TAICS

TAICS TS-0037 v1.0 : 2020

空氣品質微型感測裝置資安測試規範

Cybersecurity test specification for air quality micro sensing devices

2020 / 11 / 26

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

空氣品質微型感測裝置資安測試規範

Cybersecurity test specification for air quality micro sensing devices

出版日期: 2020/11/26
終審日期: 2020/11/09

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：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 毛敬豪 所長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 副主任

技術編輯：財團法人資訊工業策進會 賴怡伶 工程師

此規範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、安華聯網科技股份有限公司、社團法人台灣智慧建築協會、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣商品檢測驗證中心、財團法人資訊工業策進會、國立交通大學、群暉科技股份有限公司德凱認證股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

中華資安國際股份公司、卡訊電子股份有限公司、行政院環保署、柏昇科技股份有限公司、建構民生公共物聯網計畫推動小組、訊舟科技股份有限公司、振興發科技有限公司、國立台灣科技大學、捷思環能股份有限公司、經濟部標準檢驗局、福華電子股份有限公司、維新應用科技股份有限公司、廣域科技股份有限公司

本規範由經濟部工業局支持研究制定。

目錄

前言

本規範依據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

行政院環保署針對空氣品質，於 2012 年發布了空氣品質等級指標與空氣品質標準，並於空氣品質監測網發布，一般民眾可便利地了解日常空氣品質，更提供各主管機於污染熱區的觀察與監測。環保署更在 2017 年起在工業區、道路等場域，布建空氣品質微型感測裝置進行污染熱區監測，至 2020 年預計布建達 10,200 個空氣品質微型感測裝置。

空氣品質微型感測裝置為環境感測物聯網平台架構中的前端聯網裝置，提供環保署監控我國各地重點污染熱點之空氣品質，當聯網設備遭遇網路資安威脅與攻擊的機率逐漸升高，空氣品質微型感測裝置應用上便可能面臨資安威脅。本規範制定之目的為協助環保署與各地方政府相關單位，於其規畫布建之空氣品質感測之物聯網設備上加強資安防護能力，藉由空氣品質微型感測裝置資安測試規範將標準條文轉換成具體化之檢測方法，引領空氣品質微型感測裝置與其相關物聯網應用廠商有效率地導入資安防護概念與技術。

TAICS TS-0037「空氣品質微型感測裝置資安測試規範」(以下簡稱本測試規範)，依據台灣資通產業標準協會所制定之 TAICS TS-0036「空氣品質微型感測裝置資安標準」[1]訂定，其中具體明列資安檢測之測試項目、測試條件、測試方法與檢測結果等事項，俾利空氣品質微型感測裝置裝置製造商、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。

1. 適用範圍

本規範為依據 TAICS TS-0036 v1.0「空氣品質微型感測裝置資安標準」規定，所訂定之測試規範。適用範圍為由微控制器(MCU)、感測組件、網路傳輸模組/裝置所組成之空氣品質微型感測裝置，如下圖 1 所示，主要用於即時監測空氣品質並掌握污染來源。

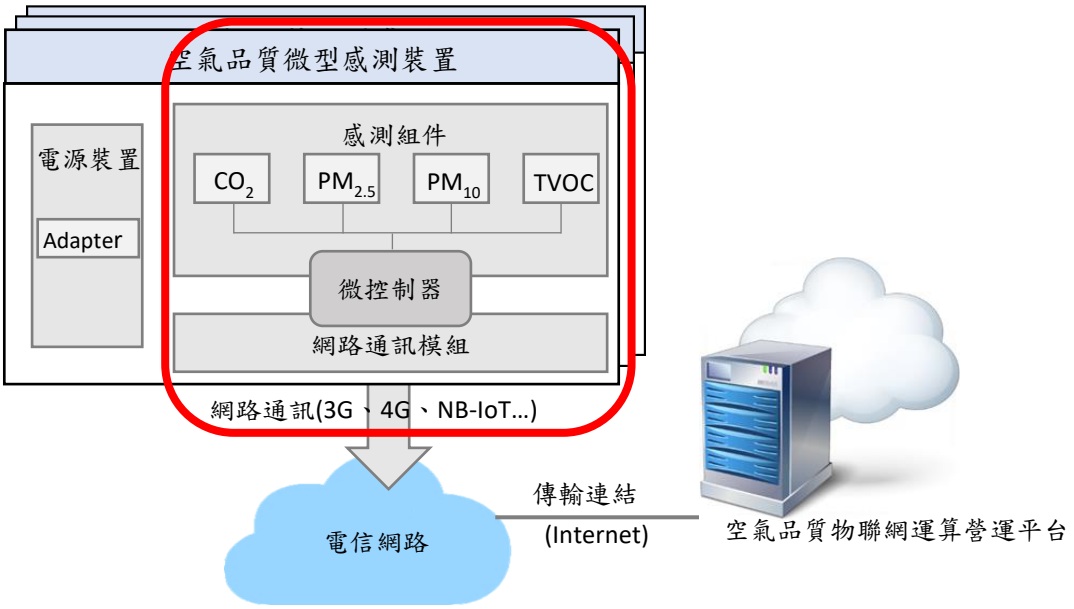

圖 1 適用範圍示意圖

2. 引用標準

下列法規、標準或文件因本規範所引用，成為本規範之一部分。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

[1] TAICS TS-0036：2020 空氣品質微型感測裝置資安標準

3. 用語及定義

TAICS TS-0036「空氣品質微型感測裝置資安標準」所述，及下列用語及定義適用於本標準。

3.1 密碼套件(Cipher suite)

係指使用於安全通道(SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分驗證、加密、訊息鑑別碼(MAC)和金鑰交換演算法。

3.2 網路埠(Port)

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/接收通訊資料的端口。

3.3 網路埠掃描(Port scan)

使用網路掃描工具對網路埠掃描來偵測電腦有開啟哪些網路埠或網路服務，以此確認可使用的埠口，進一步探尋其漏洞，藉此找到未經授權的存取點。

3.4 儲存紀錄(Logs)

係指產品本身所產生的資料檔案，例如：安全事件紀錄、感測數據之暫存檔案等。

4. 測試項目分級

本節依據 TAICS TS-0036「空氣品質微型感測裝置資安標準」制定相對應之安全測試項目與測試方法。

實機測試標準等級總表，如表 1 所示，第一欄為安全測試構面，包括：(1)身分識別、鑑別、權限控管、(2)資料機密性與完整性、(3)系統完整性、(4)軟韌體更新、 (5)已知漏洞安全及(6)資源可用性；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。

安全等級依(1)相關資安風險高低、(2)資料保護程度，分為 1 級、2 級二個等級，裝置須先通過初階安全等級之測試，始可進行高階等級之測試。

表 1 實機測試標準等級總表

安全構面	安全要求分項	安全等級	
		1 級	2 級
5.1 身分識別、鑑別、權限控管	5.1.1 鑑別機制	5.1.1.1 5.1.1.2	5.1.1.3
	5.1.2 權限管控	5.1.2.1	-
5.2 資料機密性與完整性	5.2.1 安全敏感性資料儲存	5.2.1.1 5.2.1.2	5.2.1.3
	5.2.2 傳輸資料保護	5.2.2.2	5.2.2.1 5.2.2.3 5.2.2.4
5.3 系統完整性	5.3.1 安全啟動	-	5.3.1.1
5.4 軟韌體更新	5.4.1 更新安全	5.4.1.1 5.4.1.2	-
5.5 已知漏洞安全	5.5.1 作業系統與網路服務	5.5.1.1 5.5.1.2	-
5.6 資源可用性	5.6.1 資源管理	-	5.6.1.1

