TAICS

TAICS TS-0021-1 v2.0 : 2019

智慧巴士資通訊系統資安測試規範－第一部：一般要求v2

Intelligent Bus Telematics System Security Test Specification - Part 1: General Requirements v2

2019/08/13

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

智慧巴士資通訊系統資安測試規範

-第一部：一般要求 v2

Intelligent Bus Telematics System Security Test Specification

- Part 1: General Requirements v2

出版日期: 2019/08/13

終審日期: 2019/07/26

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：安華聯網科技股份有限公司 洪光鈞 總經理

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 蔡正煜 副主任

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 博士

TC5 物聯網資安工作組：財團法人資訊工業策進會 李岳翰

TC5 物聯網資安工作組：財團法人資訊工業策進會 林志濰

此標準制定之協會會員參與名單為(以中文名稱順序排列)：

中華電信股份有限公司、互聯安睿資通股份有限公司、台灣車聯網產業協會、安華聯網科技股份有限公司、行動檢測服務股份有限公司、果核數位股份有限公司、財團法人工業技術研究院、財團法人台灣電子檢驗中心、財團法人資訊工業策進會、財團法人電信技術中心、國立交通大學、趨勢科技股份有限公司。

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、用新科際整合有限公司、亞旭電腦股份有限公司、松穎科技股份有限公司、研華股份有限公司、國立雲林科技大學、晶復科技股份有限公司、極星國際航電股份有限公司、銓鼎科技股份有限公司、慧友電子股份有限公司、馥鴻科技股份有限公司、寶錄電子股份有限公司、寶儷明股份有限公司。

本規範由經濟部工業局支持研究制定。

目錄

前言

本規範係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業規範。

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。

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

引言

隨著硬體設備以及網路傳輸快速進步，物聯網應用已進入蓬勃發展階段。經濟部工業局於 2017 年宣示進入物聯網資安產業標準元年，致力於推動資安以及其檢測標準，包括影像監控系統資安標準、車聯網系統資安標準、物聯網通用資安標準、輔助應用程式資安標準、工控系統資安標準、醫療儀器資安標準及銷售點終端系統資安標準等，藉由資安標準訂定，國內物聯網產業能將產品優質化並更具有競爭力。智慧巴士為車聯網的子項目，目前公車產業已有八成公車(約兩萬兩千輛)轉換為智慧巴士，公車做為交通基礎建設的一部份，每年各縣市政府也會持續維護並更新公車相關軟硬體設備。因此為防範日益增多的車聯網資安事件，例如巴西 Curitiba city 巴士總站與中國麗水市內的智慧站牌遭不明入侵播放色情影片，以及美國舊金山交通運輸系統遭駭停擺，導致市政府不得不免費讓民眾搭乘直到系統修復為止等，希望藉由 TAICS TS-0020 智慧巴士資通訊系統資安標準系列(以下簡稱 TAICS TS-0020 系列)之制定，提供產品商或系統服務商在研發產品時有可遵循之安全設計準則，以提升國內智慧巴士資通訊系統相關產品之品質及競爭力。

本規範乃配合「台灣資通產業標準協會」(Taiwan Association of Information and Communication Standards，以下簡稱 TAICS)制定之 TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」標準所訂定，其中具體明列資安檢測之測試項目、測試條件、測試方法及預期結果等事項；並確保測試程序的完整性及測試資料的一致性，俾利智慧巴士資通訊系統裝置製造商、系統整合商及物聯網資安檢測實驗室等作為相關產品檢測技術的參考藍本。

本規範因應 TS-0020-1 版本更新，進行文件內容改版。改版內容將安全要求加入分級制度、增加網路管理介面安全要求，另對原測試規範內容進行調整。改版差異請見版本修改紀錄。

1. 適用範圍

本規範依據 TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」訂定，適用於下述產品之資安檢測：

(a) 安裝於座位在十人座以上或總重量逾三千五百公斤之營業用大客車、座位在二十五人座以上或總重量逾三千五百公斤之幼童專用車上，主要功能以行車資訊串接、安全輔助、駕駛輔助及車輛管理輔助為目的之車載機產品。

(b) 架設於營業用大客車所行駛營運路線站點，提供到站資訊或即時動態資訊之智慧站牌產品。

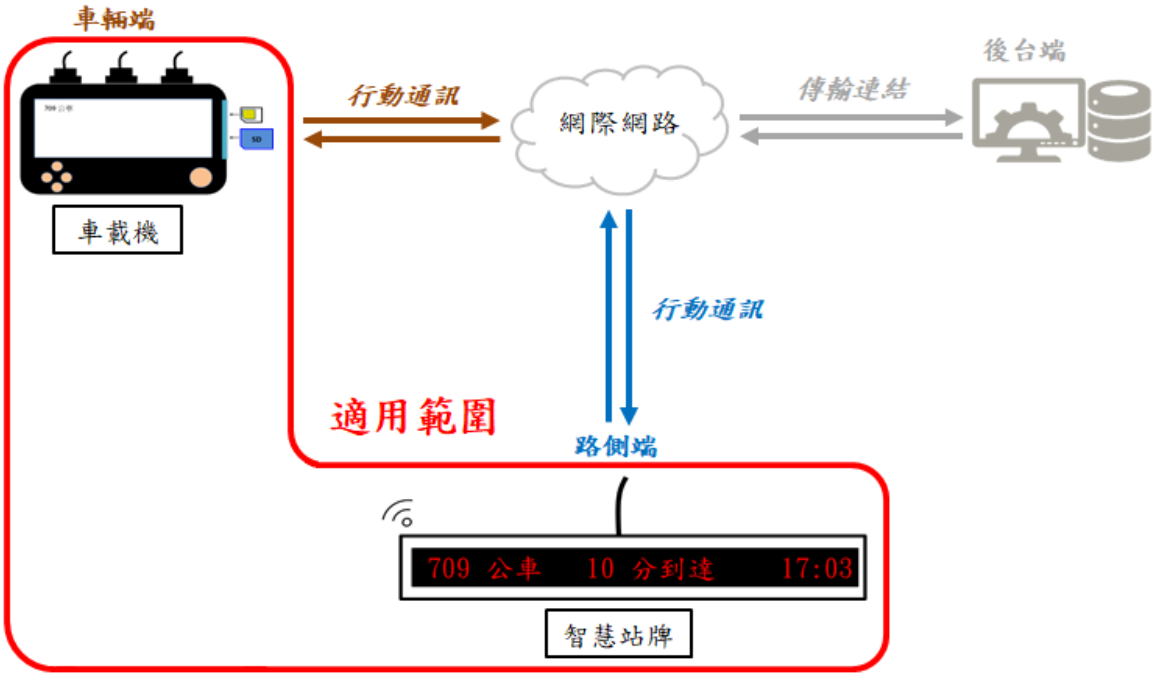

圖 1 適用範圍示意圖

2. 引用標準

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

TAICS TS-0020-1 「智慧巴士資通訊系統資安標準－第一部：一般要求」

台灣車聯網產業協會 「營業大客車車載機產業標準」v2.0

台灣車聯網產業協會 「營業大客車智慧站牌產業標準」V1.5

3. 用語及定義

TAICS TS-0020-1「智慧巴士資通訊系統資安標準－第一部：一般要求」所述及下列之用語及定義適用於本規範。

3.1 網路埠掃描 (Port Scan)

網路埠，又稱為通訊埠或者連接埠，作為連網裝置與外部來源之間傳送/接收通訊資料，一般駭客使用網路埠掃描來偵測電腦有開啟哪些網路埠或網路服務，進一步探尋其常見弱點與漏洞，藉此找到未經授權的存取點。

3.2 日誌滾動 (Log Rotate)

日誌滾動是指系統管理中一個自動化歸檔過期日誌文件的過程，每次增加新日誌文件時，舊日誌文件名後面的數字就會增加，當舊日誌文件後面的數字超過設定臨界值時，可以被刪除或者存到他處來釋放儲存空間。日誌滾動提供了一個有效的方法來限制日誌文件的大小，同時保留近期的日誌用於分析。

4. 測試項目

本節依據 TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」制定相對應之安全測試項目與測試方法。

實機測試總表，如表 1 所示，第一欄為安全構面，包括：(1)系統安全、(2)通訊安全；第二欄為安全要求分項；第三欄為安全等級。本實機測試總表，須依循章節 5.1 至 5.2 之技術規範內容。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，產品須先通過較低安全等級之測試，始可進行進階等級之測試。

表 1 實機測試總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
系統安全	5.1.1 作業系統與網路服務安全測試	-	5.1.1.1 5.1.1.2	-
	5.1.2 網路服務管控測試	5.1.2.1	-	-
	5.1.3 軟韌體版本更新測試	5.1.3.1 5.1.3.4	5.1.3.2	5.1.3.3 5.1.3.5
	5.1.4 日誌檔與警示測試	5.1.4.1 5.1.4.2 5.1.4.3	-	-
	5.1.5 安全敏感性資料儲存測試	-	5.1.5.1 5.1.5.2	
	5.1.6 網頁管理介面安全測試	-	5.1.6.1	-
通訊安全	5.2.1 資料完整性及來源驗證測試	-	-	5.2.1.1
	5.2.2 安全敏感性資料傳輸測試	5.2.2.1(a)	-	5.2.2.1(b)
	5.2.3 傳輸對象限制測試	5.2.3.1	-	
	5.2.4 Wi-Fi 通訊安全測試	5.2.4.1 5.2.4.2	5.2.4.3	-

