的本身不支援日誌儲存容量告警機制或無法發出告警訊息。

-不適用

本測試項目無不適用之條件。

5.1.4 作業系統及網路服務

5.1.4.1 網路設備、代理伺服器、組態伺服器及應用伺服器之作業系統及網路服務，不應存在美國國家弱點資料庫所公布及更新之常見弱點與脆弱性資料(CVE)且通用脆弱性評分系統(CVSS)最新版本之分數評比 7 分以上或高風險等級

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.4.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的之作業系統及網路服務是否存在已知高資安風險之脆弱性。

(d) 前置條件

測試標的至少 1 個通訊介面支援使用 IP 網路進行資料傳輸。

(e) 測試方法及步驟

(1) 測試人員將安裝掃描工具之測試電腦與測試標的連接至同一區域網路，測試電腦與測試標的間，不得有入侵防禦系統或防火牆等資安防護工具。

(2) 測試人員將測試標的還原至出廠預設設定值，並依測試環境需求設定網路位址。

(3) 測試人員以掃描工具對測試標的網路位址(IP)執行測試作業。

(f) 判定條件

-符合要求

作業系統及網路服務未檢測出美國國家脆弱性資料庫之資安脆弱性；或所有檢測出之資安脆弱性其公告最新版之脆弱性評分系統(CVSS)皆未達 7.0 分。

-不符合要求

作業系統及網路服務檢測出美國國家脆弱性資料庫所公告之資安脆弱性，且該資安脆弱性對應之最新版脆弱性評分系統(CVSS)為 7.0 分(含)以上。

-不適用

測試標的不支援使用 IP 網路進行資料傳輸。

5.1.4.2 網路設備、代理伺服器、組態伺服器及應用伺服器應具抵禦阻絕服務(DoS)攻擊之能力，即當網路介面充斥資料或收到錯誤訊息時，網路設備、代理伺服器、組態伺服器及應用伺服器應不應長時間無法運作。

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.4.(b)。

(b) 適用安全等級

第 2 級、第 3 級。

(c) 測試目的

查證待測標的在 DoS 攻擊結束後，網路設備可自動恢復運作。

(d) 前置條件

測試標的至少 1 個通訊介面支援使用 IP 網路進行資料傳輸。

(e) 測試方法及步驟

(1) 測試人員將安裝掃描工具之測試電腦與測試標的連接至同一個區域網路，測試電腦與測試標的間，不得有入侵防禦系統或防火牆等資安防護工具。

(2) 測試人員將測試標的還原至出廠預設設定，並依測試環境需求設定網路位址。

(3) 測試人員以 DoS 測試工具對測試標的網路位址(IP)執行 UDP Flooding 測試作業 300 秒後停止攻擊。

(f) 判定條件

-符合要求

待測標的在 DoS 攻擊結束後，網路設備 30 分鐘內可自動恢復運作。

-不符合要求

待測標的在 DoS 攻擊結束後，網路設備無法 30 分鐘內自動恢復運作。

-不適用

測試標的不支援使用 IP 網路進行資料傳輸。

5.1.4.3 防火牆規則設定及維護應文件化，並提供定期檢視機制

(a) 測試依據

「本系列規範第 7-1 部」之 6.1.4.(c)。

(b) 適用安全等級

第 2 級、第 3 級。

(c) 測試目的

確保廠商對待測標之防火牆規則設定應有相關管理作業程序。

(d) 前置條件

(1) 待測標的本身支援防火牆功能。

(2) 廠商應提供書面資料，說明防火牆規則與管理程序。

(e) 測試方法及步驟

(1) 測試人員檢視書面資料，內容是否包括如何設定防火牆規則。

(2) 測試人員檢視書面資料，內容是否包括要求使用者定期檢視防火牆規則之書面資料。

(f) 判定條件

-符合要求

廠商有提供該待測標的之防火牆規則設定、管理及更新之書面資料。

-不符合要求

廠商未提供該待測標的之防火牆規則設定、管理及更新之書面資料。

-不適用

待測標的本身無防火牆功能。

5.2 軟體及韌體更新

5.2.1 更新安全

5.2.1.1 網路設備、代理伺服器、組態伺服器及應用伺服器應支援遠端更新功能

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.1.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的與應用程式是否支援透過網路更新軟體或韌體功能。

(d) 前置條件

(1) 廠商應提供測試用的應用程式新版韌體或軟體檔案。

(2) 待測標的與更新伺服器需能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(e) 測試方法及步驟

(1) 測試人員登入待測標的管理介面，依網路環境設定更新伺服器域名或 IP 位址。

(2) 測試人員記錄目前待測標的版本資訊後，於待測標的管理介面執行待測標的之軟體或韌體更新功能。

(3) 更新完畢之後，測試人員重新啟動待測標的，並重新登入待測標的管理介面檢視目前待測標的版本資訊是否為新的版本資訊。

(f) 判定條件

-符合要求

待測標的可透過網路連接至更新伺服器，並更新至更新伺服器上的待測標的之版本。

-不符合要求

待測標的不支援網路更新功能。

-不適用

本測試項目無不適用之測試情況。

5.2.1.2 網路設備、代理伺服器、組態伺服器，以及應用伺服器進行韌體更新時，即使發生更新未成功，系統應仍能回復正常運作

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.1.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的韌體更新過程發生異常時，仍可回復正常運作。

(d) 前置條件

(1) 廠商應提供測試用之新版韌體。

(2) 待測標的與更新伺服器需能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(e) 測試方法及步驟

(1) 測試人員登入待測標的之管理介面，依網路環境設定更新伺服器域名或 IP 位址。

(2) 測試人員記錄目前待測標的之版本資訊後，於待測標的之管理介面執行待測標的更新功能。

(3) 測試人員於更新過程中，拔除待測標的電源至少 10 秒後，重新接上電源。

(4) 測試人員登入待測標的之管理介面，確認所有設定與待測標的之版本是否與更新前一致。

(f) 判定條件

-符合要求

測試標的仍可正常運作，且版本與系統更新前一致。

-不符合要求

測試標的無法正常運作，或系統已更新至新版本。

-不適用

測試標的不支援系統更新功能。

5.2.1.3 網路設備、代理伺服器、組態伺服器及應用伺服器之更新路徑應通過安全通道，以確保韌體之機密性、完整性、可用性及正確性，且安全通道版本應符合 TLS V1.2[1]或 DTLS V1.2 以上規範

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.1.(c)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的之應用程式使用安全通道進行更新作業。

(d) 前置條件

(1) 廠商應提供遠端更新主機所使用的網路位址。

(2) 廠商應提供應用程式的更新檔案，該版本可觸發測試標的進行更新作業。

(e) 測試方法及步驟

(1) 測試人員將測試電腦與測試標的連接至同一區域網路，並側錄測試標的與伺服器連接封包。

(2) 測試人員將測試標的還原至出廠預設設定，並依測試環境需求設定網路位址，確保測試標的可正常連接至更新主機。

(3) 測試人員檢視所側錄之封包，確認更新路徑與更新檔案傳輸所採用安全通道協定版本。

(f) 判定條件

-符合要求

更新路徑與韌體檔案所使用的安全通道皆符合 TLS v1.2[1](含)以上或 DTLS v1.2(含)以上的版本。

-不符合要求

待測標的不支援遠端更新，或更新路徑與更新檔案所使用的安全通道支援非 TLS v1.2[1](含)以上或 DTLS v1.2(含)以上的版本。

-不適用

本測試項目無不適用之情況。

5.2.1.4 網路設備、代理伺服器、組態伺服器及應用伺服器於更新韌體前，應使用數位簽章查證韌體之完整性及來源

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.1.(d)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的於更新韌體前，應查證更新檔案的完整性及來源。

(d) 前置條件

(1) 廠商應提供書面資料，說明更新檔案簽章方式，供測試人員以非正確私鑰執行簽章作業；或協助測試人員產生以非正確私鑰所簽章之更新檔案。

(2) 廠商所提供之韌體更新檔案，該版本可觸發測試標的進行更新作業。

(e) 測試方法及步驟

(1) 測試人員自行產生加密金鑰。

(2) 測試人員依書面資料，並以上述步驟產生之私鑰對更新檔案執行簽章作業。

(3) 測試人員將簽章後的更新檔案上傳至測試標的，並執行更新作業。

(f) 判定條件

-符合要求

測試人員無法以不正確私鑰所簽章之更新檔案完成更新作業。

-不符合要求

測試人員可以不正確私鑰所簽章之更新檔案完成更新作業。

-不適用

本測試項目無不適用之情況。

5.2.1.5 網路設備、代理伺服器、組態伺服器及應用伺服器應具備定期檢查是否有可用之安全更新，並顯示待測標的版本更新狀態之機制

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.1.(e)。

(b) 適用安全等級

第 2 級、第 3 級。

(c) 測試目的

查證待測標的否支援自動檢查系統更新之功能。

(d) 前置條件

(1) 廠商應提供測試用新版韌體或軟體更新檔。

(2) 待測標的與更新伺服器需能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(e) 測試方法及步驟

(1) 測試人員登入待測標的管理介面，依網路環境設定更新伺服器域名或 IP 位址。

(2) 測試人員記錄目前待測標的版本資訊後，於待測標的之管理介面確認待測標的是否有顯示新的更新版本資訊。

(f) 判定條件

-符合要求

待測標的會顯示更新伺服器上有新的更新版本資訊。

-不符合要求

待測標的不支援透過網路更新，或是不會顯示更新伺服器上有新的更新版本資訊。

-不適用

本測試項目無不適用之情況。

5.2.2 版本安全

5.2.2.1 網路設備、代理伺服器、組態伺服器及應用伺服器之硬體及韌體版本應唯一

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.2.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的之硬體與韌體版本皆為唯一。

(d) 前置條件

廠商應提供書面資料，說明待測標的相對應版本查找程序及確保硬體及韌體版本應唯一之機制。

(e) 測試方法及步驟

(1) 測試人員根據待測標的書面資料，透過手動逐一確認或是設備管理平台確認待測標的硬體與韌體資訊。

(2) 測試人員檢視同一型號待測標的是否有多種硬體與韌體資訊。

(f) 判定條件

-符合要求

測試人員確實可執行版本查找程序且硬體與韌體版本唯一，並認同該機制可執行。

-不符合要求

測試人員無法執行查找程序或硬體與韌體不唯一，或不認同該機制可執行。

-不適用

本測試項目無不適用之條件。

5.2.2.2 相關服務提供者應能提供各韌體版本的加密雜湊值作為韌體版本之追溯管控

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.2.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證廠商是否有記錄所有待測標的之版本資訊。

(d) 前置條件

廠商應提供待測標的版本資訊與韌體檔案。

(e) 測試方法及步驟

(1) 測試人員將產生所有韌體檔案的加密雜湊值。

(2) 測試人員與待測標的版本的加密雜湊值進行比對，檢視所有待測標的版本資訊的加密雜湊值是否一致。

(f) 判定條件

-符合要求

待測標的加密雜湊值與版本所記錄的加密雜湊值一致。

-不符合要求

廠商無待測標的版本，或加密雜湊值與版本記錄的不一致。

-不適用

本測試項目無不適用之要求。

5.2.2.3 網路設備、代理伺服器、組態伺服器及應用伺服器內各硬體模組應可獨立替換

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.2.(c)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的之各硬體模組是否可獨立替換。

(d) 前置條件

(1) 該待測標的需支援可更新部分硬體模組功能。

(2) 廠商應提供硬體模組替換元件。

(3) 廠商應提供書面資料，說明如何替換硬體模組。

(e) 測試方法及步驟

(1) 測試人員參書面資料，確認待測標的是否支援更新待測標的內特定硬體模組功能。

(2) 若待測標的支援替換硬體模組，測試人員依書面資料替換硬體模組，並檢視替換後之待測標的功能與設定是否與原設定一致。

(f) 判定條件

-符合要求

待測標的在替換硬體模組後，與原設定一致。

-不符合要求

待測標的在替換硬體模組後，需重新進行待測標的設定。

-不適用

待測標的不支援硬體模組替換功能。

5.2.2.4 網路設備、代理伺服器、組態伺服器及應用伺服器之韌體簽章金鑰應妥善保管不可外洩或被輕易取得

(a) 測試依據

「本系列規範第 7-1 部」之 6.2.2.(d)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的用於查證韌體檔案的加密金鑰是否安全存放。

(d) 前置條件

廠商應提供書面資料，說明加密金鑰保護方式。

(e) 測試方法及步驟

(1) 測試人員檢視廠商所提供的系統設計文件，確認待測標的所使用的加密金鑰具保護機制。

(2) 依廠商所使用的加密金鑰保護機制，檢視硬體平台或作業系統原廠文件。

(f) 判定條件

-符合要求

待測標的支援使用硬體或作業系統所提供之功能保護加密金鑰。

-不符合要求

待測標的對加密金鑰無相關保護機制。

-不適用

待測標的不支援韌體更新功能。

5.3 通訊安全

5.3.1 資料傳輸安全

5.3.1.1 機敏資料傳輸時，已確保資料之機密性、完整性、可用性及正確性，且伺服器傳輸協定應符合 TLS V1.2[1]或 DTLS V1.2 以上規範

(a) 測試依據

「本系列規範第 7-1 部」之 6.3.1.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的所提供之網路服務在傳輸機敏資料時是否使用安全通道確保資料之機密性、正確性、完整性及可用性。

備考：機敏資料包括但不限於身分鑑別資訊(如使用者帳戶、通行碼)及含有使用者隱私之資料，，廠商可以擴增額外機敏資料之範圍。

(d) 前置條件

(1) 測試標的需支援使用 TCP 或 UDP 網路協定傳輸機敏資料。

(2) 廠商應提供書面資資料，說明接收機敏資料的通訊介面。

(e) 測試方法及步驟

(1) 測試人員依待測標的書面資料建置測試環境，確認測試人員可直接連待測標的連接。

(2) 測試人員以安全通道掃描工具對待測標的網路位址(IP)執行測試作業，檢視待測標的所提供的網路服務所支援的安全通道協定版本。

(f) 判定條件

-符合要求

測試標的與伺服器所使用的安全通道皆符合 TLS v1.2[1](含)以上或 DTLS v1.2(含)以上的版本。

-不符合要求

測試標的或伺服器所使用的安全通道支援使用非 TLS v1.2[1](含)以上或 DTLS v1.2(含)以上的版本。

-不適用

測試標的不支援使用 IP 網路進行資料傳輸。

5.3.1.2 使用無線連接時，應提供授權、監控及限制機制

(a) 測試依據

「本系列規範第 7-1 部」之 6.3.1.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否具備無線連接[包括但不限於 Bluetooth、藍牙低功耗(Bluetooth Low Energy, BLE)、Wi-Fi、 ZigBee]管理能力。

(d) 前置條件

(1) 待測標的應支援使無線連接。

(2) 廠商應提書面資料，說明授權、監控及限制機制。

(e) 測試方法及步驟

(1) 測試人員依待測標的書面資料，設置無線連接測試環境。

(2) 測試人員使用筆記型電腦或其他設置無線連接至待測標的的連接存取點，並登入待測標的管理介面，確認是否可進行無線連接用戶端管理，至少需限制可存取的無線連接使用者。

(f) 判定條件

-符合要求

系統管理者可管理無線連接的用戶端。

-不符合要求

待測標的不支援無線連接用戶端管理功能。

-不適用

待測標的本身不支援無線連接功能。

5.3.2 資料儲存安全

5.3.2.1 代理伺服器、組態伺服器及應用伺服器儲存之機敏資料應加密儲存

(a) 測試依據

「本系列規範第 7-1 部」之 6.3.2.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的將機敏資料儲存於檔案系統時是否加密保護。

備考：機敏資料包括但不限於身分鑑別資訊(如使用者帳戶、通行碼)及含有使用者隱私之資料，，廠商可以擴增額外機敏資料之範圍。

(d) 前置條件

(1) 廠商應提供所有機敏資料儲存路徑與所使用之資料保護方式書面資料，作為審查依據。

(2) 廠商應提供具備系統管理者權限的測試標的作業系統操作介面。

(e) 測試方法及步驟

(1) 測試人員檢視廠商所提供的書面資料，以確認機敏資料儲存路徑與其保護機制。

(2) 測試人員以廠商所提供的作業系統操作介面，存取測試標的。

(3) 測試人員檢視所有機敏資料的儲存路徑，確認機敏資料內容。

(4) 測試人員搜尋檔案系統是否有其他檔案存在機敏資料以明文儲存。

(f) 判定條件

-符合要求

測試標的未儲存機資料；或通行碼資料與加解密用金鑰的保護機制採用 NIST SP800-57[3]及

ISO/IEC 19790[2]所規定之雜湊函數及加密演算法，且未發現其他通行碼及加解密用金鑰以明文方式儲存於檔案系統。

-不符合要求

通行碼資料或加解密用金鑰的保護機制未採用 NIST SP800-57[3]及 ISO/IEC 19790[2]所規定之雜湊函數及加密演算法，或發現其他通行碼及加解密用金鑰以明文方式儲存於檔案系統。

-不適用

本測試項目無不適用之情境。

5.3.2.2 代理伺服器、組態伺服器及應用伺服器儲存之機敏資料，其加密方式應採用符合 NIST SP800-57[3]及 ISO/IEC 19790[2]同等或以上等級之加密演算法

(a) 測試依據

「本系列規範第 7-1 部」之 6.3.2.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的將機敏資料以安全的加密演算法儲存於檔案系統。

(d) 前置條件

(1) 廠商應提供書面資料，說明所有機敏資料儲存路徑與所使用之資料保護方式，作為審查依據。

(2) 廠商應提供具備系統管理者權限之測試標的作業系統操作介面。

(e) 測試方法及步驟

(1) 測試人員檢視廠商所提供之書面資料，以確認機敏資料儲存路徑與其保護機制。

(2) 測試人員以廠商所提供的作業系統操作介面，存取待測標的。

(3) 測試人員檢視所有機敏資料的儲存路徑，確認機敏資料內容。

(4) 測試人員搜尋檔案系統是否有其他檔案存在機敏資料以明文儲存。

(f) 判定條件

-符合要求

測試標的未儲存機敏資料；或通行碼資料與加解密用金鑰的保護機制採用 NIST SP800-57[3]及 ISO/IEC 19790[2]所規定之雜湊函數與加密演算法，且未發現其他通行碼與加解密用金鑰以明文方式儲存於檔案系統。

-不符合要求

通行碼資料或加解密用金鑰的保護機制未採用 NIST SP800-57[3]及 ISO/IEC 19790[2]所規定之雜湊函數與加密演算法，或發現其他通行碼與加解密用金鑰以明文方式儲存於檔案系統。

-不適用

本測試項目無不適用之情境。

5.4 鑑別與授權機制

5.4.1 帳戶管理

5.4.1.1 網路設備、代理伺服器、組態伺服器及應用伺服器不應包含預設、臨時及匿名帳戶

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.1.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的所包括之帳戶皆為必要使用。

(d) 前置條件

(1) 廠商應提供書面資料，說明帳戶清單及其必要用途。

(2) 廠商應提供作業系統控制介面及操作程序。

(e) 測試方法及步驟

(1) 測試人員檢視廠商所提供之書面資料，確認是否皆為必要之帳戶。

(2) 測試人員以系統管理者登入待測標的控制檢視，檢視其帳戶與書面資料是否一致，非必要之帳戶預設需為停用狀態或刪除。

(3) 若帳戶資訊與作業系統連動時，則測試人員需透過作業系統控制介面，檢視作業系統帳戶清單是否與書面資料一致。

(f) 判定條件

-符合要求

待測標的啟用之帳戶與書面資料一致，且皆為必要之用途。

-不符合要求

待測標的啟用之帳戶與書面資料不一致，或存在非必要用途之帳戶。

-不適用

本測試項目無不適用之情境。

5.4.1.2 僅允許經授權之特定帳戶可遠端存取代理伺服器、組態伺服器及應用伺服器

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.1.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

確保未經授權之使用者無法透過遠端存取待測標的。

(d) 前置條件

(1) 廠商應提供書面資料，說明授權帳戶清單及存取權限。

(2) 確認待測標的應正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(e) 測試方法及步驟

(1) 測試人員登入待測標的之管理介面，檢視帳戶清單，並分別記錄可透過遠端存取及不可透過遠端存取之帳戶清單。

(2) 測試人員以允許遠端存取之帳戶嘗試登入待測標的，檢視是否可以成功登入。

(3) 測試人員以不允許遠端存取之帳戶嘗試登入待測標的，檢視是否可以成功登入。

(f) 判定條件

-符合要求

測試人員可使用特定帳戶以遠端方式存取待測標的，且未經授權的帳戶無法存取。

-不符合要求

未經授權的帳戶仍可以遠端方式存取待測標的。

-不適用

待測標的本身不支援使用者以遠端方式存取。

5.4.2 存取控制

5.4.2.1 代理伺服器、組態伺服器及應用伺服器應能限制某些主機網路服務之存取權限

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.2.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否具備存取控管機制，以限制僅經授權之網路服務可被存取。

(d) 前置條件

(1) 待測標的應能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(2) 廠商應提供書面資料，說明授權網路服務清單及存取權限設定。

(e) 測試方法及步驟

(1) 測試人員檢視廠商提供之書面資料，確認代理伺服器、組態伺服器及應用伺服器所管理介面所使用的通訊方式，並嘗試存取代理伺服器、組態伺服器及應用伺服器的管理介面。

(2) 針對代理代理伺服器、組態伺服器及應用伺服器，測試人員登入管理介面並依書面資料設定系統服務管控功能，設定網路服務可存取的來源 IP 位址。

(3) 測試人員以被阻擋的來源 IP 位址存取網路服務，檢視是否可以正常存取。

(f) 判定條件

-符合要求

待測標的具備網路存取控管功能，確實執行限制某些主機網路服務之存取。

-不符合要求

待測標的不具備網路存取控管功能。

-不適用

本測試項目無不適用之情境。

5.4.2.2 網路設備、代理伺服器、組態伺服器及應用伺服器應提供人員使用者至少 2 層級(例:管理者及一般使用者)以上之存取權限

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.2.(b)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否支援多使用者角色或權限之功能。

(d) 前置條件

廠商應提供書面資料，說明使用者管理功能之操作程序。

(e) 測試方法及步驟

(1) 測試人員登入待測標的管理介面，並依待測標的之書面資料檢視使用者管理功能，確認目前帳戶角色清單，記錄各帳戶角色可執行之功能。

(2) 測試人員切換不同帳戶角色登入待測標的，確認各帳戶角色可執行功能是否與設定一致。

(f) 判定條件

-符合要求

待測標的支援至少 2 種帳戶角色，並各帳戶角色可執行功能與設定一致。

-不符合要求

待測標的僅支援單一帳戶角色。

-不適用

本測試項目無不適用之情境。

5.4.2.3 代理伺服器、組態伺服器及應用伺服器應允許定義新的角色

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.2.(c)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否支援定義新帳戶角色之功能。

(d) 前置條件

廠商應提供書面資料，說明使用者管理功能之操作程序。

(e) 測試方法及步驟

(1) 測試人員登入待測標的之管理介面，並依待測標的之書面資料檢視使用者管理功能。

(2) 測試人員記錄現行帳戶角色，新增其他帳戶角色並指定可執行系統功能。

(3) 測試人員以新增的帳戶角色登入系統，確認是否可執行該系統功能。

(f) 判定條件

-符合要求

待測標的支援新增帳戶角色之功能，並僅可執行該角色所設定之系統功能。

-不符合要求

待測標的不支援新增帳戶角色之功能或無法執行設定之系統功能。

-不適用

本測試項目無不適用之情境。

5.4.3 身分鑑別

5.4.3.1 使用者或伺服器經網路存取代理伺服器、組態伺服器及應用伺服器，應通過身分鑑別

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.3.(a)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的具備支援網路存取時進行身分鑑別，其身分鑑別因子可包括但不限於帳戶通行碼、特定連接字串及加密金鑰。

(d) 前置條件

(1) 待測標的應能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(2) 廠商應提供書面資料，說明網路服務清單及系統組態設定程序。

(3) 確認各網路服務所使用的身分鑑別機制及鑑別因子。

(e) 測試方法及步驟

(1) 測試人員執行連接埠掃描，確認開啟網路服務清單及系統組設定。

(2) 測試人員檢視廠商所提供之書面資料，針對每個網路服務，確認該網路服務是否可變更系統組態設定或取得系統資料。

(3) 測試人員需針對變更系統組態設定，確認該網路服務是否支援身分鑑別功能。

(4) 測試人員使用不正確的身分鑑別因子嘗試登入該網路服務，確認未經授權之使用者無法透過該網路服務，變更系統組態設定或取得系統資料。

(f) 判定條件

-符合要求

可用於變更系統組態設定或取得系統資料之網路服務，皆需支援透過網路進行身分鑑別功能。

-不符合要求

任一可用於變更系統組態設定或存取網路服務，不支援透過網路進行身分鑑別功能。

-不適用

本測試項目無不適用之情境。

5.4.3.2 對於身分鑑別所使用之通行碼強度應有規定，以避免被輕易破解遭不當利用

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.3.(b)。

(b) 適用安全等級

第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否強制要求使用者必應使用強通行碼。

(d) 前置條件

廠商應提供書面資料，說明通行碼強度設定之規則。

(e) 測試方法及步驟

(1) 測試人員檢視書面資料確認待測標的所要求通行碼設定規則，其通行碼規則要求內容至少應包括最短長度與複雜度。

(2) 測試人員以任一帳戶登入系統進行通行碼變更，使用不符合通行碼規則之通行碼進行設定及變更，查證待測標的是否允許設置該通行碼。

(3) 測試人員以任一帳戶登入系統進行通行碼變更，使用符合通行碼規則的通行碼進行設定及變更，查證待測標的是否允許設定該通行碼。

(f) 判定條件

-符合要求

待測標的具備檢查通行碼設定規則功能，且無法設定不符合通行碼規則之通行碼。

-不符合要求

待測標的不支援檢查通行碼強度之功能。

-不適用

待測標的不支援使用帳戶通行碼身分鑑別機制。

5.4.3.3 進行遠端操控代理伺服器、組態伺服器及應用伺服器，應具防止重送攻擊之機制

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.3.(c)。

(b) 適用安全等級

第 2 級、第 3 級。

(c) 測試目的

查證待測標的具備可阻擋重送攻擊之能力。

(d) 前置條件

(1) 待測標的應能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(2) 廠商應提供書面資料，說明防止重送攻擊之機制。

(e) 測試方法及步驟

(1) 測試人員透過網路執行待測標的系統功能，並透過封包側錄工具記錄使用者端工具所發送至伺服器的應用層之網路封包。

(2) 測試人員透過封包重送工具，重送上述步驟所記錄的應用層封包內容，並檢查待測標的是否執行該網路封包對應之防護機制。

(f) 判定條件

-符合要求

待測標的不會執行及回應，測試人員重新發送之網路封包。

-不符合要求

待測標的會執行及回應，測試人員重新發送之網路封包。

-不適用

本測試項目無不適用之情境。

5.4.3.4 若使用者身分鑑別未成功，則應中斷連接

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.3.(d)。

(b) 適用安全等級

第 1 級、第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否具備中斷身分鑑別未成功之連接的能力。

(d) 前置條件

(1) 待測標的應能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(2) 廠商應提供書面資料，說明需身分鑑別之網路服務清單。

(e) 測試方法及步驟

(1) 測試人員透過網路以正確使用者帳戶與通行碼登入待測標的，確認可正常登入待測標的。

(2) 測試人員透過網路以正確使用者帳戶與錯誤通行碼登入待測標的，檢視待測標的是否會中斷網路連接，使用者需重新連接方可重新嘗試登入。

(f) 判定條件

-符合要求

待測標的在使用者身分鑑別未成功後會中斷網路連接。

-不符合要求

待測標的允許使用者身分鑑別未成功後持續進行網路連接。

-不適用

本測試項目無不適用之情境。

5.4.3.5 使用者在多次登入代理伺服器、組態伺服器及應用伺服器未成功後，代理伺服器、組態伺服器及應用伺服器應拒絕該使用者的請求，登入次數及時間應可設定

(a) 測試依據

「本系列規範第 7-1 部」之 6.4.3.(e)。

(b) 適用安全等級

第 2 級、第 3 級。

(c) 測試目的

查證待測標的是否具備帳戶鎖定功能。

(d) 前置條件

(1) 廠商應提出需身分鑑別之網路服務清單。

(2) 待測標的應能正常進行網路連接，並確認中間無防火牆阻擋其網路連接。

(e) 測試方法及步驟

(1) 測試人員以系統管理者登入待測標的，檢視帳戶鎖定功能，是否可設定登入未成功次數及鎖定時間。

(2) 測試人員透過網路以正確使用者帳戶與通行碼登入待測標的，確認可正常登入待測標的。

(3) 測試人員透過網路以正確使用者帳戶與錯誤通行碼登入待測標的，當登入未成功錯誤達所設定的未成功次數時，檢視待測標的是否會鎖定，拒絕讓使用者登入。

(4) 在帳戶鎖定期間，測試人員再次透過網路以正確使用者帳戶與通行碼登入待測標的，查證是否可登入待測標的。

(f) 判定條件

-符合要求

帳戶鎖定功能可依系統管理者所設定登入未成功次數與鎖定時間觸發，並在帳戶鎖定期間無法以正確帳戶及通行碼登入系統。

-不符合要求

帳戶鎖定功能無法設定次數與時間，或在帳戶鎖定期間使用者仍可正確帳戶登入系統。

-不適用

本測試項目無不適用之情境。

参考資料

[1] IETF/RFC 5246, The Transport Layer Security (TLS) Protocol V1.2

[2] ISO/IEC 19790,Information technology-Security techniques-Security requirementsfor cryptographic module

[3] NIST SP800-57, Recommendation for Key Management: Part 1 – General

[4] NIST SP800-92, Guide to Computer Security Log Management

5G 智慧杆系統技術規範

－第 8 部：電源供應系統要求

5G Smart pole system technical specification

- Part 8: Power supply systems requirements

中 華 民 國 111 年 9 月

目錄

節次 頁次
前言 2
0. 簡介 3
1. 適用範圍 3
2. 引用標準 3
3. 用語及定義 3
4. 智慧杆電源供應系統 4
4.1 電源供應器 4
4.2 不斷電系統 4
4.3 電量計量 4
附錄 A（參考） 5

前言

本規範係依 CNS 3689 「國家標準草案構成及格式之指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole) 現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT) 設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60 Hz 及 500 V 以下交流電源之多用途智慧杆系統用電源供應系統，包含電源供應器、不斷電系統及電量計量。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 14843-1	不斷電系統(UPS)－第 1 部：使用於操作者觸及區之不斷電系統安全通則
CNS 14843-2	不斷電系統(UPS)－第 1 部：使用於限制觸及區之不斷電系統安全通則
CNS 16069	高速公路及快速道路 LED 路燈
CNS 61347-1	光源控制裝置－第 1 部：通則及安全要求
CNS 61347-2-13	光源控制裝置－第 2 之 13 部：LED 模組用直流或交流電子式控制裝置之個別要求

全臺設置 LED 路燈技術規範(中華民國 104 年 2 月 17 日)

5G 智慧杆系統技術規範－第 5 部：電氣安全要求

3. 用語及定義

本規範適用「5G 智慧杆系統技術規範－第 1 部：一般要求」之用語及定義，及下列用語及定義適用於本規範。

3.1 智慧杆迴路控制箱(smart pole cluster terminal box, 簡稱迴路控制箱)

固定式封閉箱體，具有框架及門板，且裝有電力設備、資訊設備及通訊設備。由迴路控制箱延伸出電力電纜及通訊纜線，連結智慧杆迴路內所有智慧杆，提供智慧杆電力供應及網路連線服務。