5. 資安測試規範

5.1 身分識別、鑑別、權限控管要求測試

檢視空氣品質微型感測裝置之身分識別、鑑別、權限控管測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.1.1 鑑別機制測試

5.1.1.1 裝置識別碼唯一性測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.1.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗裝置之識別碼具唯一性。

(e) 測試條件：

(1) 須提供可與裝置相連之空氣品質物聯網運算營運平台。

(2) 須提供裝置至少 2 件。

(3) 須提供裝置識別碼編碼機制說明文件。

(f) 測試佈局：

如圖 2。

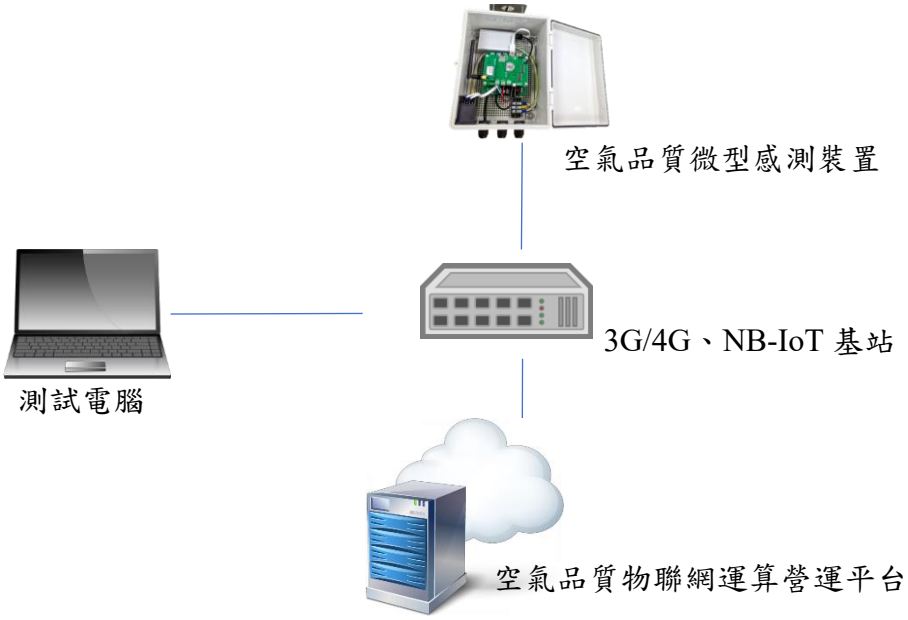

圖 2 測試示意圖

(g) 測試方法：

(1) 審閱具備此程序說明之書面資料。

(2) 檢視裝置識別碼之編碼機制。

(3) 將測試電腦與裝置連結在同一個區域網路中。

(4) 將裝置與空氣品質物聯網運算營運平台對連。

(5) 設定中間人攔截熱點，於安全通道建立階段，開啟封包側錄工具進行側錄。

(6) 側錄封包並檢視識別碼是否與裝置識別碼編碼機制一致。

(7) 將另一件裝置與空氣品質物聯網運算營運平台對連，重複步驟(5)~(6)。

(h) 檢測結果：

(1) 裝置唯一識別碼採用通用唯一識別碼編碼方法同等或以上重覆概率的編碼方式。

(2) 兩裝置之裝置識別碼相異。

(3) 通過：(1)~(2)項結果皆符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：無。

5.1.1.2 鑑別機制強度測試

實體介面

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.1.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

裝置之系統管理員帳密。

(d) 測試目的：

查驗不可透過裝置實體介面，直接存取裝置之除錯模式。

(e) 測試條件：

(1) 裝置須保持出廠預設組態。

(2) 裝置若存在除錯模式介面，須於文件中說明進入除錯模式之方法。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 檢查裝置是否存在可進入除錯模式之介面。

(2) 若存在可控制除錯模式之介面，則執行以下步驟。

(3) 根據文件所述連接相應之實體介面。

(4) 測試電腦連接裝置之 UART 埠，並開啟相應之管理介面連接工具。

(5) 透過 UART 埠存取之除錯模式。

(6) 測試電腦連接裝置之 JTAG 埠，並開啟相應之管理介面連接工具。

(7) 透過 JTAG 埠存取之除錯模式。

(8) 測試電腦連接裝置之 USB 埠，並開啟相應之管理介面連接工具。

(9) 透過 USB 埠存取之除錯模式。

(h) 檢測結果：

(1) 裝置不存在進入除錯模式之介面。

(2) 裝置透過 UART 及 JTAG 及 USB 存取除錯模式時，裝置要求身分鑑別。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用： 無。

通訊 API 介面

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.1.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

空氣品質物聯網運算營運平台所傳送之裝置控制指令資料。

(d) 測試目的：

查驗裝置之通訊 API 具備可靠的身分鑑別機制。

(e) 測試條件：

須支援空氣品質物聯網運算營運平台遠端存取裝置功能。

(f) 測試佈局：

如圖 3。

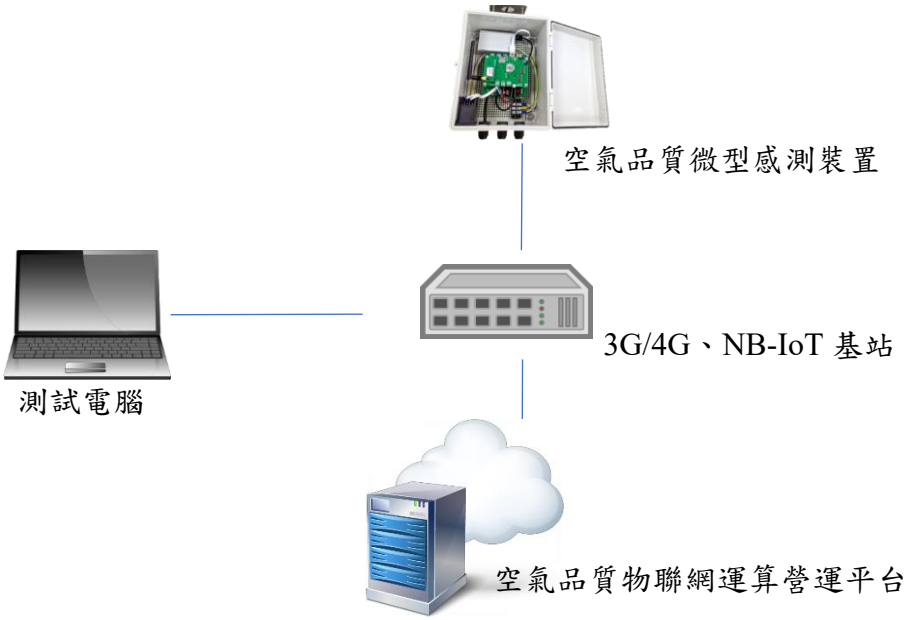

圖 3 測試示意圖

(g) 測試方法：

(1) 將測試電腦與空氣品質物聯網運算營運平台連結在同一個區域網路中。

(2) 將裝置連結空氣品質物聯網運算營運平台。

(3) 設定中間人攔截熱點，並開啟封包側錄工具進行側錄。

(4) 根據裝置使用說明，執行身分鑑別操作。

(5) 執行具通訊 API 功能之操作。

(6) 將側錄到的 API 功能操作封包，重新發送至受測裝置。

(7) 檢視通訊 API 功能之操作是否成功執行。

(8) 於另一次未進行身分鑑別操作時，嘗試執行具通訊 API 功能之操作。

(9) 檢視通訊 API 功能之操作是否成功執行。

(h) 檢測結果：

(1) 裝置須通過身分鑑別機制，方可執行通訊 API。

(2) 身分鑑別機制具備抵抗重送攻擊的能力。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用： 裝置不支援空氣品質物聯網運算營運平台遠端存取裝置功能。