5. 資安測試規範

5.1 系統安全測試

檢視產品書面送審資料是否符合產品系統安全測試執行之測試條件需求，並依下列各測試項目進行實機測試。

5.1.1 作業系統與網路服務安全測試

5.1.1.1 測試作業系統與網路服務是否存在 CVSS v3 評分為 7.0 分以上之常見資安弱點與漏洞。

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.1.1 節。

(b) 測試目的：

驗證產品之作業系統與網路服務是否存在美國國家弱點資料庫所公開的常見弱點與漏洞資料，及通用漏洞評分系統 CVSS v3 評分為高資安風險之漏洞。

(c) 測試條件：

(1) 產品須保持出廠預設狀態。

(2) 廠商須提供作業系統層最高權限帳號(telnet 或 ssh 帳號等)進行登入掃描。

(d) 測試佈局：

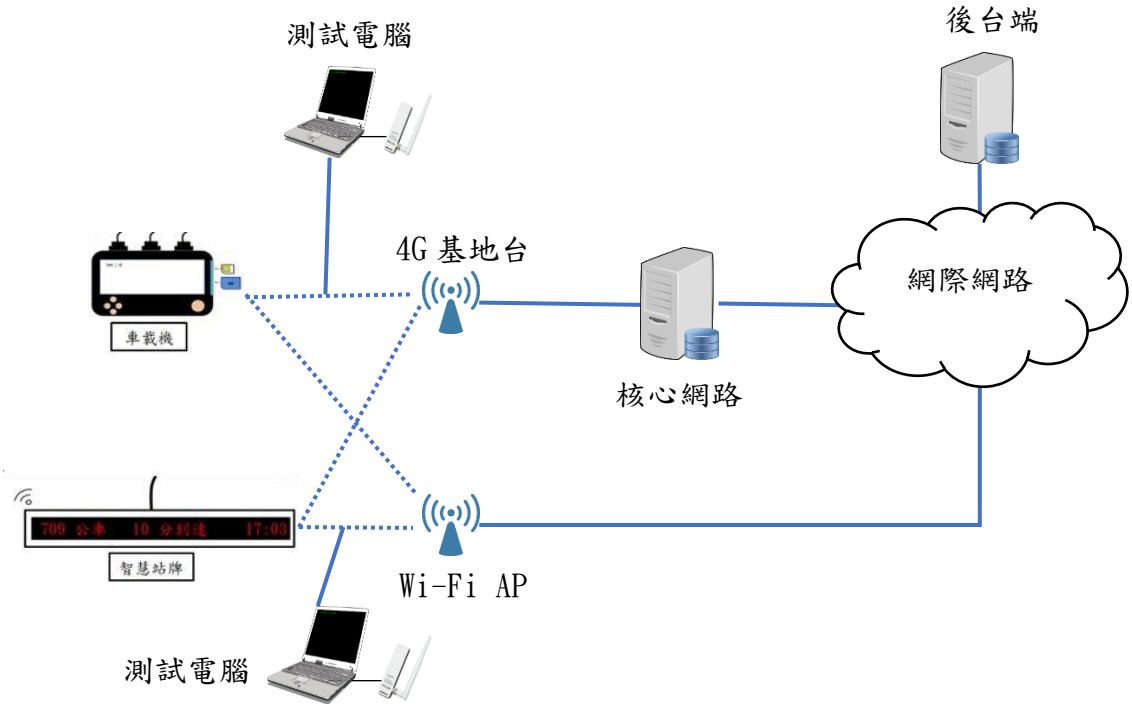

圖 2 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統及網路服務弱點掃描功能之工具，對產品執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，確認作業系統與網路服務是否存在國家弱點資料庫和通用漏洞評分系統(CVSS) v3.0 評分為 7 分以上之資安漏洞。

(f) 預期結果：

(1) 產品之作業系統與網路服務不存在美國國家弱點資料庫所公開的常見弱點與漏洞資料，及通用漏洞評分系統 CVSS v3 評分為 7 分以上之資安漏洞。

(2) 當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

5.1.1.2 測試未經授權軟體是否可以安裝及執行

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.1.2 節。

(b) 測試目的：

驗證產品是否限制未經授權軟體的安裝及執行。

(c) 測試條件：

(1) 產品須提供授權軟體清單。

(2) 產品須提供進入作業系統和安裝軟體及執行軟體之方法。

(3) 產品若無法於執行狀態下安裝軟體，則此測項不適用。

(d) 測試佈局：

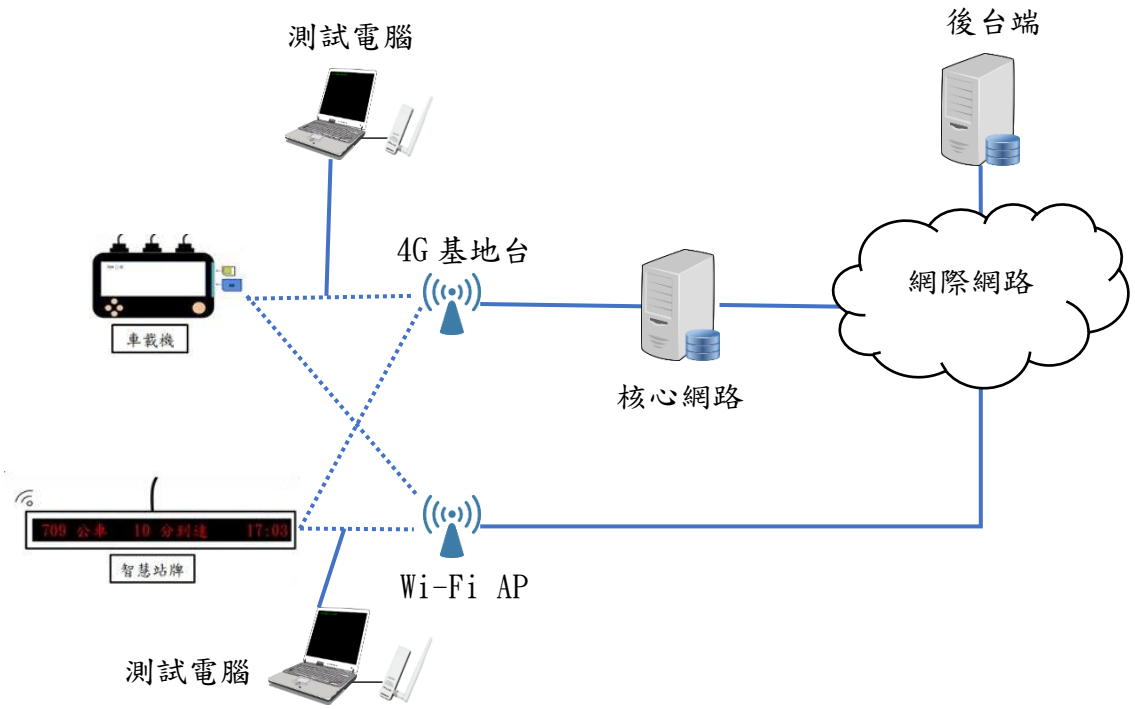

圖 3 測試示意圖

(e) 測試方法：

(1) 依照產品宣告之方法進入作業系統層。

(2) 安裝未經授權之軟體。

(3) 執行未經授權之軟體。

(f) 預期結果：

未經授權的軟體無法被安裝及執行。

5.1.2 網路服務管控測試

5.1.2.1 網路服務最小化測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第5.1.2.1 節。

(b) 測試目的：

驗證產品非必要服務所需的網路埠是否預設為關閉(產品開啟之網路服務與廠商提供規格須一致)。

(c) 測試條件：

(1) 產品須保持出廠預設狀態。

(2) 廠商須提供所啟用之網路服務與對應埠之宣告。

(d) 測試佈局：

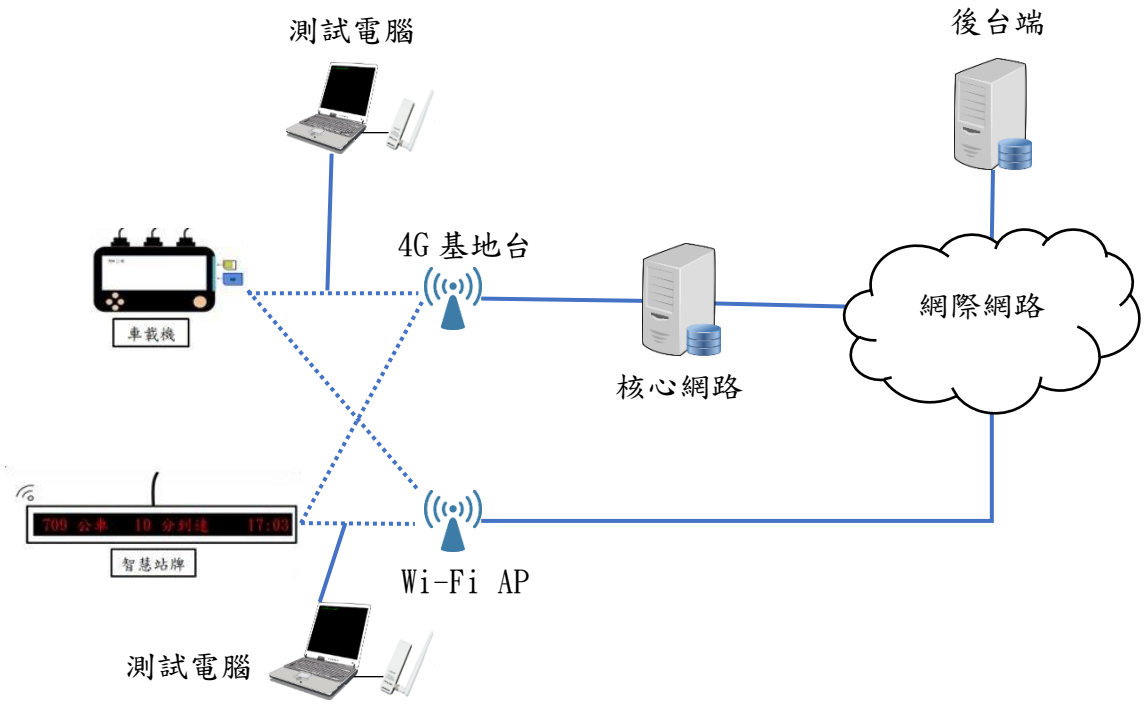

圖 4 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具網路埠掃描功能之工具，對產品執行 TCP 與 UDP 埠 0~65535 之掃描。