4. 智慧杆電源供應系統

4.1 電源供應器

4.1.1 智慧杆迴路控制箱電源供應器

智慧杆迴路控制箱之輸入供應電源為 60 Hz、110 Va.c. 或 220 Va.c.，輸出電源應為 48 Vd.c.。

4.1.2 智慧杆附掛設備電源供應器

智慧杆之附掛設備，除智慧照明(LED 路燈)外，其餘附掛設備輸入供應電源應為 48 Vd.c.。

具備網際網路協定(Internet Protocol, IP)的附掛設備，採用乙太網路供電(Power over Ethernet, PoE)。

4.1.3 智慧照明(LED 路燈)電源供應器

應符合「5G 智慧杆系統技術規範－第 5 部電氣安全要求」及能源局公告「全臺設置 LED 路燈技術規範」之相關要求。

LED 路燈內電源供應器，應符合 CNS 61347-1 第 6 節規定之安裝方式及 CNS 61347-2-13 第 6 節規定之防電擊保護項目。

4.2 不斷電系統

智慧杆迴路控制箱電源供應系統應配有不斷電系統(Uninterruptible Power System, UPS)，以備停電時緊急供電，維持智慧杆設備基本運作及防止附掛設備不會因突然斷電而造成損壞。

不斷電系統需符合 CNS 14843-1 及 CNS 14843-2。

停電時，不斷電系統應至少可供微型基地臺維持 2 小時以上正常運作，其餘附掛設備則依實際使用需求建置適合輸出功率及電池容量。

4.3. 電量計量

附掛設備電量計量使用多迴路交流電表對各項設備獨立計費，多項直流設備共用同一電源供應單元時，應個別安裝直流電表獨立計算其耗電比例，並依前端交流電表計量依比例計費。

電源供應單元依使用單位配置，單一電源供應單元可配置多個直流設備，但需考量負載量。

附錄 A

(參考)

A.1 各附掛設備功率

使用多迴路交流電表對各項設備或依使用單位獨立計費，電源供應單元依使用單位配置，單一電源供應單元可配置多個直流設備，但需要考量負載量。

部分附掛設備使用電源及功率參照表 A.1，實際數值依現場附掛設備輸入為主，並依實際掛載需求進行調整。

表 A.1 附掛設備

附掛設備	輸入電壓	消耗功率
5G 微型基地臺	110 Va.c. 或 220 Va.c.	600 W (max)
智慧照明(LED 路燈)	110 Va.c. 或 220 Va.c.	140 W (max)
Wi-Fi 裝置	110 Va.c. 或 220 Va.c.	30 W (max)
空氣品質感測器	110 Va.c. 或 220 Va.c.	15 W (max)
氣象感測器(風、光、溫、濕、雨)	110 Va.c. 或 220 Va.c.	15 W (max)
交通號誌	110 Va.c. 或 220 Va.c.	20 W (max)*號誌燈數量
語音緊急求助裝置(緊急呼救)	Vd.c. 或 PoE	25 W (max)
互動數位看板-螢幕互動	110 Va.c. 或 220 Va.c.	100 W (max)
車聯網 RSU	Vd.c. 或 PoE	30 W (max)
自駕車路側裝置(光達)	Vd.c. 或 PoE	12 W
自駕車路側裝置(雷達)	Vd.c. 或 PoE	23 W

備考 1.此表資訊僅供參考，實際數值依實際附掛設備為主。

備考 2.「CNS 16069 高速公路及快速道路 LED 路燈」標準中規定，LED 路燈之電源供應器輸出功率 150 W 以下之額定輸出電流為 700 mA± 5%；輸出功率超過 150 W 之額定輸出電流為 1,400 mA± 5%。

備考 3.邊緣運算伺服器及核心網伺服器不列在杆體內。

備考 4.附掛設備輸入供應電源應為 48 Vd.c.。

5G 智慧杆系統技術規範
－第 9 部：性能要求

5G Smart pole system technical specification
- Part 9 : Performance requirements

中 華 民 國 111 年 9 月

目　錄

節次　　頁次

前言 2
0. 簡介 3
1. 適用範圍 3
2. 引用標準 3
3. 用語及定義 3
4. 系統組成 4
5. 附掛設備 4
5.1 智慧照明 4
5.1.1 性能要求 4
5.1.2 試驗法 4
5.2 空氣品質偵測器 5
5.2.1 性能要求 5
5.2.2 試驗法 5
5.3 交通號誌 5
5.3.1 性能要求 5
5.3.2 試驗法 5
5.4 交通標誌 5
5.4.1 性能要求 5
5.4.2 試驗法 5
5.5 交通看板 5
5.5.1 性能要求 5
5.5.2 交通資訊通訊格式 5
5.5.3 試驗法 5
5.6 影像監控系統 5
5.6.1 性能要求 5
5.6.2 試驗法 6
5.7 車聯網 C-V2X（路側設備） 6
5.7.1 性能要求 6
5.7.2 試驗法 6
參考資料 7

前言

本規範係依 CNS 3689 「國家標準草案構成及格式之指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole) 現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT) 設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統，包含智慧照明、空氣品質監測器、交通號誌、交通標誌、交通看板、影像監控系統、車聯網 (C-V2X)。

2. 引用標準

下列標準及規範因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版 (包括補充增修)。無加註年分者，適用該最新版 (包括補充增修)。

CNS 16069　高速公路及快速道路 LED 路燈

CNS 15652-1　智慧照明系統 － 第 1 部：系統功能

CNS 14546　發光二極體交通號誌燈燈面及燈箱

CNS 14555　道路用發光二極體文字顯示型交通資訊看板

CNS 13092　發光二極體顯示幕 (戶外用)量測法

CNS 16120-1　影像監控系統安全－第 1 部：一般要求事項

CNS 16132-1　影像監控系統安全測試方法 －第 1 部：一般要求事項

CNS 16132-2　影像監控系統安全測試方法 －第 2 部：網路攝影機

3. 用語及定義

本規範適用〝5G 智慧杆系統技術規範－第 1 部：一般要求〞之用語定義，及下列用語及定義適用於本規範。

3.1 蜂巢式車聯網 (cellular vehicle-to-everthing, C-V2X)

由 3GPP 主導制定之新興智慧運輸系統車聯網技術。

3.2 車聯網 (internet of vehicle, IOV)

車與車、車與路、車與人、車與感知設備間能相互溝通，以連接性 (connectivity)為基礎，結合先進感知及互動技術，透過多元通訊技術，整合人車路資訊，提供涵蓋聯網汽車 (connected car)、聯網駕駛 (connected driver)，以及連接用戶體驗 (connected user experience)之技術及解決方案，進而達成車輛與其他網路通訊環境連結的動態移動通訊系統。

3.3 發光二極體 (light emmtting diode, LED)

為一種半導體元件，通以正向驅動電流時，其半導體內之載子相結合而行直接放光。

3.4 光強度 (luminous intensity)

於指定方向之單位立體角內所放射之光通量。

3.5 輝度 (luminance)

從某一指定方向所觀察到單位投影面積上之發光強度。

3.6 路側設備 (roadside unit, RSU)

安裝於道路周邊之無線通訊模組，可接收遠端訊息並發送至車輛端接收設備，以傳遞各式交通訊息。

3.7 車對任何物體 (vehicle-to-everything, V2X)

V2X 通訊技術為車聯網發展必要之核心技術，其中車載專用短距通訊技術 (Wireless Access in Vehicular Environments/Dedicated Short Range Communications, WAVE/DSRC) 為車輛到車輛 (vehicle-to-vehicle, V2V)與車輛到基礎設施 (vehicle-to-infrastructure, V2I)間之通用射頻 (radio frequency, RF)通訊技術，針對車用環境支援公共安全 (public safety)及私人營運 (private operation)之中短距離通訊服務。

4. 系統組成

本規範中所列附掛設備包含：智慧照明、空氣品質監測器、交通號誌、交通標誌、交通看板、影像監控系統及車聯網 C-V2X。

5. 附掛設備

5.1 智慧照明

5.1.1 性能要求

(a) 燈具照明

- 當智慧杆設置於市區道路時，依所設立位置之屬性 (市區道路、服務道路、人行道)，其性能要求應符合內政部營建署〝市區道路及附屬工程設計規範〞第 19 章〝道路照明〞之 19.1~19.45 規定。
- 當智慧杆設置於高速公路或快速道路時，其燈光分布型式、光強度、光通量及其他性能要求應符合 CNS 16069〝高速公路及快速道路 LED 路燈〞規定。

(b) 智慧照明功能：智慧照明系統所包含之功能、控制等功能要求，應符合 CNS 15652〝智慧照明系統〞規定。

5.1.2 試驗法

應用於智慧照明裝置之燈具測試，應符合 CNS 16069 之 7.2、7.3、7.10、7.11、7.12、7.13 要求。

5.2 空氣品質偵測器

5.2.1 性能要求

當智慧杆具偵測周遭一定範圍內之空氣品質檢測功能時，其上所搭載之偵測模組所提供的空氣品質由包含氣體或微粒子組成、數量或濃度等資料，藉以作為該區空氣品質指標判定或進行長期資料監控分析之用，相關資訊可透過通訊介面進行資訊傳輸及交換。

針對偵測器所提供資料之項目，例：小時平均值、8 小時平均值、日平均值等資料定義及意義，應依行政院環境保護署之〝空氣品質標準〞所規範內容為主。

5.2.2 試驗法

空氣品質偵測器應經由環保署所建置之空氣品質感測器性能測試驗證平台進行性能測試與檢驗，檢驗結果符合要求時，此項可判定符合。

5.3 交通號誌

5.3.1 性能要求

當智慧杆包含有交通號誌杆之功能需求時，其上所搭載交通號誌種類為 CNS 14546 中所規定之項目，包含行車管制號誌燈、車道用交通號誌箭頭及行人專用號誌。各項燈號之光強度或輝度、色度、尺寸及重量等均應依 CNS 14546 之規定。

5.3.2 試驗法

智慧杆所掛載之交通號誌，應依 CNS 14546〝發光二極體交通號誌燈燈面及燈箱〞所定義的測試規定進行各項檢驗。

5.4 交通標誌

5.4.1 性能要求

當智慧杆具提供車輛駕駛人及行人有關道路路況之警告、禁制、指示等資訊功能時，其所搭載標誌物件之形式，應符合交通部〝道路交通標誌標線號誌設置規則〞之相關規範。

5.4.2 試驗法

交通標誌之種類及相關尺寸、顏色、字體、形狀、懸吊位置等，應符合交通部〝道路交通標誌標線號誌設置規則〞第 2 章的相關規範。

5.5 交通看板

5.5.1 性能要求

當智慧杆具發光二極體之顯示幕資訊看板功能時，其所搭載的產品功能，應符合 CNS 14555〝道路用發光二極體文字顯示型交通資訊看板〞規定。

5.5.2 交通資訊通訊格式

當看板顯示資訊係顯示由交通資訊中心及交通控制中心所發布之即時交通資訊時，其通訊格式應包含交通部〝即時路況資料標準〞格式標準。

5.5.3 試驗法

交通看板所採用之發光二極體顯示幕規格，應依 CNS 13092〝發光二極體顯示幕(戶外用)量測法〞進行對應的檢測。

5.6 影像監控系統

5.6.1 性能要求

當智慧杆具透過影像方式進行用路人流監控、交通流量監控或車牌辨識等功能時，其所搭載攝

影機應具備網路傳輸功能以將擷取影像傳遞至後端處理平台或提供即時監控之功能，攝影機之通訊功能應符合 CNS 16120-1 之規定。

5.6.2 試驗法

網路攝影機試驗依 CNS 16132-1 及 CNS 16132-2 之第 5 節與第 6 節的規定。

5.7 車聯網 C-V2X (路側設備)

5.7.1 性能要求

當智慧杆具車與車 (V2X)或車與周遭所有與車相關之交通基礎設施溝通的通訊功能時，基本包含下列功能：

(a) 路側對遠端通訊功能：能進行遠端與路側設備 (RSU)之訊息交換，遠端可透過網路擷取路側設施的資訊，路側設施可接收到遠端所送過來之訊息。

(b) 車對路側設備通訊功能：能與通訊範圍內之車輛做路側設施與車輛訊息的交換。

RSU 具備無線通訊界面，此通訊界面負責與車輛上的 OBU 通訊，透過此無線通信介面讓 OBU 與 RSU 的資訊做交換，RSU 的有線介面可以與既有的實體通訊網路界接，使得 RSU 具備接收與發送路側的訊息到遠端，遠端資訊也是透過此通訊界面將遠端訊息送至 RSU 來達到車輛與後端的應用結合的目的。

RSU 發送資訊種類及通訊格式，應符合 SAE J2735 所規範之訊息格式標準 (例：C-V2X)，訊息內容至少包含:

(a) 地圖訊息架構 (LayerType, Intersection/RoadSegment, restrictionList)

(b) Probe Vehicle Data (PVT) 訊息架構 (StartVector, vehicleType, snapshots)

(c) Intersection Collision Avoidance (ICA)訊息架構 (intersectionID, laneNumber, partOne, EventFlag)

(d) Personal Safety Message (PSM)訊息架構 (basicType)

(e) Basic Safety Message

5.7.2 試驗法

5.7.2.1 一般

測試申請單位應提供送測 RSU 產品，預設測試用發送訊息封包內容定義表，作為檢測結果比對。

5.7.2.2 試驗步驟

(a) 將 RSU 架設於測試場域中，並依預設測試用發送訊息封包進行訊息傳送。

(b) 架設車聯網用車載機進行訊息接收並輸出資訊，透過記錄用電腦進行訊息紀錄後，與設定訊息封包資訊進行比對傳輸正確性。

(c) 測試報告內容應詳述測試日期、使用儀器型號及軟體版本、測試設定條件及測試與比對結果。

參考資料

[1] 交通部　　〝道路交通標誌標線號誌設置規則〞

[2] 內政部營建署　〝市區道路及附屬工程設計規範〞

[3] 環境保護署　　〝空氣品質標準〞

[4] 交通部　　〝即時路況資料標準〞格式標準

[5] SAE J2735　　V2X Communications Message Set Dictionary

5G 智慧杆系統技術規範

-第 10-1 部：5G 微型基地臺一般要求

5G Smart pole system technical specification

- Part 10-1: General requirements for 5G micro base station

中 華 民 國 111 年 9 月

目錄

節次 頁次

前言……2

0. 簡介……3

1. 適用範圍 3

2. 引用標準 3

3. 用語及定義 4

3.1 基地臺 4

3.2 第五代行動通信基地臺 4

3.3 微型基地臺 4

4. 縮寫 4

5. 一般要求 4

5.1 硬體設計 4

5.2 操作頻段 5

5.3 基地臺類型 5

5.3.1 BS Type 1-C 5

5.3.2 BS Type 1-H 5

5.3.3 BS Type 1-O 5

5.3.4 BS Type 2-O 5

5.4 傳輸介面 5

5.5 型式認證 5

5.6 設置及發射電波 5

5.7 銜接行動通信網路性能 5

6. 環境要求 5

6.1 保護等級 6

6.2 操作溫度 6

6.3 操作溼度 6

6.4 環境可靠度 6

參考資料 7

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole) 現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT) 設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統。

2. 引用標準

下列標準及規範因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 14336-1	資訊技術設備－安全性－第 1 部：一般要求
CNS 13438	資訊技術設備－射頻擾動特性－限制值與量測方法
國家通信傳播委員會	行動通信基地臺射頻設備技術規範
國家通信傳播委員會	公眾電信網路審驗技術規範
國家通信傳播委員會	公眾電信網路基地臺設置使用管理辦法

3. 用語及定義

5G 智慧杆系統技術規範- 第 1 部：一般要求所規定，以及下列用語及定義適用於本規範。

3.1 基地臺(base station)

指設置於陸地，具構成無線電通信鏈路以供行動臺間及行動臺與其他使用者通信之設備。

3.2 第五代行動通信基地臺(5G mobile communication base station, gNodeB)

指基地臺設備規格採分頻雙工模式時，在上下行各 20MHz 頻寬條件下，下行速率可達 200 Mbps 以上；或設備規格採分時雙工模式時，在 100MHz 頻寬條件下，下行速率可達 500 Mbps 以上。

3.3 微型基地臺(micro base station)

指射頻設備最大輸出功率大於 1.26W(31 dBm)且 10W(40 dBm)以下之基地臺。

4. 縮寫

AAU	主動式天線單元(active antenna unit)
BS	基地臺(base station)
CU	中央單元(central unit)
DU	分散式單元(distribute unit)
EIRP	有效等向輻射功率(equivalent isotropically radiated power)
FDD	分頻雙工(frequency division duplex)
FR1	頻段 1 (frequency range 1)
FR2	頻段 2 (frequency range 2)
gNodeB	5G 基地臺 (5G next generation NodeB, gNodeB)
IP	異物防護(ingress protection)
NR	新無線電(new radio)
OTA	空中介面(over the air)
RH	相對溼度(relative humidity)
RIB	輻射介面邊界(radiated interface boundary)
RU	無線電單元(radio unit)
TAB	收發器陣列邊界(transceiver array boundary)
TDD	分時雙工(time division duplex)

5. 一般要求

5.1 硬體設計

5G 微型基地臺之硬體包括無線電單元、分散式單元與中央單元，可採一體式(All-in-

One)或分離式設計。其中無線電單元之射頻模組與天線系統應採取整合之主動式天線單元設計，射頻模組與天線系統一體化。5G 微型基地臺之尺寸及重量涉及結構安全，應將其納入智慧杆整體之設計，並依第 3 部：安裝與結構相關要求及試驗法之規定。

5.2 操作頻段

5G 微型基地臺依其上行及下行之多工屬性，可區分為分頻雙工(FDD)及分時雙工(TDD)，操作頻段應經國家通訊傳播委員會核准之 5G 頻段。

5.3 基地臺類型

5G 微型基地臺之類型應依[1]定義，以頻段區分為 BS Type 1-C、BS Type 1-H、BS Type 1-O 及 BS Type 2-O。

5.3.1 BS Type 1-C

操作於 FR1 頻段之新無線電 5G 微型基地臺，其組成僅含傳導要求部分，具獨立之天線連接埠。

5.3.2 BS Type 1-H

操作於 FR1 頻段之新無線電(NR) 5G 微型基地臺，其組成包含於各收發器陣列邊界(TAB)連接器上定義的傳導要求，及於輻射介面邊界(RIB)上定義的空中介面要求。

5.3.3 BS Type 1-O

操作於 FR1 頻段之新無線電 5G 微型基地臺，其組成僅含符合輻射介面邊界定義之空中介面要求。

5.3.4 BS Type 2-O

操作於 FR2 頻段之新無線電 5G 微型基地臺，其組成僅含符合輻射介面邊界定義之空中介面要求。

5.4 傳輸介面

5G 微型基地臺傳輸介面至少應包含 1Gbps 乙太網路或 10Gbps 光纖收發模組。

5.5 型式認證

5G 微型基地臺之射頻設備、電氣安全及電磁相容的測試項目及合格標準，應符合「行動通信基地臺射頻設備技術規範」之型式認證要求。

5.6 設置及發射電波

5G 微型基地臺之天線高度及方向、接地裝置、最大有效等向輻射功率、電波功率密度及操作頻段的不必要發射及混附發射區域之不必要發射等，應符合「公眾電信網路設置管理辦法」之基地臺設置及「行動寬頻基地臺審驗技術規範」之發射電波要求。

5.7 銜接行動通信網路性能

5G 微型基地臺之行動通信網路性能，應符合「公眾電信網路審驗技術規範」之要求。

6. 環境要求

6.1 保護等級：5G 微型基地臺具固定裝置，可穩固安裝於智慧杆上，且其防塵防水等級室外至少為 IP65

6.2 操作溫度：-10℃ ~ 50℃

6.3 操作溼度：20%RH ~ 93%RH

6.4 環境可靠度：須符合第 4 部環境可靠度要求。

參考資料

[1]3GPP TS 38.104: 5G New Radio－Base Station Radio Transmission and Reception

5G 智慧杆系統技術規範

-第 10-2 部：5G 微型基地臺性能測試要求

5G Smart pole system technical specification

- Part 10-2: Requirements of performance test for 5G micro base station

中 華 民 國 111 年 9 月

目錄

節次 頁次

前言……4

0. 簡介……5

1. 適用範圍 5

2. 引用標準 5

3. 用語及定義 5

3.1 基地臺 5

3.2 第五代行動通信基地臺 5

3.3 微型基地臺 6

4. 縮寫 ……6

5. O-DU 與 O-RU 間之符合性測試 7

5.1 概述 7

5.1.1 O-RAN 架構介紹 8

5.1.1.1 O-RAN 定義及維護之介面說明 8

5.1.1.1.1 A1 介面 8

5.1.1.1.2 O1 介面 9

5.1.1.1.3 O2 介面 9

5.1.1.1.4 E2 介面 9

5.1.1.1.5 O-Cloud 通知介面 9

5.1.1.1.6 開放式前傳介面 9

5.1.1.2 3GPP 定義及維護之介面說明……9

5.1.1.2.1 E1 介面 9

5.1.1.2.2 F1-c 介面 10

5.1.1.2.3 F1-u 介面 10

5.1.1.2.4 NG-c 介面 10

5.1.1.2.5 NG-u 介面 10

5.1.1.2.6 X2-c 介面 10

5.1.1.2.7 X2-u 介面 10

5.1.1.2.8 Xn-c 介面 10

5.1.1.2.9 Xn-u 介面 10

5.1.1.2.10 Uu 介面 11

5.1.2 O-RU 之 U-Plane 及 C-Plane 測試 11

5.1.3 O-RU 與 O-DU 間之 S-Plane 測試 11

5.1.4 測試要求狀態 11

5.2 測試組態 13
5.2.1 O-RU 為待測裝置之測試組態 13
5.2.2 O-DU 為待測裝置之測試組態 14
5.3 符合性量測 16
5.3.1 M-Plane 量測 16
5.3.1.1 管理告警要求 16
5.3.1.1.1 訂閱通知 16
5.3.1.2 M-Plane 連線監視 17
5.3.1.2.1 M-Plane 連線監視(正案例) 17
5.3.1.2.2 M-Plane 連線監視 (負案例) 18
5.3.1.3 O-RU 資訊元素檢索 19
5.3.1.3.1 未應用過濾器檢索 19
5.3.1.3.2 應用過濾器檢索 20
5.3.2 O-RU 之 UC-Plane 量測 20
5.3.2.1 UC-Plane 標準測試定義 20
5.3.2.1.1 UC-Plane 量測 O-RU TEST SCENARIO 21
5.3.2.1.1.1 情境#1 (FR1 無線電 FDD 傳導測試) 21
5.3.2.1.1.2 情境#2 (FR1 無線電 FDD 非傳導 OTA 測試) 23
5.3.2.1.1.3 UC-Plane 測試組態 24
5.3.2.1.1.4 測試執行通用步驟，O-RU TEST SCENARIO 26
5.3.2.2 TER 用於 U-Plane-及 C-Plane 測試之最小能力 27
5.3.2.2.1 信號分析儀 27
5.3.2.2.2 信號產生器 27
5.3.2.2.3 CUSM- Plane 模擬器(CUSM-E) 28
5.3.2.3 FR1 FDD 傳導信號測試 28
5.3.2.3.1 UC-Plane O-RU 情境類別 NR 通用測試 28
5.3.2.3.1.1 UC-Plane O-RU 情境類別之 3GPP DL 28
5.3.2.3.1.2 UC-Plane O-RU 情境類別擴充 3GPP DL-資源分配 30
5.3.2.3.1.3 UC-Plane O-RU 基本類別 FDD 測試 UL 31
5.3.2.3.1.4 UC-Plane O-RU 情境類別擴充使用 RB 參數 3GPP DL-資源分配 33
5.3.2.3.1.5 UC Plane O-RU 情境類別擴充使用 RB 參數 3GPP UL-資源分配 36
5.3.2.3.2 UC-Plane O-RU 情境類別延遲管理(DLM) 39
5.3.2.3.2.1 UC-Plane O-RU 情境類別 DLM Test #1：下行 1-正測試 42
5.3.2.3.2.2 UC-Plane O-RU 情境類別 DLM Test #2：上行-正測試 43
6. 互運性測試 45
6.1 概述 45
6.1.1 假設 45

6.1.2 一般測試條件及聲明 46
6.2 測試組態標準 46
6.2.1 DUT 46
6.2.2 測試工具 46
6.2.3 時間同步 47
6.2.4 細胞設置 47
6.2.5 SystemInformation-MIB 49
6.2.6 Systeminformation-SIB1 50
6.2.7 Systeminformation-SIB2 51
6.2.8 Systeminformation-SIB3 52
6.2.9 PDU 會談建立程序 53
6.2.10 PDU 多方會談修正 54
6.2.11 閒置模式呼叫及服務請求程序 57
6.2.12 下行 UDP 資料傳送 59
6.2.13 上行 UDP 資料傳送 61
6.2.14 雙向 UDP 資料傳送 62
7. 資通安全測試要求 63
7.1 概述 64
7.2 依 3GPP SA3 之 gNB 安全保證規範要求 64
7.3 資通安全測試項目 65
7.3.1 RRC-signalling 完整性保護 66
7.3.2 UE 與 gNB 間之使用者資料完整性保護 66
7.3.3 RRC 完整性檢查失效 67
7.3.4 UP 完整性檢查失效 67
7.3.5 RRC-signalling 加密 68
7.3.6 UE 與 gNB 間之使用者資料加密 68
7.3.7 UE 與 gNB 間之使用者資料重送保護 68
7.3.8 RRC-signalling 重送保護 69
7.3.9 使用者資料加密依 SMF 發送之安全政策 70
7.3.10 使用者資料完整性依 SMF 發送之安全政策 70
7.3.11 AS 演算法選擇 71
7.3.12 gNB 金鑰更新 72
7.3.13 Xn-handovers 之降階攻擊防護 72
附錄 A (參考) 測試設置 74
附錄 B (參考) 測試簡述 76
參考資料 80

前言

本規範係依 CNS 3689「國家標準草案構成及格式指引」規定草擬完成。

本規範並未建議所有安全事項，使用本規範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。

0. 簡介

都市因應不同用途，設置路燈杆、號誌杆、標誌杆及監控杆等不同用途之杆體。杆體建置差異化造成維護成本高漲，因此，將多杆功能合一之〝智慧杆〞(smart pole) 現已成為智慧都市設計之重要指標。智慧杆除傳統照明、號誌等功能外，可搭載不同物聯網(Internet of things, IoT) 設備，提供安全監控、環境監測、緊急求助及互動式引導等應用服務。智慧杆亦可搭載 5G 微型基地臺，解決 5G 通訊距離較短、大型基地臺不易設置等問題，提升高速行動通訊網路涵蓋率。

本系列規範整合照明、電信網路、資通訊物聯網等不同領域產業，並針對資訊安全及設備性能制訂指標，以加速相關產業國產化及應用發展。本系列規範分為下列各部：

- 第 1 部：一般要求。
- 第 2-1 部：資訊互運性及通訊介面要求。
- 第 2-2 部：資訊互運性及通訊介面測試要求。
- 第 3 部：安裝與結構相關安全要求及試驗法。
- 第 4 部：環境可靠度要求。
- 第 5 部：電氣安全要求。
- 第 6 部：電磁相容要求。
- 第 7-1 部：資訊安全要求。
- 第 7-2 部：資訊安全測試要求。
- 第 8 部：電源供應系統要求。
- 第 9 部：性能要求。
- 第 10-1 部：5G 微型基地臺一般要求。
- 第 10-2 部：5G 微型基地臺性能測試要求。

1. 適用範圍

本規範適用於 60Hz 及 500V 以下交流電源之多用途智慧杆系統。

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

國家通信傳播委員會　公眾電信網路審驗技術規範

3. 用語及定義

5G 智慧杆系統技術規範 - 第 1 部：一般要求所規定，以及下列用語及定義適用於本規範。

3.1 基地臺(base station)

指設置於陸地，具構成無線電通信鏈路以供行動臺間及行動臺與其他使用者通信之設備。

3.2 第五代行動通信基地臺(5G mobile communication base station, gNodeB)

指基地臺設備規格採分頻雙工模式時，在上下行各 20MHz 頻寬條件下，下行速率可

達 200 Mbps 以上；或設備規格採分時雙工模式時，在 100MHz 頻寬條件下，下行速率可達 500 Mbps 以上，以下簡稱 5G 基地臺(gNodeB)。

3.3 微型基地臺(micro base station)

指射頻設備最大輸出功率大於 1.26W(31 dBm)且 10W(40 dBm)以下之基地臺。

4. 縮寫

5GC 5G 核心(5G core)

AS 存取層(access stratum)

C-Plane 控制平面(control plane)

CUSM-E 控制、使用者、同步及管理之平面的模擬器(C-Plane, U-Plane, S-Plane and M-Plane emulator)

CU 中央單元(central unit)

CUS –Plane 控制、使用者及同步之平面(C-Plane、U-Plane、S-Plane)

DCI 下行控制資訊(downlink control information)

DLM 延遲管理(delay management)

DL-SCH 下行共享通道 (downlink shared channel)

DMRS 解調參考信號(demodulation reference signal)

DU 分散式單元(distribute unit)

DUT 待測裝置(device under test)

EN-DC 4G 與 5G 之雙連結 (E-UTRAN new radio – dual connectivity)

EMS 設備管理系統(equipment management system)

EPS 演進封包系統（evolved packet system, EPS）

F1AP F1 應用協定(F1 application protocol)

FCAPS 錯誤、組態、計費、性能、安全(fault, configuration, accounting, performance, security)

FDD 分頻雙工(frequency division duplex)

FR1 頻段 1 (frequency range 1)

FR2 頻段 2(frequency range 2)

gNodeB 5G 基地臺 (5G next generation NodeB, gNodeB)

HTTP2 超文字傳輸協定第 2 版(hypertext transfer protocol 2.0)

LLS 較低層分割(lower layer split)

M-Plane 管理平面(management plane)

MIB 主要資訊區塊(master information block)

NAS 非存取層 (non-access stratum, NAS）

Near-Real Time RIC 近即時無線電接取網路智慧控制器(near-real-time RAN intelligent controller)

NETCONF 網路組態協定(network configuration protocol)

NGAP 下世代應用協定 (NG application protocol)

Non-Real Time RIC 非即時無線電接取網路智慧控制器(non-RT RAN intelligent controller)

NR 新無線電(new radio)

NSA	獨立組網(non-standalone)
O-CU	O-RAN 中央單元(O-RAN central unit)
O-Cloud	開放式無線電接取網路之雲端(O-RAN cloud)
O-DU	O-RAN 分散式單元(O-RAN distributed unit)
O-RAN	開放式無線電接取網路(open radio access network)
O-RU	O-RAN 無線電單元(O-RAN radio unit)
OTA	空中介面(over the air)
PDCCH	實體下行控制通道(physical downlink control channel)
PFCP	封包轉發控制協定(packet forwarding control protocol)
PRB	實體資源區塊(physical resource block)
PRTC	基準主時鐘(primary reference time clock)
PTP	精確時間協定(precision time protocol)
RAN	無線電接取網路(radio access network)
RDN	無線電分配網路(radio distribution network)
RIB	輻射介面邊界(radiated interface boundary)
RLC	無線電鏈路控制協定(radio link control protocol)
RRC	無線電資源控制協定(radio resource control protocol)
RRU	遠端射頻單元(remote radio unit)
RU	無線電單元(radio unit)
S-Plane	同步平面 (synchronization plane)
SA	獨立組網(stand alone)
SCAS	安全保證規範(security assurance specifications)
SIB	系統資訊區塊(system information block)
SMO	服務管理及編排(service management and orchestration)
SRS	探測參考信號(sounding reference signal)
SSB	同步信號區塊(synchronization signal block)
SyncE	同步乙太網路(synchronous Ethernet)
TAB	收發器陣列邊界(transceiver array boundary)
TDD	分時雙工(time division duplex)
TED	O-DU 之測試設備(test equipment, O-DU)
TER	O-RU 之測試設備(test equipment, O-RU)
U-Plane	使用者平面(user plane)
UCI	上行控制資訊(uplink control information)