(i) 檢測結果：

(1) 通過：(a)、(b)二項檢測結果皆符合，或(a)項檢測結果符合且(b)項檢測結果為不適用。

(2) 不通過：(a)、(b)二項檢測結果皆不符合。

(3) 不適用：無。

5.1.1.3 金鑰唯一性測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.1.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

裝置之安全通道的憑證。

(d) 測試目的：

查驗裝置安全通道之金鑰具唯一性。

(e) 測試條件：

裝置須存在安全通道之金鑰。

(f) 測試佈局：

如圖 4。

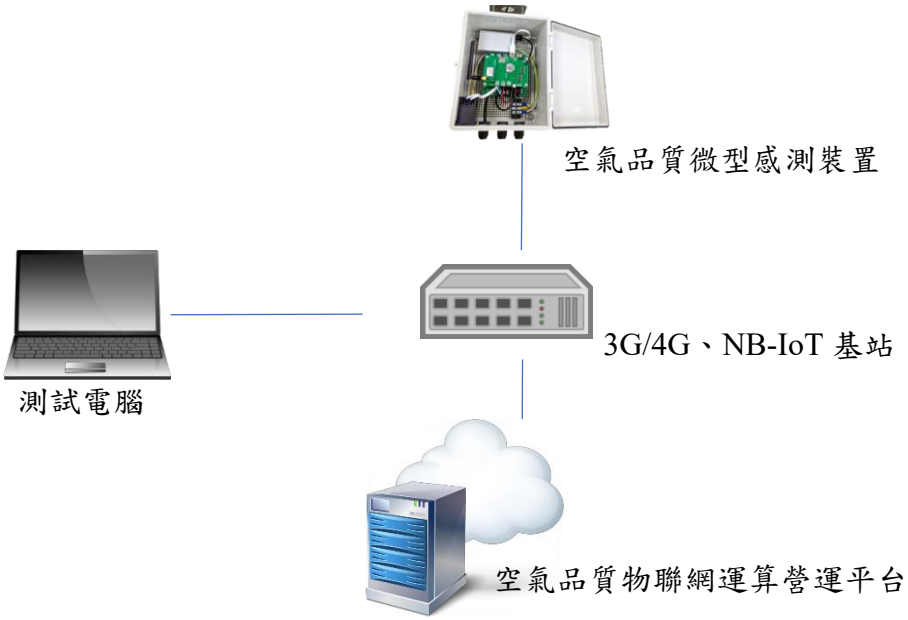

圖 4 測試示意圖

(g) 測試方法：

(1) 將測試電腦與裝置連結在同一個區域網路中。

(2) 將裝置與空氣品質物聯網運算營運平台對連。

(3) 設定中間人攔截熱點，於安全通道建立階段，開啟封包側錄工具進行側錄。

(4) 側錄封包並擷取裝置之憑證，檢視其指紋碼(fingerprint)。

(5) 重置裝置至出廠預設狀態。

(6) 重覆步驟(2)~(5)。

(h) 檢測結果：

(1) 裝置重置出廠預設狀態前後，憑證之指紋碼是相異的。

(2) 通過：(1)項結果符合。

(3) 不通過：結果不符合。

(4) 不適用：裝置不存在安全通道之金鑰。

5.1.2 權限管控測試

5.1.2.1 權限管控機制

實體介面

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.1.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 裝置之一般使用者帳密。

(2) 裝置之系統管理者帳密。

(d) 測試目的：

查驗裝置實體介面之存取具有權限控管機制且遵從最小權限原則。

(e) 測試條件：

(1) 須提供裝置之角色存取權限宣告。

(2) 須具備可存取裝置實體之介面。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據文件所述連接相應之實體介面。

(2) 若裝置支援 UART，將測試電腦連接裝置之 UART。

(3) 透過 UART 埠存取裝置之除錯模式。

(4) 以一般使用者帳密登入。

(5) 存取裝置資源，檢視該帳號之身分類型與其對應之權限是否與裝置自我宣告相符。

(6) 以系統管理者帳密登入。

(7) 存取裝置資源，檢視該帳號之身分類型與其對應之權限是否與裝置自我宣告相符。

(8) 若裝置支援 JTAG，將測試電腦連接裝置之 JTAG。

(9) 透過 JTAG 埠存取裝置之除錯模式。

(10) 重複(5)~(7)步驟。

(11) 透過 USB 埠存取裝置之除錯模式。

(12) 重複(5)~(7)步驟。

(13) 檢視廠商之角色存取權限宣告是否符合最小權限原則。

(h) 檢測結果：

(1) 於 UART 及 JTAG 及 USB 介面之身分授權與裝置角色存取權限宣告相符。

(2) 裝置須支援創建多個不同權限使用者之功能。

(3) 裝置之存取權限宣告符合最小權限原則。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項結果不符合其一。

(6) 不適用：裝置不具備存取裝置實體之介面。

通訊 API

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.1.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