(3) 檢視掃描結果所呈現之網路服務與對應埠。

(4) 比對產品自我宣告中所聲明之網路服務與對應埠。

(f) 預期結果：

產品所開啟之網路服務與對應埠，與產品自我宣告之內容相符。

5.1.3 軟韌體版本更新測試

5.1.3.1 韌體更新測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.3.1 節。

(b) 測試目的：

驗證產品韌體是否具備更新機制。

(c) 測試條件：

(1) 廠商須提供韌體更新方法的說明。

(2) 產品須為 RTOS 或 Non-OS 設備，否則此測項不適用。

測試佈局：

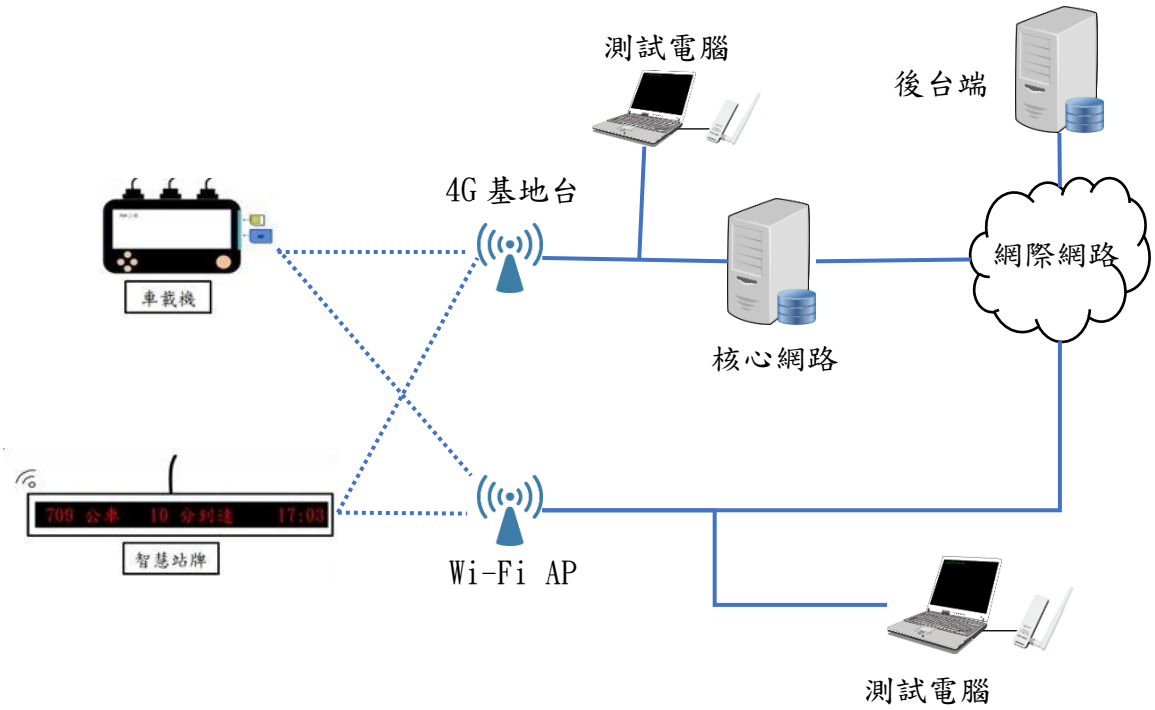

圖 5 測試示意圖

(d) 測試方法：

依據廠商提供之更新方法，執行產品更新，並檢視更新是否成功。

(e) 預期結果：

產品具備韌體更新機制。

5.1.3.2 應用程式更新及更新失敗備援測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.3.2 節。

(b) 測試目的：

驗證產品應用程式是否具備更新機制，以及更新失敗時，是否回復至更新版本前之狀態。

(c) 測試條件：

(1) 廠商須提供應用程式更新方法的說明。

(2) 本測項對象為執行「營業大客車車載機產業標準」、「營業大客車智慧站牌產業標準」所記載功能之應用程式。詳細功能分類請見附錄 C。

(d) 測試佈局：

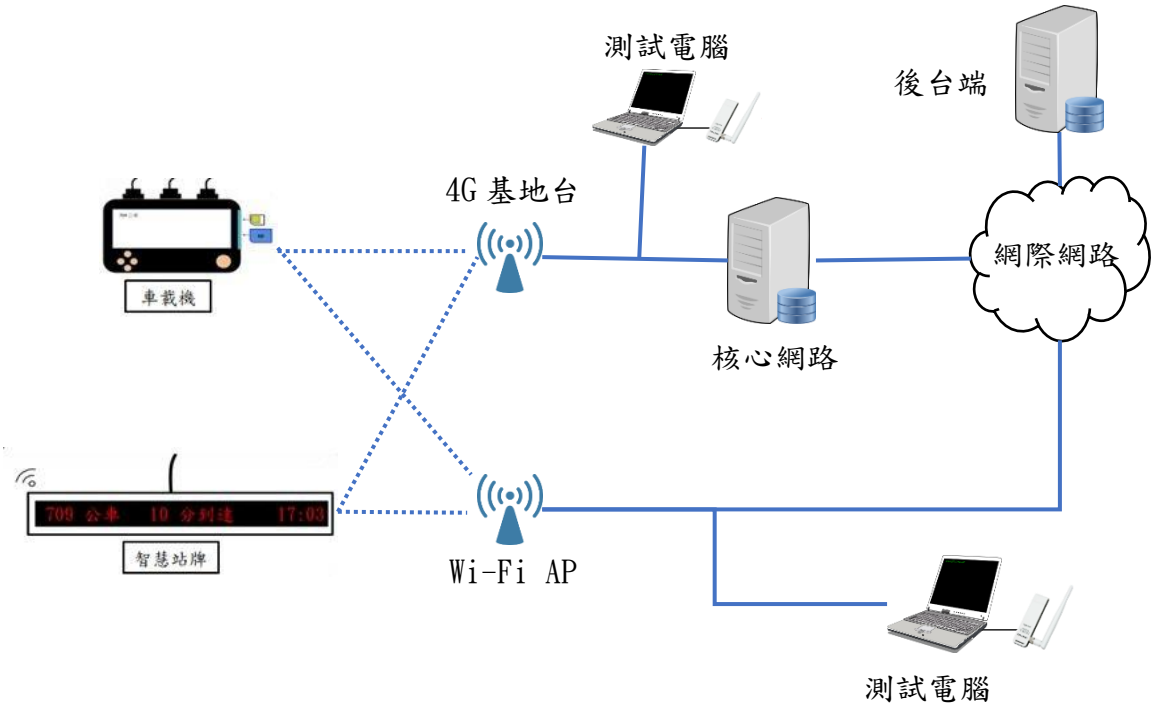

圖 6 測試示意圖

(e) 測試方法：

(1) 依據廠商提供之更新方法執行產品更新，並檢視更新是否成功。

(2) 於更新過程中(非檔案下載階段)，觸發更新中斷。

(f) 預期結果：

(1) 產品具備應用程式更新機制。

(2) 若更新失敗，產品仍可回復至更新版本前之狀態。

5.1.3.3 作業系統更新及更新失敗備援測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.3.3 節。