5. O-DU 與 O-RU 間之符合性測試

5.1 概述

本節 O-DU 與 O-RU 間之符合性測試要求，係依[1]之規定。

本規範定義用於確證 O-RU 與 O-DU 間，於 O-RAN CUS 規範之較低層拆分選項 7.2x

(Lower Layer Split Option 7.2x)介面中所定義之協定的符合性測試。此等符合性測試之指引原則，僅使用由 O-RAN CUS 規範或相關 3GPP 規範定義之標準介面。此等測試之結構係避免包含僅用於此等測試目的之特殊介面的任何裝置要求。

此等測試並非為評估 O-DU 或 O-RU 裝置之性能而編寫，但某些測試需獲得量測結果並評估成功或失敗，依正在測試的通訊協定部分正確處理樣本資料。

本規範之主體(於任何節次)中，其中包含的資訊為規範性涵義，除非明確描述為參考性，對各合規系統皆具有規範性 (註明為「選擇性」之功能，可包含或不含於合規系統內，但若包含，則必須符合選擇性的功能說明)。本規範之“附錄”所含資訊為參考性。

5.1.1 O-RAN 架構介紹

依[2]之 Chapter 4. O-RAN Architecture，如圖 1，說明如下：

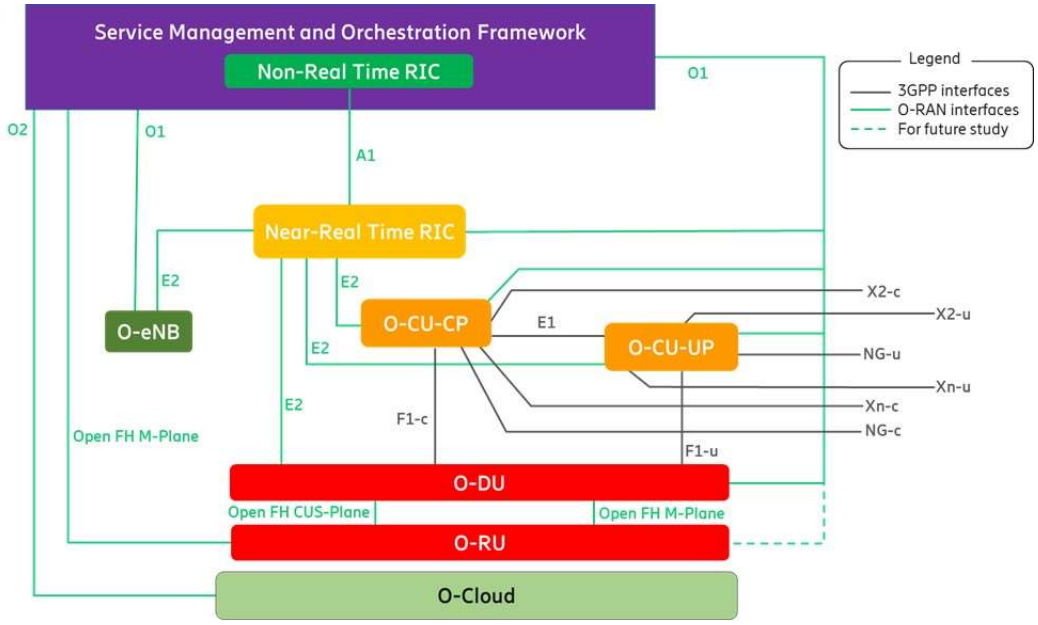


圖 1 O-RAN 架構圖

5.1.1.1 O-RAN 定義及維護之介面說明

圖 1 中之下列介面係由 O-RAN 定義及維護：

The following interfaces are defined and maintained by O-RAN:

(a) A1 介面

(b) O1 介面

(c) O2 介面

(d) E2 介面

(e) O-Cloud 通知介面 O-Cloud Notification

(f) 開放式前傳介面 Open Fronthaul interface

5.1.1.1.1 A1 介面

A1 介面為 SMO 中 Non-RT RIC 功能與 Near-RT RIC 功能間之介面。 A1 介面支援[3]定義之三種類型的服務：

(a)政策管理服務

(b)強化資訊服務

(c)機器學習(machine learning, ML)模型管理服務

5.1.1.1.2 O1 介面

O1 介面位於 [4] 定義之 O-RAN 受管理元素與管理實體間。

5.1.1.1.3 O2 介面

O2 介面位於 SMO 與 O-Cloud 間，如[5]介紹。

5.1.1.1.4 E2 介面

E2 介面為邏輯介面連接 near-RT RIC 與 E2 節點，參照[6]定義 。

(a) 一個 E2 節點僅連接至一個 near-RT RIC。

(b) 一個 near-RT RIC 可連接至多個 E2 節點。

5.1.1.1.5 O-Cloud 通知介面

O-Cloud 通知介面允許事件消費者，如部署於 O-Cloud 上之 O-DU，訂閱源自 O-Cloud 的事件/狀態。雲端基礎設施將提供事件產生者，使雲端工作負載能接收僅有基礎設施能知道之事件/狀態。

5.1.1.1.6 開放式前傳介面

開放式 FH（前傳）介面位於 O-DU 與 O-RU 功能間，參照[7][8]。

開放前傳介面包括 CUS（控制使用者同步）平面及 M（管理）平面。

混合模式下，開放前傳 M-Plane 介面連接 O-RU 至 SMO 以實現 FCAPS 功能。

5.1.1.2 3GPP 定義及維護之介面說明

圖 1 中之下列介面係由 3GPP 定義及維護，且為 O-RAN 一部份：

(a) E1 介面

(b) F1-c 介面

(c) F1-u 介面

(d) NG-c 介面

(e) NG-u 介面

(f) X2-c 介面

(g) X2-u 介面

(h) Xn-c 介面

(i) Xn-u 介面

(j) Uu 介面

5.1.1.2.1 E1 介面

由 3GPP 定義之 E1 介面位於 gNB-CU-CP 與 gNB-CU-UP 邏輯節點間，參照[9][10]。於

O-RAN 中，重複使用 3GPP 所定義 E1 介面之原理及協定堆疊，但於 O-CU-CP 與 O-CU-UP 功能間採用。

5.1.1.2.2 F1-c 介面

由 3GPP 定義之 F1-c 介面位於 gNB-CU-CP 與 gNB-DU 邏輯節點間 ，參照[9][11]。於 O-RAN，重複使用 3GPP 所定義 F1-c 介面之原理及協定堆疊，但於 O-CU-CP 與 O-DU 功能間採用，與定義互運性總則規範。

5.1.1.2.3 F1-u 介面

由 3GPP 定義之 F1-u 介面位於 gNB-CU-UP 與 gNB-DU 邏輯節點間，參照[9][11]。於 O-RAN，重複使用 3GPP 所定義 F1-u 介面之原理及協定堆疊，但於 O-CU-UP 與 O-DU 功能間採用，與定義互運性總則規範。

5.1.1.2.4 NG-c 介面

由 3GPP 定義之 NG-c 介面位於 gNB-CU-CP 與 5GC AMF 間 ，參照[12]，亦視為 N2。於 O-RAN，重複使用 3GPP 所定義 NG-c 介面之原理及協定堆疊，但於 O-CU-CP 與 5GC 間採用。

5.1.1.2.5 NG-u 介面

由 3GPP 定義之 NG-u 介面位於 gNB-CU-UP 與 5GC UPF 間，參照[12]，亦視為 N3。於 O-RAN，重複使用 3GPP 所定義 NG-u 介面之原理及協定堆疊，但於 O-CU-UP 與 5GC 採用。

5.1.1.2.6 X2-c 介面

3GPP 定義之 X2-c 介面，於 eNB 間或 EN-DC 中之 eNB 與 en-gNB 間傳輸控制平面資訊，參照 [12] [13]。於 O-RAN，重複使用 3GPP 所定義 X2-c 介面之原理及協定堆疊，但用於定義互運性剖繪規範。

5.1.1.2.7 X2-u 介面

3GPP 定義之 X2-u 介面，於 eNB 間或 EN-DC 中 ，eNB 與 en-gNB 間傳輸使用者平面資訊，參照 [12][13]。 於 O-RAN，重複使用 3GPP 所定義 X2-u 介面之原理及協定堆疊，但用於定義互運性剖繪規範。

5.1.1.2.8 Xn-c 介面

3GPP 定義之 Xn-c 介面，於 eNBs 與 ng-eNBs 間或於 ng-eNB 與 gNB 間傳輸控制平面資訊，參照[12][14]。於 O-RAN，重複使用 3GPP 所定義 Xn-c 介面之原理及協定堆疊，但用於定義互運性剖繪規範。

5.1.1.2.9 Xn-u 介面

3GPP 定義的之 Xn-u 介面，於 eNBs 與 ng-eNBs 間或於 ng-eNB 與 gNB 間傳輸使用者平面資訊，如參照[12][14]。於 O-RAN，重複使用 3GPP 所定義 Xn-u 介面之原理及協定

堆疊，但用於定義互運性剖繪規範。

5.1.1.2.10 Uu 介面

於 3GPP，UE 至 e/gNB 介面表示為 Uu 介面。Uu 為自 L1 至 L3 之完整協定堆疊，因此，從整體而言，其終止於 NG-RAN。

若 NG-RAN 被分解，不同之協定終止於不同的參考點，且未被 O-RAN 定義。因 Uu 訊息仍從 UE 流向預期之 e/gNB 被管理功能，於 O-RAN 架構中未將其顯示為至特定被管理功能之分隔介面。UE 與 NG-RAN 間 Uu 介面更多資訊，請參閱[9]之 5.2 及 5.3。

5.1.2 O-RU 之 U-Plane 及 C-Plane 測試

本測試規範定義確證 O-RU 之符合性測試。測試涵蓋 O-RAN CUS 規範中定義之許多選擇性功能。因此，對於任何既定之 O-RU 實施，此等測試的子集合可能不適用。測試者應了解每項測試對於特定 O-RU 提供特性之適用性。

5.1.3 O-RU 與 O-DU 間之 S-Plane 測試

此符合性測試規範定義 O-RU 及 O-DU 之時間同步測試，包括功能與性能測試。功能測試確證 O-RU 及 O-DU 依各種 PTP 與選擇性 SyncE 輸入條件，達成正確同步管理狀態之能力。性能測試確證 O-DU 或 O-RU 恢復時鐘之符合性。

關於 S-Plane 之範圍，O-RAN CUS 規範中已定義多種同步選項，用以分送同步至 O-RU (LLS-C1、LLS-C2、LLS-C3 及 LLS-C4)，取決於所考慮之特定 O-RAN 部署，並非全部此等均可能相關。測試 S-Plane 時，測試者應依說明之特定部署情境，確定哪些測試案例為相關的。作為一般指南適用如下：

(a) O-DU 與 O-RU 直接連線：

(1) LLS-C1 通常為確證之主要同步選項。

(2) LLS-C4 可作為 C1 之替代或補充。

(b) O-DU 與 O-RU 間之同步網路：

(1) LLS-C2 用於經由 O-DU 與橋接網路交付同步至 O-RU 的情況。於此拓樸結構中，同步 O-DU 之 PRTC 可為本地或遠端。

(2) LLS-C3 用於非經由 O-DU 之情況，分送同步至 O-RU 的情況。於此情況下，1 個以上的 PRTC 可能為遠端，也可能為本地。

(3)LLS-C4 可作為 LLS-C2/C3 之替代或補充。

對於 LLS-C1 與 LLS-C2，本地 PRTC 嵌入或與 O-DU 共構。遠端 PRTC 置於網路中之任何位置(後傳或前傳)。

5.1.4 測試要求狀態

表 1 為符合性測試之測試清單及測試狀態為 REQUIRED 或 CONDITIONAL MANDATORY。REQUIRED 測試為針對規範要求支援之那些 DUT 功能。DUT 選用功能意指對應之符合性測試為 CONDITIONAL MANDATORY，僅當 DUT 支

援選用功能時才測試。

M-Plane 符合性測試適用於 O-RU 與 O-DU。有些 M-Plane 測試僅針對 O-RU 之協定符合性，對 O-DU 的符合性測試，則非必要。因此對於 M-Plane 測試，表 1 有 2 欄「測試要求」，以說明測試對 O-RU 與 O-DU 為 REQUIRED、CONDITIONAL MANDATORY 或 OPTIONAL 測試。若測試為 OPTIONAL，則無需包含於裝置之符合性測試，但必要時可納入。

表 1　M-Plane 之 O-RU 及 O-DU 符合性測試要求

O-RAN 測試編號	**第 10-2 部 測試編號**	**O-RU 測試要求**	**O-DU 測試要求**	**測試說明**
M-Plane				
3.1.2.1	5.3.1.1.1	MANDATORY	MANDATORY	訂閱告警(Subscription to Notifications)
3.1.3.1	5.3.1.2.1	MANDATORY	MANDATORY	M-Plane 連線監視(正案例) [M-Plane connection supervision (positive case)]
3.1.3.2	5.3.1.2.2	MANDATORY	MANDATORY	M-Plane 連線監視(負案例) [M-Plane Connection Supervision (negative case)]
3.1.4.1	5.3.1.3.1	MANDATORY	MANDATORY	未應用過濾器檢索 (Retrieval without Filter Applied)
3.1.4.2	5.3.1.3.2	MANDATORY	MANDATORY	應用過濾器檢索 (Retrieval with filter applied)

表 2 UC-Plane 之 O-RU 符合性測試要求

O-RAN 測試編號	**第 10-2 部 測試編號**	**O-RU 測試要求**	**測試說明**
UC-Plane：FR1 FDD 傳導訊號測試			
UC-Plane O-RU 情境類別 NR 測試通用(NRG)			
3.2.3.1.1	5.3.2.3.1.1	MANDATORY	UC-Plane O-RU 情境類別之 3GPP DL(UC-Plane O-RU Scenario Class Base 3GPP DL)
3.2.3.1.2	5.3.2.3.1.2	MANDATORY	UC-Plane O-RU 情境類別之擴充 3GPP DL-資源分配 (UC-Plane O-RU Scenario Class Extended 3GPP DL – Resource allocation)
3.2.3.1.3	5.3.2.3.1.3	MANDATORY	UC Plane O-RU 基本類別 FDD 測試 UL (UC Plane O-RU Base Class FDD Test UL)
3.2.3.1.4	5.3.2.3.1.4	MANDATORY	UC-Plane O-RU 情境類別之擴充使用 RB 參數 3GPP DL-資源分配 (UC-Plane O-RU Scenario Class Extended using RB Parameter 3GPP)
3.2.3.1.5	5.3.2.3.1.5	MANDATORY	UC Plane O-RU 情境類別之擴充使用 RB 參數 3GPP UL-資源分配 (UC Plane O-RU Scenario Class Extended using

			RB Parameter 3GPP UL – Resource Allocation)
UC-Plane O-RU 情境類別之延遲管理			
3.2.3.4.1	5.3.2.3.2.1	MANDATORY	UC-Plane O-RU 情境類別 DLM Test #1：下行-正測試 (UC-Plane O-RU Scenario Class DLM Test #1: Downlink 1 – Positive testing)
3.2.3.4.2	5.3.2.3.2.2	MANDATORY	UC-Plane O-RU 情境類別 DLM Test #2：上行-正測試 (UC-Plane O-RU Scenario Class DLM Test #2: Uplink – Positive testing)

5.2 測試組態

本規範說明符合性測試需具特定能力之測試設備，以支援各協定的測試，包括 M-Plane、U-Plane、C-Plane 及 S-Plane。另外，此測試定義測試設備與 DUT 間之特定連線。本節說明測試設備之高階要求，細節說明於各測試中。如本規範 5.1 所述，M-Plane、C-Plane 及 U-Plane 符合性測試之初始重點為 O-RU。除 O-RU 之 S-Plane 測試，更新版亦包括 O-DU 的 S-Plane 測試。下述之初始測試組態著重於測試 O-RU 所需的測試設備及組態。本規範 O-RU 與 O-DU 間之 S-Plane 測試節包含 S-Plane 之 O-DU 測試組態說明。

5.2.1 O-RU 為待測裝置之測試組態

當測試 O-RU 時，以測試設備 O-RU (TER)連線。如圖 2 所示，TER 圍繞 DUT 並連接至前傳介面本身及無線電介面。於無線電介面處，TER 收集自 DUT 之 RF 信號(下行)，並傳送 RF 信號至 DUT 接收器(上行)。因此，TER 含 3 個主要組件：CUSM 平面模擬器(CUSM-E)、訊號分析儀與訊號產生器，如圖 2 所示。於[15]之 LTE、[16]之 NR 傳導測試及[17]之非傳導測試中，說明 RF 測試介面。前傳介面為如上所述之標準乙太網路。此時，信號分析儀接收自 O-RU 發射之 RF 信號，而執行評估 DL 資料流，CUSM-E 接收自信號產生器所發送之 RF 信號，而執行評估 UL 資料流。

當 O-RU 做為 DUT 時，測試設備 RU(「TER」用於連線至 DUT、執行測試並評估測試結果。)

測試設備RU(「TER」)提供執行測試所需之一切，包括：

- M-Plane指令，以收集O-RU能力與組態設定O-RU。
- 經由G.8275.1同步化(對O-RU是應測試的)。
- C-Plane與U-Plane資料流至O-RU。
- 收集RF能量，以確定O-RU是否正確反應DL C-Plane及U-Plane資料。
- O-RU接收之射頻能量輻射(注意：此可能是實際輻射，或經由多種射頻纜線連線傳送)
- 收集O-RU UL前傳資料流且依傳送至O-RU天線或RF連接器的RF能量並評估其正確性。

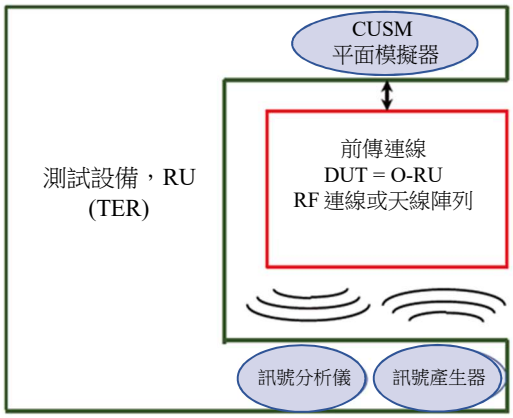


圖 2 測試設置，DUT = O-RU

雖 M-Plane 符合性測試通常不需圖 2 中 TER 顯示之全部功能，但本規範目的是顯示 O-RU 做為 DUT 之全部測試所需的一般能力，包括 U-Plane、C-Plane 及 S-Plane 測試。若測試僅限於 M-Plane，則所需之測試設備組態亦可參考。

備考：圖 2 顯示為 CONDITIONAL MANDATORY 之輔助電路與 RS-485 嗅探器/注入器之 M-Plane 測試設備功能，僅當 DUT 有支援才需要。O-RAN Conformance Test Specification 3.1.9.1 外部輸入/輸出埠，3.1.9.2 外部輸出埠狀態控制或 3.1.11.1 ALD 通訊測試。

當 O-RU 做為 DUT 時，測試設備 RU(「TER」用於連線至 DUT、執行測試並評估測試結果。

M-Plane符合性測試設備，RU(「TER」)提供操作測試所需之一切，包括：

- M-Plane指令，以收集O-RU能力與組態設定O-RU。
- 需要經由G.8275.1(對O-RU是強制性的)進行同步產生「無外部同步源」警報。
- 需RS-485嗅探器/注入器，以確證ALD通訊協定及O-RU操作，執行ALD通訊測試(此測試是CONDITIONAL MANDATORY：僅當DUT支援ALD埠時才需要)。
- 需要輔助電路，以強制變更輸入線之邏輯狀態，並確認外部輸入/輸出埠測試的輸出線電壓(此測試是CONDITIONAL MANDATORY：僅當DUT支援外部輸入/輸出埠時才需要)。

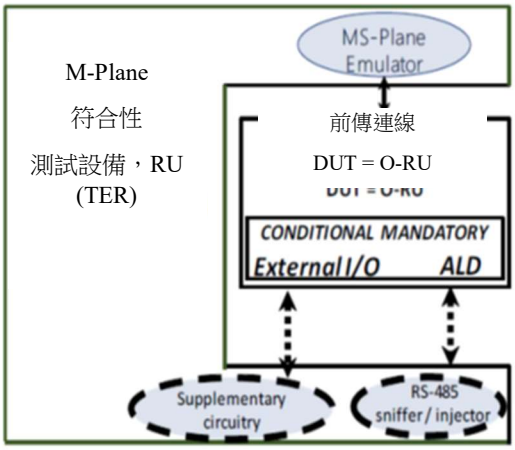


圖 3 M-Plane 測試設置，DUT = O-RU

5.2.2 O-DU 為待測裝置之測試組態

測試 O-DU 之開放式前傳介面時，以測試裝置 O-DU (TED)連接。如圖 4 所示，TED 有 2 種情況：

(a) 獨立 O-DU-做為 DUT：此時，TED 環繞 O-DU DUT，經由其 F1 介面至 Core + O-CU 模擬器(及 NSA 內其他 X2 信號模擬器)、經前傳介面至 O-RU+UE 模擬器及經 O1 或 EMS 介面至測試組態實體。

(b) 組合 O-CU+O-DU(來自同一供應商)做為 DUT：此時，TED 環繞組合 O-CU + O-DU DUT，經 NG (SA)或 S1 和 X2 (NSA) 介面至核心模擬器(及 NSA 內其他 X2 信號模擬器)、經前傳介面至 O-RU+UE 模擬器及經 O1 或 EMS 介面至測試組態實體。

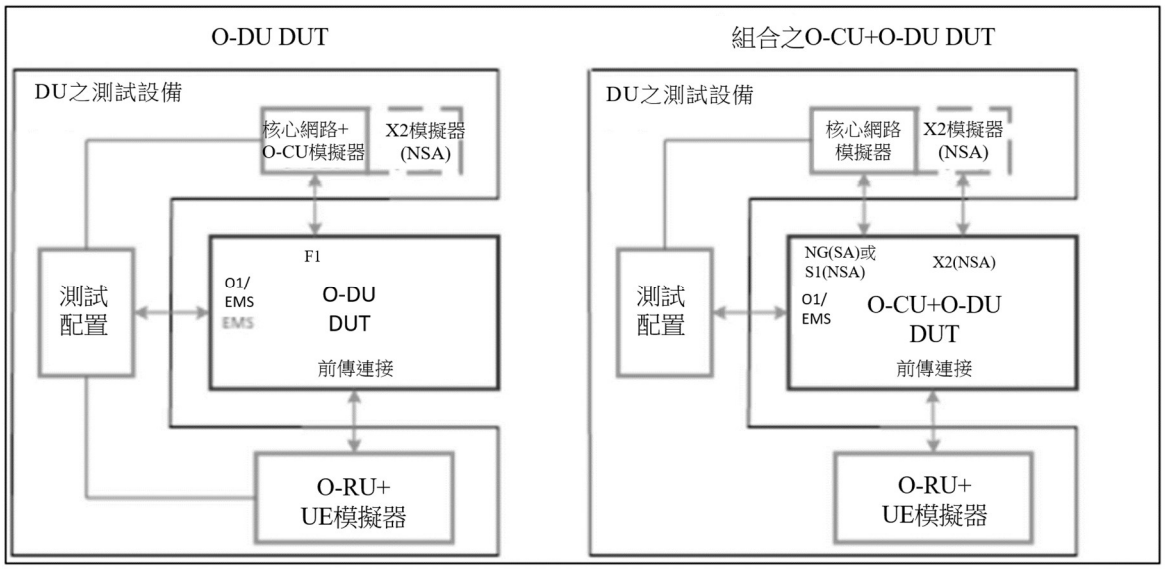


圖 4 測試設置，DUT = O-DU

注意此等測試假設產品等級 DUT 不宜置於任何特殊之測試模式，亦不需任何特殊的測試埠。於前傳介面，O-RU+UE 模擬器將執行下列功能：

(a) 交換所需之前傳資料，以執行待測特性。此需模擬 O-DU DUT 所見之必要前傳訊信號，猶如連接至實際之 O-RU，其具 1 個實際的 UE(或於波束成形測試時，連接多個 UE)，以執行實際連線基地臺。

(b) 詳細觀察並分析 O-DU DUT 之前傳資料串流，以確定是否符合規範。

注意除前傳之 C-Plane、U-Plane 與 M-Plane 信號，亦包括用於將 O-DU DUT 與 O-RU+UE 模擬器同步化所需之 S-Plane。

由於 O-DU 目的在於支援具不同功能組合之各類 O-RU，例：CAT-A 或 CAT-B、FR1 或 FR2、多個 UE 之不同波束成形方法及不同的壓縮方式等，重要的是 O-RU+UE 模擬器具彈性，以強健且可重複的方式有效模擬各種情境，以測試各種特性。同樣地，Core+O-CU 模擬器(NSA 模式增加 X2 信號模擬器)同樣應於 F1 或 NG (或 NSA 之 S1 及 X2)介面處，模擬並觀察適當之信號，以有效地環繞 O-DU 或 O-CU+O-DU DUT。

注意 TED 所需之核心、O-CU、eNB、O-RU 及 UE 模擬器功能，是將 O-DU 或 O-CU+O-DU DUT 置於允許其執行實際連線至 UE 之狀態，以執行待測試之各種開放式前傳特性。因此不需完全模擬其商業等效設備之全部功能。相反地，本規範不排除使用商業等效元件代替模擬器，但必須支援一定程度之可組態性及可重複性，以確保有效且可重複執行 O-DU 前傳所需的特性。使用節點模擬器或商業等效元件，必須有效且可重複複製所需之測試結果及報告。

為包含 O-DU DUT 之各種潛在選擇性特性、部分類型及部分擴充，TED 宜使用 O1(若可用)或 EMS 介面提供 O-DU 或 O-CU+O-DU DUT，以將其置於適當模式，執行將要測試之特定特性，再與 O-RU+UE 模擬器協調，以觸發適當的前傳介面行為。

雖 M-Plane 符合性測試通常不需 TED 顯示之全部功能，但注意：若上表 CONDITIONAL MANDATORY 所示之輔助電路與 RS-485 嗅探器/注入器的 M-Plane 測試設備功能，僅當 DUT 可支援時才需要。O-RAN Conformance Test Specification 3.1.9.1 外部輸入/輸出埠，3.1.9.2 外部輸出埠狀態控制或 3.1.11.1 ALD 通訊測試。

圖 3，本規範目的為顯示 O-DU 做為 DUT 全部測試所需之一般能力，包括 U-Plane、C-Plane 及 S-Plane 測試。若測試僅限於 M-Plane，則可簡化所需之測試設備組態。

5.3 符合性量測

5.3.1 M-Plane 量測

本節介紹 O-RAN 前傳 M-Plane 協定之符合性測試。M-Plane 以 NETCONF 網路元件管理協定及 YANG 資料模型語言(Data Modeling Language)為基礎。NETCONF 協定使用客戶端及伺服器模型進行資訊交換及遠端程序化呼叫 RPC 之執行。每個 NETCONF 處理均涉及客戶端及伺服器之雙向交換。O-DU 需支援 NETCONF 客戶端，而 O-RU 需支援 NETCONF 伺服器。為行使 O-DU（客戶端）或 O-RU（伺服器）而編寫之任何測試，均適用於 O-DU 及 O-RU。

以下內容說明 M-Plane 之符合性測試。儘管所有此等 M-Plane 符合性測試均適用於 O-DU 及 O-RU，但某些測試主要著重於 O-RU NETCONF 伺服器之能力及功能，因此，以下各測試均標示為針對 O-DU、O-RU 或兩者之符合性測試。表 1 列出所有 M-Plane 測試範例及其是否適用於 O-DU 、 O-RU 或兩者之符合性測試。

5.3.1.1 管理告警要求

5.3.1.1.1 訂閱通知

(a) 測試說明及適用性

此情境對於 O-RU 及 O-DU 測試均屬 MANDATORY。

此測試確證 O-RU 是否正確處理 NETCONF 訂閱通知。

此情境對應[18]之 8.2 管理告警要求。

(b) 測試進入準則

支援 M-Plane 確證之 5.2.1 所述 TER 最小功能，為可操作的，並已組態設定及連接至 O-RU。

(c) 試驗法

(1) 初始條件

對於 IPv4 或 IPv6 之傳送及交握(Transport and Handshake)能力。成功個別地完成針對 IPv4 或 IPv6 之傳輸及交遞測試程序。

(2) 程序

(2.1) TER NETCONF 客戶端觸發訂閱:

<rpc><create-subscription><stream>NETCONF</stream></create-subscription></rpc>

至 O-RU NETCONF 伺服器，以訂閱關於監視過程之通知。

備考：<stream>NETCONF</stream> 為意圖性的，表示 TER NETCONF 客戶端訂閱 O-RU NETCONF 伺服器可產生之所有通知(含告警通知)。

(2.2) O-RU NETCONF 伺服器回應

<rpc-reply><ok/></rpc-reply>

至 TER NETCONF 客戶端。

備考：NETCONF 通信依 RFC 6241。

(d) 測試要求

依 5.3.1.1.1 C. 測試方法之程序(b)2.，可成功執行。

Test scenario step 2 is performed successfully.