空氣品質物聯網運算營運平台所傳送之裝置控制指令資料。

(d) 測試目的：

查驗裝置通訊 API 之使用具有權限控管機制。

(e) 測試條件：

(1) 裝置須提供角色存取權限之宣告。

(2) 裝置須支援通訊 API。

(3) 裝置須提供通訊 API 之傳輸方式。

(f) 測試佈局：

如圖 5。

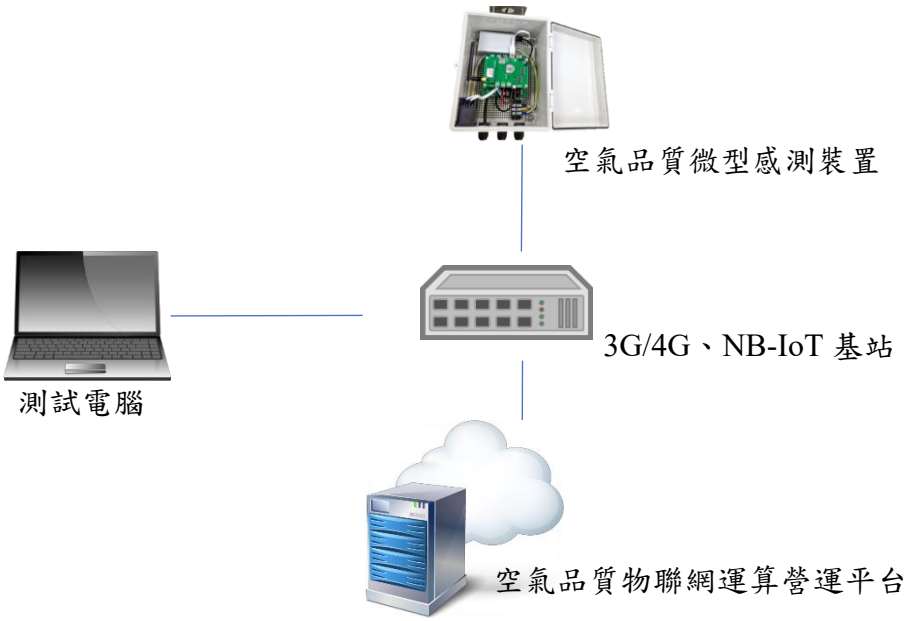

圖 5 測試示意圖

(g) 測試方法：

(1) 將測試電腦與空氣品質物聯網運算營運平台連結在同一個區域網路中。

(2) 將裝置連結空氣品質物聯網運算營運平台。

(3) 操作空氣品質物聯網運算營運平台執行裝置控制相關動作。

(4) 開啟 http 請求封包側錄工具並進行側錄。

(5) 發送具一般使用者權限之裝置控制 http 請求封包。

(6) 查看封包內容，檢視操作是否符合角色存取權限之宣告。

(7) 發送具系統管理者權限之裝置控制 http 請求封包。

(8) 查看封包內容，檢視操作是否符合角色存取權限之宣告。

(9) 嘗試以一般使用者權限，發送該權限外之裝置控制 http 請求封包。

(10) 檢視該請求是否成功被執行。

(11) 嘗試以系統管理者權限，發送該權限外之裝置控制 http 請求封包。

(12) 檢視該請求是否成功被執行。檢視廠商之角色存取權限宣告是否符合最小權限原則。

(h) 檢測結果：

(1) 於通訊 API 之身分授權與裝置角色存取權限宣告相符。

(2) 裝置須支援創建多個不同權限使用者之功能。

(3) 裝置之存取權限宣告符合最小權限原則。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項結果不符合其一。

(6) 不適用：裝置不具備存取裝置之通訊 API。

(i) 檢測結果：

(1) 通過：(a)、(b)二項檢測結果皆符合。

(2) 不通過：(a)、(b)二項檢測結果皆不符合。

(3) 不適用：(a)、(b)二項檢測結果皆不適用。

。

5.2 資料機密性與完整性測試

檢視空氣品質微型感測裝置之資料機密性與完整性測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.2.1 安全敏感性資料儲存測試

5.2.1.1 安全敏感性資料加密儲存測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗裝置之安全敏感性資料於儲存狀態下須加密保護。

(e) 測試條件：

(1) 裝置須提供安全敏感性資料儲存保護之演算法書面資料作為審查依據。

(2) 裝置須提供系統管理者權限供測試用。

(3) 裝置若存在除錯模式介面，須於文件中說明進入系統除錯模式之方法。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 檢查裝置是否存在可進入除錯模式之方法。

(2) 若存在可存取除錯模式之介面，則執行以下步驟。

(3) 將測試電腦連接裝置。

(4) 若裝置支援 UART，將測試電腦連接裝置之 UART。

(5) 透過 UART 埠存取除錯模式。

(6) 透過搜尋工具，查找安全敏感性資料位置。

(7) 檢視保護加解密金鑰所採用的保密機制。

(8) 若裝置支援 JTAG，將測試電腦連接裝置之 JTAG。

(9) 過 JTAG 埠存取除錯模式。

(10) 重複(5)~(7)之步驟。

(11) 若裝置支援 USB，將測試電腦連接裝置之 USB。

(12) 過 USB 埠存取除錯模式。

(13) 重複(5)~(7)之步驟。

(h) 檢測結果：

(1) 無法進入除錯模式介面。

(2) 加解密用金鑰的保密機制採用 NIST SP 800-140C 所核可同等或以上強度之加密演算法。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(2)項結果不符合。

(5) 不適用：裝置無存放安全敏感性資料。

5.2.1.2 韌體安全測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

產品之韌體檔案。

(d) 測試目的：

查驗裝置之韌體不存在明文或可被解密回復之安全敏感性資料。

(e) 測試條件：

(1) 須提供裝置之韌體燒錄工具與方法。

(2) 裝置須提供所使用之加密演算法書面資料作為審查依據。

(3) 裝置須提供所有相連空氣品質物聯網運算營運平台之宣告。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 檢視受測廠商之官網是否存在裝置韌體可供下載。

(2) 若廠商之官網不存在裝置韌體，則執行以下步驟。

(3) 審閱可證明所使用加密演算法之書面資料。

(4) 若燒錄接腳存在，使用廠商提供之工具，嘗試進行韌體萃取。

(5) 若韌體可萃取，使用具二進制檔案字串搜尋功能之工具，查找是否具有安全敏感性資料；若韌體不可萃取，由廠商提供裝置之韌體。

(6) 使用具韌體拆解功能之工具，對裝置之韌體進行拆解。

(7) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(8) 確認系統通行碼資料的保密機制是否採用 NIST SP 800-140C 所核可同等或以上強度之雜湊函數。

(9) 確認金鑰是否可被擷取。

(10) 確認是否存在非公開之 email 資料。

(11) 確認是否存在裝置所宣告之相連伺服器外之 IP 資料。

(12) 確認是否存在裝置所宣告之相連伺服器外之 URL 資料。

(h) 檢測結果：

(1) 韌體檔案不應置於公開存取之位置。

(2) 晶片中的韌體須加密保護且採用 NIST SP 800-140C 所核可同等或以上強度之加密演算法。

(3) 韌體無法解析出安全敏感性資料。

(4) 系統之更新來源應與廠商自我宣告中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。

(5) 通過：(1)(2)(4)三項結果皆符合，或(1)(3)(4)結果皆符合。

(6) 不通過：(1)(2)(4)三項結果不符其一，或(1)(3)(4)結果不符合其一。

(7) 不適用：無。

5.2.1.3 安全敏感性資料隔離保護測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

裝置所提供之安全區域設計資料。

(d) 測試目的：

查驗裝置安全敏感性資料之存放與正常作業系統隔離。

(e) 測試條件：

(1) 裝置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) 裝置須聲明使用到安全區域之資安功能的書面資料作為審查依據。

(f) 測試佈局：

無。

(g) 測試方法：

審閱具備此功能證明之書面資料。

(h) 檢測結果：

(1) 書面資料證實裝置之安全敏感性資料存放於安全區域。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用： 裝置無存放安全敏感性資料。

5.2.2 傳輸資料保護測試

5.2.2.1 控制指令完整性安全測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.2.1

(b) 安全等級：

2 級。

(c) 測試資料：

空氣品質物聯網運算營運平台之控制指令封包。

(d) 測試目的：

查驗裝置具備驗證空氣品質物聯網運算營運平台之控制指令完整性功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 7。