(b) 測試目的：

驗證產品作業系統是否具備更新機制，以及更新失敗時，是否回復至更新版本前之狀態。

(c) 測試條件：

廠商須提供作業系統更新方法的說明。

(d) 測試佈局：

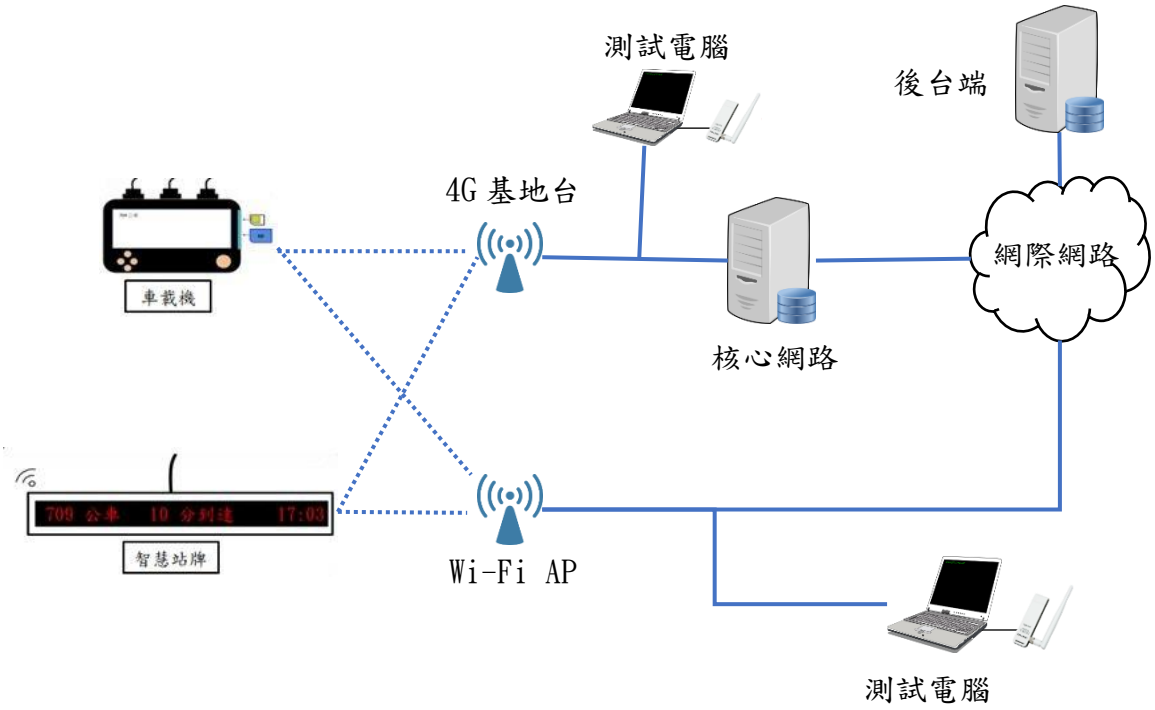

圖 7 測試示意圖

(e) 測試方法：

(1) 依據廠商提供之更新方法，執行產品更新，並檢視更新是否成功。

(2) 於更新過程中(非檔案下載階段)，觸發更新中斷。

(f) 預期結果：

(1) 產品具備作業系統更新機制。

(2) 若更新失敗，產品仍可回復至更新版本前之狀態。

5.1.3.4 更新檔之完整性測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.3.4 節。

(b) 測試目的：

驗證產品軟韌體更新是否驗證更新檔的完整性。完整性驗證功能須採用 FIPS PUB 140-2 Annex A[1]所核可之雜湊(hash)演算法。

(c) 測試條件：

(1) 產品須提供其完整性校驗機制。

(2) 產品須提供更新所使用之韌體或軟體檔案。

(d) 測試佈局：

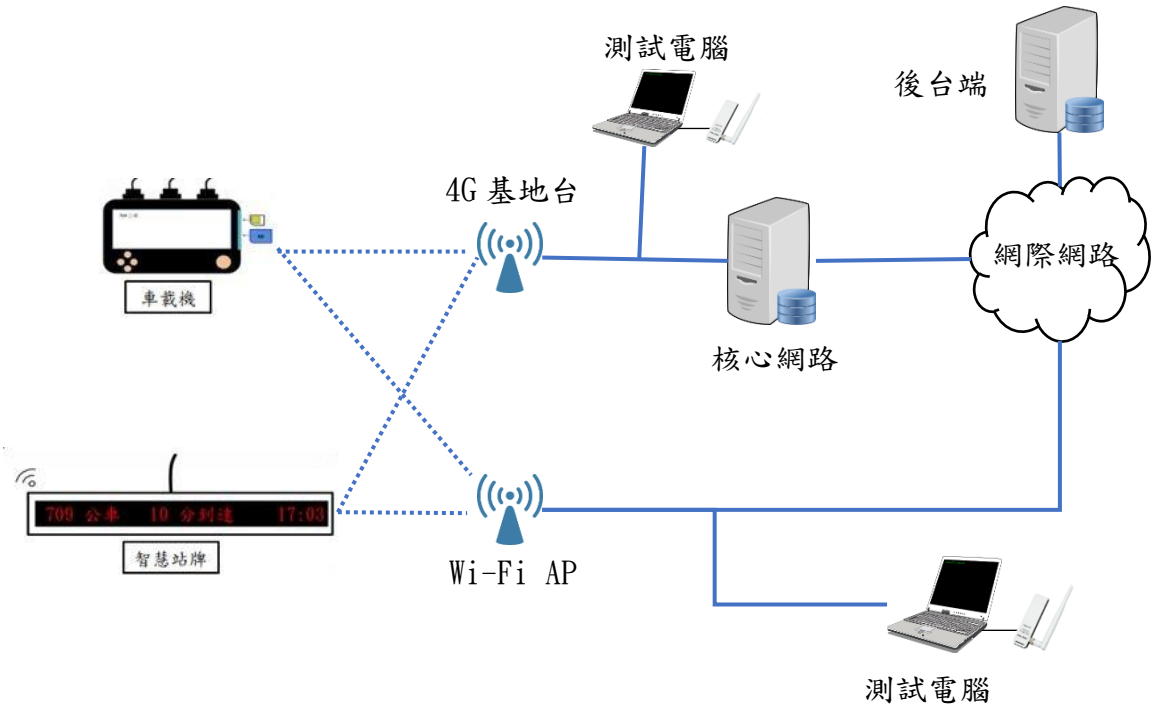

圖 8 測試示意圖

(e) 測試方法：

(1) 使用十六進位編輯器或其他可編輯二進位檔案之工具對更新檔進行修改。

(2) 依據廠商提供之更新方法，執行產品更新，並檢視更新是否成功。

(f) 預期結果：

產品更新失敗。

5.1.3.5 更新檔之合法性測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.3.5 節。

(b) 測試目的：

驗證產品軟體更新是否驗證更新檔的合法性。合法性驗證功能須採用 FIPS PUB 140-2 Annex A[1]所核可之簽章演算法。

(c) 測試條件：

(1) 情境 1：線上更新

(i) 產品須提供所有相連伺服器之宣告。

(ii) 受測廠商須協助觸發產品之線上更新。

(iii) 產品須保持出廠預設環境狀態。

(2) 情境 2：手動更新

(i) 產品須提供其數位簽章使用機制。

(ii) 產品須提供更新所使用之韌體或軟體檔案。

(d) 測試佈局：

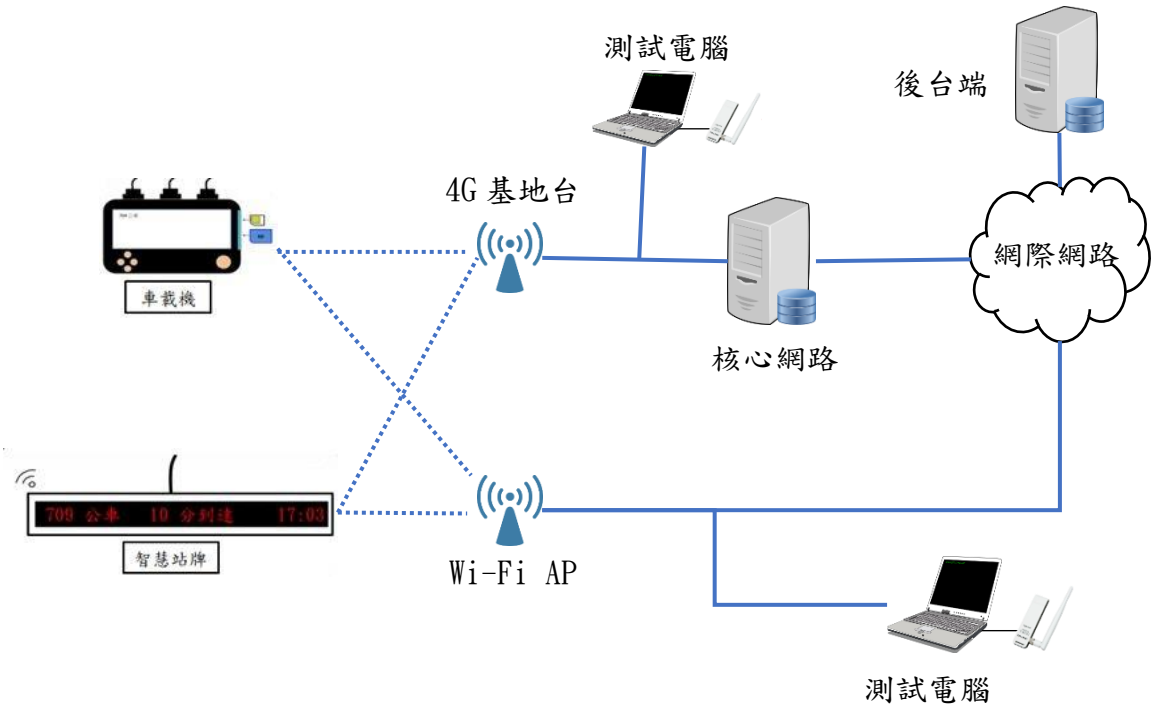

圖 9 測試示意圖

(e) 測試方法：

(1) 情境 1：

(i) 啟動安全通道掃描工具，對更新伺服器進行掃描。

(ii) 比對掃描結果，檢視伺服器所支援的密碼套件，是否符合 FIPS PUB 140-2 Annex A 所核可之簽章演算法。

(iii) 將測試電腦連接產品，並啟動更新。

(iv) 側錄更新伺服器與產品之間的封包，檢視所側錄之封包是否採用安全通道。

(v) 再次啟動更新。

(vi) 於更新伺服器發送憑證予產品之間攔截更新伺服器憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。