5.3.1.2 M-Plane 連線監視

5.3.1.2.1 M-Plane 連線監視(正案例)

(a) 測試說明及適用性

此情境對於 O-RU 及 O-DU 測試均屬 MANDATORY。

此測試確證 O-RU 能正確管理連線監視過程。

此情境對應於[18]之 3.6 監視 NETCONF 連線

(b) 測試進入準則

支援 M-Plane 確證 5.2.1 所述 TER 之最小功能，為可操作的，並已組態設定及連接至 O-RU。

(c) 試驗法

(1)初始條件

具 IPv4 或 IPv6 之傳送及交握(Transport and Handshake)能力。

(2) 程序

(2.1) O-RU NETCONF Server supervision timer 到期。

(2.2) O-RU NETCONF 伺服器發送監視通知訊息至 TER NETCONF 客戶端。

此示例中之時間為通用顯示，且將是測試期間的現在時間。

```
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>YYYY-MM-DDTHH:MM:SS.FZ</eventTime>
  <supervision-notification xmlns="urn:o-ran:supervision:1.0"/>
</notification>
```

(2.3) TER NETCONF 客戶端回應

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-
id="20">
  <supervision-watchdog-reset xmlns="urn:o-ran:supervision:1.0">
        <supervision-notification-interval>60</supervision-
notification-interval>
        <guard-timer-overhead>10</guard-timer-overhead>
    </supervision-watchdog-reset>
</rpc>
```

至 O-RU NETCONF 伺服器。

(2.4) O-RU NETCONF 伺服器傳送回應至 TER NETCONF 客戶端

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message
id="20">
<next-update-at xmlns="urn:o-ran:supervision:1.0">2020-10- YYYY-
MM
DDTHH:MM:SS.FZ </next-update-at>
</rpc-reply>
```

(2.5) 注意 TER NETCONF 客戶端可於監視看門狗(watchdog)重置訊息中變更監視計時器之值。若執行此選擇性測試，則 O-RU NETCONF 伺服器必須相應地調整計時器。

(2.6) O-RU NETCONF 伺服器向 TER NETCONF 客戶端發送有關步驟 2.3 rpc-reply 中發送之時間日期的監視通知。

(2.7) 將步驟 2.1 至 2.4 循環進行 30 次，包括第一次通過步驟 2.1 至 2.4。

備考：NETCONF 通信依 RFC 6241。

(d) 測試要求

依 5.3.1.1.2 C. 測試方法之程序(b)5.，可成功執行。

5.3.1.2.2 M-Plane 連線監視 (負案例)

(a) 測試說明及適用性

此情境對於 O-RU 及 O-DU 測試均屬 MANDATORY。

此測試確證 O-RU 能正確管理連線監視過程。

此情境對應於[18]之 3.6 監視 NETCONF 連線

(b) 測試進入準則

支援 M-Plane 確證 5.2.1 所述 TER 最小功能，為可操作的，並已組態設定及連接至 O-RU。

(c) 試驗法

(1) 初始條件

具 IPv4 或 IPv6 之傳輸及交遞(Transport and Handshake)能力。

(2) 程序

(2.1) O-RU NETCONF Server supervision timer 到期。

(2.2) O-RU NETCONF 伺服器將監視通知訊息發送至 TER NETCONF 客戶端。

(2.3) TER NETCONF 客戶端回應

<rpc supervision-watchdog-reset></rpc>

至 O-RU NETCONF 服器。

(2.4) O-RU NETCONF 伺服器傳送回應至 TER NETCONF 客戶端

<rpc-reply><next-update-at>date-time</next-update-at></rpc-reply>

(2.5) 注意 TER NETCONF 客戶端可於監督看門狗(watchdog)重置訊息中變更監視計時器之值。若執行此選擇性測試，則 O-RU NETCONF 伺服器必須相應地調整計時器。

(2.6) O-RU NETCONF 伺服器向 TER NETCONF 客戶端發送有關步驟 2.3 中 rpc-reply 發送之時間日期的監視通知。

(2.7) TER NETCONF 客戶端不會向 O-RU NETCONF 伺服器發出<rpc monitoring-watchdog-reset> </ rpc>，且會使看門狗(watchdog)計時器於 O-RU 上到期。

(2.8) O-RU NETCONF 伺服器進入監視失敗情境。相關細節請參照 O-RAN M-Plane 規範 11.1。

(d) 測試要求

依 5.3.1.2.2 C. 測試方法之程序(b)7.，可成功執行。

5.3.1.3 O-RU 資訊元素檢索

5.3.1.3.1 未應用過濾器檢索

(a) 測試說明及適用性

此情境對於 O-RU 及 O-DU 測試均屬 MANDATORY。

此情境確證 O-RU NETCONF 伺服器正確執行常規之 get 指令。

此為與 NETCONF 實施有關之通用高級測試。與[18]中之特定章節沒有直接關聯。

(b)測試進入準則

支援 M-Plane 確證 5.2.1 所述 TER 最小功能，為可操作的，並已組態設定及連接至 O-RU。

(c) 試驗法

(1)初始條件

具 IPv4 或 IPv6 之傳輸及交遞(Transport and Handshake)能力。

(2) 程序

(2.1) TER NETCONF 客戶端向 O-RU NETCONF 伺服器觸發<rpc> <get>。

(2.2) O-RU NETCONF 伺服器以<rpc-reply> <data>回應，其中<data>包含 O-RU NETCONF 伺服器能揭露之所有資訊元素。

(d) 測試要求

依 5.3.1.3.1 C. 測試方法之程序(b)2.，可成功執行。

5.3.1.3.2 應用過濾器檢索

(a) 測試說明及適用性

此情境對於 O-RU 及 O-DU 測試均屬 MANDATORY。

此情境確證 O-RU NETCONF 伺服器正確執行應用過濾器之 get 命令。

此為與 NETCONF 實施有關之通用高級測試。與[18]中之特定章節沒有直接關聯。

(b) 測試進入準則

支援 M-Plane 確證 5.2.1 所述 TER 最小功能，為可操作的，並已組態設定及連接至 O-RU。

(c) 試驗法

(1)初始條件

具 IPv4 或 IPv6 之傳輸及交遞(Transport and Handshake)能力。

(2) 程序

(2.1) TER NETCONF 客戶端向 NETCONF 伺服器觸發<rpc> <get> <filter>。 <filter>參數包含 O-RU NETCONF 伺服器應作為過濾器之正規表達式。

例: 1 個過濾器過濾所有低位準之 rx 端點(low-level-rx-endpoints)：

```
<rpc message-id="101" xmlns="urn:o-ran:uplane-conf:1.0" >
    <get>
        <source>running</source>
        <filter type = "subtree">
            <top xmlns="urn:o-ran:uplane-conf:1.0/">
                <user-plane-configuration>
                    <low-level-rx-endpoints>
                    </low-level-rx-endpoints>
                </user-plane-configuration>
            </top>
        </filter>
    </get>
</rpc>
```

(2.2) O-RU NETCONF 伺服器回應<rpc-reply> <data>，其中<data>包含符合<filter>之所有物件細節（如上述各示例過濾器：所有低位準 rx 端點）

(d) 測試要求

依 5.3.1.3.2 C. 測試方法之程序(b)2.，可成功執行。

5.3.2 O-RU 之 UC-Plane 量測

5.3.2.1 UC-Plane 標準測試定義

以下節次描述實施 U-Plane 及 C-Plane O-RAN 選擇性 7.2x 協定之設備測試場景。此符合性測試文件之初始重點為確證 O-RU 作為待測裝置(DUT)。

5.3.2.1.1 UC-Plane 量測 O-RU TEST SCENARIO

於此等測試集中，DUT 為 O-RU。

本規範敘述下列情境之符合性測試：

FR1 無線電 FDD 傳導測試 Conducted FDD tests for FR1 radios

O-RU 必須僅針對適用於 O-RU 功能之情境進行測試。

對於上述情境 #1，RF 測試設置如[16]之[NR] 及 [15]之[LTE] 中所述。

注意 O-RAN 符合性測試應為“離線”，且不會於 O-DU 及/或 O-RU 運行，並為實際使用者提供服務時執行。O-RU 製造商亦需提供[16]、[17]之[NR]及[15]之[LTE] 4.6 描述的相同聲明。此將確定無線電對多載波操作之支援（例：是否於不同之連接器上支援多載波操作）。

由於本規範目的為測試 O-RAN 前傳符合性，而非重複 3GPP RF 測試，因此僅有 [16]、[17]之[NR] 及[15]之[LTE] 之選定部分將用於 RF 測試。此等選定之測試特性僅用於測試 O-RU 是否正確解譯且產生 O-RAN C-Plane 及 U-Plane 訊息。[16][17][NR]及[15][LTE] 中使用之測試波形亦將增加一些內容，以充分發揮 O-RAN 前傳協定之特性。此等選定及添加內容總結如下：

5.3.2.1.1.1 情境#1 (FR1 無線電 FDD 傳導測試)

(a) 對於類型 1-C 無線電（具天線埠連接器及被動天線之無線電）的下行測試，將使用 [16] D.1.1 中所描述之測試組態。除非測試明確需要多埠且無線電支援多埠，否則將僅使用單一天線埠。 RF 測試設備於 [16] 4.2.1 描述之點連接。注意天線埠為連接至陣列元件之導電埠。

(b) 對於 1-C 類無線電（具天線埠連接器及被動天線之無線電）之上行測試，將使用 [16] D.2.1 中描述之測試組態，除非測試明確需要多埠且無線電支援多埠，否則將僅使用單一天線埠。RF 測試設備於[16] 4.2.1 描述之點連接。注意天線埠為連接至陣列元件之導電埠。

(c) 對於類型 1-H 無線電（具 TAB 連接器及主動天線系統之無線電）之下行測試，[16] D.3.1 描述之測試組態將用於傳導測試，除非測試明確需要多個連接器，否則將僅使用 1 個 TAB 連接器。 RF 測試設備於[16] 4.2.2 描述之點連接。注意，收發器陣列邊界 (TAB) 連接器為透過無線電分配網路 (RDN) 連接至陣列元件之導電埠。

(d) 對於類型 1-H 無線電（具 TAB 連接器及主動天線系統之無線電）之上行測試，[16] D.4.1 中描述之測試組態將用於傳導測試，除非測試明確需要多個連接器，否則將僅使用 1 個 TAB 連接器。RF 測試設備於[16] 之 4.2.2 描述之點連接。注意收發器陣列邊界 (TAB) 連接器為透過無線電分配網路 (RDN) 連接至陣列元件之導電埠。

(e) 基本下行測試將自 NR-FR1-TM1.1 及 E-TM1.1 描述之測試模型開始。後續測試將調整此模型，以測試 O-RAN 介面之附加功能（例：修改酬載資料、遮蔽某些符號等），注意此測試模型描述 O-RAN 封包中包含之 IQ 資料，而

非 O-RAN 特定參數。此測試模型亦可加入以下 O-RAN 特定參數：

包括透過 M-Plane 組態設定之“庫存(stock)” eAxC 值：

(1) DU_Port_ID：2 位元， 標稱值 00b

(2) BandSector：標稱 6 位元， 標稱值 000000b

(3) CC_ID：標稱 4 位元， 標稱值 0000b (大部分測試僅使用 1 個組成載波)

(4) RU_port_ID：標稱 4 位元， 標稱值 0000b 至 0011b 或特定測試所需之任何最大值

(f) 無線電製造商聲明支援多載波時，將為各載波指定不同之 eAxC，注意[16]之[NR] 及 [15]之[LTE] 描述之大多數測試，均需於支援上、中、下無線電頻段進行測試，本規範放寬此要求，因目的為測試前傳符合性而非無線電性能。

(g) 壓縮：DL 及 UL 中之靜態 16 位元定點 IQ 位元寬。

(h) 波束成形：無成形波束(beamId = 0x0000)，假設於某未確定波束寬度下表示準向輻射（垂直於天線表面）（重申波束權重幅度必須等於 1）

(i) 傳送：L2 乙太網路，eCPRI，無分段及無 QOS

(j)延遲參數：此測試將光纖直接連接至 O-RU 執行，且由於延遲管理之目的，網路延遲被認為可忽略不計。因此，T12_min = T12_max = 0 且 T34_min = T34_max = 0。

無線電將報告支援之下列參數數值：

(1) T2a_min/max_up

(2) Ta3_min/max_up

(3) T2a_min/max_cp_ul

(4) Tcp_adv_dl

此等參數將用於計算以下延遲管理測試所需之延遲窗口。

注意由於固定之零網路延遲，T1a_min_up = T2a_min_up 及 T1a_max_up = T2a_max_up。同理，Ta4_min_up = Ta3_min_up 及 Ta4_max_up = Ta3_max_up。同理，T1a_min_cp_ul = T2a_min_cp_ul 及 T1a_max_cp_ul = T2a_max_cp_ul。

(k) 上行測試將自用於固定參考通道之基本 3GPP 測試信號開始，用於接收靈敏度及通道內選擇性，如[16]之 [NR] 及[15]之[LTE] 所述。所有 O-RAN 特定參數將與上述下行測試相同。與下行測試一樣，後續測試將基於此基本波形修改參數，依需執行 O-RAN 特定特性。

(l) 上行測試將使用[16]之[NR] 及[15]之[LTE] 描述之用於測試 3GPP 接收器靈敏度之功率位準，至少高 30dB 的功率位準進行，此為確保 O-RU 接收清晰之信號。因此可準確地對其進行解碼及解調，以確保 O-DU 接收信號源發送之正確資料。同樣，此測試是為確保 O-RAN 前傳之正確操作，而非測試接收器靈敏度。

5.3.2.1.1.2 情境#2 (FR1 無線電 FDD 非傳導 OTA 測試)

(a) 對於選擇透過 OTA 而非傳導進行 1-H 型無線電之下行測試，[17] E.1.2 描述測試組態，其中測試天線將置於 OTA 無反射室內，且量測參考[17] 4.2-1 定義之 RIB 處的 OTA 輻射特性。RF 分析儀測試設備連接至位於 OTA 無反射室外之測試天線。

(b) 對於 1-O 或 2-O 無線電（無實體天線或 TAB 連接器之無線電，因此僅能透過 OTA 量測）之下行測試，測試組態於[17]E.1.2 描述，其中測試天線將置於 OTA 無反射室內，量測參考[17] 4.2-2 中定義之 RIB 處的 OTA 輻射特性。RF 分析儀測試設備連接至位於 OTA 無反射室外之測試天線。

(c) 對於選擇透過 OTA 而非傳導進行 1-H 型無線電之上行測試，測試組態於 TS [17] E.2.1 描述，其中測試天線將置於 OTA 無反射室內，且量測參考[17] 4.2-1 定義之 RIB 處的 OTA 輻射特性。 RF 產生器測試設備連接至位於 OTA 無反射室外之測試天線。

(d) 對於 1-O 或 2-O 無線電（無實體天線或 TAB 連接器之無線電，因此僅能進行 OTA 量測）之上行測試，測試組態於 [17] E.2.1 描述，其中測試天線將置於 OTA 無反射室內，量測參照[17] 4.2-2 定義之 RIB 處定義的 OTA 輻射特性，RF 產生器測試設備連接至位於 OTA 無反射室外之測試天線。

(e) 對於選擇透過 OTA 進行測試之 LTE 無線電之下行測試，測試組態於 [17] E.1.2 描述，其中測試天線將置於 OTA 無反射室內，量測參考輻射於[17] 4.2-1 定義之 RIB 處的 OTA 特性。射頻分析儀測試設備連接至位於 OTA 無反射室外之測試天線。

(f) 對於選擇透過 OTA 進行測試之 LTE 無線電之上行測試，測試組態於[17] E.2.1 描述，其中測試天線將置於 OTA 無反射室內，且量測參照[17] 4.2-1 定義之 RIB 處的 OTA 輻射特性。 RF 產生器測試設備連接至位於 OTA 無反射室外之測試天線。

(g) 注意[17] E1.2 及 E.2.1 所示之無反射室為通用的，因此可使用任何 OTA 無反射室，即遠場、CATR、近場、響應等。

(h) 同樣，[17] E.1.2 及 E.2.1 之定位器，可依波束成形量測技術決定需不需要。

(i) 此外，依要量測之波束成形方法，可能亦需 1 支以上之測試天線及 1 部以上之 RF 分析儀及/或 1 個產生器埠。

(j) 基本下行測試將自[16] 之 NR-FR1-TM1.1 及[15]之 E-TM1.1 描述之測試模型開始，其分別用於 NR FR1 及 LTE 無線電。後續測試將調整此模型，以測試 O-RAN 介面之附加特性（例：修正酬載資料、遮蔽某些符號等）。注意此測試模型描述 O-RAN 封包中包含之 IQ 資料，而非 O-RAN 特定參數。該測試模型亦可加入 O-RAN 特定參數：

包括透過 M-Plane 組態設定之“庫存”eAxC 值：

(1) DU_Port_ID：2 位元， 標稱值 00b

(2) BandSector：標稱 6 位元， 標稱值 000000b

(3) CC_ID：標稱 4 位元， 標稱值 0000b (大部分測試僅使用 1 個組成載波)

(4) RU_port_ID：標稱 4 位元， 標稱值 0000b 至 0011b 或特定測試所需之任何最大值

(k) 無線電製造商聲明支援多載波時，將為各載波分配不同之 eAxC。 注意 [17]之[NR] 及 [15]之[LTE] 描述之大多數測試均需於支援上、中、下之無線電頻段進行測試， 該規範放寬要求，因目的為測試前傳符合性而非無線電性能。

(l) 壓縮： DL 及 UL 中之靜態 16 位元定點 IQ 位元寬

(m) 波束成形：無波束成形（beamId = 0x0000），假設是指於某個未確定波束寬度下之準向輻射（與天線表面垂直）（重申波束權重幅度必須等於 1）

(n) 傳送：L2 乙太網路、無分段及無 QOS 之 eCPRI

(o) 延遲參數：此測試將光纖直接連接至 O-RU 執行，出於延遲管理之目的，網路延遲被認為可忽略不計。因此，T12_min = T12_max = 0 且 T34_min = T34_max = 0.

無線電將報告支援之下列參數數值：

(1) T2a_min/max_up

(2) Ta3_min/max_up

(3) T2a_min/max_cp_ul

(4) Tcp_adv_dl

此等參數將用以計算延遲管理測試所需之延遲窗口。

由於固定之零網路延遲，需注意 T1a_min_up = T2a_min_up 且 T1a_max_up = T2a_max_up. 同理，Ta4_min_up = Ta3_min_up 且 Ta4_max_up = Ta3_max_up. 同理， T1a_min_cp_ul = T2a_min_cp_ul 且 T1a_max_cp_ul = T2a_max_cp_ul.

(p) 如[17]之[NR] 及[15]之[LTE] 所述，上行測試將自用於固定參考通道之基本 3GPP 測試信號開始，其用於接收器靈敏度及通道內選擇性。所有 O-RAN 特定參數將與上述用於下行測試之參數相同。與下行測試一樣，後續測試將基於此基本波形修改參數，依需執行 O-RAN 特定特性。

(q) 上行測試將使用比用於測試[17]之表 7.3.5.2-1、表 7.3.5.2-2 及表 7.3.5.2 描述之 3GPP 接收器靈敏度之參考靈敏度功率位準高至少 30dB 之功率位準進行輻射-3[NR FR1]，表 7.3.5.3-1 [NR FR2] 及[15]表 7.2-1 至表 7.2-12 [LTE]，為確保 O-RU 接收到清晰之信號，因此可準確地對其進行解碼及解調，以確保 O-DU 接收到信號源發送之正確資料。同樣，此等測試之目的為確保 O-RAN 前傳之正確操作，而非測試接收器靈敏度。

5.3.2.1.1.3 UC-Plane 測試組態

圖 2 中所示之 TER 提供 M-Plane、S-Plane 的命令及序列，以正確設置 O-RU 使用前傳連線進行測試，意味著執行所有 UC-Plane 測試之準則及先決條件為

正確操作 O-RU 之同步及 M-Plane 功能。TER 提供特定之 C-Plane 及 U-Plane 資料流，並自 O-RU 之輻射能量中收集資料，再依收集之 RF 能量評估 O-RU 是否正確接收及解譯前傳 DL 資料流。

對於多數測試，單一 RF 檢測器足以檢測輻射信號，但對於波束成形測試，必須量測 RF 模式，以確證是否依 C-Plane 命令及流經前傳介面之 U-Plane 資料生成正確之波束。

此外，TER 使用信號產生器生成 RF 能量並將其饋送至 O-RU 預定將使用之 O-RU 天線（或天線連接器），結合由 O-RU 發送之 C-Plane UL 命令。透過前傳連線之 TER，於前傳連線上生成 UL 資料流，由 TER 接收及評估。 對於幾乎所有測試，單一 RF 發射器亦能令人滿意地生成輻射信號，即使是波束成形測試，其中接收功率位準將確證波束主瓣是否於前傳介面上正確指定，但基於上行通道資訊之波束成形測試情況除外，其需多個 RF 發射器，以模擬多個上行空間串流。

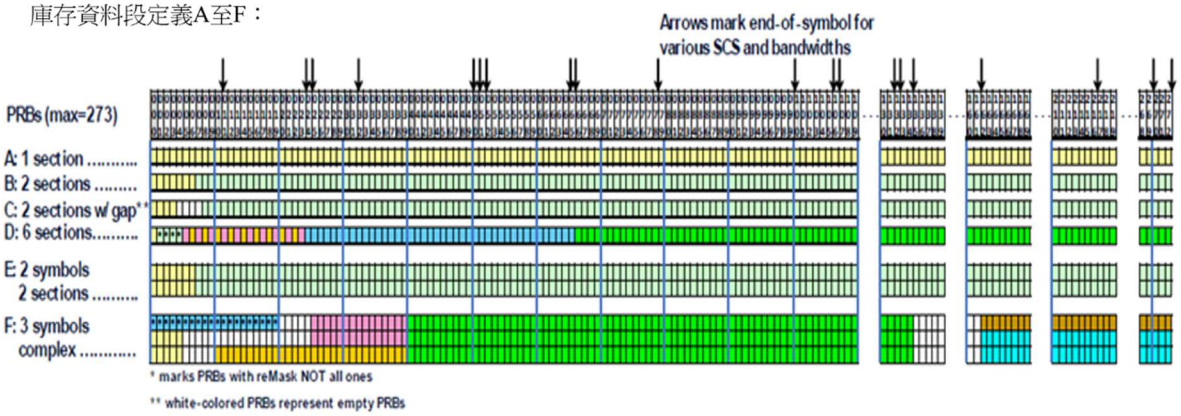
此處將使用 3GPP 指定之測試以簡化測試，因對於 3GPP 符合性測試，O-RU 無論如何均需支援此類測試。特定之測試案例確定哪些部分為可能的，及哪些部分必須進行變更，以充分測試 O-RAN 特性。

注意於測試 O-RU 之前傳介面符合性時，不僅是測試前傳介面，實際上是在測試整個 O-RU，包括與前傳介面無關之數位及類比處理。因此，測試“通過”可有把握地解釋為前傳介面運行正常，但測試“失敗”可能表明前傳介面或 O-RU 內之某些其他操作有問題，因此失敗之測試可能需要一些故障排除。

雖[16]、[17]之[NR]及[15]之[LTE]描述此等測試中使用之基本波形，但並未描述宜如何將各種通道放入 O-RAN 段。[16]NR-FR1-TM1.1 之[NR FR1]、[17]NR-FR2-TM1.1 之[NR FR2]及[15]E-TM1.1 之 [LTE] 的信號與封包資料緊密相連。所有測試均會使用下述之節次，將該資料劃分為“庫存”資料段。為加速測試之定義及創建，本節定義 1 組標準測試環境及模式，包括 DL 中資料段之“庫存”排列（與 UL 相同），無論測試中使用之特定頻寬及 SCS，均可使用。

具體而言，應具有於測試定義（編號“A”至編號“F”）中引用之“庫存”1 個符號、2 個符號及 3 個符號資料彙集，以支援各種測試案例，測試案例應指定測試時槽之資料段定義，除非測試另有特別說明，否則所有時槽均應依相同之資料段定義。於許多情況下，僅有 1 個時槽內之某些符號會受測試；其餘符號之測試預為保留未定義，且可能具依 O-DU 正常操作定義之資料段（例：設置為攜帶與 LTE 或 NR 一致之同步或參考信號）。若 DUT 不支援特定類型之資料段，則於符號中省略該資料段，且對應之 U-Plane 資料應於 DL 中設置為零（並安排於 UL 無 RF 功率）。圖 5 顯示“庫存”資料段定義。

庫存資料段定義A至F：



A: 1個符號僅1段:最簡單情況

B: 1個符號2段:稍微複雜

C: 1個符號2段有間隔:處理間隔測試能力

D: 1個符號多段:測試單一PRB段, rb位元, 使用非全一reMask參數, 多資料段

E: 2個符號2段:測試多符號段, symInc位元

F: 3個符號多段:測試資料間隔, reMask參數,多符號段

圖 5 上行及下行庫存資料段定義

另一“庫存”U-Plane 資料為 PN23 資料，表示為調變前使用者資料，如[16]所指定[CCITT Recommendation O.151 (10/92) https://www.itu.int/rec/T-REC-O.151-199210-I/en]，其假設自訊框邊界開始，且於 DL 及 UL 之所有訊框中均屬相同，除非特定測試聲明不同。無論頻寬及 SCS 如何（此與資料段之處理不同，資料段將依每個符號之 PRB 數量截斷），PN 序列將於訊框之持續時間內運行。然而，於許多情況下，僅有訊框內之某些符號會實際進行測試（如特定測試所定義），因此將包含測試 PN 序列資料，其餘符號預計於測試中將保留未定義，且可能內含依 O-DU 正常操作之資料（例：設置為攜帶與 LTE 或 NR 一致之同步或參考信號）。注意 PN 序列初始值由種子提供，該種子可包含於測試命令參數內。若省略該參數，PN 序列生成器將使用全 1 之“種子”值。

對於所有測試，測試定義應定義受測試之特定時槽及符號（攜帶“庫存”C-Plane 資料段定義及“庫存”” U-Plane 資料），其餘時槽及符號未定義但攜帶正常之 3GPP 同步與控制資料及清空用戶資料。 每個訊框中所有要測試之時槽及符號均屬相同，因此測試不必等待特定之訊框碼，亦不會重置或以其他方式擾亂正常之訊框碼序列。為使測試儘可能不干擾正常之 O-DU 及 O-RU 操作。若有特殊需要確證特定資料訊框資料槽之構造，測試可選擇將測試資料歸零，並為除單一資料槽或資料訊框外之所有資料段保留未定義的資料段；若此為必要，將於特定之測試定義中描述，但此預期為一例外情況。

5.3.2.1.1.4 測試執行通用步驟，O-RU TEST SCENARIO

以下測試 O-RU 時使用通用測試步驟，但特定測試可能會偏離此通用程序：

(a)為測試執行組態設定測試設備 O-RU (TER)，其可能包括定義要執行之特

定測試。亦可能包括使用腳本語言以描述測試。

(b)組態設定 O-RU，包括收集 O-RU 能力，使用 M-Plane 命令組態設定 O-RU 運行，使用 G.8275.1 同步 O-RU。

(c)發送適當之 C-Plane 及 U-Plane DL 資料流，並使用 RF 檢測設備收集 O-RU 輻射能量（或自天線連接器收集）。

(d)評估自 O-RU 之 RF 能量模式，以確定 O-RU 是否正確接收及解譯前傳 C-Plane 及 U-Plane 資料流。於某些情況下，亦包括對 RF 信號進行解碼及解調，以確保正確解譯所有 UC-Plane 訊息

(e)發送適當之 C-Plane 訊息，以定義所需之 UL U-Plane 流，同時使 RF 信號產生器輻射（或饋入天線連接器）適當之 RF 能量模式以進行測試。

此也意味著滿足適當之時序窗口，以允許 O-RU 於信號產生器開始發送 RF 前之解碼及處理 C-Plane 訊息。

(f)收集前傳介面上之 O-RU UL 資料流，並評估正確性；通常僅是 U-Plane 資料，但於受限情況下 (LAA_ Licensed-Assisted Access) 亦可能包括 UL C-Plane 訊息。

(g)由於 FDD 上行及 TDD 測試需要 TER 組件間之嚴格時序約束，因此建議當 C-Plane 信令開始用於訊框時，CUSM 模擬器向 RF 測試設備發送信號。RF 測試設備如何使用此信號，以同步傳輸及接收依實施而定。

5.3.2.2 TER 用於 U-Plane-及 C-Plane 測試之最小能力

由於 O-RAN 協定之許多特性依賴於 O-DU 指示 O-RU 使用特定壓縮方法，將資料置入特定資源區塊中，因此測試設備必須支援允許將前傳側之資料與無線電 RF 端之資料比對。

5.3.2.2.1 信號分析儀

(a)必須具解碼及解調透過空中或傳導介面接收之 RF 信號的能力。此資料必須可用於與前傳介面上發送之資料進行比較。

(b)必須能為波束成形測試確定任何信號之相位及振幅。

(c)顯然必須支援受測無線電之頻率範圍。

5.3.2.2.2 信號產生器

(a) 必須提供能建構正確 5G 或 LTE 波形之軟體。

(b) 宜能自動建構 3GPP 符合性測試之波形，且宜提供編輯該波形參數之機制。

(c) 必須能與 O-DU 模擬器同步，以確保上行 C-Plane 及 U-Plane 訊息之正確時序。

5.3.2.2.3 CUSM- Plane 模擬器(CUSM-E)

(a) 必須能自上行 U-Plane 訊息中提取 IQ 資料，並對資料進行解調及解碼，以確保其與上行 C-Plane 訊息中之命令相同。

(b) 必須能與 RF 信號源同步。

(c) 宜能依無線電支援之同步組態作為 PTP 主設備或從設備運行。

(d)必須能接受頻域 IQ ，並依使用者於正確段之輸入，對其進行封裝。

5.3.2.3 FR1 FDD 傳導信號測試

5.3.2.3.1 UC-Plane O-RU 情境類別 NR 通用測試

本節之所有下行測試均使用 3GPP 測試波形，其子載波間隔為 30 kHz，頻寬為 100 MHz，如[16] NR-FR1-TM1.1 及 5.3.2.1.1.3 所述。依無線電之能力，此測試信號有多種變化。若無線電不支援 M-plane 中報告之案例測試，所使用之數值集，則由測試開發人員修改，以適應於無線電測試。通常可透過使用上述庫存測試模式完成，測試為預期依本規範之相同測試精神，但符號編號及 PRB 數量等項目可能需變更。

本節所有上行測試均使用 [16] A1 描述之 3GPP 測試波形，特別是 G-FR1-A5-1（30 kHz 子載波間隔，QPSK，100 MHz BW）。下行測試時，若無線電不支援此信號，則由測試開發人員於不改變測試精神之情況下，變更測試參數。

5.3.2.3.1.1 UC-Plane O-RU 情境類別之 3GPP DL

(a)測試說明及適用性

此測試為 MANDATORY。

此測試之目的為確保無線電能符合 O-RAN 前傳最基本的下行要求。後續之測試將以此為基礎行使前傳之其他能力。

針對 FDD，使用標準之 3GPP NR-FR1-TM1.1 測試訊框，O-DU 模擬器（即 5.2.1 所述 TER 之 O-RAN 介面）將產生 O-RU 於下行上傳輸標準 NR-FR1-TM1.1 信號所需之 C-Plane 及 U-Plane 訊息。該信號如圖 6 所示:

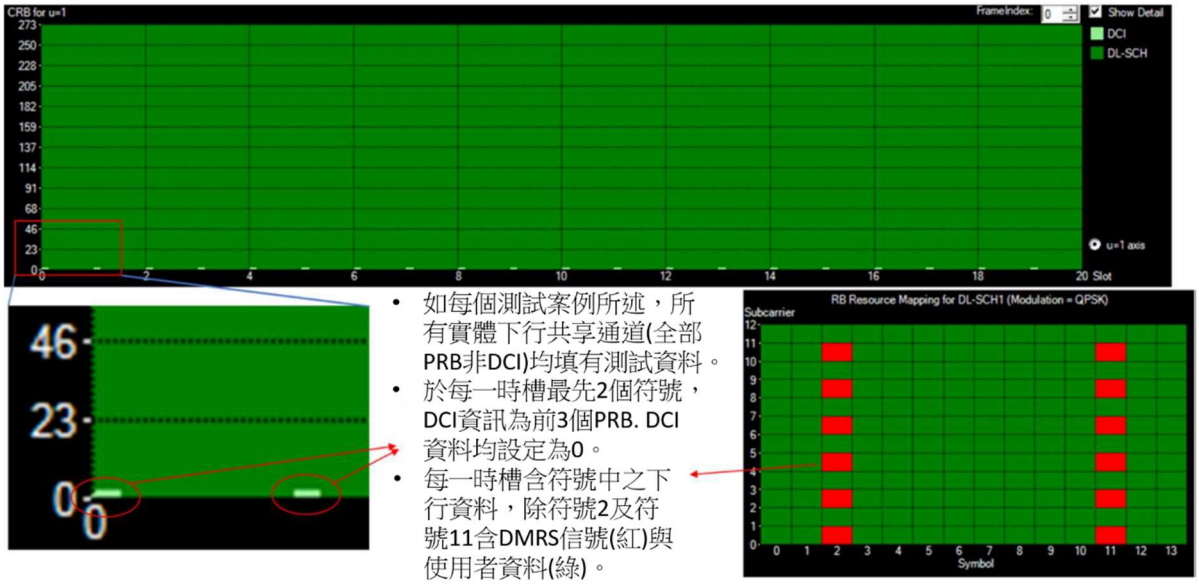


圖 6 NR-FR1-TM1.1 FDD 測試信號

此測試訊框包括由 3 個 PRB 組成之每個時槽前 2 個符號中的 PDCCH。訊框中所有剩餘之 PRB 均包含實體下行共享通道資料。該組態不含 PDCCH 通道之所有符號對應於庫存資料段 A。若無線電不支援 5.3.2.3.1 所述數值集，則可將備用測試訊框用於較少數量之 PRB，且仍宜使用。