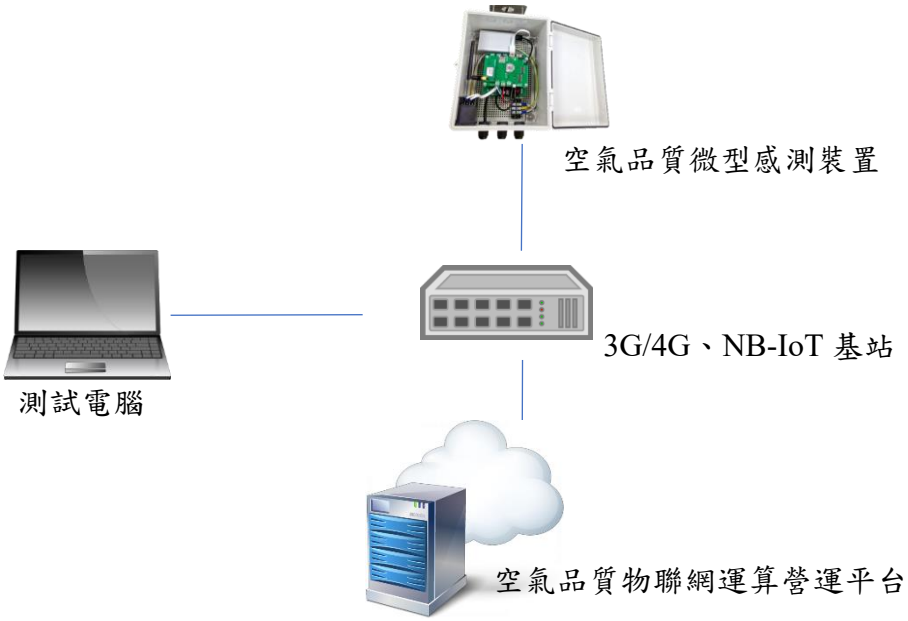

圖 6　測試示意圖

(g) 測試方法：

(1) 將測試電腦與空氣品質物聯網運算營運平台連結在同一個區域網路中。

(2) 將裝置連結空氣品質物聯網運算營運平台並開啟服務。

(3) 攔截傳送中之控制指令。

(4) 竄改攔截到的指令內容，並轉發給裝置。

(5) 檢視竄改過之資料是否可被裝置接受。

(6) 檢視雜湊演算法是否採用 NIST SP 800-140C 同等或以上強度之雜湊演算法。

(h) 檢測結果：

(1) 雜湊演算法須採用 NIST SP 800-140C 同等或以上強度之雜湊演算法。

(2) 裝置不可接受遭竄改之指令。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(i) 不適用：裝置無接收控制指令功能。

5.2.2.2 安全敏感性資料之傳輸保護測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

空氣品質物聯網運算營運平台之 IP 位址。

(d) 測試目的：

查驗裝置安全敏感性資料之傳輸，預設是否採用強度足夠之安全通道。

(e) 測試條件：

(1) 裝置須保持出廠預設環境狀態。

(2) 裝置須提供與裝置對連之空氣品質物聯網運算營運平台。

(f) 測試佈局：

如圖 8。

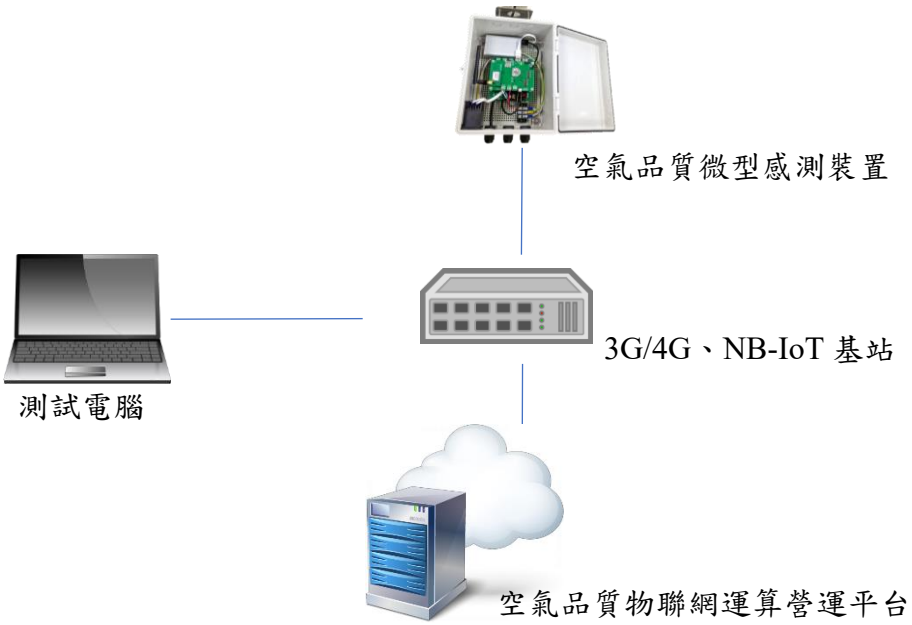

圖 7 測試示意圖

(g) 測試方法：

(1) 開啟安全通道掃描工具，對空氣品質物聯網運算營運平台進行掃描。

(2) 比對掃描結果是否為附錄 A 中所包含之密碼套件。

(3) 將測試電腦與空氣品質物聯網運算營運平台連結在同一個區域網路中，開始側錄封包。

(4) 將裝置與空氣品質物聯網運算營運平台連線。

(5) 檢視所側錄之夾帶安全敏感性資料的封包是否採用安全通道。

(h) 檢測結果：

(1) 裝置與空氣品質物聯網運算營運平台之安全敏感性資料傳輸，預設採用安全通道。

(2) 安全通道僅支援「附錄 A」中所建議之密碼套件。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：裝置無存在安全敏感性資料。

5.2.2.3 傳輸資料正確性安全測試

狀況 1：資料防竄改測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.2.3

(b) 安全等級：

2 級。

(c) 測試資料：

空氣品質物聯網運算營運平台之 IP 位址。

(d) 測試目的：

驗證裝置感測資料之傳輸，預設是否採用強度足夠之安全通道。

(e) 測試條件：

(1) 裝置須保持出廠預設環境狀態。

(2) 裝置須提供與裝置對連之空氣品質物聯網運算營運平台。

(f) 測試佈局：

如圖 9。

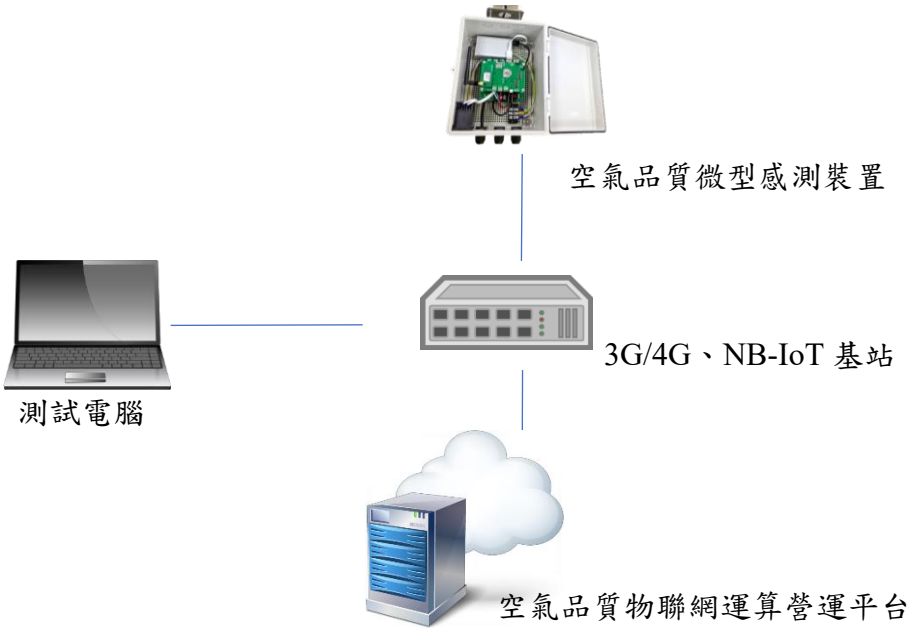

圖 8 測試示意圖

(g) 測試方法：

(1) 開啟安全通道掃描工具，對裝置進行掃描。

(2) 比對掃描結果是否為附錄 A 中所包含之密碼套件。

(3) 將測試電腦設定於空氣品質物聯網運算營運平台與裝置之間，開始側錄封包。

(4) 於空氣品質物聯網運算營運對裝置發送憑證之間時攔截此憑證，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。