(vii) 發送已竄改之憑證予產品，於安全通道建立的交握過程中監聽封包，檢視產品是否接受此憑證。

(2) 情境 2：

(i) 竄改更新檔之憑證簽章。

(ii) 依據廠商提供之更新方法，執行產品更新，並檢視更新是否成功。

(f) 預期結果：

(1) 產品更新失敗。

(2) 產品軟體之簽章演算法，採用 FIPS PUB 140-2 Annex A 所核可之簽章演算法。

5.1.4 日誌檔與警示測試

5.1.4.1 安全事件紀錄測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.4.1 節。

(b) 測試目的：

驗證事件紀錄是否具時間戳記及事件內容。

(c) 測試條件：

(1) 情境 1：

(i) 產品本身具事件紀錄功能。

(ii) 產品須提供讀取介面觀看日誌內容 (如產品螢幕觀看或 USB 介面讀取等)，否則此測項不通過。

(2) 情境 2：

(i) 產品日誌存放在後台伺服器。

(ii) 廠商須提供日誌紀錄。

(d) 測試佈局：

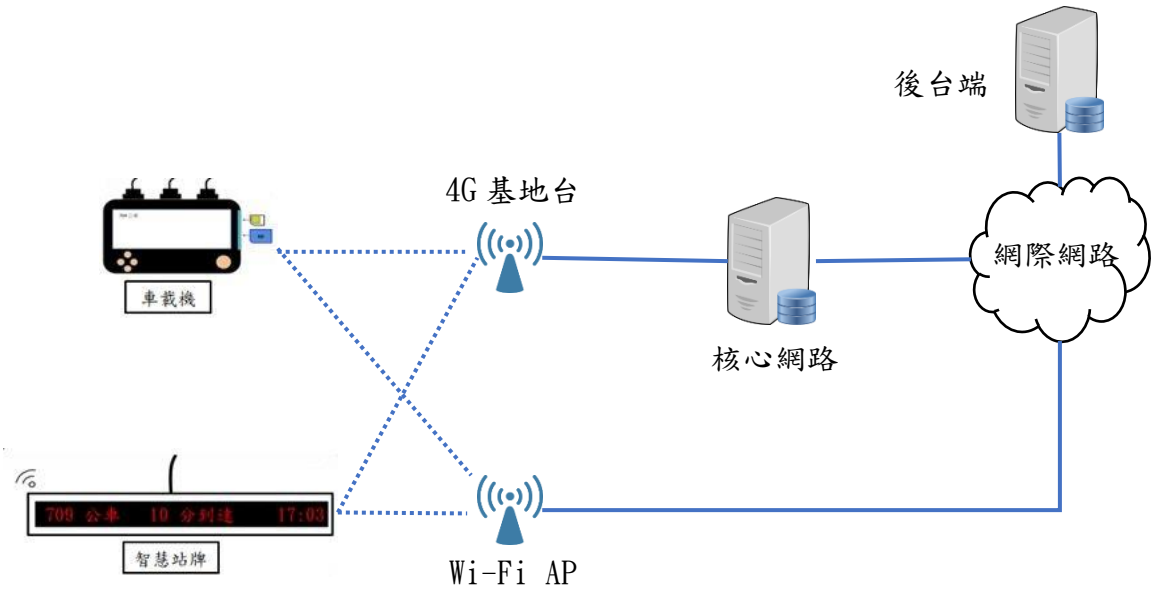

圖 10 測試示意圖

(e) 測試方法：

(1) 情境 1：

(i) 根據產品使用說明，開啟相應之讀取介面，瀏覽安全事件日誌。

(ii) 檢視日誌內容是否具時間戳記及事件內容。

(2) 情境 2：

(i) 檢視廠商提供之日誌資料，是否具時間戳記及事件內容。

(f) 預期結果：

產品提供安全事件日誌，且日誌內包含時間戳記及事件內容。

5.1.4.2 安全事件紀錄日誌檔之日誌滾動功能測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.4.2 節。

(b) 測試目的：

驗證產品是否具備日誌滾動(log rotate)機制處理日誌儲存空間不足之狀況。

(c) 測試條件：

(1) 產品日誌存放在後台伺服器，則此測項不適用。

(2) 廠商須提供日誌滾動觸發條件。

(3) 產品須提供讀取介面供使用者觀看日誌內容 (如產品螢幕觀看或 USB 介面讀取等)，否則此測項不通過。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 不斷觸發安全事件日誌，以填充安全事件紀錄儲存容量，直到儲存空間不足。

(2) 檢視產品是否無法正常記錄安全事件。

(f) 預期結果：

(1) 產品不會發生儲存空間不足的現象。

(2) 產品仍可正常記錄安全事件。

5.1.4.3 產品異常警示功能測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.4.3 節。

(b) 測試目的：

驗證產品發生異常時，是否進行推播或告警等警示機制。

(c) 測試條件：

無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 觸發產品定義之異常事件，如中斷網路，或網路遮罩。

(2) 發生異常事件時，檢視產品是否會通知管理者或推播警示、告警訊息。通知方式包含但不限近端螢幕顯示警訊、訊號燈熄滅，遠端通知警示等。

(f) 預期結果：

產品發生異常狀態時，發出推播或告警等警示機制。

5.1.5 安全敏感性資料儲存測試

5.1.5.1 安全敏感性資料權限管控測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第5.1.5.1 節。

(b) 測試目的：

驗證產品所儲存的安全敏感性資料，是否經授權方可存取。

(c) 測試條件：

(1) 產品須提供安全敏感性資料保存方式之書面資料作為審查依據。

(2) 產品須提供系統管理者權限供測試用。

(3) 產品須提供能進入作業系統層之介面。

(4) 產品不存在進入作業系統層之介面，則此測項不適用。

(d) 測試佈局：

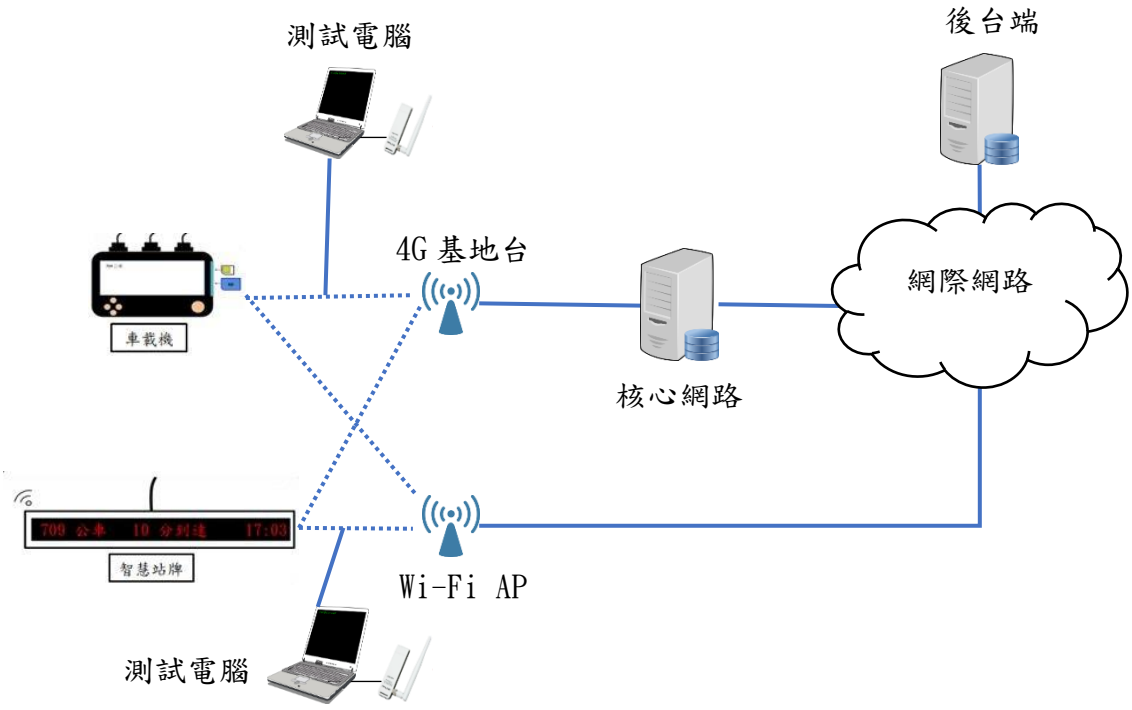

圖 11 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 依據產品所提供之安全敏感性資料保存方式，檢視其存取權限。