此測試之目的為確保無線電設備可使用本規範 5.3.2.1.1.3 的預設參數值（或類似的 3GPP 波形）傳輸基本 3GPP 測試訊框，但僅使用 1 支天線上之 1 個空間串流。此測試適用於 A 類及 B 類無線電（不需預編碼）。如 TM-FR1-TM1.1，此測試中之所有使用者資料均為零。

(b)測試進入準則

O-RU 必須支援本規範 5.3.2.1.1.1 之預設參數值。測試數值集為 30 kHz 子載波間隔及 100 MHz 頻寬，如 TM-FR1-TM1.1 所述。僅適用於 5G 新無線電。無線電必須具傳導天線埠（FR1）或 TAB 連接器。

O-RU 必須具 1 支傳導天線埠（或 TAB 連接器）以連接至信號分析儀。其亦需支援上述 5.3.2.1.1.1 定義之預設參數值。

(c) 試驗法

(1) 初始條件

組態設定 O-RU，包括收集 O-RU 能力，使用 M-Plane 命令組態設定 O-RU，進行操作及使用 G.8275.1 同步 O-RU。將信號分析儀連接至 O-RU 天線埠，並為分析儀組態設定所需之任何設置資訊，以使其能同步及解調變傳輸之信號。

(2) 程序

於 O-DU 模擬器中建構描述上述 NR-FR1-TM1.1 信號之適當 IQ 信號。使用 O-DU 模擬器控制介面，以建構描述信號之適當 C-Plane 訊息。每個符號均宜使用 section type 1 訊息，由單一 section（DL-SCH 及 DCI）描述。此測試不

使用 section type 0 訊息。將 IQ 資料封裝於 U-Plane 訊息中。將此等訊息播放至與 5.3.2.1.1.1 所述之時序窗口有關的 O-RU。依信號分析儀同步並允許其解調及解碼測試訊框所需，重複整個訊框數次。

(d)測試要求

(1)信號分析儀量測之信號宜滿足此無線電類別（即 EVM(Error Vector Magnitude)）之基本 3GPP 信號性能要求。

(2)信號分析儀接收之測試訊框宜與上述信號相同。若包含所有相同之 PRB 分配及所有零資料，則測試成功。

5.3.2.3.1.2 UC-Plane O-RU 情境類別擴充 3GPP DL-資源分配

(a)測試說明及適用性

此測試為 MANDATORY。

此測試之目的為確保無線電可準確地解譯 C-Plane 之資源分配訊息，將 U-Plane 資料傳輸至正確的資源區塊中，並於下行中準確地傳輸此資料。此測試適用於 A 類及 B 類無線電（不需預編碼）。測試以傳導方式，因此不會有通道失真或干擾。無線電必須通過此測試，始視為符合 O-RAN 要求。

針對 FDD 之標準 3GPP NR-FR1-TM1.1 測試訊框，使用 O-DU 模擬器（即 5.2.1 所述 TER 之 O-RAN 介面將產生 C-Plane 及 U-Plane 訊息，其需 O-RU 於下行傳輸 NR-FR1-TM1.1 標準信號。該信號如圖 7 所示：

3GPP NR-FR1-TM1.1 FDD 測試信號

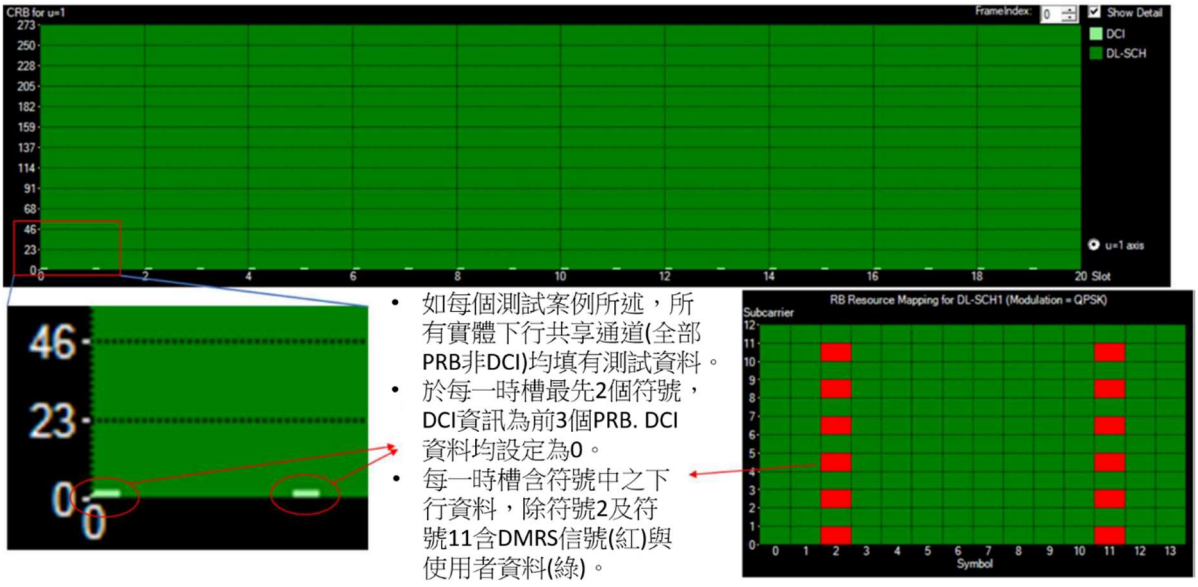


圖 7 NR-FR1-TM1.1 FDD 測試信號

此測試訊框包括由 3 個 PRB 組成之每個時槽前 2 個符號中的 PDCCH。訊框中所有剩餘之 PRB 均含實體下行共享通道資料。此測試需非零資料（PN23 序列）以填充所有分配之資源區塊。此組態於不含 PDCCH 通道之所有符號中對應於庫存資料段 A。

(b)測試進入準則

如 NR-FR1-TM1.1 所述，測試數值集為 30 kHz 子載波間隔及 100 MHz 頻寬。僅適用於 5G 新無線電。無線電必須具傳導天線埠（FR1）或 TAB 連接器。

(c) 試驗法

(1) 初始條件

組態設定 O-RU，包括收集 O-RU 能力，使用 M-Plane 命令組態設定 O-RU，以進行操作及使用 G.8275.1 同步 O-RU。將信號分析儀連接至 O-RU 天線埠，並為分析儀組態設定所需之任何設置資訊，以使其能同步及解調傳輸之信號。

(2) 程序

於 O-DU 模擬器中建構描述上述 NR-FR1-TM1.1 信號之適當 IQ 信號。使用 O-DU 模擬器控制介面，以建構描述信號之適當 C-Plane 訊息。每個符號均宜使用 section type 1 訊息，由單一 section（DL-SCH 及 DCI)描述。此等部分中之資料必須為 PN23 序列，並使用全為 1 之初始種子。此測試不使用 section type 0 訊息。將 IQ 資料封裝於 U-Plane 訊息中。將此等訊息播放到與 5.3.2.1.1.1 所述之時序窗口有關的 O-RU。依信號分析儀同步並允許其解調及解碼測試訊框所需，重複整個訊框數次。

(d)測試要求

(1)信號分析儀量測之信號宜符合此無線電類別（即 EVM(Error Vector Magnitude)）之基本 3GPP 信號性能要求。

(2)信號分析儀接收之測試訊框宜與上述信號相同。若包含所有相同之 PRB 分配及資料，則測試成功。

5.3.2.3.1.3 UC-Plane O-RU 基本類別 FDD 測試 UL

(a)測試說明及適用性

此測試為 MANDATORY。

此測試之目的為確保無線電能符合 O-RAN 前傳最基本的上行要求，以正確解譯 C-Plane 訊息，並自 RF 信號正確構造上行 U-Plane 訊息。後續之測試將以此為基礎行使前傳之其他能力。

此測試確證使用傳導接收器特性測試部分[15]第 7 節之 3GPP 參考靈敏度位準定義[16]之 7.2 所述之參考靈敏度功率位準至少 30 dB 以上，來確證 O-RU 之上行操作正確。此為提高所有無線電將正確接收所有資料之可能性，本節的測試精神非確證測試接收機的靈敏度，主要確證對 O-RAN 協定之合規性。

3GPP G-FR1-A5-1 上行 FDD 測試信號

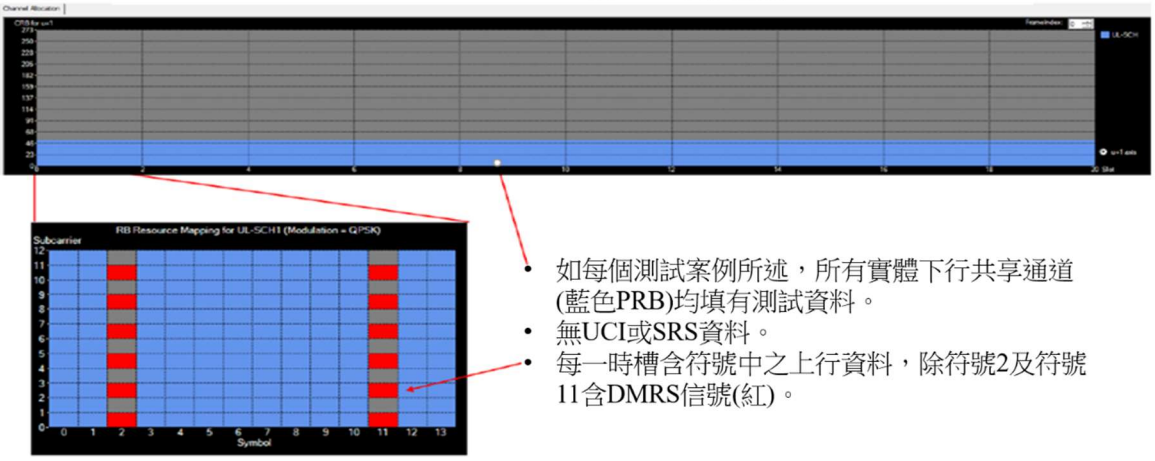


圖 8 G-FR1-A5-1 上行 FDD 測試信號

該信號於[16] 之表 A.1-1 描述，並參照 G-FR1-A1-5，其功率增加至表 7.2.5-1 所述之 30dB 以上。於此等條件下，符合 3GPP 之 O-RU 宣傳送與上行信號匹配之上行 U-Plane 資訊。

TER 於天線連接器或 TAB 連接器上產生上行信號，同時於前傳介面上產生相應之 C-Plane 訊息。

TER 將捕獲 DUT 產生之 U-Plane 訊息，並確證酬載是否與上行信號匹配。

(b)測試進入準則

O-RU 必須支援本規範 5.3.2.1.1.1 之預設參數值。測試數值集為 30 kHz 子載波間隔及 100 MHz 頻寬，如[16]之 G-FR1-A-5 所述。僅適用於 5G 新無線電。無線電必須具傳導之天線埠（FR1）或 TAB 連接器。注意，若無線電不支援此測試中使用之數值集及頻寬，則可將該信號變更為[16]之表 A.1-1 的任何 3GPP 靈敏度測試信號。若無線電支援該數值集及頻寬，則將使用本節描述之測試信號。

(c) 試驗法

利用上行信號眾所周知之酬載（PN23 序列）與於 O-RAN 介面上傳送之信號酬載進行比較。自 U-Plane 訊息中提取 IQ 資訊，並將其解調以檢索酬載。

(1) 初始條件

組態設定 O-RU，包括收集 O-RU 能力，使用 M-Plane 命令組態設定 O-RU，以進行操作及使用 G.8275.1 同步 O-RU。將信號源連接至 O-RU 天線埠，並組態設定此信號源，以便自 CUSM-E 接收觸發信號後，傳輸所需之 3GPP 測試信號。

信號源功率位準宜至少調整至比 3GPP 接收機靈敏度測試中使用之設置高 30 dB。

(2) 程序

(2.1) 於 RF 信號源上加載上行測試波形（G-FR1-A1-5：SCS30k_51RB）。

(2.2) 將信號源組態設定為當自 O-DU 模擬器接收已發送 C-Plane 訊息之觸發信號時，始於 10ms 訊框邊界上播放測試波形。

(2.3) 將 C-Plane 訊息序列加載至測試設備 O-RU（TER）上。

(2.4) 設定測試設備 O-RU（TER），以捕獲 DUT 前傳訊息。

(2.5)發送 C-Plane 訊息，以遵守時序窗口後，再啟動測試以播放 RF 上行訊框。

(2.6)記錄源自 DUT 之 U-Plane 訊息，以獲得完整之訊框，以及與天線埠相對應之 eAxC(extended antenna carrier)。

(2.7)提取 IQ 資訊。

(2.8)提取酬載。

(2.9)比較酬載二進制序列。

(d)測試要求

(1) 若酬載二進制序列於發送至 DUT 之上行測試訊框與自 DUT 接收之 U-Plane 資料間匹配，則判定為“測試成功”

(2) 若任一測試條件不成立，則整個測試之判定為“測試失敗”

5.3.2.3.1.4 UC-Plane O-RU 情境類別擴充使用 RB 參數 3GPP DL-資源分配

(a)測試說明及適用性

此測試為 MANDATORY。

此測試之目的為確保無線電能準確地解譯具 rb 參數集之 C-Plane 資源分配訊息，將 U-Plane 資料傳輸至正確之資源區塊中，並於下行準確地傳輸此資料。本測試適用於 A 類及 B 類無線電（不需預編碼）。測試以傳導方式，因此不會有通道失真或干擾。無線電必須通過此測試，始視為符合 O-RAN 要求。

針對 FDD 之標準 3GPP NR-FR1-TM1.1 測試訊框，使用 O-DU 模擬器（即 5.2.1 所述 TER 之 O-RAN 介面）將產生 C-Plane 及 U-Plane 訊息，其需要 O-RU 於下行傳輸 NR-FR1-TM1.1 標準信號。該信號如圖 9 所示：

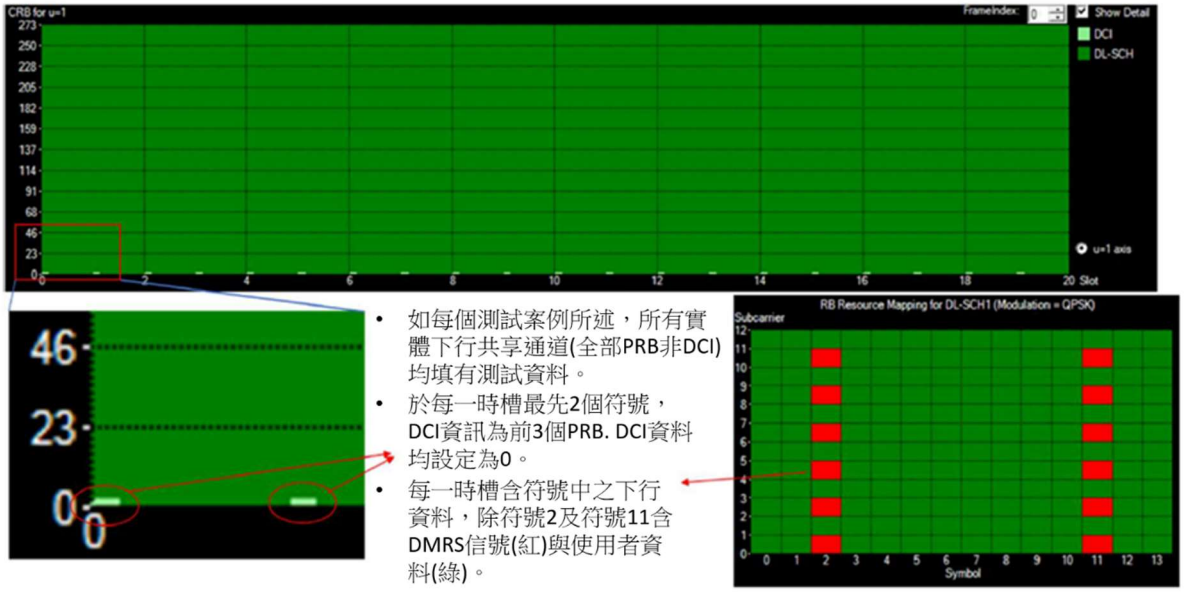


圖 9 NR-FR1-TM1.1 FDD 測試信號

本測試訊框包括由 3 個 PRB 組成之每個時槽前 2 個符號中的 PDCCH。訊框中所有其餘 PRB 均包含實體下行共享通道資料。

此測試需要非零資料，以填充所有分配之資源區塊。

(b)測試進入準則

O-RU 必須支援 5.3.2.1.1.1 之預設參數值，測試數值集為 30 kHz 子載波間隔及 100 MHz 頻寬，如 NR-FR1-TM1.1 所述。 限用於 5G 新無線電。無線電必須具傳導天線埠 (FR1) 或 TAB 連接器， 信號分析儀必須具解碼下行共享通道之能力。

(c) 試驗法

(1) 初始條件

組態設定 O-RU，包括收集 O-RU 能力，組態設定 O-RU 以使用 M-Plane 命令操作，並以 G.8275.1 同步 O-RU。將信號分析儀連接至 O-RU 天線埠，並使用所需之任何設置資訊，以組態設定分析儀，使其同步及解調傳輸之信號。

(2) 程序

於 O-DU 模擬器中建構描述上述 NR-FR1-TM1.1 信號之適當 IQ 信號，使用 O-DU 模擬器控制介面建構描述信號的適當 C-Plane 訊息。每個分配之符號都，宜使用 section type 1 訊息， 由 sections（DL-SCH 及 DCI）描述。

各時槽之符號 #3 宜為上述 3.2.1.1.5 所示之庫存資料 section type 6 “D” 。 符號 #3 之控制平面僅包括 PRB 編號 5 至 編號 23。C-Plane 訊息之 rb 位元集於本節中設置為 1， 所有其他 DL-SCH 符號及除 PRB 5 至 PRB 23 外的所有其他 PRB 將不含資料。有 2 種方法可執行測試：

(2.1) 傳送含 rb 位元集之單一資料段及發送的 PN23 序列，如圖 10 所示：

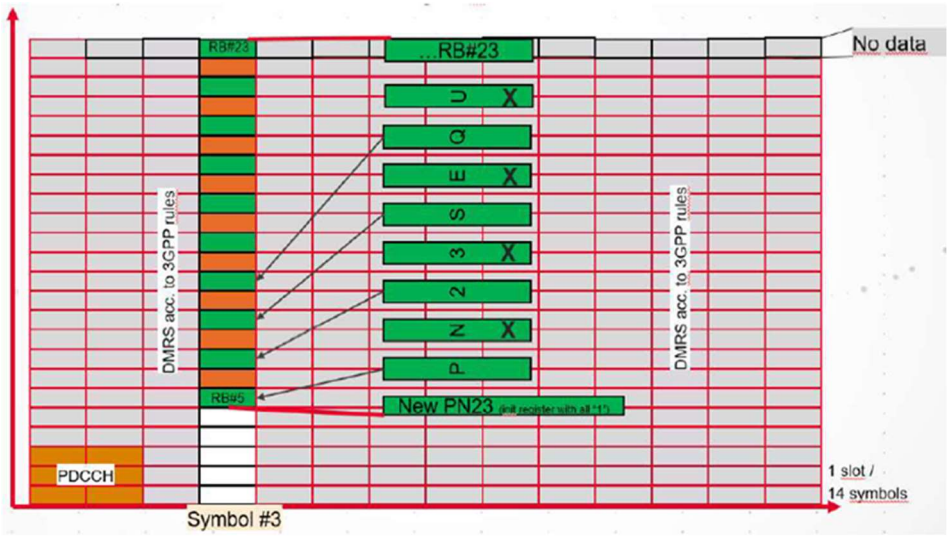


圖 10 含 rb 位元集之單一資料段及發送之 PN23 序列

啟動 1 個新 PN23 序列，但每隔 1 個 PRB 僅含 PN23 序列之奇數部分（如綠色所示）。其他 PRB（如橙色所示）將不含資料，且不會發送至 O-RU。因此，將使用單一資料段，及相應之 U-plane 訊息將僅包含如上所示奇數 PRB 的資料。PN23 序列之未使用部分（以 X 標記顯示）將被捨棄。

(2.2) 2 個資料段，1 個包含 PN23 序列之奇數部分，另一個包含偶數部分，如圖 11：

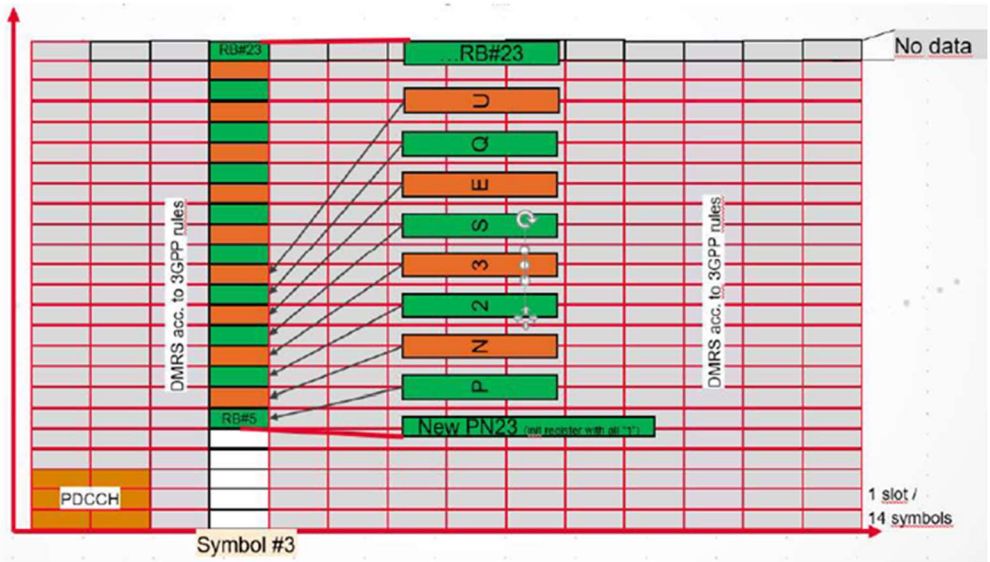


圖 11 資料段含 PN23 序列之奇數及偶數部分

將開始 1 個新 PN23 序列，但第一個區段之每一其他 PRB 將僅含 PN23 序列之偶數部分。第二個區段之 C-Plane 訊息均將使用 rb 位元集。對應於第一個資料段之 U-Plane 訊息將僅含 PN23 序列之奇數部分，對應於第二個資料段之 U-Plane 訊息將僅含偶數部分。因此，連續之 PN23 序列

將僅於 PRB 5 至 PRB 23 中發送。

宜包括附加區段以描述 DCI 符號及 TS [16]所述之參考信號。將此等訊息播放至 O-RU 及 5.3.2.1.1.1 所述之時序窗口。將整個訊框重複同步信號分析儀，並允許其解調及解碼測試訊框所需之次數。

(d)測試要求

(1) 信號分析儀量測之信號宜滿足該無線電類別（即 EVM）的基本 3GPP 信號性能要求。

(2) 若使用選項#1 進行測試，則信號分析儀接收之測試訊框，宜僅含符號#3 PRB 5 至 PRB 23 中每隔一個 PRB 中之 PN23 序列資料。

(3) 若使用選項#2 進行測試，則信號分析儀接收之測試訊框，宜僅含符號#3 PRB 5 至 PRB 23 中每個 PRB 中之 PN23 序列資料。

5.3.2.3.1.5 UC Plane O-RU 情境類別擴充使用 RB 參數 3GPP UL-資源分配

(a) 測試說明及適用性

此測試為 MANDATORY。

此測試於基本上行測試中增加解譯 rb 參數之能力。

使用傳導接收器特性測試部分（[19] 第 7 節）之 3GPP 參考靈敏度位準定義（[16]之 7.2 ），確證 O-RU 正確之上行操作及功率位準至少高於[16]表 7.2.5-1 中所描述的參考靈敏度功率位準 30 dB。此為提高無線電正確接收所有資料之可能性，本節之測試精神非確證測試接收機的靈敏度，主要確證對 O-RAN 協定的符合性。

SCS15k_25RB 上行 FDD 測試信號

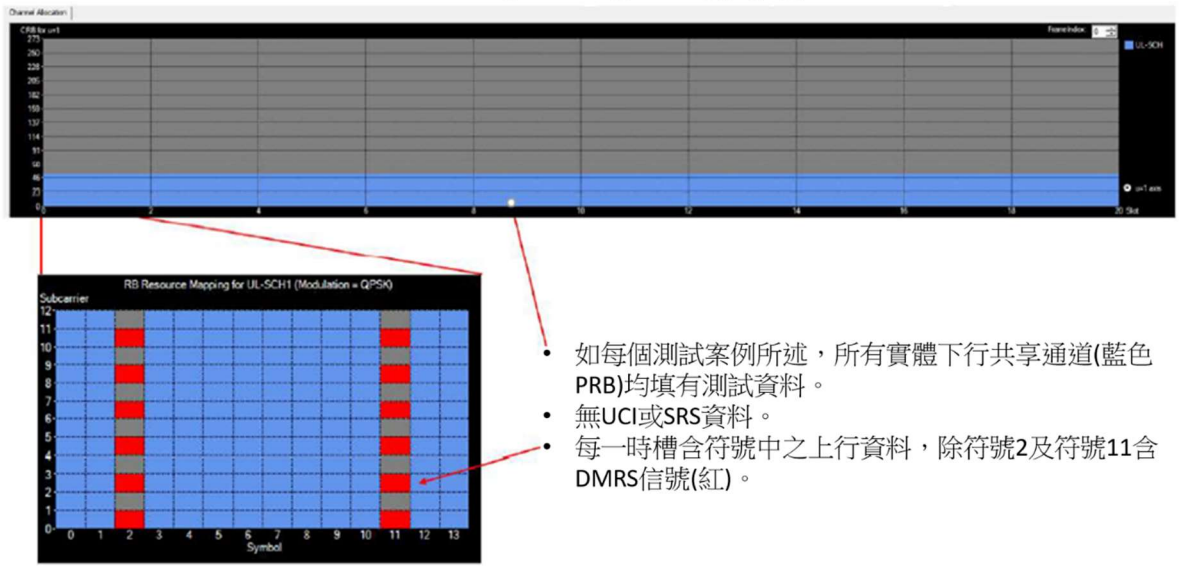


圖 12 SCS15k_25RB 上行 FDD 測試信號

使用 RF 源，測試設備將產生 3GPP 測試信號，如圖 12 所示。

無線電將解調及解碼此信號，並依 O-DU 模擬器使用上行 C-Plane 訊息之指示，將頻域 IQ 發送至 O-DU-模擬器。

TER（測試設備，O-RU）於天線連接器或 TAB 連接器上產生上行信號，同時於前傳介面上產生相應之 C-Plane 訊息。

TER 將捕獲 DUT 產生之 U-Plane 訊息，並確證酬載是否與上行信號匹配。

(b)測試進入準則

O-RU 必須支援本規範 5.3.2.1.1.1 之預設參數值。測試數值集為 30 kHz 子載波間隔及 100 MHz 頻寬，如[16]之 G-FR1-A-1 中所述。僅適用於 5G 新無線電。無線電必須具傳導天線埠 (FR1) 或 TAB 連接器，無線電必須報告其支援 rb 參數。注意若無線電不支援此測試中使用之數值集及頻寬，此信號可能變更為[16]表 A.1-1 中之任一 3GPP 靈敏度測試信號。而若無線電支援該數值集及頻寬，則將使用本節描述之測試信號。

(c) 試驗法

利用上行信號眾所周知之酬載（虛擬隨機序列），將其與於 O-RAN 介面上通信之信號的酬載進行比較。從 U-Plane 訊息中提取 IQ 資訊並解調以檢索提取酬載。

(1) 初始條件

組態設定 O-RU，包括收集 O-RU 能力，使用 M-Plane 命令組態設定 O-RU 以進行操作，以及使用 G.8275.1 同步 O-RU。 將信號源連接至 O-RU 天線埠，並組態設定信號源於接收到自 CUSM-E 之觸發信號時，傳輸所需的 3GPP 測試信號。

信號源功率位準宜至少調整至比 3GPP 接收機靈敏度測試中使用之設置高 30 dB。

(2) 程序

(2.1) 於 RF 信號源上加載上行測試波形（G-FR1-A1-5：SCS30k_51RB）。

注意此信號有 1 個 PN23 序列作為使用者資料。

(2.2) 將信號源組態設定為自 O-DU 模擬器接收 C-Plane 訊息已發送之觸發信號時，始於 10ms 訊框邊界播放測試波形。

(2.3) 於測試設備 O-RU (TER) 上加載 C-Plane 訊息序列—於此測試中，將僅使用符號編號 6，且將使用所有 51 個 PRB 。除可用於同步測試設備所需之 DRMS 信號外，所有其他符號將不含資料。進行此測試有 2 種選擇：

(2.3.1)傳送含 rb 位元集之單一資料段及發送之 PN23 序列，如圖 13 所示：

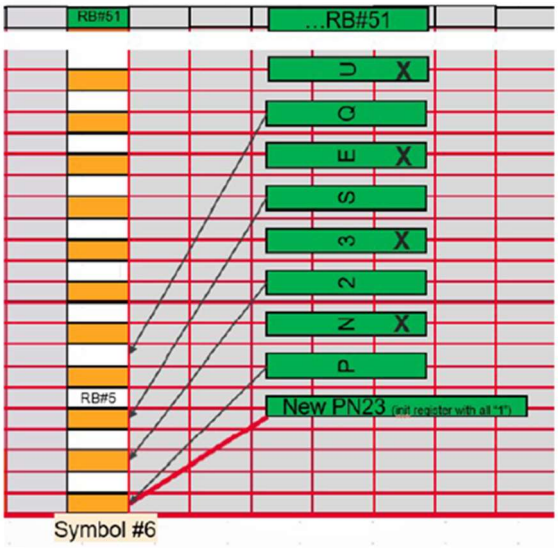


圖 13　含 rb 位元集之單一資料段及發送的 PN23 序列

將啟動 1 個新 PN23 序列，但每隔 1 個 PRB 將僅含 PN23 序列之奇數部分（如橙色所示）。其他 PRB（如白色所示）將不含資料，且不會發送至 O-RU。因此，將使用單一資料段，且相應之 U-Plane 訊息將僅包含如上所示的奇數 PRB。PN23 序列中未使用之部分（顯示為標記 X) 將被捨棄。

(2.3.2）2 個資料段，1 個含 PN23 序列之奇數部分，另一個含偶數部分，如圖 14 所示：

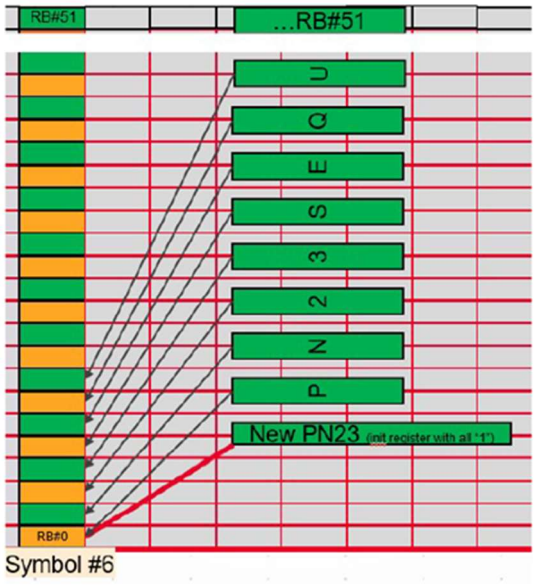


圖 14　含奇數及偶數部分之 PN23 序列

將啟動 1 個新 PN23 序列，但 1 個區段中之其他每個 PRB 將僅含 PN23 序列的奇數部分（如綠色所示）。

第二個資料段將包含 PN23 序列之偶數部分。這 2 個部分之 C-Plane 訊息將使用 rb 位元集。對應於第一個資料段之 U-Plane 訊息將僅包含 PN23 序列奇數部分，第二個資料段對應之 U-Plane 訊息將僅包含偶數部分。因此，一個連續之 PN23 序列將僅於 PRB 0-至 PRB 51 中發送。