(5) 發送已竄改之憑證予裝置，檢視裝置是否接受此憑證。

(6) 檢視所側錄之夾帶感測資料的封包是否採用安全通道。

(h) 檢測結果：

(1) 裝置與空氣品質物聯網運算營運平台之感測資料傳輸，預設採用安全通道。

(2) 安全通道僅支援「附錄 A」中所建議之密碼套件。

(3) 裝置不接受此憑證。

(4) 通過： (1)~(3)三項結果皆符合。

(5) 不通過： (1)~(3)三項結果不符合其一。

(6) 不適用： 無。

狀況 2：資料真確性測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.2.3

(b) 安全等級：

2 級。

(c) 測試資料：

裝置之感測資料封包。

(d) 測試目的：

查驗裝置支援空氣品質物聯網運算營運平台驗證資料真確性之功能。

(e) 測試條件：

(1) 裝置須提供系統管理者權限供測試用。

(2) 裝置須提供能進入作業系統層之介面。

(f) 測試佈局：

如圖 10。

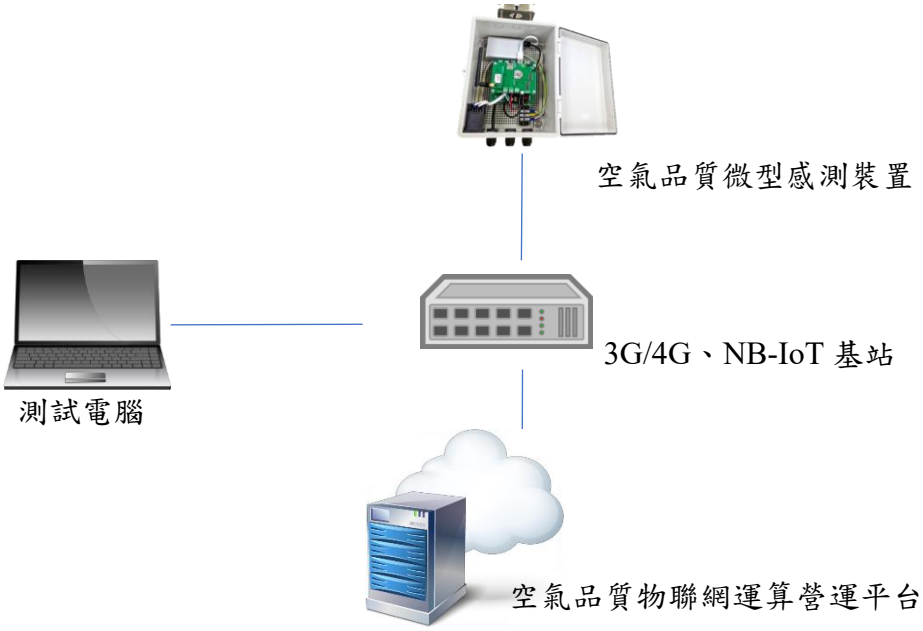

圖 9 測試示意圖

(g) 測試方法：

(1) 將測試電腦與空氣品質物聯網運算營運平台連結在同一個區域網路中。

(2) 將裝置連結空氣品質物聯網運算營運平台並開啟服務。

(3) 攔截傳送中之感測資料。

(4) 調換簽章，並轉發給空氣品質物聯網運算營運平台。

(5) 檢視竄改過之封包是否可被接受。

(h) 檢測結果：

(1) 簽章演算法須採用 NIST SP 800-140C 同等或以上強度之雜湊演算法。

(2) 封包內容存在支援驗證資料真確性之簽章。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：裝置無傳輸身分鑑別因子。

(6) 通過：(a)、(b)二項檢測結果符合其一。

(7) 不通過：(a)、(b)二項檢測結果皆不符合。

(8) 不適用：無。

5.2.2.4 傳送指令真確性安全測試

資料防竄改測試：

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.2.4

(b) 安全等級：

2 級。

(c) 測試資料：

空氣品質物聯網運算營運平台之 IP 位址。

(d) 測試目的：

查驗裝置與空氣品質物聯網運算營運平台間之控制指令傳輸，預設是否採用強度足夠之安全通道。

(e) 測試條件：

(1) 裝置須保持出廠預設環境狀態。

(2) 裝置須提供與裝置對連之空氣品質物聯網運算營運平台。

(f) 測試佈局：

如圖 11。

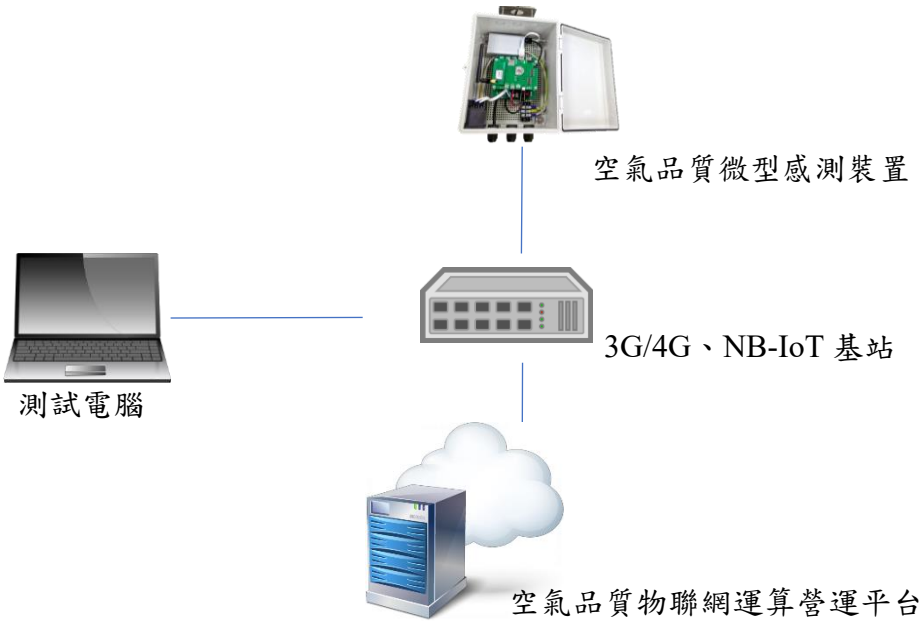

圖 10 測試示意圖

(g) 測試方法：

(1) 開啟安全通道掃描工具，對空氣品質物聯網運算營運平台進行掃描。

(2) 比對掃描結果是否為附錄 A 中所包含之密碼套件。

(3) 將測試電腦與空氣品質物聯網運算營運平台連結在同一個區域網路中。

(4) 將裝置與空氣品質物聯網運算營運平台連線，同時側錄封包。

(5) 檢視所側錄之夾帶控制指令的封包是否採用安全通道。

(h) 檢測結果：

(1) 裝置與空氣品質物聯網運算營運平台之控制指令傳輸，預設採用安全通道。

(2) 安全通道僅支援「附錄 A」中所建議之密碼套件。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：裝置無接收控制指令功能。