(f) 預期結果：

(1) 存取權限有區分為使用者、管理者。

(2) 產品所儲存的安全敏感性資料，須經管理者權限授權方可存取。

5.1.5.2 安全敏感性資料加密儲存測試

(a) 測試依據：

TAICS TS-0020-2 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.5.2 節。

(b) 測試目的：

驗證產品是否加密儲存安全敏感性資料，且加密方式是否採用 FIPS PUB 140-2 Annex A 所核可之演算法。

(c) 測試條件：

(1) 產品須提供安全敏感性資料儲存保護之加密演算法書面資料作為審查依據。

(2) 產品須提供系統管理者權限供測試用。

(3) 產品須提供能進入作業系統層之方法。

(4) 產品不存在進入作業系統層之介面，則此測項不適用。

(d) 測試佈局：

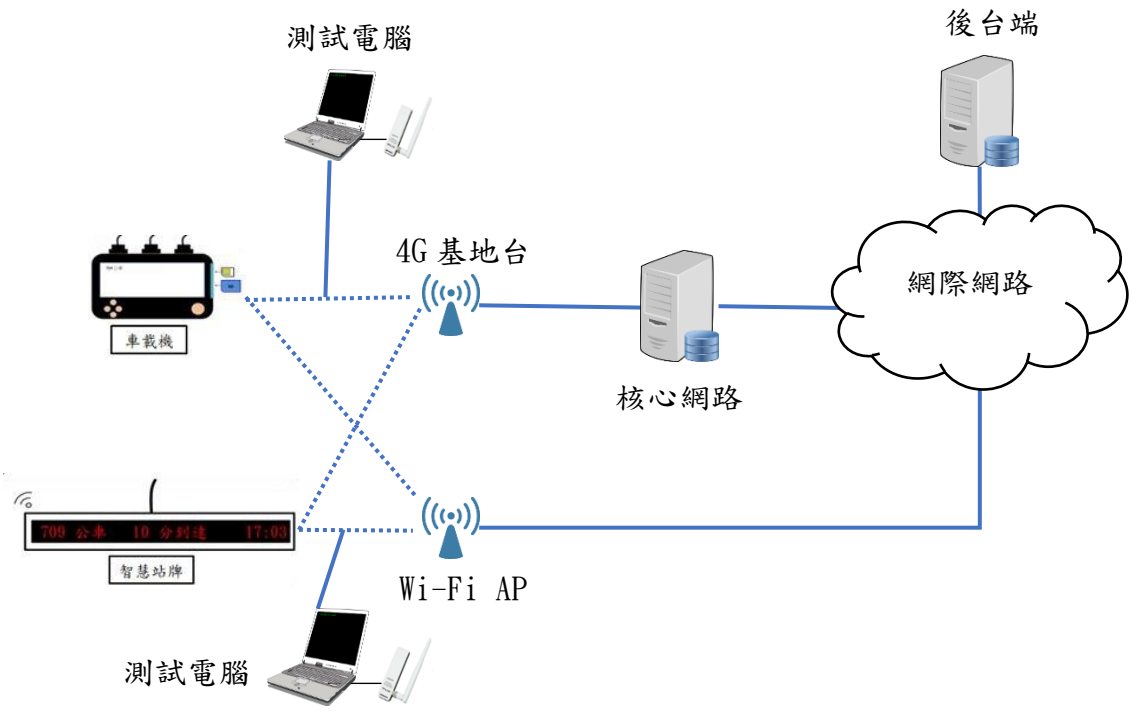

圖 12 測試示意圖

(e) 測試方法：

(1) 審閱能證明符合此安全要求之書面資料。

(2) 將測試電腦連接產品。

(3) 檢視保護安全敏感性資料所採用的保密機制。

(f) 預期結果：

安全敏感性資料的保密機制採用 FIPS 140-2 Annex A 所核可之加密演算法。

5.1.6 網頁管理介面安全測試

5.1.6.1 網頁管理介面常見資安風險測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.1.6.1 節。

(b) 測試目的：

驗證產品之網頁管理介面是否存在已知資安漏洞。

(c) 測試條件：

(1) 產品須提供系統管理者權限供測試用。

(d) 測試佈局：

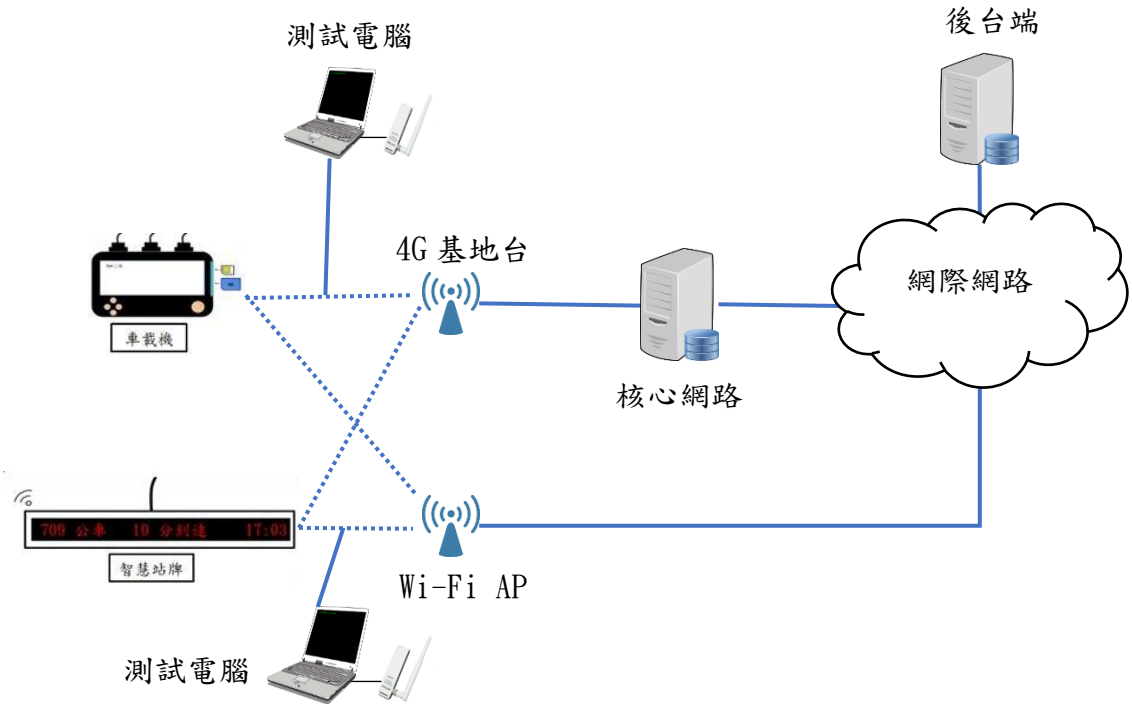

圖 13 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 開啟網頁管理介面，檢視網頁是否使用超文本傳輸協定。

(3) 啟動具備網頁弱點掃描功能之工具，對產品網頁介面執行弱點掃描。

(4) 檢視該弱點掃描工具所產生之報告，是否存在引發 Injection 及 Cross-Site Scripting (XSS)之資安攻擊風險。

(f) 預期結果：

產品之網頁管理介面，不存在引發 OWASP web Top 10 之 Injection 及 XSS 資安攻擊風險。

5.2 通訊安全測試

檢視產品書面送審資料是否符合產品通訊安全測試執行之測試條件需求，並依下列各測試項目進行實機測試。

5.2.1 資料完整性及來源驗證測試

5.2.1.1 資料完整性與驗證其來源測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.2.1.1 節。