(2.3.2.1) 設定測試設備 O-RU (TER)， 以捕獲 DUT 前傳訊息

(2.3.2.2) 啟動測試以播放 C-Plane 訊息並觸發信號源於訊框邊界上播放 RF 信號

(2.3.2.3) 記錄源自 DUT 之 U-Plane 訊息的完整訊框及對應於天線埠的 eAxC

(2.3.2.4) 提取 IQ 資訊

(2.3.2.5) 提取酬載

(2.3.2.6) 比較酬載二進制序列

(d) 測試要求

(1)若酬載二進制序列於發送至 DUT 之上行測試訊框與自 DUT 接收的 U-Plane 資料間匹配，則判定為“測試成功”。特別是符號#6 宜含 PN23 序列之每一間格 PRB 或 PRB 0 至 PRB 51 中的連續 PN23 序列，取決於所選擇的測試選項。

(2)若任一個測試條件不成立，則整個測試之判定為“測試失敗”

5.3.2.3.2 UC-Plane O-RU 情境類別延遲管理(DLM)

本節描述 O-RU 延遲管理之符合性測試。

測試案例之測試設置如 5.2.1。

執行情境類別延遲管理之符合性測試案例時，使用哪種時序方法並不重要。不同時序方法描述於 CUS 規範[20] 2.3.2、2.3.3、2.3.4 及 2.3.5。

延遲管理下行測試將測試 O-RU 於各自接收窗口之末端接收 C-Plane 及 U-Plane 訊息時，是否能準確傳輸資料。上行測試將測試當 CUSM-E 於正確之上行接收窗口內傳輸上行 C-Plane 訊息時，O-RU 是否能準確將接收之資料傳輸至 CUSM-E。並測試 O-RU 是否於正確之接收窗口內發送其 U-Plane 訊息。

圖 15 顯示下行 C-Plane 及 U-Plane 訊息之簡化時序關係。

O-RU C-plane 接收窗口大小為： (T2a_max_up +Tcp_adv_dl) – (T2a_min_up +Tcp_adv_dl) = C-Plane reception window。起始點 (before t=0)為： T2a_max_up + Tcp_adv_dl = start of C-Plane 傳輸窗口。

使用者平面接收窗口大小為： T2a_max_up - T2a_min_up。起始點 (before t=0)為 T2a_max_up。

舉例，若 T2a_max_up = 264 µs、Tcp_adv_dl = 63 µs、T2a_min_up = 53 µs，C-Plane 接收窗口大小則為 211 µs， 若 C-plane 傳輸窗口起始為 327 µs， U-plane 接收窗口則為 211 µs 及 U-plane 傳輸窗口起始為 264 µs。

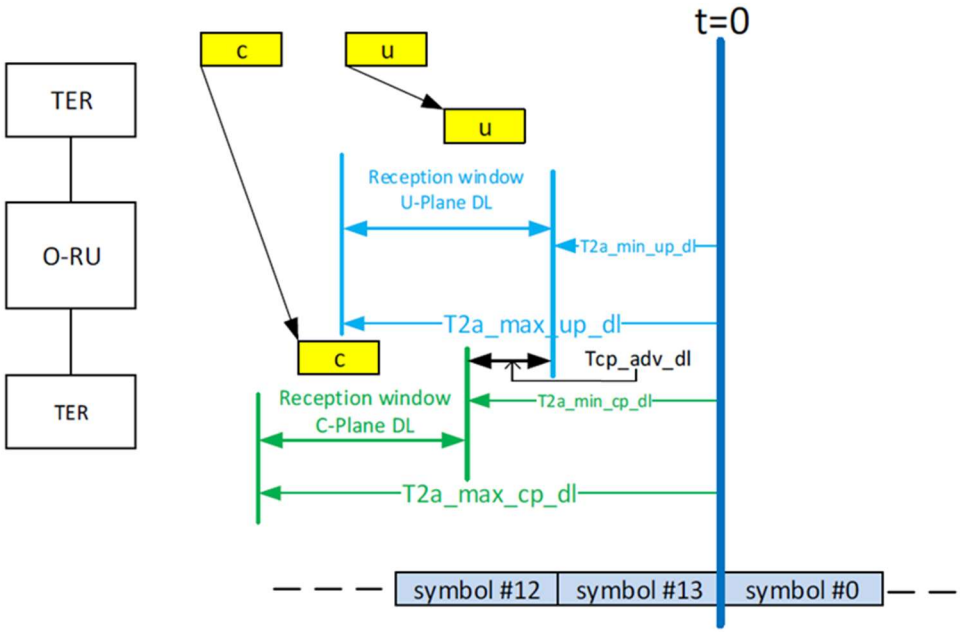


圖 15　下行之簡化時序

O-RU 延遲管理上行測試案例，若測試 C-Plane 前傳訊息 1 於各自接收窗口中被接收，則相應之 U-Plane 訊息將於 O-RU 的傳輸窗口中發送。

圖 16 顯示上行 C-Plane 及 U-Plane 訊息之簡化時序關係。

類似於下行案例， C-plane 接收窗口大小為 T2a_max_cp_ul - T2a_min_cp_ul， C-Plane 接收窗口起始點 (before t=0)為 T2a_max_cp_ul。U-Plane 傳輸窗口大小為： Ta3_max_up - Ta3_min_up。起始點 (after t=0) 為 Ta3_min_up。

若依與下行案例相同之範例值，C-Plane 接收窗口為 211 µs，C-Plane 接收窗口起始點則為 274 µs，U-Plane 傳輸窗口為 70 µs，U-Plane 傳輸窗口起始點則為 20 µs。

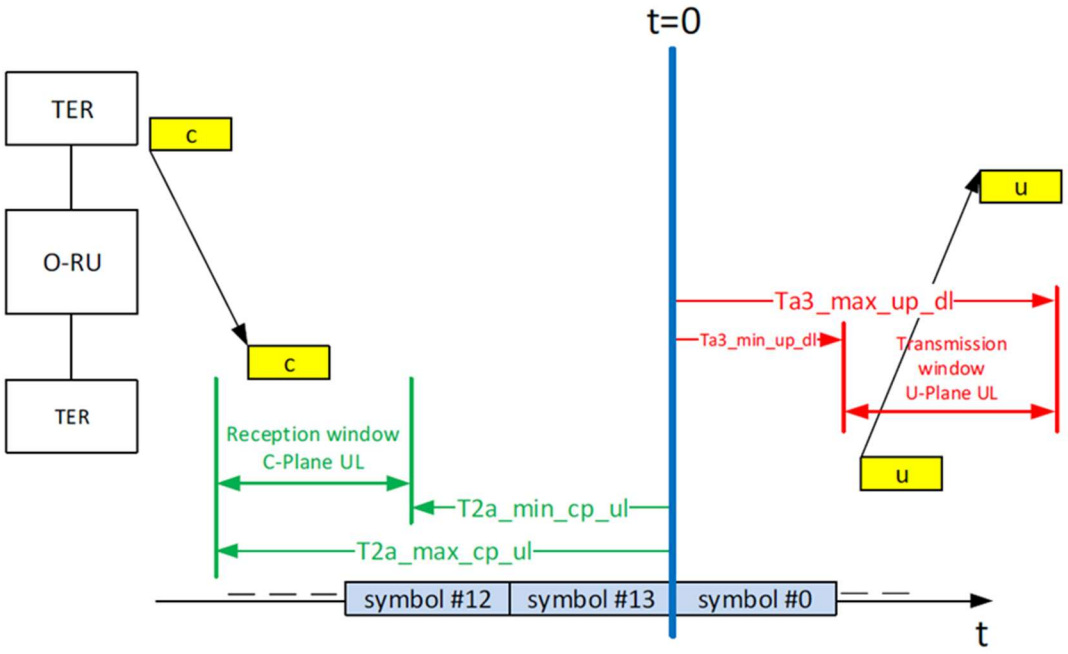


圖 16　上行之簡化時序

下行測試使用之測試訊框為(預設)3GPP NR-FR1-TM1.1 FDD 信號，如圖 17。若無線電不支援此信號，則可替換為無線電支援之 3GPP 測試波形，但每個時槽至少有 1 個符號以測試流量。

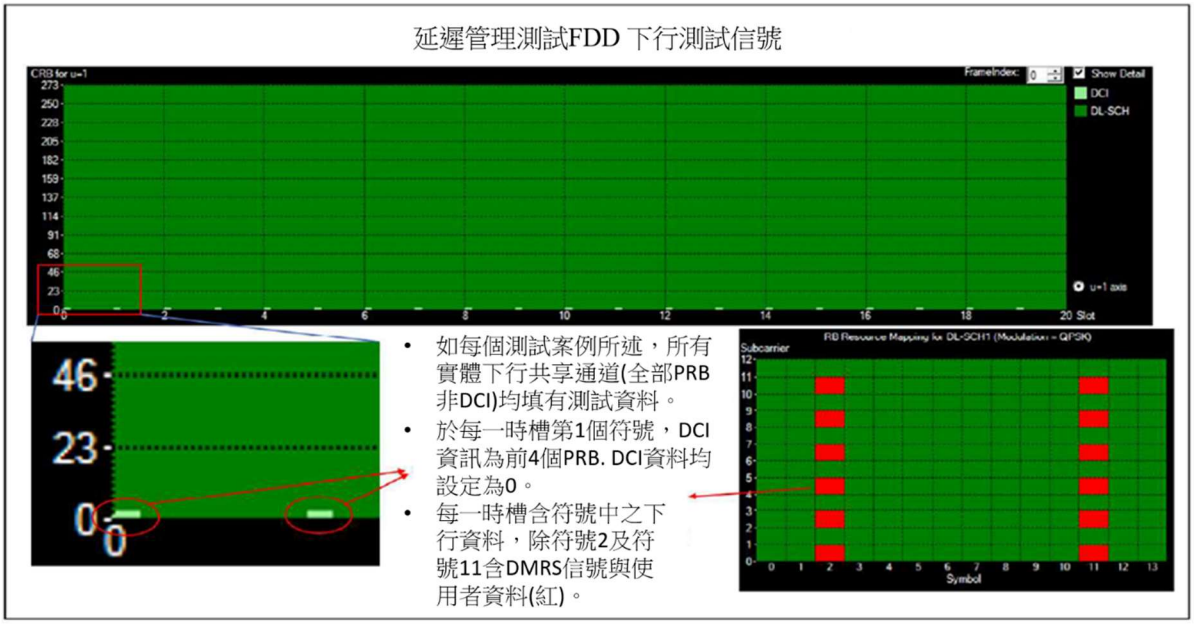


圖 17 延遲管理測試 FDD 下行測試信號

Figure 3.2.3.4-3 FDD Downlink Test Signal for Delay Management Tests

上行測試使用之測試訊框為(預設)3GPP G-FR1-A5-1 FDD 信號，如圖 18。若無線電不支援此信號，則可替換為無線電支援之 3GPP 測試波形，但每個時槽至少有 1 個符號以測試流量。

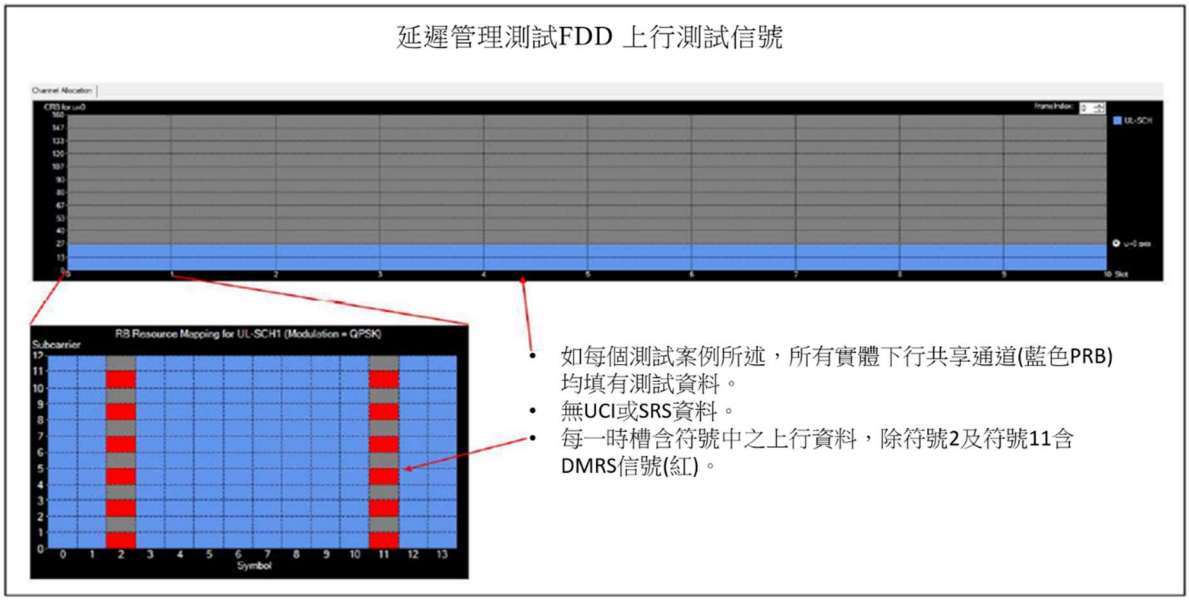


圖 18 延遲管理測試 FDD 上行測試信號

5.3.2.3.2.1 UC-Plane O-RU 情境類別 DLM Test #1：下行 1-正測試

(a) 測試說明及適用性

此測試為 MANDATORY。

當於 O-RU 之接收窗口中接收 C-Plane 及 U-Plane 訊息時，本測試案例將確證空中介面之時序是否符合 CUS 規範中規定的要求。

當預期結果為正面時，可執行 4 個不同之下行測試案例，即 O-RU 必須能於空中介面上傳輸接收之 U-Plane 資料，如圖 19 所示。此等測試中，取決於無線電之能力，C-Plane 接收窗口可能適用於時槽或符號邊界。亦即，於某些無線電中，C-Plane 接收窗口位於每個時槽之開始，且所有 C-Plane 訊息均將於該窗口內一次發送。其他無線電將要求於每個符號之接收窗口中發送 C-Plane 訊息。於所有情況下，無論無線電是否具足夠大之緩衝區存儲多個符號之 U-Plane 資料，均會於與每個符號相對應之接收窗口中發送 U-Plane 訊息。

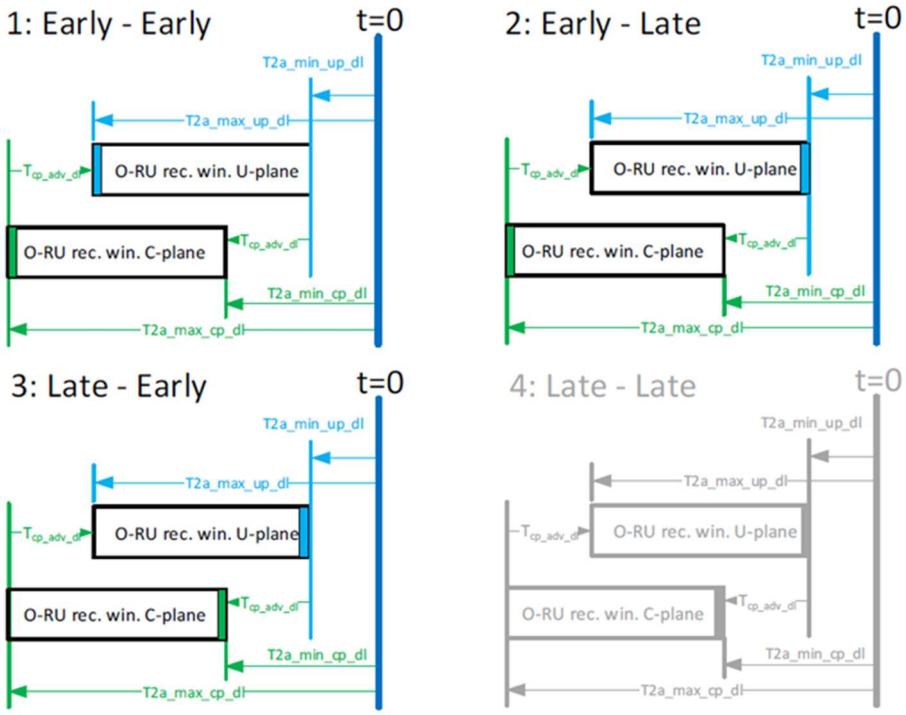


圖 19 下行正測試案例

案例 1 “C-Plane Early–– U-Plane Early”; O-RU 於 C-Plane 訊息之接收窗口開始時接收 C-Plane 訊息（圖中以綠色小框指示）。於 U-Plane 訊息之接收窗口開始時接收相應的 U-Plane 資料 （圖中以藍色小框指示），即 Tcp_adv_dl later。

案例 2 “C-Plane Early-U-Plane Late”; O-RU 於 C-Plane 訊息之接收窗口開始時接收 C-Plane 訊息。於 C-Plane 訊息後，相應之 U-Plane 資料接收最早的 Tcp_adv_dl（即於 U-Plane 接收窗口之末端）。

案例 3 “C-Plane Late –U-Plane Early”; O-RU 於 C-Plane 訊息之接收窗口末端接收 C-Plane 訊息，。於 C-Plane 訊息後，相應之 U-Plane 資料接收最早的

Tcp_adv_dl，即於接收窗口之末端。

案例 4 “C-Plane Late –U-Plane Late”; 此案例於圖中顯示為灰色，因實際上與案例 3 相同之情況下，不可比於案例 3 中較遲接收 U-Plane 訊息。

(b)測試進入準則

O-RU 必須具 1 個傳導天線埠（或 TAB 連接器），以連接至信號分析儀。接收窗口將由 CUSM-E 依 M-Plane 無線電報告之延遲參數進行計算及使用。

(c) 試驗法

(1)初始條件

組態設定 O-RU，包括收集 O-RU 能力，組態設定 O-RU 以使用 M-Plane 命令進行操作，並使用 G.8275.1 同步 O-RU。將 RF 信號分析儀連接至 O-RU 天線埠，確定無線電宣告正確接收窗口，以支援使用無線電重新供電之延遲管理參數。

(2) 程序

組態設定 CUSM-E 發送 C-Plane 及 U-Plane 訊息，以便依圖 19 中描述之 3 種情況（1 至 3）於各 Plane 之接收窗口內接收此等訊息。

備考：確保 C-Plane 訊息至少接收 Tcp_adv_dl earlier，然後 O-RU 再對應 U-Plane 訊息。

於 RF 信號分析儀上觀察接收之信號，並比較所選信號上的解碼資料至該符號之發送 PN23 序列。

(d)測試要求

若接收之資料與傳輸的資料匹配，則測試成功。

5.3.2.3.2.2 UC-Plane O-RU 情境類別 DLM Test #2：上行-正測試

(a)測試說明及適用性

此測試為 MANDATORY。

此測試案例將確證上行方向上之 U-Plane 資料，藉由 O-RU 正確傳輸至傳輸窗口內， CUSM-E 將於無線電使用 M-Plane 指定之 C-Plane 接收窗口（2 次測試）兩端發送 C-Plane 訊息，。C-Plane 訊息將描述如上所示之一個測試訊框。該訊框於每個時槽中將有 1 個指定之符號（不含 DMRS 資訊）。C-Plane 訊息將要求無線電自每個時槽發送該符號之資料。

發送正確之 C-Plane 訊息後，CUSM-E 將觸發信號產生器發送有效之測試信號至無線電之 RF 埠。該信號將於由 C-Plane 訊息指定之同一符號中（每個時槽）包含 1 個已知的新 PN23 序列。

此等上行測試案例之正測試結果，對特定 C-Plane 訊息之相應 U-Plane 資料於 O-RU 的傳輸窗口內傳輸。若於 O-RU 之傳輸窗口內接收 C-Plane 訊息，則~~在~~於 O-RU 之傳輸窗口中傳輸該訊息，如圖 20 所示。

資料將藉由外部信號產生器傳輸至無線電，且上行信號將如上所述。信號產生

器發送之測試資料將於各時槽之 1 個符號中，包含 1 個已知的新 PN23 序列。CUSM-E 將期望接收與各時槽中正確符號相同之資料。

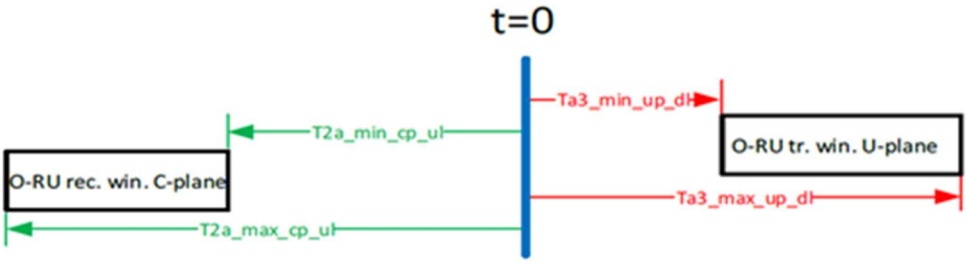


圖 20　C-Plane 與 U-Plane 訊息間之關係

上行案例可識別 2 種不同測試案例。於接收窗口之開始或接收窗口之末端接收 C-Plane 訊息。此等測試案例，如圖 21 所示:

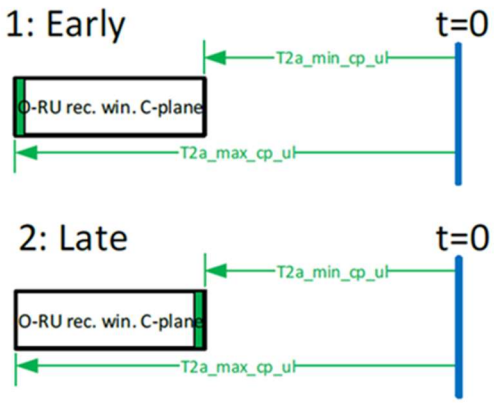


圖 21　早與晚 C-Plane 訊息測試案例

案例 1 “Early”; O- RU 於 C-Plane 訊息接收窗口開始時，接收 C-Plane 訊息（圖中以綠色小框指示）。

案例 2 “Late”; O-RU 於 C-Plane 訊息接收窗口結束時，接收 C-Plane 訊息。

(b)測試進入準則

O-RU 必須具傳導天線埠（或 TAB 連接器），以連接至信號分析儀。

(c) 試驗法

(1)初始條件

組態設定 O-RU，包括收集 O-RU 能力，組態設定 O-RU 使用 M-Plane 命令，並使用 G.8275.1 同步 O-RU。將 RF 信號產生器連接至 O-RU 天線埠。

(2) 程序

組態設定 CUSM-E 發送 C-Plane，以便此等訊息依圖 21 中描述之 2 種情況（1 至 2），於接收窗口內接收。發送此等訊息後，將觸發信號發送至信號產生器，指示其於 t = 0 時，發送正確之 RF 測試訊框。

如 M-Plane 上無線電所述之上行傳輸期間，CUSM 宜於前傳介面上接收 U-Plane 訊息。

(d) 測試要求

若於正確時間窗口內，CUSM-E 接收正確資料，則通過測試案例。

6. 互運性測試

6.1 概述

本節依 O-RAN WG8: Stack Reference Design Workgroup 公布 Stack Interoperability Test Specification 訂定互運性之測試要求。

本節參考[21]，規定於獨立組網(SA)模式下，O-RAN O-CU 及 O-DU 部署情境與其他 O-RAN 元件互運性測試之要求、條件、組態、資料檔及序列。

以下介面(邏輯或實體)適用於 IOT 測試案例。

(a) RLC-MAC

(b) L1-L2

(c) RRC-SDAP

(d) SDAP-PDCP

(e) RRC-PDCP

6.1.1 假設

本測試規範目前版本，採用以下假設：

(a) 假設 F1 介面符合 3GPP 版本規範[11][22][23][24]。

(b) O-CU 及 O-DU 符合相同版本之 O-RAN 軟體架構規範[25]。

互運性測試及支援測試環境中所有元素，符合相同版本之 3GPP 規範，若 3GPP 適用。

表 3 互運性測試總表

測試案例 (O-RAN 參考 #節次)	測試案例 (第 10-2 部測試規範參考 #節次)	模組名稱	測試案例
3.2	6.2.4	O-CU、O-DU	細胞設置
3.3	6.2.5	O-C、O-DU	SystemInformation-MIB
3.4	6.2.6	O-CU、O-DU	SystemInformation-SIB1
3.5	6.2.7	O-CU、O-DU	SystemInformation-SIB2
3.6	6.2.8	O-CU、O-DU	SystemInformation-SIB3
3.7	6.2.9	O-CU、O-DU	PDU 會談建立程序

3.11	6.2.10	O-CU、O-DU	PDU 多方會談修正
3.12	6.2.11	O-CU、O-DU	閒置模式呼叫及服務請求程序
3.13	6.2.12	O-CU、O-DU	下行 UDP 資料傳送
3.14	6.2.13	O-CU、O-DU	上行 UDP 資料傳送
3.15	6.2.14	O-CU、O-DU	雙向 UDP 資料傳送

6.1.2 一般測試條件及聲明

本規範中，考量實際硬體(參照附錄 A)及模擬環境中之情境。設定參數定義依[25]及 3GPP 文件，確證測試應以此等參數執行。

6.2 測試組態標準

執行互運性測試，以確證 O-CU 軟體是否可與 O-DU 軟體及系統組件交互運作，訊息流及訊息元素應依 3GPP 及 O-RAN 之軟體架構[25]。

6.2.1 DUT

O-DU 及 O-CU 為 DUT 之實體組件，其他網路元件，如 O-RU，可為實際的硬體，或依測試要求模擬之工具。於某些測試案例中，O-DU 或 O-CU 可為模擬之工具。

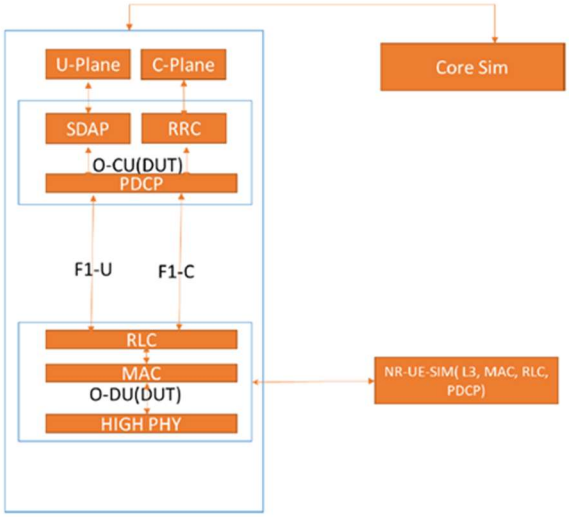


圖 22 DUT 組態

6.2.2 測試工具

於所有測試案例，O-RU 可為實際或模擬之工具。 於某些測試案例，O-DU 或 O-CU 可為模擬之工具。

6.2.3 時間同步

除非另有說明，否則 O-DU 及 O-RU 組件需與通用系統時間及主時間源同步。

6.2.4 細胞設置

測試目的

此測試案例之目的為解釋分別啟動 O-DU 及 O-CU 時之細胞設置。

參考要求

有關詳細之要求，參照[25]之 7.2 及 8.1.3。

初始條件

以下為本測試之先決條件。

(a) 使用預設之 O-CU 組態檔，以組態設定 O-CU 中所有模組(NR RRC、NR PDCP 及 SDAP)。

(b) 使用預設之 O-DU 組態檔，以組態設定 O-DU。

(c) O-RU 連線至 O-DU(選用)。

(d) O-CU 連線至 O-DU。

(e) O-CU 透過 NG 介面連接至 5GC，且 O-CU 為運行中。

(f) 可使用 YANG 資料模型或靜態組態檔，以組態設定 O-CU 及 O-DU。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試可支援 NR 之 UE 模擬器。

(2) 支援 N1、N2 及 HTTP 訊息所使用之 5G 核心或 CN 模擬器。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 有關測試設置之詳細資訊，參照 A.1。

(2) 測試剖繪檔 2，參照附錄 B 測試剖繪檔 B.2。

測試程序

以下表 4 說明細胞設置之測試程序：

表 4 細胞設置

St.	程序	訊息流	預期輸出
1	O-DU 發送 F1 SETUP REQUEST，以建立 O-DU 與 O-CU 間之連線。	**O-DU→O-CU**	查證 O-DU 向 O-CU-CP(控制單元)發送 F1 SETUP REQUEST，其中包含[25] 之 4.1.5.1.2 提到之所有強制性 IE。

2	O-CU 向 AMF 發送 NGAP SETUP REQUEST。	**O-CU→AMF**	查證 NGAP SETUP REQUEST 宜包含 3GPP 規範[27]之 9.2.6.1 提到之所有強制性 IE。
3	O-CU 自 AMF 接收 NGAP SETUP RESPONSE。	**O-CU←AMF**	查證 AMF 發送 NGAP SETUP RESPONSE，其中包含 3GPP 規範[27]之 9.2.6.1 提到之所有強制性 IE。
4	O-DU 自 O-CU 接收 F1 SETUP RESPONSE。	**O-DU←O-CU**	查證 O-CU 向 O-DU 發送 F1 SETUP RESPONSE，其中包含[26]之 4.1.5.1.2 提到的所有強制性 IE。
5	使用適當命令於 O-CU 新增服務細胞。使用 CLI 發送命令至 O-CU。	**O-DU←O-CU**	O-CU 向 O-DU 發送 F1AP gNB-DU CONFIGURATION UPDATE。 O-CU sends the F1AP gNB-DU configuration update to O-DU. F1AP gNB-CU CONFIGURATION UPDATE 宜包含[26]之 4.1.6.1.2.1 提到之所有強制性 IE。 O-DU 宜依 IE Served-Cells-To-Add-List 新增細胞資訊。
6	O-DU 向 O-DU 發送 gNB-DU CONFIGURATION UPDATE ACKNOWLEDGE。	**O-DU→O-CU**	查證 O-DU 向 O-CU 發送 gNB-DU CONFIGURATION UPDATE ACKNOWLEDGE。 F1AP gNB-DU CONFIGURATION UPDATEACKNOWLEDGE 宜包含[26]之 4.1.6.1.2.1 提到之所有強制性 IE。
7	自 O-CU 啟動新增之細胞。	**O-DU←O-CU**	O-CU 向 O-DU 發送 F1AP gNB-DU CONFIGURATION UPDATE。 F1AP gNB-DU CONFIGURATION UPDATE 宜包含[26] 之 4.1.6.1.2.4 提到之所有強制性 IE。
8	O-DU 向 O-CU 發送 gNB-DU CONFIGURATION UPDATE ACKNOWLEDGE。	**O-DU→O-CU**	查證 O-DU 向 O-CU 發送 gNB-DU CONFIGURATION UPDATE ACKNOWLEDGE。 F1AP gNB-DU CONFIGURATION UPDATEACKNOWLEDGE 宜包含[26]之 4.1.6.1.2.1 提到之所有強制性 IE。

9	查證新增細胞之狀態。	**O-DU**	查證 CLI 顯示 O-CU 及 O-DU 為運作中，且出現新增之細胞，以及 O-RU 的 RF 狀態為作用中。

6.2.5 SystemInformation-MIB

測試目的

此測試案例之目的為查證 MIB 的廣播。

參考要求

有關詳細之要求，參照[25]之 8.1.3。.

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) F1AP 已建立。

(c) RU 連線至 O-DU(選用)。

(d) 使用 O-DU 組態檔中定義之預設 SSB 組態。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試支援 NR 之 UE 模擬器。

(2) 支援 N1、N2 及 HTTP 訊息所使用之 5G 核心或 CN 模擬器。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 有關測試設置之詳細資訊，參照 A.1。

(2) 測試剖繪檔 2，參照附錄 B 測試剖繪檔 B.2。

測試程序

表 5 說明 SystemInformation-MIB 之測試程序。

表 5 SystemInformation-MIB

	程序	訊息流	預期輸出
1	UE 已開啟。	-	查證 O-DU 宣傳輸 SS Block，以及 MIB，且宜包含： systemFrameNumber、 subCarrierSpacingCommon、ssb-SubcarrierOffset、dmrs-TypeA-Position 及 pdcch-ConfigSIB1。

2	O-DU 依定義之週期發送 SSB 組態。	**UE←O-DU/O-CU**	查證 UE 日誌(測試工具)，O-DU 於 SFN 內前半訊框中每個組態設定之 SSB 週期中廣播 SS 突發區塊(burst block)。
3	UE 自 O-DU 接收	**UE←O-DU/O-CU**	查證 UE 接收源自 O-DU 之 BCCH-BCH-Message MIB，以及 MIB 包含依 3GPP 規範[28]之 6.2.2 之 IE。於測試工具上查證此點。

6.2.6 Systeminformation-SIB1

測試目的

此測試案例之目的為查證 SIB1 的廣播。

參考要求

有關詳細要求，參照[25]之 8.1.3。

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) O-RU 連線至 O-DU(選用)。

(c) MIB 宜包含 PDCCH-ConfigSIB1。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試支援 NR 之 UE 模擬器。

(2) 支援 N1、N2 及 HTTP 訊息所使用之 5G 核心或 CN 模擬器。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1)有關測試設置之詳細資訊，參照 A.1。

(2)有關 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

測試程序

表 6 說明 SystemInformation-MIB 之測試程序。

表 6 SystemInformation-SIB1

	程序	訊息流	預期輸出
1	O-DU 發送 SIB1。	**UE←O-DU/O-CU**	查證 SIB1 子載波間隔之 subCarrierSpacingCommon 及指示 SIB1 之 ssb-subcarrierOffset 是否存在。 UE 已接收具組態設定週期之 SIB1，且 SIB1 包含依 3GPP 規範[28]之 IE。

6.2.7 Systeminformation-SIB2

測試目的

本測試案例之目的為查證 O-DU 對 SIB2 的廣播。

參考要求

有關詳細要求，參照[25]之 8.1.3。

初始條件

以下為本測試之先決條件。

(a)細胞設置成功。

(b)O-CU 於 F1 設置回應中發送 SIB2 及 SIB3，且 F1 設置成功。

(c)O-RU 連線至 O-DU。

(d)MIB 及 SIB1 廣播成功。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試支援 NR 之 UE 模擬器。

(2) 5G 核心或核心模擬器是用於終止 UE(模擬器)NAS 協定，並支援 NGAP、HTTP2 及 PFCP 之協定。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 有關測試設置之詳細資訊，參照 A.1。

(2) 有關 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(3) 有關 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

測試程序

表 7 說明 SystemInformation-SIB2 之測試程序。

表 7 SystemInformation-SIB2

	程序	訊息流	預期輸出
1	UE 接收源自 O-DU 之 SIB2 廣播。	**UE←O-DU/O-CU**	查證 O-DU 依自 SIB1 解碼之排程資訊向 UE 廣播 SIB2。 依 3GPP 規範[28]之 6.3.1 查證所有強制性 IE。

6.2.8 Systeminformation-SIB3

測試目的

本測試案例之目的為查證 O-DU 對 SIB3 的廣播。

參考要求

有關詳細要求，參照[25]之 8.1.3。

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) O-CU 於 F1 設置回應中發送 SIB2 及 SIB3，且 F1 設置成功。

(c) O-RU 連線至 O-DU。

(d) MIB 及 SIB1 廣播成功。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試支援 NR 之 UE 模擬器。

(2) 5G 核心或核心模擬器是用於終止 UE(模擬器)NAS 協定，並支援 NGAP、HTTP2 及 PFCP 之協定。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 有關測試設置之詳細資訊，參照 A.1。

(2) 有關 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(3) 有關 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

測試程序

表 8 說明 SystemInformation-SIB3 之測試程序。

表 8 SystemInformation-SIB3

	程序	訊息流	預期輸出
1	UE 接收源自 O-DU 之 SIB3 廣播。	**UE←O-DU/O-CU**	查證 O-DU 依自 SIB1 解碼之排程資訊向 UE 廣播 SIB3。 依 3GPP 規範[28]之 6.3.1 查證所有強制性 IE。

6.2.9 PDU 會談建立程序

測試目的

此測試案例之目的為查證端點對端點環境中 UE PDU 會談的建立程序。此案例說明成功建立 PDU 會談後，將指派 PDU IP 予 UE。

參考要求

有關詳細要求，參照[25]之 2.2 及 9.2.2。

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) O-DU 與 O-CU 間之 F1AP 連線成功。

(c) UE 已解碼 MIB 及 SIB1。

(d) RACH 程序成功。

(e) RRC 設置成功。

(f) 註冊成功

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試可支援 NR 之 UE 模擬器。

(2) 5G 核心或核心模擬器是用於終止 UE(模擬器)NAS 協定，並支援 NGAP、HTTP2 及 PFCP 之協定。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1)有關測試設置之詳細資訊，參照 A.1。

(2)有關 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(3)有關 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

(4)有關 RACH 測試剖繪檔之詳細資訊，參照 B.6。

測試程序

表 9 說明 PDU 會談建立程序之測試程序。

表 9　PDU 會談建立

	程序	訊息流	預期輸出
1	UE 發送帶有 PDU 會談 ID 之 PDU 會談建立請求(參照 3GPP 規範[29]之 8.3.1)。	**UE→O-DU/O-CU**	查證 O-DU 接收 UL 資訊傳送訊息，其中包含做為 NAS 訊息之 PDU 會談建立請求。 查證 O-DU 向 O-CU 發送 UL RRC 訊息傳送，其中包含 RRC 容器之 PDU 會談建立請求。 依 O-RAN.WG5.C.1[26]之 6.1.2.3 的 F1-C IE 處理，查證 UL RRC 訊息傳送之所有強制性 IE。 查證 O-CU 向 AMF 發送上行 NAS 傳輸，其中 NAS PDU 做為 PDU 會談向 AMF 建立請求。 依 3GPP 規範[27]之 9.2.5.3 查證所有強制性 IE。
2	UE 接收 RRC 重組態及 PDU session establishment accept。	**UE←O-DU/O-CU**	查證 O-CU 接收源自 AMF 之 PDU 會談資源設置請求，其中 NAS-PDU 做為 PDU 會談建立接受。 依 3GPP 規範[27]之 9.2.1.1 查證所有強制性 IE。 查證 O-CU 向 O-DU 發送 UE 全景設置請求，以建立 DRB。 依[26]之 6.1.1.3 的 F1-C IE 處理，查證 UE 全景設置請求之所有強制性 IE。 查證成功建立 DRB 後，O-DU 向 O-CU 發送 UE 全景設置回應。 依[26]之 6.1.1.3 的 F1-C IE 處理，查證 UE 全景設置請求之所有強制性 IE。 查證 O-CU 向 O-DU 發送 DL RRC 訊息傳送，其中 RRC 容器具 RRC 重組態。 依[26]之 6.1.2.3 中 F1-C IE 處理，查證 DL RRC 訊息傳送之所有強制性 IE。 查證 O-DU 向 UE 發送 RRC reconfiguration，其中包含做為 NAS 酬載之 PDU 會談建立接受。
3	UE 發送 RRC 重組態完成 UE sends RRC reconfiguration complete.	**UE→O-DU/O-CU**	查證 O-DU 自 UE 接收 RRC 重組態完成。 查證 O-DU 向 O-CU 發送 UL RRC 訊息傳送，其中 RRC 容器之 RRC 重組態完成。 依[26]之 6.1.2.3 中 F1-C IE 處理，查證 UL RRC 訊息傳送之所有強制性 IE。 查證 O-CU 透過 NG 介面向 AMF 發送 PDU 會談資源設置回應。 依 3GPP 規範[27]之 9.2.1.2 查證所有強制性 IE。

6.2.10　PDU 多方會談修正

測試目的

此測試案例之目的為查證端點對端點環境中的網路啟始 PDU 修正程序。此測試案例為藉由新增 1 個 5QI 3 之 GBR 流(Flow)及 1 個 5QI 6 之非 GBR 流，以說明網路啟

始之 PDU 會談的修正。

參考要求

有關詳細要求，參照[25] 之 2.2、7.2 及 9.2.2。

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) DU 與 O-CU 之間之 F1AP 連線成功。

(c) UE 已解碼 MIB 及 SIB1。

(d) RACH 程序成功。

(e) RRC 設置成功。

(f) 註冊成功，Follow ON 位元為 1。

(g) UE 啟始 PDU 會談建立程序成功。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試支援 NR 之 UE 模擬器。

(2) 使用支援 N1、N2 及 HTTP 訊息之 5G 核心或 CN 模擬器。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 有關測試設置之詳細資訊，參照 A.1。

(2) MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(3) 有關 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

(4) 有關 RACH 測試剖繪檔之詳細資訊，參照 B.6。

測試程序

表 10 說明網路啟始之 PDU 修正程序的測試程序。

	程序	訊息流	預期輸出
1	AMF 向 O-CU 發送 NGAP PDU Session Resource Modify Request。	**O-CU/O-DU←AMF**	查證 O-CU 接收發送 NGAP PDU Session Resource Modify Request，其中包含 PDU 會談及 5G CN 欲新增資料流之相關資訊。 NGAP PDU Session Resource Modify Request 宜包含 3GPP 規範[27]之 9.2.1.5 及 9.3.4.3 提到的所有強制性 IE。 驗查證 O-CU 是否向 O-DU 發送 F1AP UE Context Modification Request。 F1AP UEContext Modification Request 宜包含[26]之 6.3.1.1.1 提到的所有強制性 IE。 查證 O-DU 向 O-CU 發送 F1AP UE Context Modification Response。 F1AP UE Context Modification Response 宜包含[26]之 6.3.1.1.1 提到的所有強制性 IE。 查證 O-CU 向 O-DU 發送 RRC 容器中帶有 RRC reconfiguration 訊息之 F1AP DL RRC Message Transfer Request，且該訊息宜包含[26]之 6.3.1.1.1 提到的所有強制性 IE。
2	UE 接收 RRC 重組態及 5G SM：PDU session Modification Command message。	**UE←O-DU/O-CU**	查證 O-DU 向 UE 發送 RRC reconfiguration 重訊息，且 RRC reconfiguration 訊息宜包含 3GPP 規範[28]中提到之所有強制性 IE。
3	UE 發送 RRCReconfiguration Complete。	**UE→O-DU/O-CU**	查證 O-DU 接收 RRC Reconfiguration Complete 訊息，以及向 O-CU 發送 F1AP UL RRC 訊息傳送，其中包含 RRC 容器內的 RRC Reconfiguration Complete。 依[26]之 6.1.1.3F1-C IE 處理，查證 UL RRC 訊息傳送之所有強制性 IE。
4	O-CU 向 AMF 發送 NGAP PDU Session Resource Modify Response。	**O-DU/O-CU→AMF**	查證 AMF 接收 NGAP PDU Session Resource Modify Response。 NGAP PDU Session Resource Modify Response 宜包含 3GPP 規範[27]之 9.2.1.6 及 9.3.4.3 提到之所有強制性 IE。 查證 O-CU 向 O-DU 發送 F1AP UE Context Modification Request。 F1AP UE Context Modification Request 訊息宜包含[26]之 6.3.1.1.1 提到之所有強制性 IE。 查證 O-DU 向 O-CU 發送 F1AP UE Context Modification Response 訊息。 F1AP UE Context Modification Response 訊息宜包含[26]之 6.3.1.1.1 提到之所有強制性 IE。

5	UE 發送 UL Information Transfer message，其中包含 NAS 訊息 5GSM：PDU Session Modification Complete。	**UE→O-DU/O-CU**	查證 O-DU 接收到發送 UL Information Transfer，以及向 O-CU 發送 UL RRC 訊息。 查證 O-CU 向 AMF 發送 NGAP 上行 NAS Transport，其中 NAS 酬載為 5GSM：PDU PDU Session Modification Complete。

6.2.11 閒置模式呼叫及服務請求程序

測試目的

此測試案例之目的為查證端點對端點環境中的 UE 閒置模式呼叫及服務請求程序。

此測試案例說明 UE 自 RRC-IDLE 狀態轉換成 RRC-CONNECTED 狀態。

參考要求

有關詳細要求，參照[25]之 2.2、7.2 及 9.2.2。

初始條件

以下為本測試之前提條件。

(a) 細胞設置成功。

(b) O-DU 與 O-CU 之間之 F1AP 連線成功。

(c) UE 已解碼 MIB 及 SIB1。

(d) RACH 程序成功。

(e) RRC 設置成功。

(f) 註冊成功。

(g) UE 進入 RRC-IDLE 狀態。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境必要之測試工具：

(1) 測試可支援 NR 之 UE 模擬器。

(2) 5G 核心或核心模擬器為用於終止 UE(模擬器)NAS 協定，並支援 NGAP、HTTP2 及 PFCP 之協定。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 有關測試設置之詳細資訊，參照 A.1。

(2) 有關 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(3) 有關 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

(4) 有關 RACH 測試剖繪檔之詳細資訊，參照 B.6

測試程序

表 11 說明閒置模式呼叫及服務請求程序之測試步驟

表 11 閒置模式呼叫及服務請求

	程序	訊息流	預期輸出
1	UE 進入 RRC-IDLE 狀態，且於 UPF 接收 DL 資料。	**UE←O-DU/O-CU**	查證 O-CU 透過 NG 介面自 AMF 接收 Paging 訊息。 依 3GPP 規範[27]之 9.2.4 查證所有強制性 IE。
2	UE 接收呼叫訊息	**UE←O-DU/O-CU**	查證 O-CU 透過 F1 介面向 O-DU 發送 Paging 訊息。 依 3GPP 規範[23]之 9.2.6 查證所有強制性 IE。 查證 O-DU 向 UE 發送 Paging 訊息。 依 3GPP 規範[28]之 6.2.2 查證所有強制性 IE。
3	UE 發送帶有 S-TMSI 之 RRC SETUP REQUEST。	**UE→O-DU/O-CU**	查證 O-DU 接收 RRC SETUP REQUEST，以及向 O-CU 發送啟始 UL RRC 訊息傳送，其中 RRC 容器包含 RRC SETUP REQUEST 訊息。 依[26]之 6.1.1.3 F1-C IE 處理，查證啟始 UL RRC 訊息傳送之所有強制性 IE。
4	UE 接收 RRCsetup 訊息	**UE←O-DU/O-CU**	查證 O-CU 向 O-DU 發送 DL RRC 訊息傳送，其中 RRC 容器有 RRC setup 訊息，以建立 SRB1。 依[26]之 6.1.2.3 的 F1-C IE 處理，查證 DL RRC 訊息傳送之所有強制性 IE。 依 O-DU 向 UE 發送 RRC setup 訊息。 依 3GPP 規範[28]之 6.2.2 查證 RRC 設置之所有強制性 IE。
5	UE 透過 SRB1 發送 RRC setup complete 訊息，其中 Service Request 做為 NAS 酬載。	**UE→O-DU/O-CU**	查證 O-DU 自 UE 接收 RRC setup complete 訊息，其中 Service request 做為 NAS 酬載，以及向 O-CU 發送 UL RRC 訊息傳送，其中 RRC setup complete 且 RRC 容器中有 Service Request。 依[26]之 6.1.2.3 F1-C IE 處理，查證 UL RRC 訊息傳送之所有強制性 IE。 查證 O-CU 向 AMF 發送啟始 UE 訊息，其中 NAS 酬載做為 Service Request。 依 3GPP 規範[27]之 9.2.5.1 查證 Initial UE 訊息之所有強制性 IE。

6	UE 接收 RRC 重組態，其中 Service Accept 訊息做為 NAS 酬載。	**UE←O-DU/O-CU**	查證 O-CU 接收 Initial context setup request 訊息，其中 NAS 酬載做為服務接受。 查證 O-CU 向 O-DU 發送 DL RRC 訊息傳送，其中在 RRC 容器中包含 RRC reconfiguration 及 service accept 訊息。 依[26]之 6.1.2.3 的 F1-C IE 處理，查證 DL RRC 訊息傳送之所有強制性 IE。 查證 O-DU 發送 RRC Reconfiguration 訊息，其中包含 Service accept 訊息做為 NAS 酬載。 依 3GPP 規範[28]之 6.2.2 查證 RRC reconfiguration 訊息之所有強制性 IE。
7	UE 發送 RRC reconfiguration complete 訊息。	**UE→O-DU/O-CU**	查證 O-DU 接收 RRC Reconfiguration complete 訊息，以及向 O-CU 發送 UL RRC 訊息傳送，其中 RRC 容器包含 RRC reconfiguration complete。 依[26]之 6.1.2.3 F1-C IE 處理，查證 UL RRC 訊息傳送之所有強制性 IE。 查證 O-CU 向 AMF 發送 Initial context setup response 訊息。 依 3GPP 規範[27]之 9.2.2.2 查證 Initial context setup response 訊息之所有強制性 IE。

6.2.12 下行 UDP 資料傳送

測試目的

此測試案例之目的為查證 PDU 會談中 5QI 9 預設流之下行的峰值及平均流通量。

參考要求

有關詳細要求，參照[25]之 2.2。

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) O-DU 與 O-CU 之間之 F1AP 連線成功。

(c) UE 已解碼 MIB 及 SIB1。

(d) RACH 程序成功。

(e) RRC 設置成功。

(f) 註冊成功，Follow ON 位元為 1。

(g) 5QI 9 之 UE PDU 會談建立程序成功。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試可支援 NR 之 UE 模擬器。

(2) 支援 N1、N2 及 HTTP 訊息所使用之 5G 核心或 CN 模擬器。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1)有關測試設置之詳細資訊，參照 A.1、A.2。

(2)有關 RACH 測試剖繪檔之詳細資訊，參照 B.6。

(3)有關 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(4)有關 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

(5)有關流通量測試剖繪檔之詳細資訊，參照 B.7。

測試程序

表 12 說明下行連續流通量之測試程序。

表 12 下行連續流通量

	程序	訊息流	預期輸出
1	使用任何訊務量產生器工具或 IPERF 應用程式於 5QI 9 流之下行中觸發 712 Mbps 之 UDP 資料傳送。	**O-CU/O-DU← UPF**	查證 O-CU 接收監督者 NG-U 連線中期望流之 DL UDP 訊務量。 O-CU 將流向對映至監督者 DRB，此將由駐留 O-CU 之 SDAP 協定完成，然後將 UDP 訊務量轉發至 O-DU。 查證 O-DU 接收 UDP 訊務量，且封包未顯著遺失。
2	量測 UE 上之峰值及平均流通量。	**UE←O-DU/O-CU**	對照理論值查證。參照附錄 B.7。

6.2.13 上行 UDP 資料傳送

測試目的

此測試案例之目的是查證 PDU 會談中 5QI 9 預設流之上行的峰值及平均流通量。

參考要求

有關詳細要求，參照[25]之 2.2。

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) O-DU 與 O-CU 間之 F1AP 連線成功。

(c) UE 已解碼 MIB 及 SIB1。

(d) RACH 程序成功。

(e) RRC 設置成功。

(f) 註冊成功，Follow ON 位元為 1。

(g) 5QI 9 之 UE PDU 會談建立程序成功。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試可支援 NR 之 UE 模擬器。

(2) 支援 N1、N2 及 HTTP 訊息所使用之 5G 核心或 CN 模擬器。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 有關測試設置之詳細資訊，參照 A.1、A.2。

(2) 有關 RACH 測試剖繪檔之詳細資訊，參照 B.6。

(3) 有關 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(4) 有關 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

(5) 有關流通量測試剖繪檔之詳細資訊，參照 B.7。

測試程序

表 13 說明上行連續流通量之測試程序。

表 13 上行連續流通量

	程序	訊息流	預期輸出
1	使用任何訊務量產生器工具或 IPERF 應用程式於 5QI 9 流的上行中觸發 285 Mbps 之 UDP 資料傳送。	**UE→O-DU/O-CU**	查證 O-DU 於期望之監督者 DRB 上接收 UL UDP 訊務量，以及使用 GTP-U 使用者平面連線轉發至 O-CU。 O-CU 將 DRB 對映至流對映，此將由駐留 O-CU 之 SDAP 協定完成，然後將 NG-U 通道上之 UDP 訊務量轉發至 UPF。 查證 UPF 接收 UDP 訊務量，且封包未顯著遺失。
2	量測 UE 上之峰值及平均流通量。	**O-DU/O-CU→UPF**	對照理論值查證。參照附錄 B.7。

6.2.14 雙向 UDP 資料傳送

測試目的

此測試案例之目的為查證 PDU 會談中 5QI 9 預設流之上下行的峰值及平均流通量。

參考要求

有關詳細要求，參照[25]之 2.2。

初始條件

以下為本測試之先決條件。

(a) 細胞設置成功。

(b) O-DU 與 O-CU 間之 F1AP 連線成功。

(c) UE 已解碼 MIB 及 SIB1。

(d) RACH 程序成功。

(e) RRC 設置成功。

(f) 註冊成功，Follow ON 位元為 1。

(g) 5QI 9 之 UE PDU 會談建立程序成功。

測試設置及組態

(a) DUT：單一 O-DU 及單一 O-CU。

(b) 此測試情境中必要之測試工具：

(1) 測試可支援 NR 之 UE 模擬器。

(2) 支援 N1、N2 及 HTTP 訊息所使用之 5G 核心或 CN 模擬器。

(3) 協定分析儀：用於記錄與觀察 F1AP、NGAP、NAS、HTTP2 及 PFCP 之協定內容。

(c) 組態：

(1) 對於測試設置之詳細資訊，參照 A.1、A.2。

(2) 對於 RACH 測試剖繪檔之詳細資訊，參照 B.6。

(3) 對於 MIB 及 SSB 測試剖繪檔之詳細資訊，參照 B.2。

(4) 對於 SIB1 測試剖繪檔之詳細資訊，參照 B.3。

(5) 對於流通量測試剖繪檔之詳細資訊，參照 B.7。

測試程序

表 14 說明雙向連續流通量之測試程序。

表 14 雙向連續流通量

	程序	訊息流	預期輸出
1	使用任何訊務量產生器工具或 IPERF 應用程式於 5QI 9 流之上行中觸發 285 Mbps 的 UDP 資料傳送。	**UE→O-DU/O-CU**	查證 O-DU 期望的監督者 DRB 上是否接收到 UL UDP 訊務量，以及使用 GTP-U 使用者平面連接轉發至 O-CU。 O-CU 將 DRB 對映至流對映，此將由駐留 O-CU 之 SDAP 協定完成，然後將 NG-U 通道上之 UDP 訊務量轉發至 UPF。 查證 UPF 接收 UDP 訊務量，且封包未顯著遺失。
2	查證 UPF 之峰值及平均流通量。	**O-DU/O-CU→UPF**	對照理論值查證。參照附錄 B.7。
3	使用任何訊務量產生器工具或 IPERF 應用程式於 5QI 9 流之下行中觸發 712 Mbps 之 UDP 資料傳送。	**O-CU/O-DU← UPF**	查證 O-CU 是否接收到監督者 NG-U 連線中期望流之 DL UDP 訊務量。 O-CU 將流對映至監督者 DRB，這將由駐留 O-CU 之 SDAP 協定完成，然後將 UDP 訊務量轉發至 O-DU。 查證 O-DU 是否接收到 UDP 訊務量，且封包未顯著遺失。
4	量測 UE 上之峰值及平均流通量。	**UE←O-DU/O-CU**	對照理論值來查證。參照附錄 B.7。

7. 資通安全測試要求

7.1 概述

本節依 O-RAN TIFG: Test & Integration Focus Group 公布 End-to-end Test Specification 訂定資通安全之測試要求。

本節描述評估及評鑑無線電接取網路端點對端點 (end-to-end, E2E) 資通安全面向之測試。一般測試方法及組態宜依[30]相關節次所述。

因整個 O-RAN 系統為待測系統，於端點對端點測試之情境中，可視為 1 組整合的黑盒子，於此列出之資通安全測試案例歸類如下：

(a) 3GPP SA3 工作小組要求之 5G 基地臺資通安全保證規範 (gNB security assurance specification)，適用於 5G-NR 非獨立組網 (non- standalone， NSA) / 獨立組網 (standalone， SA)。

(b) 其他需特別接入 O-RAN 組件之主要介面或內部功能之資通安全測試案例，皆非本節所涵蓋範圍。

7.2 依 3GPP SA3 之 gNB 安全保證規範要求

從網路架構及功能面向來看，端點對端點 O-RAN 系統 (代測系統，SUT) 等效於 5G 基地臺，因此於端點對端點無線電接取網路 (RAN) 之資通安全評估應依：

(a) [31]概述之 5G 基地臺特定資通安全要求、威脅及測試案例。

(b) [30]之 7.1 測試案例。

表 15 說明[31]之 4.2.2 及[30]之 7.1 列出之所有必需測試例。

表 15 5G 基地臺資通安全確保規範 (gNB SCAS) 測試案例總表

測試案例 (O-RAN 參考 #)	測試案例 (3GPP 參考 #)	測試案例 (第 10-2 部測試規範參考 #)	測試名稱	說明
7.1.1	4.2.2.1.1	7.3.1	RRC-signalling 完整性保護	gNB 應支援透過 NG-RAN 空中介面傳送之 RRC-signalling 受完整性保護。
7.1.2	4.2.2.1.2	7.3.2	UE 與 gNB 間之使用者資料完整性保護	查證透過 NG-RAN 空中介面傳送之使用者資料封包受完整性保護。
7.1.3	4.2.2.1.4	7.3.3	RRC 完整性檢查失效	查證 gNB 可正確地處理 RRC 完整性檢查失效。
7.1.4	4.2.2.1.5	7.3.4	UP 完整性檢查失效	查證 gNB 可正確地處理 UP完整性檢查失效。
7.1.5	4.2.2.1.6	7.3.5	RRC-signalling 加密	查證透過NG-RAN 空中介面傳送介於UE與gNB間之RRC -signalling資料受機密性保護。

7.1.6	4.2.2.1.7	7.3.6	UE 與 gNB 間之使用者資料加密	查證透過 NG-RAN 空中介面傳送之的使用者資料封包受機密性保護。
7.1.7	4.2.2.1.8	7.3.7	UE 與 gNB 間之使用者資料重送保護	查 UE 與 gNB 間之使用者資料支持完整性保護及重送攻擊保護
7.1.8	4.2.2.1.9	7.3.8	RRC-signalling 重送保護	查證 UE 與 gNB 間透過 NG-RAN 空中介面傳送之 RRC-signalling 受重送保護。
7.1.9	4.2.2.1.10	7.3.9	使用者資料加密依 SMF 發送之安全政策	查證使用者資料以 SMF 傳送之安全政策受機密性保護。
7.1.10	4.2.2.1.11	7.3.10	使用者資料完整性依 SMF 發送之安全政策	查證使用者資料以 SMF 傳送之安全政策受完整性保護。
7.1.11	4.2.2.1.12	7.3.11	AS 演算法選擇	gNB 存取層加密及完整性演算法優先順序。
7.1.12	4.2.2.1.13	7.3.12	gNB 金鑰更新	查證gNB 金鑰(KgNB)更新功能運作正常，查證當達到重複使用資料無線電承載識別碼時，gNB 金鑰 (KgNB) 更新功能運作正常。
7.1.13	4.2.2.1.14	7.3.13	Xn-handovers 之降階攻擊防護	查證當發生 Xn 交握時預防降階攻擊之檢查機制。

7.3 資通安全測試項目

整個 O-RAN 系統為待測系統 (SUT)，可視為端點對端點測試中整合之黑盒子 ，參照[32]，即 SUT 的內部功能及架構超出範圍。預計所有涉及之 O-RAN 功能及介面均可適當地互相操作，且於終端用戶設備及應用主機或另一個終端用戶設備間，建立端點至端點的通訊鏈路。SUT 內部功能互運性及符合性測試超出本文範圍。SUT 將處於服務模式，並以正常操作狀態運行。

端點對端點 KPIs 定義 為終端用戶設備與應用(訊務量)主機，或另一個終端用戶設備

間之整個端點對端點通訊鏈路，如圖 23。

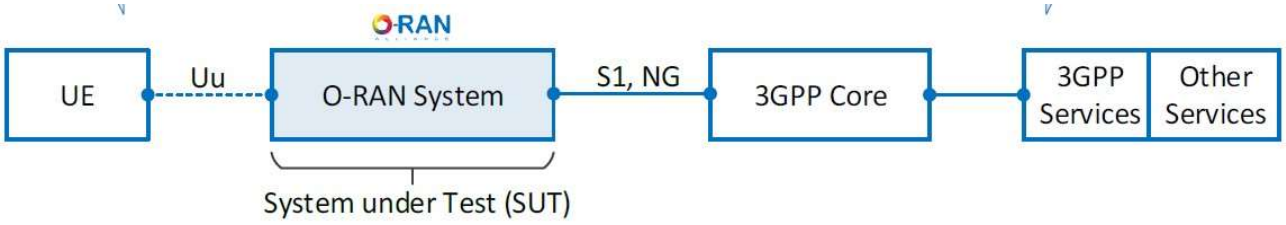


圖 23　端點對端點測試架構

7.3.1　RRC-signalling 完整性保護

(a) 目的

(1)依[31]之 4.2.2.1.1，並參考[33]之 5.3.3 及[34]之 D.2.2.2。

(2)查證 UE 與 gNB 透過 NG-RAN 空中介面傳送之 RRC-signalling 受完整性保護。

(b) 先決條件

(1)gNB 網路產品應連接於模擬或實際網路環境中，可模擬 UE。

(2)測試者應有權限接取完整性演算法及完整性保護金鑰。

(3)測試者可通過 NG RAN 空中介面擷取訊息，也可於 UE 處擷取訊息。

(c) 執行步驟

(1) NIA0 於 UE 與 gNB 上停用。

(2) gNB 向 UE 發送 AS SMC 訊息，UE 回應 AS SMP。

(3) 檢查 gNB 於發送 AS SMC 訊息後，UE 進入 CM-Idle 狀態前，發送之任何 RRC 訊息受完整性保護。

(d)預期結果

於 gNB 發送 AS SMC 後，NG RAN 空中介面上之任何 RRC-signalling 均受完整性保護。

7.3.2　UE 與 gNB 間之使用者資料完整性保護

(a) 目的

(1) 依[31]之 4.2.2.1.2，並參考[33]之 5.3.3 所述。

(2) 查證使用者封包於 NG RAN 空中介面上受完整性保護。

(b)先決條件

(1) gNB 網路產品應連接於模擬/實際網路環境中，可模擬 UE。

(2) 測試者應啟用使用者平面完整性保護，並確保不使用 NIA0。

(3) 測試者應了解完整性演算法及完整性保護金鑰。

(4) 測試者可通過 NG RAN 空中介面擷取訊息，也可於 UE 處擷取訊息。

(c)執行步驟

(1) NIA0 於 UE 與 gNB 上停用。

(2) gNB 發送帶有“on”完整性保護指示之 RRCConnectionReconfiguration。.

(3) 於發送 RRCConnectionReconfiguration 後及 UE 進入 CM-Idle 狀態前，檢查 gNB 發送之任何使用者資料受完整性保護。

(d)預期結果

於 gNB 發送 RRCConnectionReconfiguration 後，於 UE -與 gNB 間透過 NG RAN 空中介面發送之任何使用者平面封包均受完整性保護。

7.3.3 RRC 完整性檢查失效

(a) 目的

(1) 依[31]之 4.2.2.1.4，並參考[33]之 6.5.1 與[34]之 D.2.2.2。

(2) 查證 gNB 可正確地處理 RRC 完整性檢查失效。

(b) 先決條件

(1)使用 UE 之測試環境。

(2)可模擬 UE。

(3)於 gNB 上啟用 RRC 完整性保護。

(c) 執行步驟

(1) UE 於無 MAC-I 之情況下，向 gNB 發送 RRC 訊息。

(2) UE 向 gNB 發送帶有錯誤 MAC-I 之 RRC 訊息。

(3) gNB 查證源自 UE 之 RRC 訊息的完整性。

(d) 預期結果

RRC 訊息於執行步驟(1)或執行步驟(3)後被 gNB 捨棄

7.3.4 UP 完整性檢查失效

(a) 目的

(1) 依[31]之 4.2.2.1.5，並參考[33]之 6.6.4 所述。

(2) 若 gNB 或 UE 於完整性保護開始後，收到 1 個完整性檢查失效且 MAC-I 錯誤或遺漏之 PDCP PDU，則該 PDU 應被捨棄。

(3)查證 gNB 可正確地處理 UP 完整性檢查失效。

(b)先決條件

(1) 使用 UE 之測試環境。

(2) 可模擬 UE。

(3)於 gNB 上啟用 RRC 完整性保護。

(c) 執行步驟

(1) UE 於無 MAC-I 之情況下，向 gNB 發送 PDCP PDU。

(2) UE 向 gNB 發送 1 個帶有錯誤 MAC-I 之 PDCP PDU。

(3) gNB 查證源自 UE 之 PDCP PDU 的完整性。

(d) 預期結果

PDCP PDU 於執行步驟(1)或執行步驟(3)後被 gNB 捨棄。

7.3.5 RRC-signalling 加密

(a) 目的

(1) 依[31]之 4.2.2.1.6，並參考[33]之 5.3.2 所述。

(2) 查證 UE 與 gNB 間透過 NG RAN 空中介面發送之 RRC-signalling 資料受機密性保護。

(b) 測試先決條件

(1)gNB 網路產品應連接於模擬/實際網路環境中，可模擬 UE。

(2)測試者應有權限接取 NG RAN 空中介面或可於 UE 處擷取訊息。

(c) 執行程序

(1)UE 向 AMF 發送 Registraton Request。

(2)AMF 向 gNB 發送 KgNB 及 UE 安全能力。

(3)gNB 選擇一種演算法，發送 AS SMC 至 UE。

(4)gNB 自 UE 接收 AS SMP。

(d) 預期結果

gNB 發送加密之 AS SMC 後，控制平面封包發送至 UE 。

7.3.6 UE 與 gNB 間之使用者資料加密

(a) 目的

(1) 依[31]之 4.2.2.1.7，並參考[33]之 5.3.2 所述。

(2) gNB 應於 NG RAN 空中介面上，提供 UE 與 gNB 間使用者資料封包之加密。

(b) 先決條件

(1) gNB 網路產品應連接於模擬/實際網路環境中，可模擬 UE。

(2) 測試者應有權限接取 NG RAN 空中介面或可於 UE 擷取訊息。

(c) 執行步驟

(1) UE 向 SMF 發送 PDU 會談建立請求。

(2) SMF 向 gNB 發送帶有必需或首選之 UP 加密的 UP 安全政策。

(3) gNB 發送帶有加密保護指示“on”之 RRCConnectionReconfiguration。

(4) 於發送 RRCConnectionReconfiguration 後，UE 進入 CM-Idle 狀態前，檢查 gNB 發送之任何使用者資料。

(d) 預期結果

gNB 發送 RRCConnectionReconfiguration 後，發送至 UE 之使用者平面封包受機密性保護。

7.3.7 UE 與 gNB 間之使用者資料重送保護

(a) 目的

(1)依[31]之 4.2.2.1.8，並參考[33]之 5.3.3 所述。

(2)gNB 應於 UE 與 gNB 間，提供使用者資料完整性保護及重送保護。

(b) 先決條件

(1) gNB 網路產品應連接於模擬/實際網路環境中， 可模擬 UE。

(2) 測試者應有權限接取 NG RAN 空中介面。

(3) 測試者應啟用 RRC-signalling 封包之使用者平面受完整性保護。

(c) 執行步驟

(1) 測試者應使用任何網路分析儀，透過 NG RAN 空中介面，擷取 UE 與 gNB 間發送之使用者平面資料。

(2) 測試者應過濾於 UE 與 gNB 間所發送之使用者平面資料封包。

(3) 測試者應重送所擷取之使用者平面封包，或使用任何封包製作工具，以建立使用者平面封包，類似所擷取的使用者平面封包，並重送至 gNB。

(4) 測試者應透過 NG RAN 空中介面擷取，檢查 gNB 是否處理重送之使用者平面封包，以查看是否由 gNB 接收任何相對應之回應訊息。

(5) 若沒有由 gNB 接收對重送封包相對應之回應，則測試者應確認，gNB 已丟棄或忽略重送封包，提供重送保護。

(6) 測試者應由結果中查證，若重送之使用者平面封包不被 gNB 接受，則 NG RAN 空中 介面受重送保護。

(d) 預期結果

UE 與 gNB 間透過 NG 空中介面發送之使用者平面封包，受重送保護。

7.3.8 RRC-signalling 重送保護

(a) 目的

(1) 依[31]之 4.2.2.1.9，並參考[33]之 5.3.3 所述。

(2) 查證 UE 與 gNB 間，透過 NG RAN 空中介面之 RRC-signalling 的重送保護。

(b) 先決條件

(1) gNB 網路產品應連接於模擬/實際網路環境中。

(2) 測試者應了解完整性演算法及相對應之保護金鑰。

(3) 測試者應有權限接取 NG RAN 之空中介面。

(4) 測試者應啟用使用者資料封包之使用者平面受完整性保護。

(c) 執行步驟

(1) 測試者應使用任何網路分析儀，透過 NG RAN 空中介面，擷取 UE 與 gNB 間所發送之資料。

(2) 測試者應過濾 RRC 信令封包。

(3) 測試者應檢查過濾後之 RRC 信令封包的 RRC SQN，並應使用任何封包工具，以產生及所擷取的封包類似於 RRC 信令封包，或測試者應重送所擷取的 RRC 上行封包至 gNB，以透過 gNB 執行重送攻擊。

(4) 測試者應檢查重送之 RRC 信令封包，是否被 gNB 處理，或透過 NG RAN 空

中介面擷取，查看是否自 gNB 接收任何回應訊息。

(5) 若 gNB 沒有對重送封包發送相對應之回應，則測試者應確認，gNB 已丟棄/忽略重送封包，提供重送保護。

(d) 預期結果

透過 NG RAN 空中介面之 RRC 信令受重送保護。

7.3.9 使用者資料加密依 SMF 發送之安全政策

(a) 目的

(1) 依[31]之 4.2.2.1.10，並參考[33]之 5.3.2 所述。

(2) gNB 應依 SMF 發送之安全政策，啟用使用者資料加密。

(b) 先決條件

(1) gNB 網路產品應連接於模擬/實際網路環境中，可模擬 UE 及 5GC。

(2) 測試者應有權限接取 NG RAN 空中介面。

(3) 測試者應了解 RRC 及 UP 加密演算法及保護金鑰。

(4) RRC 加密於 gNB 已啟用。

(c) 執行步驟

(1) 測試者透過發送 PDU 會談建立請求訊息，觸發 PDU 會談建立程序。

(2) 測試者應觸發 SMF 向 gNB 發送加密保護“需要”或“不需要”之 UP 安全政策。

(3) 測試者應透過 NG RAN 空中介面，擷取 gNB 與 UE 之 RRC 連接重組態程序，並過濾 gNB 發送至 UE 的 RRC 連接重組態訊息。

(4) 測試者應解密 RRC 連接重組態訊息，並檢索於解密訊息中，顯示 UP 加密保護指示。

(5)測試者應查證 gNB 收到之 UP 安全政策，是否與 gNB 於 RRC 連接重組態訊息中，通知 UE 的 UP 加密保護指示相同。

(6) 測試者應擷取 UE 與 gNB 間發送之 RRC 連接重組態完整訊息。

(7) 測試者應使用任何網路分析儀，擷取於 UE 與 gNB 間所發送之使用者平面資料。

(8) 測試者應檢查擷取之 UP 資料，是否依 UP 安全政策啟用/停用。

(d) 預期結果

(1) 當接收到之 UP 密碼保護指示設置為“必需”時，擷取的使用者平面資料顯示為亂碼（即不再是明文），並且依 SMF 發送的 UP 安全政策，使用者平面封包受機密性保護。

(2) 當接收之 UP 密碼保護指示設置為“不需要”時，擷取的使用者平面資料顯示為明文，且依 SMF 之 UP 安全政策，使用者平面封包未受機密性保護。

7.3.10 使用者資料完整性依 SMF 發送之安全政策

(a) 目的

(1)依[31]之 4.2.2.1.11，並參考[33]之 5.3.2 所述。

(2)gNB 應依 SMF 發送之安全政策，提供使用者資料完整性保護。

(b) 先決條件

(1) gNB 網路產品應連接於模擬/實際網路環境中，可模擬 UE 及 5GC。

(2) 測試者應有權限接取 NG RAN 空中介面。

(3) 測試者應了解完整性演算法及保護金鑰。

(4)RRC 加密於 gNB 已啟用。

(c) 執行步驟

(1) 測試者透過發送 PDU 會談建立請求訊息，觸發 PDU 會談建立程序。

(2) 測試者應觸發 SMF 向 gNB 發送加密保護“需要”或“不需要”之 UP 安全政策。

(3) 測試者應透過 NG RAN 空中介面， 擷取 gNB 與 UE 之 RRC 連接重組態訊息。

(4) 測試者應解密 RRC 連接重組態訊息，並檢索於解密訊息中，顯示 UP 完整性保護指

(5) 測試者應檢查 UP 完整性是啟用/禁用，以查證是否於 gNB 接收之 UP 安全政策與 gNB 於 RRC 連接重組態訊息中，通知 UE 的 UP 完整性保護指示相同。

(6)測試者應使用任何網路分析儀，擷取 UE 與 gNB 間所發送之使用者平面資料。

(7)測試者應檢查是否使用者平面資料包含訊息鑑別碼。

(d) 預期結果

(1) 當接收 UP 完整性保護設置為“必需”時，使用者平面資料封包含訊息鑑別碼，依 SMF 發送之安全政策受完整性保護。

(2)當接收 UP 完整性保護設置為“不需要”時，使用者平面資料封包訊息鑑別碼不存在，並且未依 SMF 發送的安全策略，使用者平面資料未受完整性保護。

7.3.11 AS 演算法選擇

(a) 目的

(1) 依[31]之 4.2.2.1.12，並參考[33]之 6.7.3.0 及 5.11.2 所述。

(2) 服務網路應選擇要使用之演算法，取決於 UE 的 安全能力、目前服務網路個體中，已組態設定允許之安全能力清單。

(b) 先決條件

使用 gNB 之測試環境，已預先組態設定具允許之優先順序安全演算法。

(c) 執行步驟

(1)UE 向 gNB 發送附加請求訊息。

(2)gNB 接收 S1 全景建立請求訊息。

(3)gNB 發送 SECURITY MODE COMMAND 訊息。

(4)UE 回覆 AS SECURITY MODE COMPLETE 訊息。

(d) 預期結果

(1) gNB 發起 SECURITY MODE COMMAND 訊息，該訊息包括依排序清單

選擇具最高優先順序之演算法，並包含於 UE EPS 安全能力中。

(2) 查證 AS SECURITY MODE COMPLETE 訊息中之 MAC，並正確選擇及應用 AS 保護演算法。

7.3.12 gNB 金鑰更新

(a) 目的

(1) 依[31]之 4.2.2.1.13 ，並參考[33]之 6.9.4.1 與[28]之 5.3.1.2。

(2) 對於 K_{gNB}、$K_{RRC-enc}$、$K_{RRC-int}$、K_{UP-int}及 K_{UP-enc}，金鑰更新應為可能的，且當 PDCP COUNT 將重複使用具相同之無線電載送身分時，應由 gNB 發起，並使用相同之 K_{gNB}。

(3) 網路負責避免重複使用具相同 RB 身分及具相同金鑰的 COUNT，例：由於大量資料之傳送、新 RBs 的發布及建立，以及 RLC-UM 載送的多個終止點變更。為避免此種重複使用，網路可以： 對 RB 建立使用不同的 RB 身分，變更 AS 安全金鑰，或將 RRC_CONNECTED 變更為 RRC_IDLE/RRC_INACTIVE，然後轉換為 RRC_CONNECTED。.

(b) 先決條件

可模擬 UE、AMF 及 SMF。

(c) 執行步驟

(1) gNB 向 UE 發送 AS Security Mode Command 訊息。

(2) UE 以 AS Security Mode Complete 訊息回應。

(3) 設置 DRB。

(4) 於一個起作用之無線電連接，多次建立及中斷，而 UE 不會閒置（例：由 UE 進行多次 IMS 呼叫，或由 SMF 及 AMF 請求 PDU 會談修改及啟動），直至 DRB ID 重複使用。

(d) 預期結果

於 DRB ID 重複使用前，gNB 會使用一個新的 K_{gNB}，例：觸發細胞內交握或觸發轉換由 RRC_CONNECTED 至 RRC_IDLE 或 RRC_INACTIVE， 然後回至 RRC_CONNECTED。

7.3.13 Xn-handovers 之降階攻擊防護

(a) 目的

(1) 依[31]之 4.2.2.1.14，並參考[33]之 6.7.3.1 與[34]之 D.2.2.6。

(2) 於 Path-Switch 訊息中，標的 gNB 由來源 gNB 所接收 UE 之 5G 安全能力，具相對應 PDU 會談 ID 之 UP 安全政策，向 AMF 發送。

(3) 查證於 X2-handovers.交握中，防止降階攻擊。

(b) 先決條件

具來源 gNB 及目標 gNB 之測試環境，可模擬來源 gNB。

(c) 執行步驟

標的 gNB 向 AMF 發送 path-switch 訊息

(d) 預期結果

UE EPS 安全能力於 path-switch 訊息中。

附錄 A (參考) 測試設置

A.1 測試設置 1 - 使用商用 UE 之端點對端點 OTA 架構

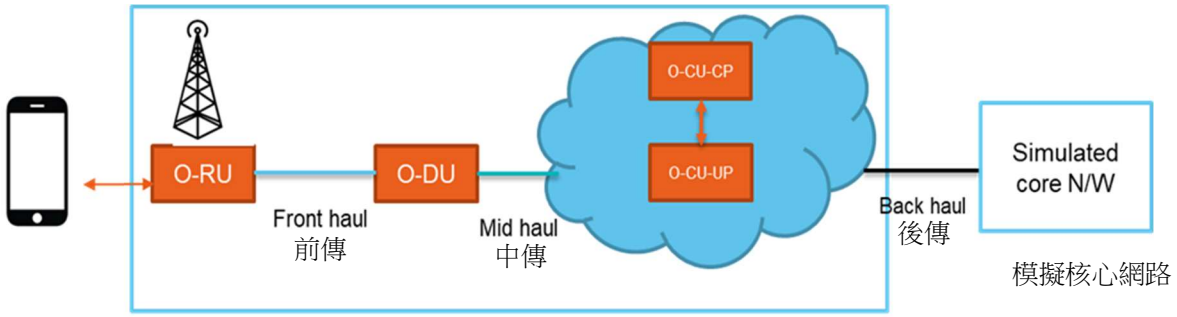


圖 24　測試設置 1 - 使用商用 UE 之端點對端點 OTA 架構

A.2 測試設置 2 - 使用 UE 模擬器之端點對端點 OTA 架構

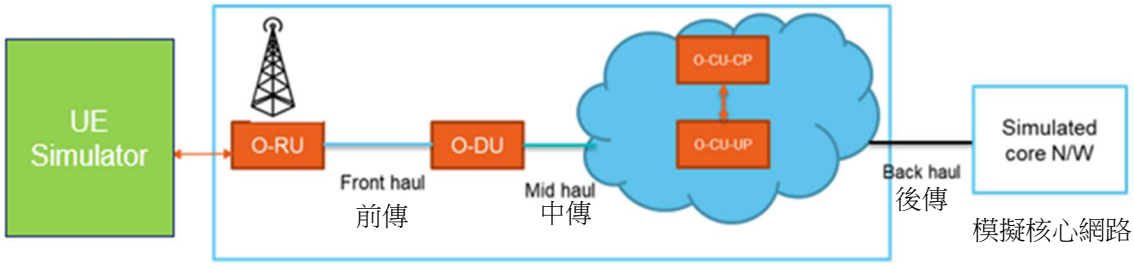


圖 25　測試設置 2 - 使用 UE 模擬器之端點對端點 OTA 架構

A.3 測試設置 3 - 模擬之 CU 及 CN 架構

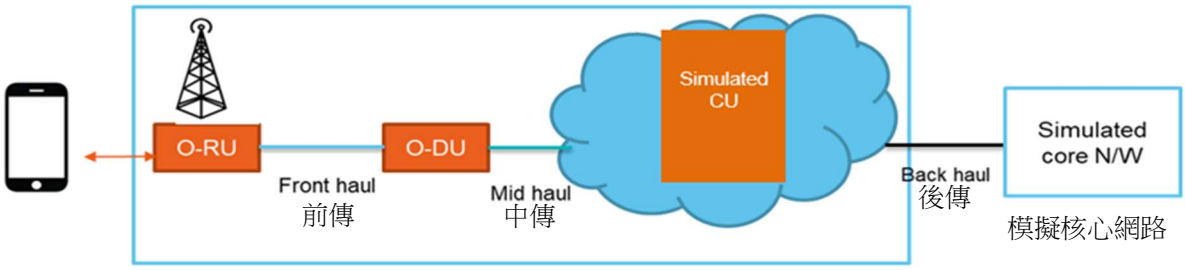


圖 26　測試設置 3 - 模擬之 CU 及 CN 架構

A.4 測試設置 4 - 對遠端 O-RU 連接至 O1 及 E2 介面之 O-DU 架構

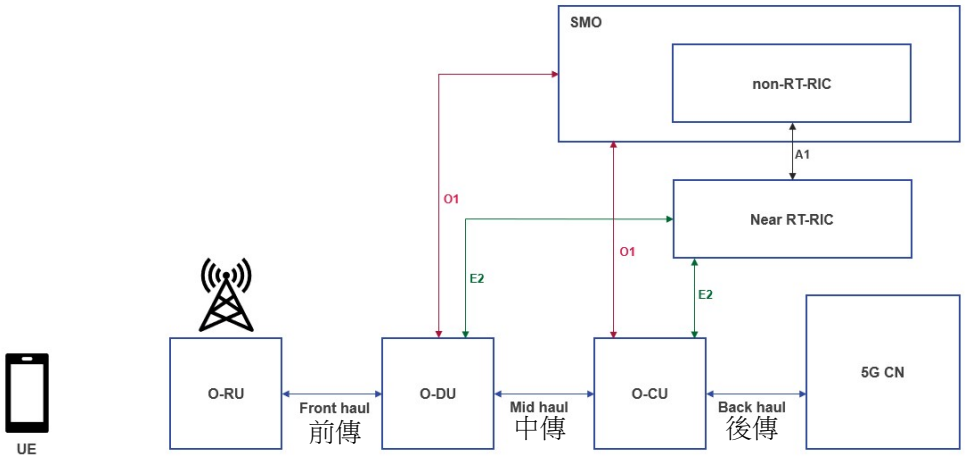


圖 27　測試設置 4 - 對遠端 O-RU 連接至 O1 及 E2 介面之 O-DU 架構

A.5　測試設置 5 - 對共置 O-RU 及 O-DU 架構之 O1 及 E2 介面

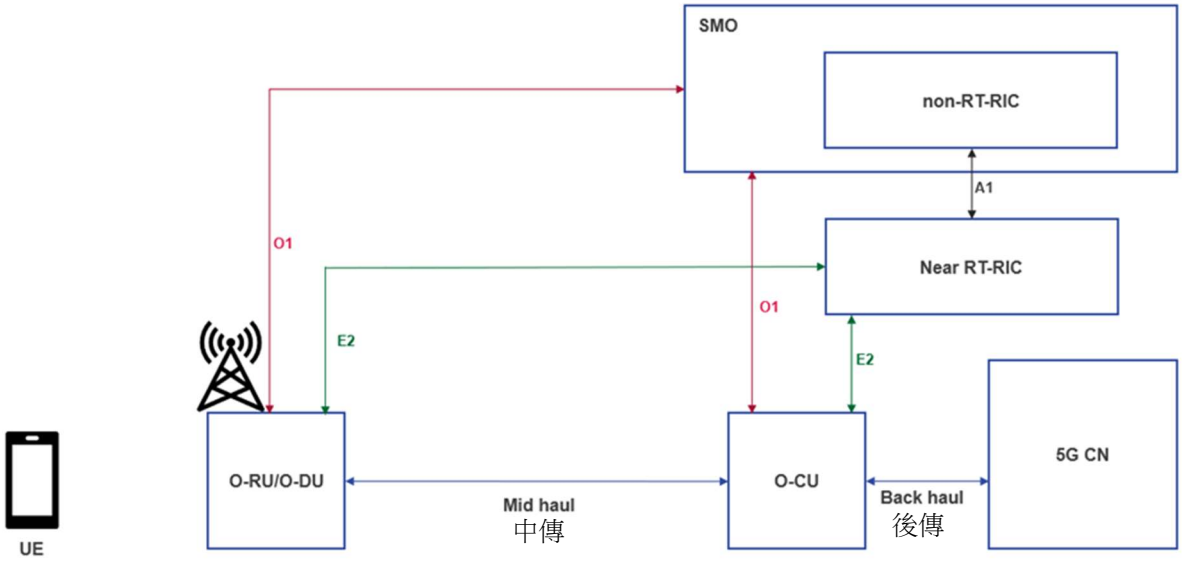


圖 28　測試設置 5 - 對共置 O-RU 及 O-DU 架構之 O1 及 E2 介面

附錄 B (參考) 測試簡述

B.1 測試剖繪 1 - 流通量測試

B.1.1 FTP 設定

TCP 資料傳送取決於以下參數：

(a) TCP 窗口大小。

(b) 串流數目 (預設：4 個串流）。

(c) TCP 最大區塊大小 (MSS)。 MSS 為 1452 位元組(1492-位元組 MTU)。

B.1.2 UDP 設定

UDP 資料傳送取決於以下參數：

(a) 讀取或寫入之緩衝區長度。UDP 預設為 1470 字元組。

(b) UDP 頻寬(bits/sec)。預設為 1 Mbit/sec。

B.2 測試剖繪 1 - MIB 及 SSB

表 16 測試剖繪 1 - MIB 及 SSB

MIB		
參數(Parameter)	可能值(Possible Values)	建議值(Recommended Values (Phase 1))
subCarrierSpacingCommon	ENUMERATED {scs15or60，scs30or120}，	1
ssb-SubcarrierOffset	INTEGER (0..15)，	15
dmrs-TypeA-Position	ENUMERATED {pos2，pos3}，	NA
pdcch-ConfigSIB1	INTEGER (0..255)，	NA
> controlResourceSetZero	-	-
> searchSpaceZero	-	-
cellBarred	ENUMERATED {barred，notBarred}，	1
intraFreqReselection	ENUMERATED {allowed，notAllowed}，	0
SSB Pattern (time-freq)		
ssb-PositionsInBurst	-	10000000...
ssb-periodicityServingCell	-	ms20
absoluteFrequencySSB	-	according to bandindicator

B.3 測試**剖繪** 2 – SIB1

表 17 測試剖繪 2 - SIB1

			預設值 (Default Values (Proposed))
SI-SchedulingInfo	si-WindowLength	ENUMERATED	s20
SchedulingInfo	si-Periodicity	ENUMERATED	rf16
SI-RequestConfig::=	ssb-perRACH-Occasion	ENUMERATED	one

B.4 測試**剖繪** 3 **- PUCCH Support- Short PUCCH Format**

表 18 測試剖繪 3 - PUCCH Support- Short PUCCH Format

PUCCH Format0	
format format	0
initialCyclicShift	0，3
nrofSymbols	1
startingSymbolIndex	13
PUCCH Format2	
format format	2
nrofSymbols	1
startingSymbolIndex	13
Number of PRB	3

B.5 測試剖繪 4 - 下行資料交付狀態報告

參考 3GPP 規範[35]中 5.5.2.2 定義之 DL DATA DELIVERY STATUS 訊框格式。所有參數均非強制性。對資料無線電承送(Radio Bearer)參數所需之緩衝區大小，需通知 CU。.

表 19 測試剖繪 4 -下行資料交付狀態報告

位元(Bits)								8 位元數 Number of Octets
7	6	5	4	3	2	1	0	
PDU Type (=1)				Highest Transmitted NR PDCP SN Ind	Highest Delivered NR PDCP SN Ind	Final Frame Ind.	Lost Packet Report	1
Spare				Data rate Ind.	Retransmitted NR PDCP SN Ind	Delivered Retransmitted NR PDCP SN Ind	Cause Report	1

資料無線電載送所需緩衝區大小	4
所需資料速率	0 or 4
遺失 NR-U 序列號碼範圍之報告數量	0 or 1
遺失 NR-U 序列號碼範圍之開始	0 or (6* Number of reported lost NR-U SN ranges)
遺失 NR-U 序列號碼範圍之結束	
最高成功交付 NR PDCP 序列號碼	0 or 3
最高傳送 NR PDCP 序列號碼	0 or 3
原因值	0 or 1
成功交付重傳 NR PDCP 序列號碼	0 or 3
重傳 NR PDCP 序列號碼	0 or 3
填充值	0-3

B.6 測試剖繪 5 - RACH 組態

表 20 測試剖繪 5 – RACH 組態

RACH IEs (3GPP)	**RACH IEs (Config file)**	**RACHConfig 1 (Format 0)**	**RACHConfig1 (Format C2)**	**RACHConfig2 (Format B4)**
RACH-ConfigDedicated				
RACH-ConfigCommon				
rach-ConfigGeneric				
> prach-ConfigurationIndex	PrachConfigIndex	1		
> msg1-FDM	PrachMsg1Fdm	1		
> msg1-FrequencyStart	PrachMsg1FreqStartRb	0		
> zeroCorrelationZoneConfig	ZeroCorrelationZoneConfig	Default		
> preambleReceivedTargetPower	preambleReceivedTargetPower	Default		
> preambleTransMax	preambleTransMax	Default		
> powerRampingStep	powerRampingStep	Default		
> ra-ResponseWindow	RaResponseWindow	sl4		
totalNumberOfRA-Preambles	TotalRaPreambles	63		
ssb-perRACH-OccasionAndCB-PreamblesPerSSB	SsbPerRachOcc	3		
	TotalCbPreamblesPerSsb	44		
msg1-SubcarrierSpacing	PrachScs	30kHz		
restrictedSetConfig	PrachRestrictSet	unrestrictedSet		

B.7 測試剖繪 6 - 流通量組態

表 21 測試剖繪 6 –流通量組態

TDD-UL-DL-ConfigCommon		Default
referenceSubcarrierSpacing	SubcarrierSpacing，	30 kHz
pattern1	TDD-UL-DL-Pattern，	-
TDD-UL-DL-Pattern ::=		-
dl-UL-TransmissionPeriodicity		ms2p5
nrofDownlinkSlots	INTEGER (0..maxNrofSlots)，	3
nrofDownlinkSymbols	INTEGER (0..maxNrofSymbols-1)，	10
nrofUplinkSlots	INTEGER (0..maxNrofSlots)，	1
nrofUplinkSymbols	INTEGER (0..maxNrofSymbols-1)，	2

時槽組態 (Time slot configuration)：DDDSU

頻寬：100 MHz

下行	建議	上行	組態
U	1	U	1
Max RBs	275	Max RBs	275
Number of layers	2	Number of layers	2
Code rate for DL (MCS 28)	5.5547	Code rate for UL (MCS 28)	5.5547
Number of Subcarriers	12	Number of Subcarriers	12
Slot config per sec	400	Slot config per sec	400
Lmax	2	Lmax	2
PDCCH aggregation level	4	PUCCH	1
Number of Res per CCEs	72	Number of Res per CCEs	72
SSB (Res)	48	-	-
DMRS (1 sym)	3300	DMRS (3Sym)	9900
PDCCH Res	1152	PUCCH Res	6600
Over head Res	4500	Over head Res	16500
Number of Total REs	68640	Number of total Res	42240
Available RBs for DL data transfer	64140	Available RBs for UL data transfer	25740
DL Throughput	712.556916	UL Throughput	285.956

參考資料

[1] O-RAN Open Fronthaul Conformance Test Specification 4.00

[2] O-RAN.WG1.O-RAN-Architecture-Description-v06.00

[3] O-RAN Working Group 2; A1 interface: General Aspects and Principles

[4] O-RAN WG1 Operations and Maintenance Architecture

[5] Cloud Architecture and Deployment Scenarios for O-RAN Virtualized RAN

[6] O-RAN Working Group 3; Near-Real-time RAN Intelligent Controller Architecture & E2 General Aspects and Principles

[7] O-RAN Fronthaul Working Group; Control, User and Synchronization Plane Specification

[8] O-RAN Alliance Working Group 4; Management Plane Specification

[9] 3GPP TS 38.401: NG-RAN; Architecture description

[10] 3GPP TS 38.460: NG-RAN; E1 general aspects and principles

[11] 3GPP TS 38.470: NG-RAN; F1 general aspects and principles

[12] 3GPP TS 38.300: NR; NR and NG-RAN Overall Description; Stage 2

[13] 3GPP TS 36.420: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 general aspects and principles

[14] 3GPP TS 38.420: NG-RAN; Xn general aspects and principles

[15] 3GPP TS 36.141: Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) conformance testing

[16] 3GPP TS 38.141-1: NR-FR1-TM1.1 [NR FR1] NR; Base Station (BS) conformance testing Part 1: Conducted conformance testing

[17] 3GPP TS 38.141-2: NR-FR2-TM1.1 [NR FR2] NR; Base Station (BS) conformance testing Part 2: Radiated conformance testing

[18] O-RAN WG4 Management Plane Specification version 06.00

[19] TS 138.104

[20] O-RAN WG4 Control, User and Synchronization Specification version 06.00

[21] O-RAN.WG8.IOT

[22] 3GPP TS 38.472: NG-RAN; F1 signalling transport, (Release 15.7.0)

[23] 3GPP TS 38.473: NG-RAN; F1 Application Protocol (F1AP), (Release 15.13.0)

[24] 3GPP TS 38.474: NG-RAN; F1 data transport, (Release 15.3.0)

[25] O-RAN.WG8.AAD.0-v02.00: Base Station O-DU and O-CU Software Architecture and APIs

[26] O-RAN.WG5.C.1-v03.00: NR C-plane profile

[27] 3GPP TS 38.413: NG-RAN; NG Application Protocol (NGAP), (Release 15.11.0)

[28] 3GPP TS 38.331: Radio Resource Control (RRC) protocol specification, (Release 15.13.0)

[29] 3GPP TS 24.501: Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3, (Release 16.8.0)

[30] O-RAN End-to-End Test Specification 2.0

[31] 3GPP TS 33.511: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

[32] O-RAN ALLIANCE, O-RAN End-to-End System Testing Framework

[33] 3GPP TS 33.501: Security architecture and procedures for 5G System

[34] 3GPP TR 33.926: Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

[35] TS 38.425: NR user plane protocol,(Release 15.7.0)