控制指令真確性測試：

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.2.2.4

(b) 安全等級：

2 級。

(c) 測試資料：

空氣品質物聯網運算營運平台之控制指令封包。

(d) 測試目的：

查驗裝置驗證空氣品質物聯網運算營運平台之控制指令的真確性。

(e) 測試條件：

(1) 裝置須提供系統管理者權限供測試用。

(2) 裝置須提供能進入作業系統層之介面。

(f) 測試佈局：

如圖 12。

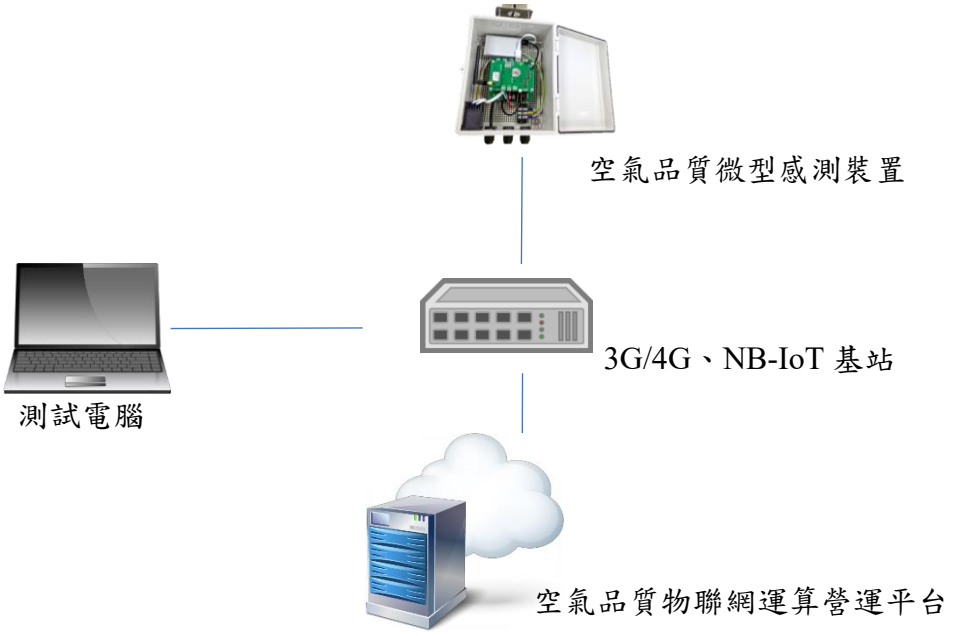

圖 11 測試示意圖

(g) 測試方法：

(1) 將測試電腦與空氣品質物聯網運算營運平台連結在同一個區域網路中。

(2) 將裝置連結空氣品質物聯網運算營運平台並開啟服務。

(3) 攔截傳送中之控制指令。

(4) 調換簽章，並轉發給裝置。

(5) 檢視竄改過之封包是否可被接受。

(h) 檢測結果：

(1) 簽章演算法須採用 NIST SP 800-140C 同等或以上強度之演算法。

(2) 裝置不接受控制指令。

(3) 通過： (1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：裝置無傳輸身分鑑別因子。

(6) 通過：(a)、(b)二項檢測結果符合其一。

(7) 不同過：(a)、(b)二項檢測結果皆不符合。

(8) 不適用：無。

5.3 系統完整性測試

檢視空氣品質微型感測裝置之系統完整性是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.3.1 安全啟動測試

5.3.1.1 安全啟動功能測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.3.1.1

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗裝置於開機階段能確保裝置之完整性及可信度。

(e) 測試條件：

裝置須提供安全啟動功能之設計文件。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱具備安全啟動功能證明之書面資料。

(2) 確認裝置在開機過程中是否驗證韌體的簽章。

(h) 檢測結果：

(1) 安全啟動功能僅能透過安全區域執行開機啟動。

(2) 書面資料證實裝置在開機過程中驗證韌體的簽章。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.4 軟韌體更新測試

檢視空氣品質微型感測裝置之軟韌體更新需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.4.1 更新安全測試

5.4.1.1 備援更新功能測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.4.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗當更新作業異常中斷時，裝置仍可恢復正常運作狀態。

(e) 測試條件：

(1) 裝置須支援更新功能，包括但不限於線上更新或手動更新方式。

(2) 支援線上更新：廠商須負責觸發線上更新。

(f) 測試佈局：

如圖 12。

圖 12 測試示意圖

(g) 測試方法：

(1) 啟動更新。

(2) 於更新過程中(非韌體檔案下載階段)，觸發更新中斷。

(h) 檢測結果：

(1) 支援更新功能。

(2) 更新中斷後，系統仍可回復正常運作狀態。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.4.1.2 韌體更新路徑的保護

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.4.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

測試用假憑證。

(d) 測試目的：

查驗裝置的韌體線上更新採用安全通道，以確保韌體之機密性、正確性及完整性，同時具有鑑別安全通道所使用憑證之合法性及有效性。

(e) 測試條件：

(1) 裝置須支援線上更新。

(2) 裝置須提供所有相連伺服器之宣告。

(3) 受測廠商須協助觸發裝置之線上更新。

(f) 測試佈局：

如圖 13。

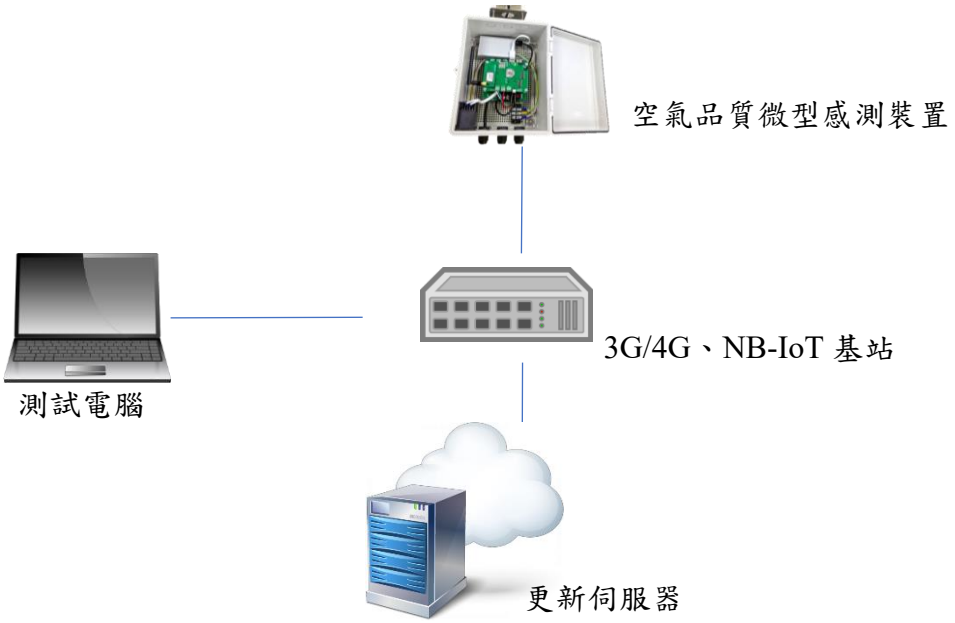

圖 13 測試示意圖

(g) 測試方法：

(1) 將測試電腦、裝置與更新伺服器連結在同一個區域網路中。

(2) 啟動韌體更新。

(3) 使用工具側錄更新伺服器與裝置之間的封包。

(4) 檢視所側錄之封包。

(5) 再次啟動更新。

(6) 於更新伺服器發送憑證予裝置之間，攔截更新伺服器憑證。

(7) 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。

(8) 發送已竄改之憑證予裝置。

(9) 於安全通道建立的交握過程中監聽封包。

(10) 檢視所側錄之封包。

(h) 檢測結果：

(1) 裝置之線上更新路徑通過安全通道，且安全通道僅支援「附錄 A」中所建議之密碼套件。

(2) 更新伺服器之憑證公鑰或憑證資訊其一被竄改，安全通道建立失敗。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一或不支援線上更新功能。

(5) 不適用：裝置不支援線上更新。

5.5 已知漏洞安全測試

檢視空氣品質微型感測裝置之已知漏洞安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.5.1 作業系統與網路服務測試

5.5.1.1 網路服務最小化測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.5.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