(b) 測試目的：

驗證資料傳輸是否透過數位簽章來確保資料的完整性與驗證其來源。

(c) 測試條件：

(1) 產品須提供可與其傳輸資料之後台端。

(2) 此處資料之定義如附錄 C 所示

(d) 測試佈局：

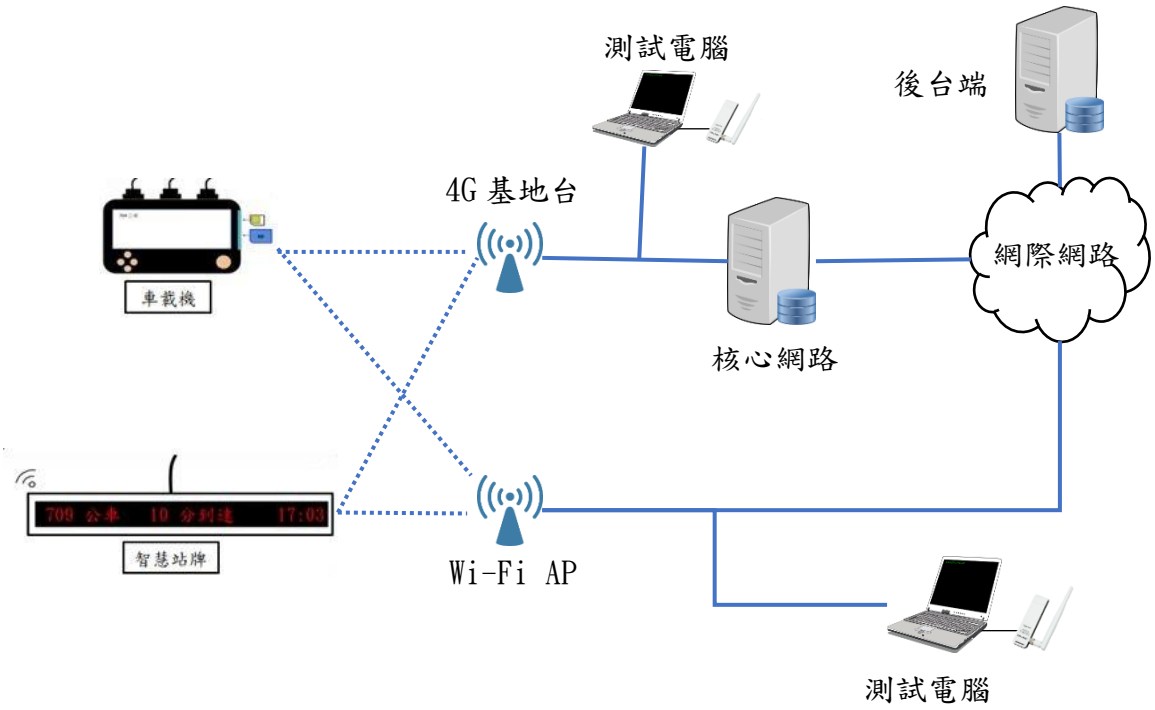

圖 14 測試示意圖

(e) 測試方法：

(1) 將產品與資料傳輸後台端建立連線。

(2) 請廠商觸發後台端傳送資料。

(3) 攔截資料並且對資料竄改，及使用未授權之電子簽章重新簽署。

(4) 將竄改及重新簽章之資料傳給受測產品，檢視其是否接收資料。

(f) 預期結果：

傳輸遭竄改過的資料，不被受測產品所接收。

5.2.2 安全敏感性資料傳輸測試

5.2.2.1 安全敏感性資料之傳輸保護測試

(a) 初階測試：

(1) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.2.2.1 節。

(2) 測試目的：

驗證產品於前端設備到接入端裝置之間所傳輸安全敏感性資料是否加密。

(3) 測試條件：

Wi-Fi 不適用此測項。

(4) 測試佈局：

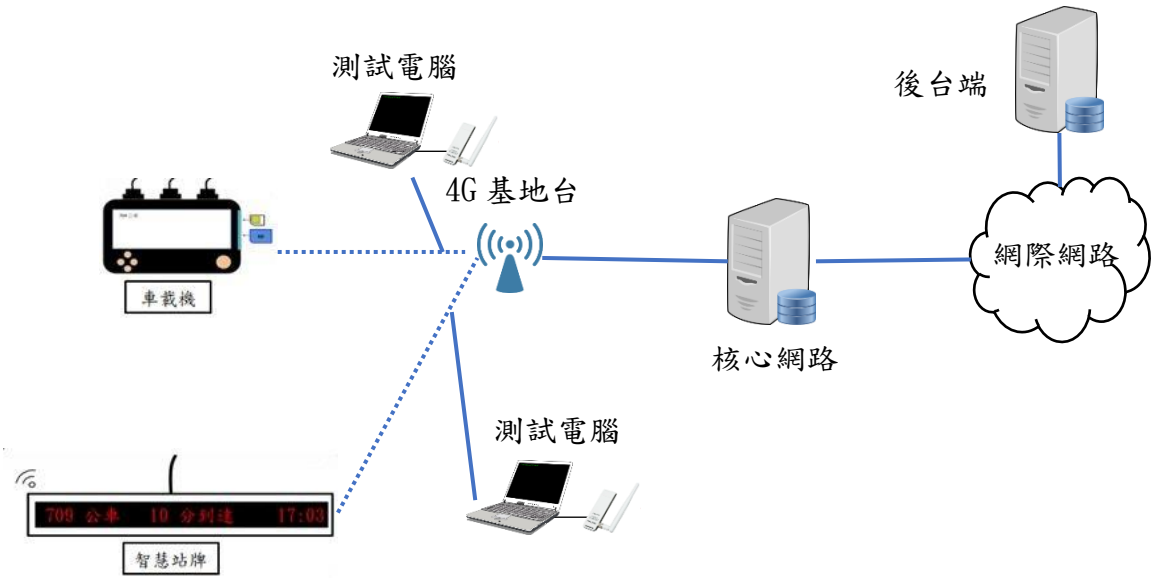

圖 15 測試示意圖

(5) 測試方法：

(i) 將產品與後台端建立連線。

(ii) 在身分鑑別程序進行期間，側錄身分鑑別封包是否加密。

(6) 預期結果：

產品於前端設備到接入端裝置之間所傳輸安全敏感性資料有加密。

(b) 中階測試：

(1) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.2.2.1 節。

(2) 測試目的：

驗證產品後端鏈路傳輸安全敏感性資料是否加密，且加密方式是否採用 FIPS PUB 140-2 Annex A 所核可之加密演算法。

(3) 測試條件：

無。

(4) 測試佈局：

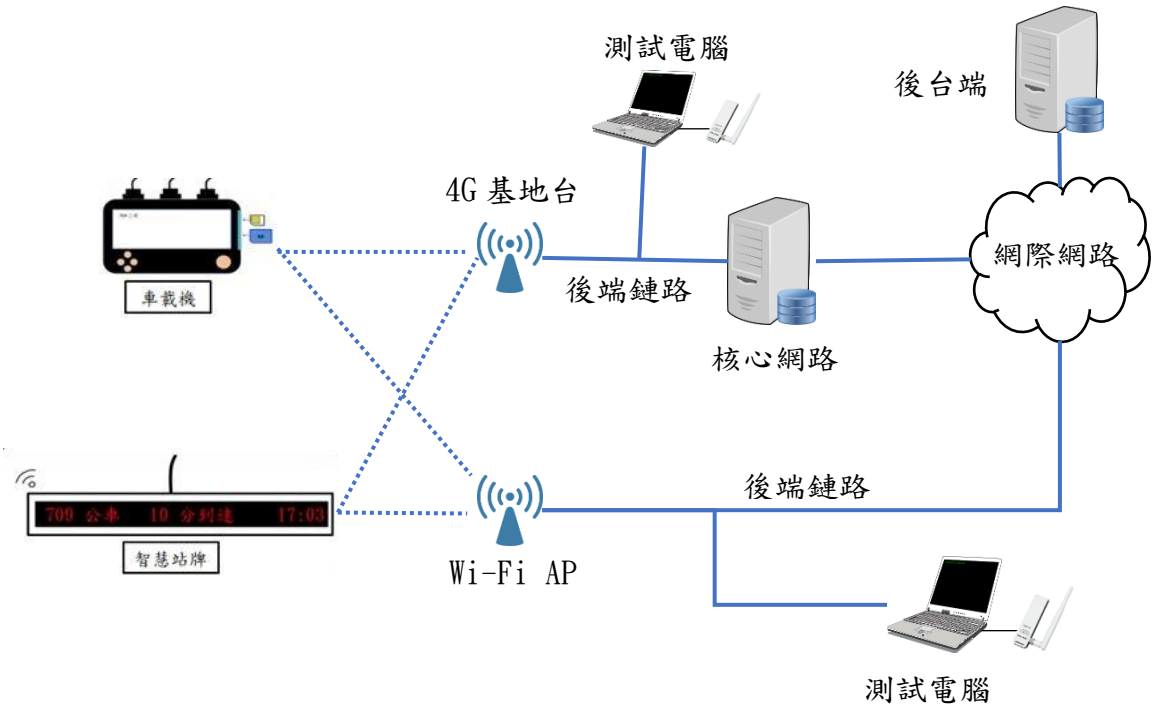

圖 16 測試示意圖

(5) 測試方法：

(i) 將產品與後台端建立連線。

(ii) 在身分鑑別程序進行期間，於接入設備(例如: 基地台、Wi-Fi AP)後端鏈路上側錄封包，檢視其是否加密。

(6) 預期結果：

產品後端鏈路傳輸安全敏感性資料採用 FIPS PUB 140-2 Annex A 所核可之加密演算法。

5.2.3 傳輸對象限制測試

5.2.3.1 產品資料傳輸測試

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」 第 5.2.3.1 節。

(b) 測試目的：

驗證產品資料遠端傳輸時，是否將資料傳輸到非認可之傳輸對象。

(c) 測試條件：

產品須提供允許傳輸的後台對象名單。

(d) 測試佈局：

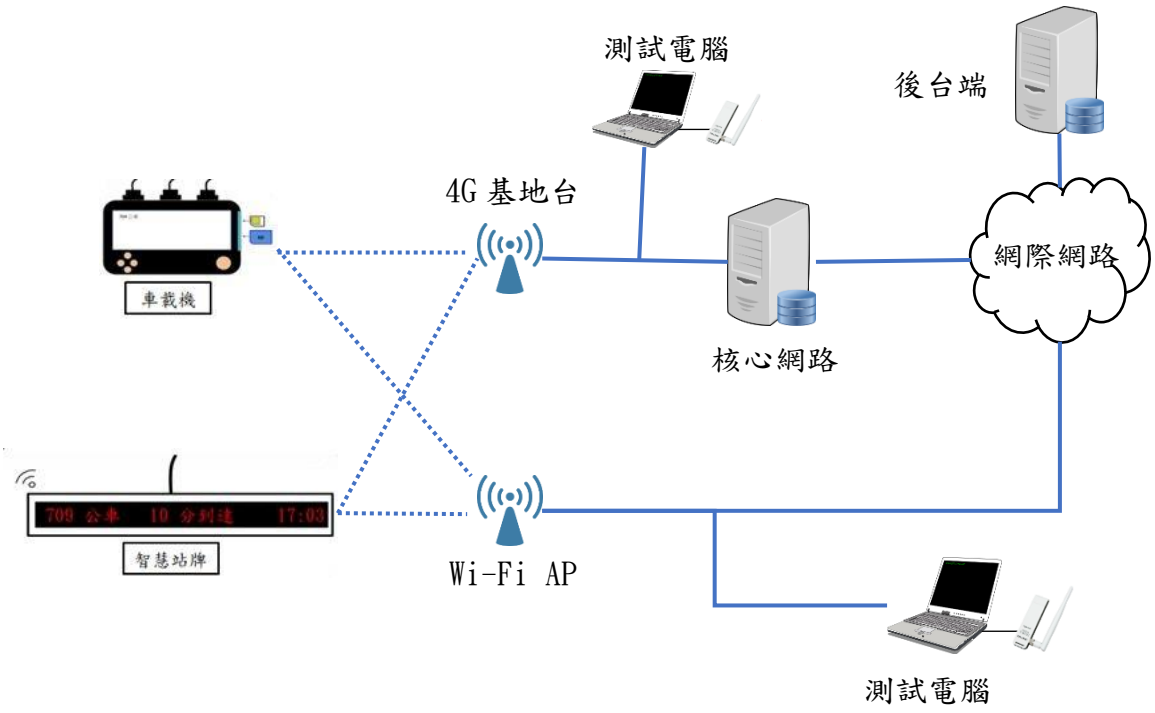

圖 17 測試示意圖

(e) 測試方法：

(1) 將產品與後台端建立連線。

(1) 側錄傳輸封包，檢視是否存在後台對象名單以外之傳輸對象。

(f) 預期結果：

傳輸對象與產品宣告一致。

5.2.4 Wi-Fi 通訊安全測試

5.2.4.1 安全的 Wi-Fi 組態設置測試(不具 Wi-Fi 功能或 WPS 功能之產品免測此項)

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.2.4.1 節。

(b) 測試目的：

驗證產品是否存在錯誤的 Wi-Fi 設定。

(c) 測試條件：

(1) 產品須支援 Wi-Fi 保護設置功能，否則此測項不適用。

(2) 產品須保持出廠預設環境狀態。

(d) 測試佈局：

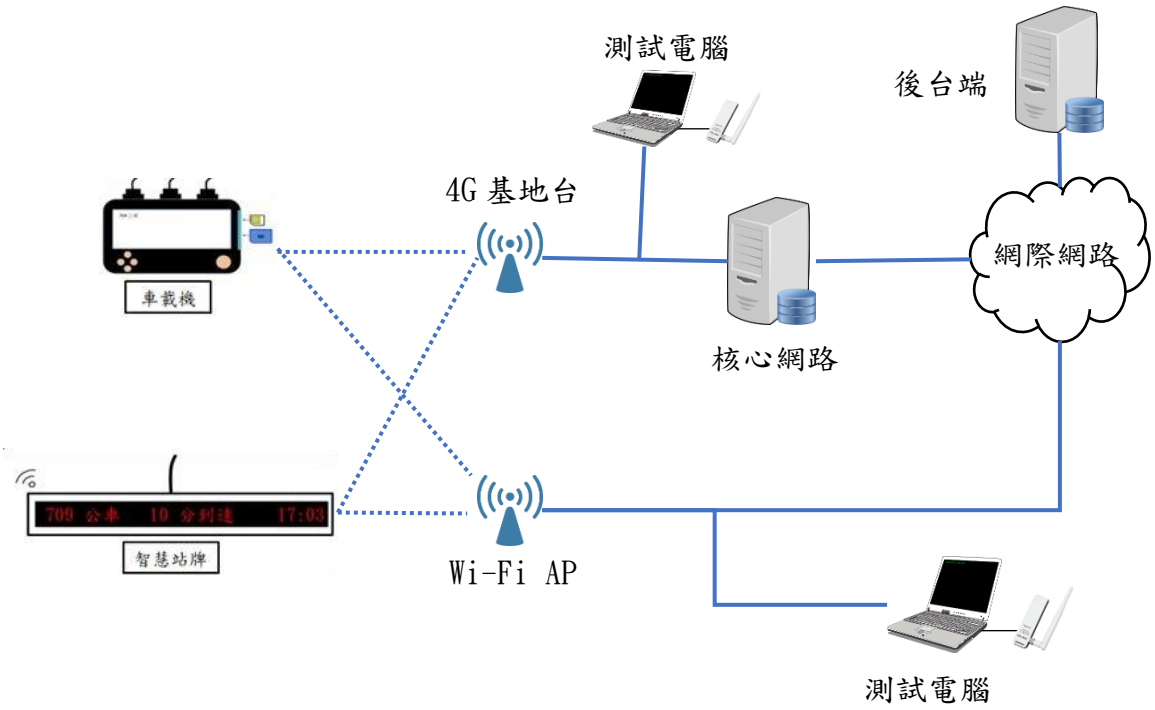

圖 18 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具。

(3) 檢視產品之操控程式或網頁管理介面，WPS PIN 是否存在供使用者操作的開/關介面，且此開/關功能是否有效。

(f) 預期結果：

(1) 有提供使用者 WPS PIN 開/關之功能。

(2) WPS PIN 功能預設為關閉。

5.2.4.2 Wi-Fi 網路之 Wi-Fi 保護設置測試(不具 Wi-Fi 功能之產品免測此項)