裝置之 IP 位址。

(d) 測試目的：

查驗裝置不應存在預期以外之網路埠。

(e) 測試條件：

(1) 裝置須保持出廠預設環境狀態。

(2) 裝置須提供所啟用之網路服務與對應埠之宣告。

(f) 測試佈局：

如圖 14。

圖 14 測試示意圖

(g) 測試方法：

(1) 將測試電腦連接裝置。

(2) 啟動具網路埠掃描功能之工具。

(3) 對裝置執行 TCP 埠 0~65535 之掃描。

(4) 檢視掃描結果所呈現之網路服務與對應埠。

(5) 對裝置執行 UDP 埠 0~65535 之掃描。

(6) 檢視掃描結果所呈現之網路服務與對應埠。

(7) 將裝置所有功能啟用，執行 24 小時動態埠監聽。

(h) 檢測結果：

(1) 裝置所開啟之網路服務與對應埠，與裝置自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」及「資料內容」相符。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：裝置無網路服務之功能。

5.5.1.2 測試作業系統與網路服務不存在 CVSS v3 評分為 9.0 分以上之常見資安弱點與漏洞

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.5.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 裝置 IP 位址。

(2) 裝置所提供之系統管理者帳密。

(d) 測試目的：

查驗裝置之作業系統與網路服務不存在已知 CVSS v3 重大資安風險之漏洞。

(e) 測試條件：

(1) 裝置須保持出廠預設環境狀態。

(2) 裝置須支援作業系統與網路服務。

(3) 裝置須提供系統管理者帳密。

(f) 測試佈局：

如圖 15。

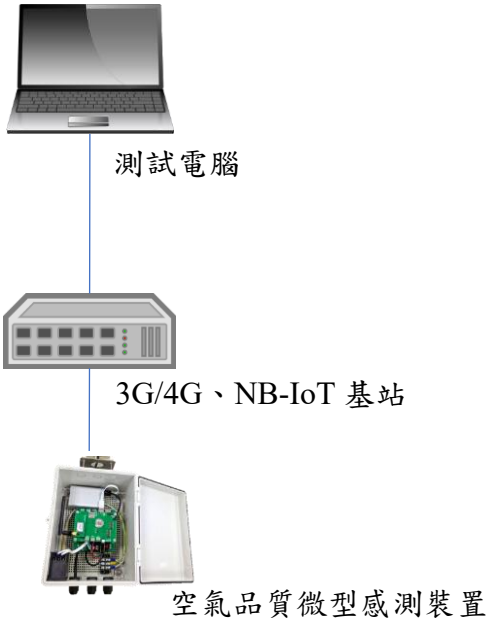

圖 15 測試示意圖

(g) 測試方法：

(1) 將測試電腦連接裝置。

(2) 啟動具作業系統及網路服務弱點掃描功能之工具。

(3) 設定裝置之 IP 位址及系統管理者帳密。

(4) 對裝置執行弱點掃描。

(h) 檢測結果：

(1) 作業系統與網路服務不存在國家弱點資料庫評分 CVSS v3 為 9.0 分以上之資安漏洞; 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。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：裝置無作業系統或網路服務之功能。

5.6 資源可用性測試

檢視空氣品質微型感測裝置之資源可用性安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.6.1 資源管理測試

5.6.1.1 儲存空間之儲存紀錄滾動功能測試

(a) 測試依據：

TAICS TS-0036-1「空氣品質微型感測裝置資安標準」5.6.1.1

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗裝置具備處理儲存紀錄的儲存空間不足之異常狀況。

(e) 測試條件：

裝置須提供系統管理者權限供測試用。

(f) 測試佈局：

如圖 16。

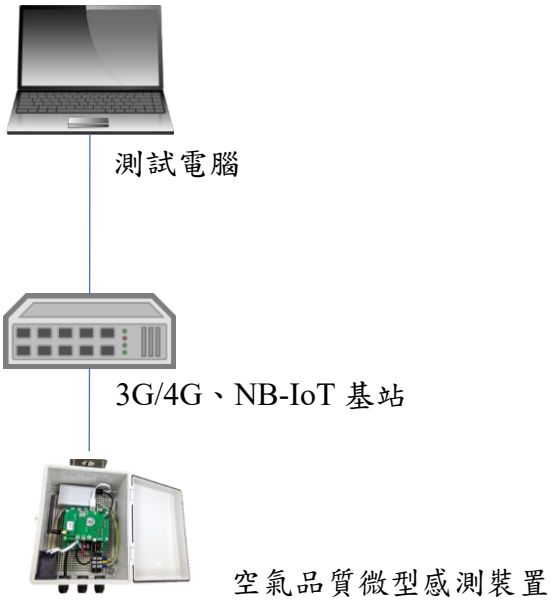

圖 16 測試示意圖

(g) 測試方法：

(1) 啟動裝置偵測空氣品質功能。

(2) 不斷觸發安全事件。

(3) 填充儲存容量，直到儲存空間不足。

(4) 檢視裝置安全事件狀態，是否可正常記錄。

(h) 檢測結果：

(1) 裝置不會發生儲存空間不足的現象。

(2) 裝置仍可正常記錄安全事件與感測數據。

(3) 通過： (1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：裝置無提供紀錄功能。

附錄 A
(規定)
安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

(a) TLSv1.2

(1) TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384

(2) TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384

(3) TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305

(4) TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

(5) TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256

(6) TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256

(7) TLS_ECDHE_ECDSA_WITH_AES256_SHA384

(8) TLS_ECDHE_RSA_WITH_AES256_SHA384

(9) TLS_ECDHE_ECDSA_WITH_AES128_SHA256

(10) TLS_ECDHE_RSA_WITH_AES128_SHA256

(b) TLSv1.3

(1) TLS_AES_128_GCM_SHA256

(2) TLS_AES_256_GCM_SHA384

(3) TLS_CHACHA20_POLY1305_SHA256

(4) TLS_AES_128_CCM_SHA256

(5) TLS_AES_128_CCM_8_SHA256

附錄 B
(規定)
產品概述說明(範例)

送測產品應檢附產品概述表，以供測試實驗室參閱：

表 B.1 設備概述表

製造商	XX 公司
設備名稱	XXX
廠牌	XXX
型號	XX-XXX
韌(軟)體版本	XX.XXX.XX
通訊介面	NB-IoT
網路服務(埠號)	https (443)
相連空氣品質物聯網運算營運平台(IP)	空氣品質監測網 (XX.XX.XX.XX)
日誌存取權限	User A ： 唯讀
日誌檔保存期限	90 天
角色存取權限	Administrator ： User A ：
使用者帳密	Admin 帳號 ： Admin 密碼 ：
外觀	<picture>及產品型錄

附錄 C
(規定)
安全功能規格說明(範例)

送測產品應檢附安全功能規格表，以供測試實驗室參閱：

表 C.1 安全功能規格表

項目	說明	申請者填寫內容
1. 除錯模式	詳細描述進入產品除錯模式之方法，或提供佐證文件。	
2. 通訊 API	詳述描述產品通訊 API 之傳輸方式，或提供說明文件。	
3. 加密演算法	列出產品所提供之加密演算法及其應用，及提供佐證文件。	
4. 安全啟動	詳細描述安全啟動之功能設計，或提供說明文件。	
5. 安全通道憑證	驗證 2 級安全項目之產品須提供	
6. 安全區域	說明產品的安全區域功能運用及其保護的資料，並提供佐證文件。	

參考資料

(1) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions, available at URL： http：//www.nist.gov/cmvp.

版本修改紀錄

版本	時間	摘要
v1.0	2020/11/26	出版

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