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.2.4.2 節。

(b) 測試目的：

驗證產品 Wi-Fi 網路之 Wi-Fi 保護設置是否使用 v2 同等或以上之版本。

(c) 測試條件：

產品具備 Wi-Fi 傳輸功能，否則此測項不適用。

(d) 測試方法：

(1) 將產品與後台建立連線，同時側錄 Wi-Fi 封包。

(2) 根據側錄結果驗證傳輸是否採用「Wi-Fi 保護存取 2」加密方式。

(e) 預期結果：

產品之 Wi-Fi 保護設置使用 v2 同等或以上之版本。

5.2.4.3 Wi-Fi 通訊協定異常輸入測試(不具 Wi-Fi 功能之產品免測此項)

(a) 測試依據：

TAICS TS-0020-1 v2.0「智慧巴士資通訊系統資安標準－第一部：一般要求」第 5.2.4.3 節。

(b) 測試目的：

驗證產品之 Wi-Fi 通訊協定是否存在未知之資安漏洞。

(c) 測試條件：

產品具備 Wi-Fi 傳輸功能，否則此測項不適用。

(d) 測試方法：

(1) 將產品以 Wi-Fi 連線至測試電腦所模擬的 Wi-Fi 存取點(AP)。

(2) 啟動具模糊測試功能之工具。

(3) 執行對 IEEE 802.11x 通訊協定所有欄位至少 10 萬筆唯一且獨立之測試項，或者最少 8 小時的異常輸入測試。

(4) 確保同時間只能進行一個測試案例。

(5) 對產品執行影像監控之操作，檢查產品是否仍正常運作。

(e) 預期結果：

產品於測試過程中不會因為某一特定異常封包而發生程序崩潰(crash)。

附錄 A
(規定)
產品概述說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表 A.1 產品概述表

製造商	xxx
產 品 名 稱	xxx
廠 牌	xxx
型號	xxx
軟、韌體版本	xxx
通訊介面	WiFi/4G
網路服務 (埠號)	https(443)
傳輸對象 (IP)	SAMBA(8.8.8.x)
產品流量限制	一分鐘 512 bits
日誌存取權限	唯讀/寫入
角色存取權限	管理者：xxx 使用者：xxx
外觀	<圖>

附錄 B
(規定)
產品安全功能說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表 B.1 備安全功能說明表

項目	說明	申請者填寫內容
身分驗證方式	依步驟描述如何做不同使用者之身分驗證(如需帳密，請於此附上)。	
登入失敗計數器時效	說明登入失敗之計數器於多少時間後，失敗次數會歸零。	
加密演算法	詳細列出產品所使用之加密演算法及其應用。	
事件紀錄可用性警示或告警機制	描述事件紀錄無法傳輸或無法儲存時，其警示或告警方式，或提供佐證文件。	
連線逾時	描述使用者登入時間多久後逾時	

附錄 C
(參考)
運研所 97 年度公車動態資訊系統交換格式

表 C.1 運研所 97 年度公車動態資訊系統交換格式：控制中心-車機通訊伺服器

分類	功能
行車資訊	定時資料回傳
	定點資料回傳
訊息傳遞	公告訊息下載(供車內 LED 顯示)
	司機訊息下載(供駕駛座前顯示)
	車輛平衡間距訊息下載
	車機異常訊息通報
	通報各車輛之行車狀況(已排未發)
	通報各車輛之行車狀況(未排已發)
基本參數設定	路線名稱設定
	路線站牌設定
	站牌資料設定
班表設定	班表下載
	班表清除
	手動請求班表下載
訊息確認	下載訊息確認回報

表 C.2 運研所 97 年度公車動態資訊系統交換格式：控制中心-站牌通訊伺服器

分類	功能
基本參數設定與查詢	站牌資料查詢
	站牌資料設定
訊息傳遞	更新站牌即時公車資訊
	更新站牌文字資訊
	站牌異常狀況回報
訊息確認	下載訊息確認回報

參考資料

[1] National Institute of Standards and Technology (NIST), Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017.

版本修改紀錄

版本	時間	摘要
v1.0	2018/11/16	v1.0 出版
v2.0	2019/08/13	v2.0 出版

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw