IoT-2007-1

感測裝置資安測試規範

-第一部：一般要求

V1.0

行動應用資安聯盟

中華民國 111 年 12 月

目錄

引言

為預防感測裝置攻擊事件的發生，並助民生公共物聯網相關感測裝置提升資安品質，制定了感測裝置的安全作法，例如：民生公共物聯網平台於全台各地區建置的智慧聯網地震儀、水位計等感測裝置，以緩解感測裝置所面臨的資安威脅。

本測試規範依據「IoT-100x-1 感測裝置資安標準-第一部：一般要求」[1]訂定，其中具體明列資安檢測之測試項目、測試條件、測試方法與測試結果等事項，俾利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

本規範適用於感測裝置之資安要求。適用範圍為物聯網感測裝置，包但不限於智慧聯網地震儀、水位計、空氣品質等感測裝置，如下圖 1 所示，主要用於協助環保署、水利署、氣象局、國震中心等監管單位收集與監控即時環境變化。

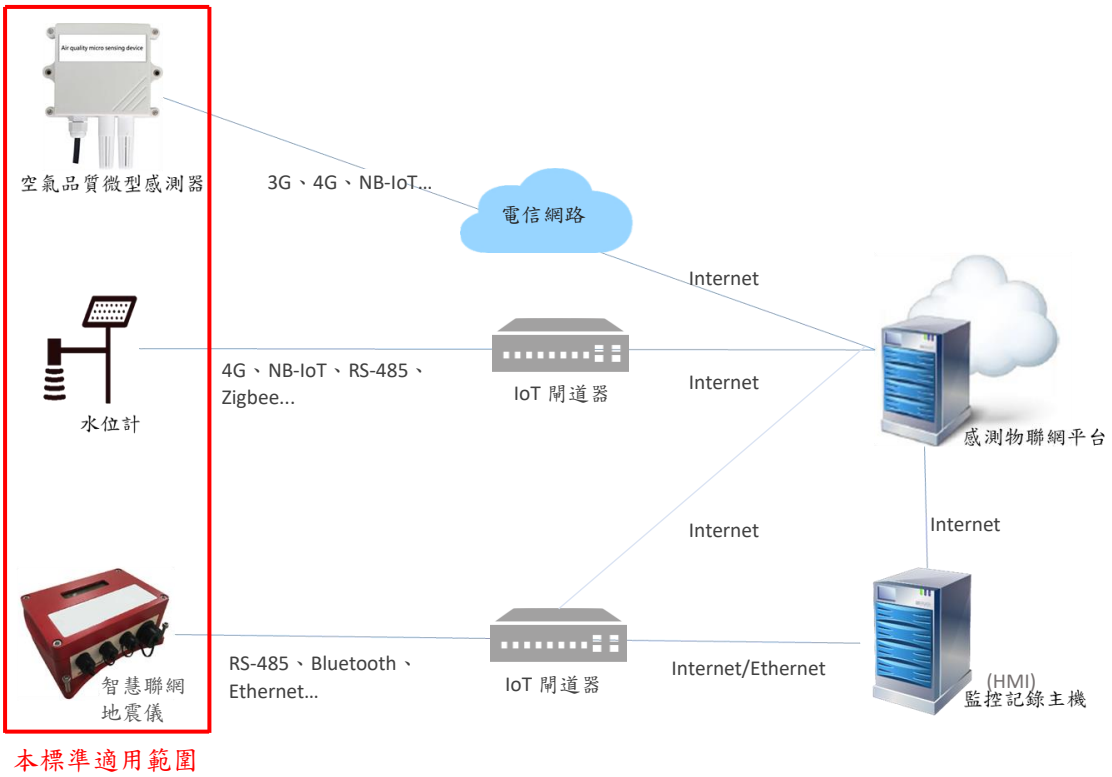

圖 1 感測物聯網架構示意圖

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] IoT-100x-1 v1.0 感測裝置資安標準-第一部：一般要求

3. 用語及定義

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」所規定之用語及定義適用於本規範。

3.1 本地端管理介面(Local Management Interface)

使用者直接存取與控制產品的操作介面，不需要連接網際網路經由管理平台操控產品，例如產品應用程式或透過電腦與產品連接並以 IP 地址開啟的網頁管理頁面等。

3.2 關聯服務(Associated services)

係指產品所提供之功能所需的數位服務，包括行動應用程式(App)、雲服務(雲端運算、雲端儲存)、第三方 API 及傳輸遙測數據的第三方服務等。

3.3 除錯模式(Debug mode)

係指一個以釐清產品故障原因為目的程式，其允許開發者透過該介面進行除錯或設定，亦稱作工程模式。

3.4 受限制設備(Constrained device)

係指此類設備預期用途受限於實體而產生的限制，包括但不限於處理資料的能力、通訊的能力、資料儲存的能力或與使用者互動的能力。例如感測器，它可能是實體限制的設備，其可能因電源、電池壽命、運算處理能力、實體的存取、功能有限、記憶體有限或網路頻寬有限，這些限制在設備運行時可能需要搭配另一設備來支援；或者，可能是透過同一實體線路供電與資料傳輸，此設備的通訊協定與加密方式就受限於該線路配置。

3.5 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，進一步探尋其漏洞，藉此找到未經授權的存取點。

4. 測試項目分級

本節依據「IoT-100x-1 感測裝置資安標準-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)身分鑑別、識別、授權、(2)資料機密性與完整性、(3)系統完整性、(4)更新安全、(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)資料保護程度及(3)產品功能與成本之綜合考量，分為 1 級(必要安全要求)與 2 級(進階安全要求)二個等級。產品應先通過 1 級安全要求之測試，始可進行 2 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 身分鑑別、識別、授權	5.1.1 鑑別機制	5.1.1.1 5.1.1.2 5.1.1.3	5.1.1.4
	5.1.2 權限控管	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 資料傳輸	5.2.2.1 5.2.2.2	5.2.2.3 5.2.2.4
	5.2.3 密碼演算法之使用	5.2.3.1	-
5.3 系統完整性	5.3.1 系統安全	-	5.3.1.1
5.4 更新安全	5.4.1 軟韌體更新	5.4.1.1 5.4.1.2 5.4.1.3	-
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	5.5.1.3
5.6 資源可用性	5.6.1 資源管理	-	5.6.1.1
	5.6.2 警示與記錄	5.6.2.1	-

5. 資安測試規範

5.1 身分識別、鑑別、授權要求測試

檢視產品有關身份識別、鑑別、授權要求之送審資料是否符合 IoT-100x-1 之安全需求，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 產品識別碼唯一性測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.1.1.1

(b) 安全等級

1 級

(c) 測試資料

(1) 廠商應提供可與產品相連之管理平台(例如：感測物聯網平台)。

(2) 廠商應提供受測產品至少 2 件。

(3) 廠商應提供產品唯一識別碼生成機制之書面資料作為審查依據。

(4) 若是由管理平台配發具唯一性的識別碼，則產品應提供此一機制之書面資料作為審查依據。

(5) 廠商應提供產品對其他裝置身分鑑別機制之說明文件作為審查依據。

(d) 測試目的

驗證產品之識別碼是否具唯一性。

(e) 測試條件

無。

(f) 測試佈局

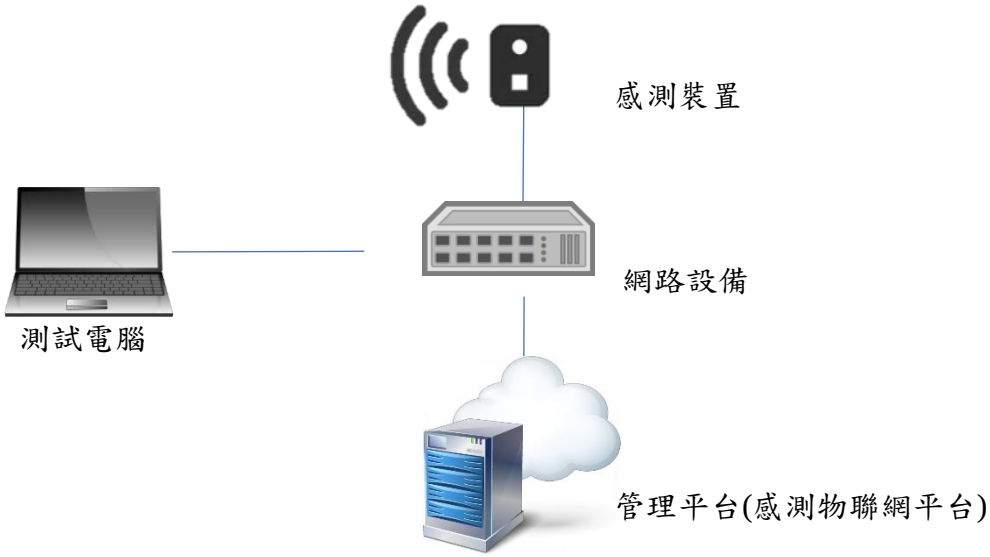

圖 2 測試示意圖

(g) 測試方法

(1) 審閱具備說明唯一識別碼之生成機制的書面證明文件。

(2) 審閱以識別碼驗證之身分鑑別機制的書面資料。

(3) 若產品識別碼為相連之管理平台所配發，審閱此機制之說明文件。

(4) 根據說明文件，查驗產品是否有相應的功能。

(h) 測試結果

(1) 兩產品之產品識別碼相異，產品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) 產品之識別碼是由管理平台所配發時，此機制所產生的產品識別碼具有不重覆的編碼方式，兩產品之產品識別碼相異。

(3) 通過：(1)(2)項結果符合其一。

(4) 不通過：(1)(2)項結果皆不符合。

(5) 不適用：無。

5.1.1.2 使用者身分識別與鑑別功能測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.1.1.2

(b) 安全等級

1 級

(c) 測試資料

(1) 產品應說明支援的使用者介面與操作方式之書面文件，例如：產品使用手冊。

(2) 產品之管理者帳號和通行碼。

(d) 測試目的

驗證產品是否具有身分識別與鑑別功能。

(e) 測試條件

產品支援網頁介面或遠端指令介面或 API 介面或本地端管理介面。

(f) 測試佈局

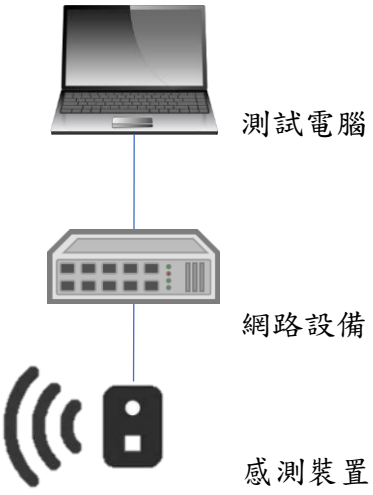

圖 3 測試示意圖

(g) 測試方法

(1) 網頁介面

(i) 將測試電腦連接產品。

(ii) 根據產品使用說明，開啟網頁介面。

(iii) 在未登入的狀況下，存取身分鑑別頁面以外的頁面，確認是否要求身分鑑別。

(iv) 以產品的系統管理員帳號和通行碼執行身分鑑別操作。

(2) 遠端指令

(i) 將測試電腦連接產品。

(ii) 根據產品使用說明，開啟所支援控制主要功能之遠端指令介面。

(iii) 以產品的系統管理員帳號和通行碼執行身分鑑別操作。

(3) API 介面

(i) 根據產品使用說明，開啟所支援 API 介面。

(ii) 驗證是否以產品的 API 驗證連接方式執行身分鑑別操作。

(4) 本地端管理介面

(i) 開啟產品的本地端管理介面。

(ii) 在未登入狀況下，存取身分鑑別以外的操作頁面，確認是否要求身分鑑別。

(iii) 以產品的系統管理員帳號和通行碼執行身分鑑別操作。

(h) 測試結果

(1) 產品在網頁介面能正常執行身分識別與鑑別功能，例如：須使用帳號、通行碼登入。

(2) 產品在遠端指令介面能正常執行身分識別與鑑別功能，例如：須使用帳號、通行碼登入。

(3) 產品在 API 介面能正常執行身分識別與鑑別功能，例如：須使用帳號、通行碼登入。

(4) 產品在本地端管理介面能正常執行身分識別與鑑別功能，例如：須使用帳號、通行碼登入。

(5) 通過：若產品支援網頁介面，則(1)項結果符合。

(6) 通過：若產品支援遠端指令介面，則(2)項結果符合。

(7) 通過：若產品支援 API 介面，則(3)項結果符合。

(8) 通過：若產品支援本地端管理介面，則(4)項結果符合。

(9) 不通過：若產品支援網頁介面，則(1)項結果不符合。

(10) 不通過：若產品支援遠端指令介面，則(2)項結果不符合。

(11) 不通過：若產品支援 API 介面，則(3)項結果不符合。

(12) 不通過：若產品支援本地端管理介面，則(4)項結果不符合。

(13) 不適用：產品不支援網頁介面則不須檢測網頁介面項目；不支援遠端指令介面則無須檢測遠端指令介面項目；不支援 API 介面則無須檢測 API 介面項目；不支援本地端管理介面則無須檢測本地端管理介面項目。

5.1.1.3 預設通行碼測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.1.1.3

(b) 安全等級

1 級

(c) 測試資料

(1) 若產品存在預設通行碼或預設帳號/通行碼，應提供產品預設鑑別之設計文件作為審查依據。

(2) 產品應為出廠預設組態。

(3) 產品應說明支援的使用者介面與操作方式之書面文件，例如：產品使用手冊。

(d) 測試目的

驗證產品是否沒有相同的預設通行碼或通行碼是否在首次上線後強制要求更改。

(e) 測試條件

產品支援通行碼或帳號/通行碼鑑別機制。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱產品之預設通行碼設計文件，檢視產品是否存在相同之預設通行碼或預設帳號/通行碼。

(2) 將測試電腦或行動裝置連接產品。

(3) 根據使用說明文件，從管理介面輸入通行碼；若支援預設帳號通行碼，則自管理介面輸入帳號/通行碼。

(4) 若產品支援預設通行碼，確認在未設定新通行碼的情況下，是否可存取產品。

(5) 若產品支援預設帳號/通行碼，確認在設定新帳號/通行碼的情況下，是否可存取產品。

(h) 測試結果

(1) 產品之預設通行碼為全球唯一。

(2) 若產品支援預設通行碼，產品未經設定新的通行碼之前，無法存取產品。

(3) 若產品支援預設帳號/通行碼，產品未經設定新帳號/通行碼前，無法存取產品。

(4) 通過：(1)(2)(3)項結果符合其一。

(5) 不通過：(1)(2) (3)項結果皆不符合。

(6) 不適用：產品不支援通行碼鑑別機制。

5.1.1.4 關鍵金鑰唯一性測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.1.1.4

(b) 安全等級

2 級

(c) 測試資料

產品應提供關鍵金鑰具唯一性其所生成機制的說明文件，作為審查依據。

(d) 測試目的

驗證產品在更新、與關聯服務間傳輸的完整性和真實性所使用的金鑰是否具唯一性。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審閱具備能證明關鍵金鑰具唯一性的金鑰生成機制證明文件。

(h) 測試結果

(1) 產品提供的文件證實產品所使用的關鍵金鑰具唯一性。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.1.2 權限管控測試

5.1.2.1 存取介面權限管控機制

(a) 實體介面

(1) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.1.2.1

(2) 安全等級

1 級

(3) 測試資料

(i) 產品應提供角色存取權限宣告之說明文件。

(ii) 若產品支援管理者與使用者角色權限，提供其帳號和通行碼。

(iii) 廠商應提供存取實體介面之操作說明文件。

(4) 測試目的

驗證產品實體介面之存取具有權限控管機制且遵從最小權限原則。

(5) 測試條件

產品支援實體介面。

(6) 測試佈局

無。

(7) 測試方法

(i) 根據說明文件，連接相應之實體介面。

(ii) 若產品支援 UART，將測試電腦連接產品之 UART。

(iii) 透過 UART 埠存取產品之除錯模式。

(iv) 以使用者帳號和通行碼登入。

(v) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(vi) 以管理者帳號和通行碼登入。

(vii) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(viii)若產品支援 JTAG，將測試電腦連接產品之 JTAG。

(ix) 透過 JTAG 埠存取產品之除錯模式。

(x) 重複(iv)~(vii)步驟。

(xi) 透過 USB 埠存取產品之除錯模式。

(xii) 重複(iv)~(vii)步驟。

(xiii)檢視廠商之角色存取權限宣告是否符合最小權限原則。

(xiv)根據廠商提供之實體介面操作文件，操作以其他實體介面存取產品除錯模式。

(xv) 重複(iv)~(vii)步驟。

(8) 測試結果

(i) 在 UART、JTAG、USB 等實體介面之身分授權與產品角色存取權限宣告相符。

(ii) 產品支援創建多個不同權限角色之功能，若僅支援單一使用者應於宣告文件中說明產品無須區分使用者角色的理由與作法。

(iii) 產品之存取權限宣告符合最小權限原則。

(iv) 通過：(i)~(iii)項結果皆符合。

(v) 不通過：(i)~(iii)項結果不符合其一。

(vi) 不適用：產品不具備存取產品實體之介面。

(b) 通訊 API

(1) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.1.2.1

(2) 安全等級

1 級

(3) 測試資料

(i) 產品應提供角色存取權限宣告之說明文件。

(ii) 廠商應提供可與產品相連之管理平台(例如：感測物聯網平台)。

(iii) 產品應提供通訊 API 之傳輸方式說明文件，例如遠端指令、API。

(iv) 管理平台所傳送之產品控制指令資料。

(v) 若產品支援管理者與使用者角色權限，提供其帳號和通行碼。

(4) 測試目的

驗證產品通訊 API 之使用具有權限控管機制。

(5) 測試條件

產品支援通訊 API。

(6) 測試佈局

如圖 2。

(7) 測試方法

(i) 產品與管理平台連結。

(ii) 操作管理平台執行產品控制相關動作。

(iii) 開啟封包側錄工具並進行側錄。

(iv) 發送具使用者權限之產品控制請求封包。

(v) 查看封包內容，檢視操作是否符合角色存取權限之宣告。

(vi) 發送具管理者權限之產品控制請求封包。

(vii) 查看封包內容，檢視操作是否符合角色存取權限之宣告。

(viii) 嘗試以使用者權限，發送該權限外之產品控制請求封包。

(ix) 檢視該請求是否成功被執行。

(x) 嘗試以管理者權限，發送該權限外之產品控制請求封包。

(xi) 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。

(8) 測試結果

(i) 於通訊 API 之身分授權與產品角色存取權限宣告相符。

(ii) 產品支援創建多個不同權限使用者之功能，若僅支援單一使用者應於宣告文件中說明產品無須區分使用者角色的理由與作法。

(iii) 產品之存取權限宣告符合最小權限原則。

(iv) 通過：(i)~(iii)項結果皆符合。

(v) 不通過：(i)~(iii)項結果不符合其一。

(vi) 不適用：產品不具備存取產品之通訊 API。

(c) 測試結果

(1) 通過：(a)(b)項結果皆符合。

(2) 不通過：(a)(b)項結果皆不符合。

(3) 不適用：若產品不支援實體介面則(a)項無須檢測、若產品不支援通訊 API 則(b)項無須檢測。

5.2 資料機密性與完整性測試

-檢視產品有關資料機密性與完整性之送審資料是否符合 IoT-100x-1 之安全要求，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

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.1.1

(b) 安全等級

1 級

(c) 測試資料

(1) 產品應保持出廠預設環境狀態。

(2) 廠商應提供產品具有哪些安全敏感性資料及其儲存保護之加密演算法之書面資料，作為審查依據。

(3) 產品之管理者權限之帳號和通行碼。

(4) 若產品存在除錯模式介面，應提供進入除錯模式的操作方法之說明文件。

(5) 廠商提供能進入產品安全敏感性資料存放位置的方法，作為測試依據。

(d) 測試目的

驗證產品之安全敏感性資料於儲存狀態下是否加密保護。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱廠商提供之書面審查資料。

(2) 根據說明文件，將測試電腦連接產品。

(3) 若產品支援 UART，將測試電腦連接產品之 UART。

(4) 透過 UART 埠存取除錯模式。

(5) 根據說明文件，透過搜尋工具，查找安全敏感性資料存放的位置。

(6) 檢視保護加解密金鑰等安全敏感性資料所採用的保密機制。

(7) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。

(8) 透過 JTAG 埠存取除錯模式。

(9) 重複(5)~(6)之步驟。

(10) 若產品支援 USB，將測試電腦連接產品之 USB。

(11) 透過 USB 埠存取除錯模式。

(12) 重複(5)~(7)之步驟。

(13) 根據說明文件，進入產品存放安全敏感性資料之位置。

(14) 檢視保護加解密金鑰等安全敏感性資料所採用的保密機制。

(h) 測試結果

(1) 產品不存在除錯模式介面。

(2) 加解密用之金鑰的保密機制採用 5.2.3.1 所要求的同等或以上強度之加密演算法。

(3) 通過：(1)(2)項結果符合其一。

(4) 不通過：(1)(2)項結果皆不符合。

(5) 不適用：產品無存放安全敏感性資料，則廠商應提供相關文件以證明產品不會存放安全敏感性資料。

5.2.1.2 韌體安全測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.1.2

(b) 安全等級

1 級

(c) 測試資料

(1) 產品之韌體檔案。

(2) 廠商應提供產品之韌體燒錄工具與方法。

(3) 廠商應提供韌體保護之加密演算法之書面資料，作為審查依據。

(d) 測試目的

驗證產品之韌體是否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

產品應具備韌體更新機制。

(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產品韌體可供下載。

(2) 若廠商之官網不存在產品韌體，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，由廠商提供產品之韌體。

(6) 使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(7) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(8) 確認安全敏感性資料的保密機制是否採用 5.2.3.1 所要求的同等或以上強度之加密演算法。

(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) 確認是否存在產品所宣告之相連伺服器以外之 IP 資料。

(12) 確認是否存在產品所宣告之相連伺服器以外之 URL 資料。

(h) 測試結果

(1) 韌體檔案不放置在公開存取之位置。

(2) 晶片中的韌體須加密保護且採用 5.2.3.1 所要求的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，或存在安全敏感性資料應加密保護且採用 5.2.3.1 所要求的同等或以上強度之加密演算法。

(4) 若產品支援線上更新，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)項結果符合；或若廠商之官網不存在產品韌體時，(2)(3)(4)結果皆符合。

(6) 不通過：(1)項結果不符合，或(2)(3)(4)項結果不符合其一。

(7) 不適用：產品為不支援韌體更新之受限制設備，則廠商應提供相關文件以證明產品的安全更新方式(例如:硬體更換、召回等)。

5.2.1.3 安全敏感性資料隔離保護測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.1.3

(b) 安全等級

2 級

(c) 測試資料

(1) 產品所提供之安全區域設計資料，作為審查依據。

(2) 產品應提供具有哪些安全敏感性資料及其保存方式之書面資料，作為審查依據。

(3) 產品應提供使用到安全區域的資安功能之聲明文件，作為審查依據。

(d) 測試目的

驗證產品安全敏感性資料之存放是否與正常作業系統隔離。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審閱廠商提供之佐證書面資料。

(h) 測試結果

(1) 書面資料證實產品之安全敏感性資料存放於安全區域，例如：TPM、TrustZone 等。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品無存放安全敏感性資料，則廠商應提供相關文件以證明產品不會存放安全敏感性資料。

5.2.2 資料傳輸測試

5.2.2.1 安全敏感性資料保護測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.2.1

(b) 安全等級

1 級

(c) 測試資料

(1) 廠商應提供與產品相連的管理平台(例如：感測物聯網平台)，以供測試使用。

(2) 產品應提供安全敏感性資料傳輸保護之加密演算法書面文件，作為審查依據。

(3) 產品應提供具有哪些安全敏感性資料及其傳輸方式之書面資料，作為審查依據。

(4) 若產品使用無加密安全機制之傳輸方式(例如：Modbus、HART 等)時，產品應提供傳輸安全的補償性措施之作法書面文件，作為審查依據。

(d) 測試目的

驗證產品之安全敏感性資料傳輸是否採用足夠強度之安全通道。

(e) 測試條件

無。

(f) 測試佈局

如圖 2。

(g) 測試方法

測試情境 1：

(1) 將測試電腦與管理平台連結，並將產品與管理平台連接後，開始側錄封包。

(2) 於產品與管理平台雙方建立交握過程中，擷取封包查驗標頭(header)內容，比對安全通道所使用的密碼演算法。

(3) 產品開始傳送安全敏感性資料至管理平台。

(4) 檢視所側錄的安全敏感性資料封包的傳送是否採用安全通道。

(5) 若產品以藍牙傳輸安全敏感性資料，開啟藍牙除錯工具(例如: Hcitool)，將產品與測試手機以藍牙方式連結，側錄藍牙訊息交握封包。

測試情境 2：

(1) 若產品使用無加密安全機制之傳輸方式(例如：Modbus、HART 等)，查驗產品提供之傳輸安全補償性措施之說明文件，例如:產品使用手冊、安全指引。

(h) 測試結果

測試情境 1：

(1) 安全通道所使用之加密演算法應符合 5.2.3.1 所規定的同等或以上等級之密碼演算法。

(2) 產品與管理平台間的安全敏感性資料傳輸，預設採用安全通道。

(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：產品不存在安全敏感性資料，則廠商應提供相關文件以證明產品不存在安全敏感性資料。

測試情境 2：

(1) 說明文件應詳述其補償性措施之作法，包括但不限於實體加固，且說明文件所述之補償性措施，不低於本規範要求之安全強度。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不存在安全敏感性資料，則廠商應提供相關文件以證明產品不存在安全敏感性資料。

5.2.2.2 指令傳輸之完整性

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.2.2

(b) 安全等級

1 級

(c) 測試資料

(1) 廠商應提供與產品連接的管理平台(例如：感測物聯網平台)，以供測試使用。

(2) 廠商應提供指令操作之說明文件。

(3) 產品應保持出廠預設環境狀態。

(d) 測試目的

驗證產品是否對指令傳輸具有完整性的保護。

(e) 測試條件

產品支援接收控制指令功能。

(f) 測試佈局

如圖 2。

(g) 測試方法

(1) 將測試電腦與管理平台連結，並將產品連接管理平台。

(2) 管理平台發送控制指令至產品。

(3) 攔截傳送中的控制指令並竄改指令內容，轉發至產品；或廠商協助竄改指令資料。

(4) 檢視竄改過的指令資料是否可被接受。

(h) 測試結果

(1) 竄改過內容的指令資料不可被接受。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援接收控制指令功能。

5.2.2.3 感測資料傳輸保護測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.2.3

(b) 安全等級

2 級

(c) 測試資料

(1) 廠商應提供與產品連接的管理平台(例如:感測物聯網平台)，以供測試使用。

(2) 廠商應提供感測資料傳輸加密所使用之加密演算法書面文件，作為審查依據。

(3) 若產品使用無加密安全機制之傳輸方式(例如：Modbus、HART 等)時，產品應提供傳輸安全的補償性措施之作法書面文件，作為審查依據。

(4) 產品應宣告感測資料所傳送之管理平台、伺服器網路位址，作為審查依據。

(5) 產品應保持出廠預設環境狀態。

(d) 測試目的

驗證產品感測資料之傳輸是否加密保護。

(e) 測試條件

無。

(f) 測試佈局

如圖 2。

(g) 測試方法

測試情境 1：

(1) 將測試電腦與管理平台連結，並將產品與管理平台連接後，開始側錄封包。

(2) 於產品與管理平台雙方建立交握過程中，擷取封包查驗標頭(header)內容。

(3) 比對安全通道所使用的密碼演算法。

(4) 產品開始傳送感測資料至管理平台。

(5) 檢視所側錄的感測資料封包是否採用安全通道。

(6) 持續監側感測資料封包，檢視感測資料是否傳送至未經宣告網路位址。

(7) 若產品以藍牙傳輸感測資料，開啟藍牙除錯工具(例如: Hcitool)，將產品與測試手機以藍牙方式連結，側錄藍牙訊息交握封包。

測試情境 2：

(1) 若產品使用無加密安全機制之傳輸方式(例如：Modbus、HART 等)，查驗產品提供之傳輸安全補償性措施之說明文件，例如:產品使用手冊、安全指引。

(h) 測試結果

測試情境 1：

(1) 安全通道所使用之加密演算法應符合 5.2.3.1 所規定的同等或以上等級之密碼演算法。

(2) 產品與管理平台間的感測資料傳輸，預設採用安全通道。

(3) 產品之感測資料無傳送至未經宣告之網路位址。

(4) 通過：(1)(2)(3)項結果皆符合。

(5) 不通過：(1)(2) (3)項結果不符合其一。

(6) 不適用：若產品特性為感測資料取樣率頻率、即時回傳且感測資料屬公開資料之產品，須提供足以佐證之書面資料。

測試情境 2：

(1) 說明文件所提供補償性措施，包括但不限於實體加固，且說明文件所述之補償性措施，不低於本規範要求之安全強度。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.2.4 指令傳輸之真實性

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.2.4

(b) 安全等級

2 級

(c) 測試資料

(1) 廠商應提供與產品相連的管理平台(例如：感測物聯網平台)，以供測試使用。

(2) 廠商應提供測試用憑證。

(3) 若產品使用無加密安全機制之傳輸方式(例如：Modbus、HART 等)時，產品應提供傳輸安全的補償性措施之作法書面文件，作為審查依據。

(d) 測試目的

驗證產品是否具備驗證傳輸指令來源身分的真實性。

(e) 測試條件

產品支援接收控制指令功能。

(f) 測試佈局

如圖 2。

(g) 測試方法

測試情境 1：

(1) 將產品與管理平台連接，啟動傳輸指令的安全通道之建立程序。

(2) 將廠商提供之測試用憑證置換憑證公鑰或憑證資訊(包括發證單位、有效期限、格式及憑證簽章)。

(3) 發送已竄改的憑證至產品。

(4) 檢視雙方連線情況。

測試情境 2：

(1) 若產品使用無加密安全機制之傳輸方式(例如：Modbus、HART 等)，查驗產品提供之傳輸安全補償性措施之說明文件，例如:產品使用手冊、安全指引。

(h) 測試結果

測試情境 1：

(1) 當指令傳輸用的安全通道憑證遭竄改後，經產品驗證後無法建立安全通道。

(2) 指令傳輸用的安全通道所使用之加密演算法應符合 5.2.3.1 所規定的同等或以上等級之密碼演算法。

(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：產品不支援接收控制指令功能。

測試情境 2：

(1) 說明文件應詳述其補償性措施之作法，包括但不限於實體加固，且說明文件所述之補償性措施，不低於本規範要求之安全強度。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援接收控制指令功能。

5.2.3 密碼演算法之使用測試

5.2.3.1 密碼演算法測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.2.3.1

(b) 安全等級

1 級

(c) 測試資料

廠商應提供產品所使用密碼演算法之技術書面文件，作為審查依據。

(d) 測試目的

驗證產品所使用的密碼演算法是否採用符合國際公認 NIST SP 800-140Cr1[(4)]所核可的同等或以上等級之要求。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審閱產品所使用的密碼演算法之技術書面文件。

(h) 測試結果

(1) 產品所使用的密碼演算法符合 NIST SP 800-140Cr1 所核可的同等或以上等級之要求。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.3 系統完整性測試

檢視產品有關系統完整性之送審資料是否符合 IoT-100x-1 之安全要求，並依下列各測試項目進行實機測試。

5.3.1 系統安全測試

5.3.1.1 啟動階段完整性測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.3.1.1

(b) 安全等級

2 級

(c) 測試資料

(1) 產品應提供安全啟動功能之技術書面文件。

(2) 廠商應提供未加密韌體檔案與韌體安裝之說明文件。

(d) 測試目的

驗證產品於開機階段是否能確保韌體、軟體的完整性。(不包含確認 bootloader 的完整性)

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱產品安全啟動功能之技術書面文件。

(2) 根據文件，竄改韌體、軟體後，重新啟動產品。

(h) 測試結果

(1) 當韌體、軟體經竄改後，產品無法被啟動。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4 更新安全測試

檢視產品有關更新安全之送審資料是否符合 IoT-100x-1 之安全要求，並依下列各測試項目進行實機測試。

5.4.1 軟韌體更新測試

5.4.1.1 軟韌體更新功能測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.4.1.1

(b) 安全等級

1 級

(c) 測試資料

(1) 若產品支援線上更新，可由廠商負責觸發產品線上更新。

(2) 若產品為受限制設備，廠商應提供產品更新方式之說明文件。

(3) 廠商應提供更新中斷保持產品可用性作法之書面文件，作為審查依據。

(d) 測試目的

驗證產品是否支援軟韌體更新功能。

(e) 測試條件

產品支援更新功能，包括但不限於線上更新或手動更新方式。

(f) 測試佈局：

無。

(g) 測試方法

(1) 啟動產品更新。

(2) 驗證產品更新結果。

(3) 根據產品可用性書面文件，重複步驟(1)，在更新過程中(非軟韌體檔案下載階段)，觸發更新中斷。

(h) 測試結果

(1) 產品具有更新功能，可正確更新軟韌體。

(2) 更新中斷後，產品仍可正常運作狀態。

(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：產品為無法手動或線上更新軟韌體之受限制設備，則廠商應提供相關文件以證明產品的安全更新方式(例如:硬體更換、召回等)。

5.4.1.2 更新安全測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.4.1.2

(b) 安全等級

1 級

(c) 測試資料

(1) 若產品支援線上更新，可由廠商負責觸發產品線上更新。

(2) 廠商應提供與產品相連的更新伺服器，以供測試使用。

(3) 廠商應提供新、舊版本之軟韌體檔案。

(4) 廠商應提出採用更新機制與加密傳輸的演算法之技術書面文件，作為審查依據。

(d) 測試目的

驗證產品是否具備軟體版本不可降為較舊版本(非關鍵基礎設施環境所設置之產品)、軟韌體檔案加密傳輸及線上更新路徑採用安全通道。

(e) 測試條件

產品支援軟韌體更新。

(f) 測試佈局

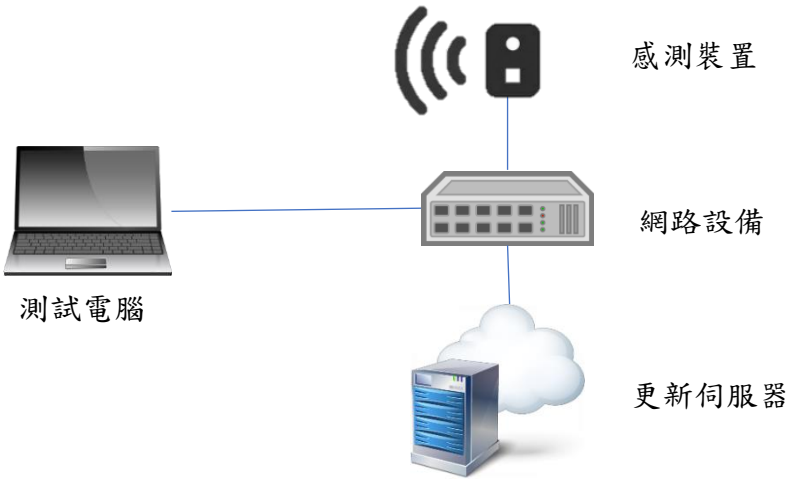

圖 4 測試示意圖

(g) 測試方法

(1) 安全功能 1：(防止安全舊版本)

(i) 使用舊的軟韌體版本執行更新安裝。

(ii) 檢視產品是否完成軟韌體安裝。

(2) 安全功能 2：(軟韌體加密傳輸)

(i) 將產品連結更新伺服器後，開始側錄封包並啟動更新。

(ii) 攔截傳送中的封包。

(iii) 查驗封包加密機制是否採用 5.2.3.1 所要求之同等或以上強度之加密演算法。

(3) 安全功能 3：(更新路徑)

(i) 將測試電腦與更新伺服器連結，並將產品與更新伺服器連接後，開始側錄封包。

(ii) 於產品與更新伺服器雙方建立交握過程中，擷取封包查驗標頭(header)內容，比對安全通道所使用的密碼演算法。

(iii) 將產品與更新伺服器連接，並啟動更新。

(iv) 檢視所側錄的軟韌體更新的封包是否採用安全通道。

(h) 測試結果

(1) 產品安裝舊版本軟韌體失敗，若產品為關鍵基礎設施環境下之應用產品時，在新版軟韌體更新失敗後，可回復舊版本並正常使用。

(2) 軟韌體加密機制採用 5.2.3.1 所要求之同等或以上強度之加密演算法。

(3) 產品線上更新路徑透過安全通道，且安全通道所使用之加密演算法應符合 5.2.3.1 所規定的同等或以上等級之加密演算法。

(4) 通過：若支援線上更新，則(1)(2)項結果皆符合、或(1)(3)項結果皆符合。

(5) 通過：若支援手動更新，則(1)項結果符合。

(6) 不通過：若支援線上更新，則(1)(2)項結果不符合其一、或(1)(3)項結果不符合其一。

(7) 不通過：若支援手動更新，則(1)項結果不符合。

(8) 不適用：產品為無法手動或線上更新軟韌體之受限制設備，則廠商應提供相關文件以證明產品的安全更新方式(例如:硬體更換、召回等)。

5.4.1.3 更新檔案真實性與完整性測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.4.1.3

(b) 安全等級

1 級

(c) 測試資料

(1) 產品之韌體更新檔。

(2) 若選擇測試方法 1，廠商提供測試用私鑰予實驗室；廠商應提供產品之數位簽章使用機制，作為審查依據。

(3) 若選擇測試方法 2，實驗室提供自簽公私鑰予廠商。

(d) 測試目的

驗證產品安裝韌體更新檔是否採用簽章驗證機制，以確保更新檔案之真實性與完整性。

(e) 測試條件

產品應支援更新機制。

(f) 測試佈局

無。

(g) 測試方法

測試方法 1 (廠商提供測試用私鑰予實驗室)：

(1) 廠商提供原始軟/韌體並提供簽章方法，實驗室使用自簽私鑰簽署該軟/韌體。

(2) 實驗室執行軟/韌體更新，檢視更新結果。

測試方法 2 (實驗室提供自簽公私鑰予廠商)：

(1) 實驗室提供自簽公私鑰予送測廠商，廠商利用該私鑰簽署軟/韌體，並將公鑰植入於產品。

(2) 實驗室執行軟/韌體更新，檢視更新結果。

(3) 受測廠商將實驗室所提供之測試私鑰加入產品之受信任私鑰列表。

(4) 實驗室執行軟/韌體更新，檢視更新結果。

(h) 測試結果

(1) 若採用測試方法 1，實驗室使用自簽私鑰簽署軟/韌體，軟/韌體更新失敗。

(2) 若採用測試方法 2，廠商使用實驗室提供之自簽公私鑰，軟/韌體更新成功。

(3) 通過：(1)~(2)項任一結果符合。

(4) 不通過：(1)~(2)項結果皆不符合。

(5) 不適用：產品為不支援軟/韌體更新之受限制設備，則廠商應提供相關設計文件以證明產品無法透過軟/韌體更新 (例如:硬體更換、召回等)。

5.5 已知漏洞安全測試

檢視產品有關已知漏洞安全之送審資料是否符合 IoT-100x-1 之安全要求，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

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.5.1.1

(b) 安全等級

1 級

(c) 測試資料

(1) 產品 IP 位址。

(2) 產品應保持出廠預設環境狀態。

(3) 產品應提供所啟用之網路服務與對應埠之宣告，作為審查依據。

(d) 測試目的

驗證產品是否存在預期以外的網路埠。

(e) 測試條件

無。

(f) 測試佈局

如圖 3。

(g) 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。

(3) 對產品執行 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) 對產品執行 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。

(h) 測試結果

(1) 產品所開啟之網路服務與對應埠，與產品自我宣告之「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) 產品未開啟自我宣告以外的網路服務。

(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：產品無網路服務功能。

5.5.1.2 測試作業系統與網路服務是否存在 CVSS v3 評分為 9.0 分以上之常見資安漏洞

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.5.1.2

(b) 安全等級

1 級

(c) 測試資料

(1) 產品 IP 位址。

(2) 產品應保持出廠預設環境狀態。

(3) 產品之系統管理者帳號和通行碼。

(d) 測試目的

驗證產品之作業系統與網路服務是否存在已知 CVSS v3[(5)]重大資安風險的漏洞。

(e) 測試條件

(1) 產品支援作業系統。

(2) 產品支援網路服務。

(3) 若產品不支援透過網路服務進行登入工具掃描，則廠商應提供與送測相同版本且未加密之測試用韌體，作為測試查驗使用。

(f) 測試佈局

如圖 3。

(g) 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。

(3) 設定產品的 IP 位址及系統管理者帳號和通行碼。

(4) 對產品執行工具掃描。

(5) 若產品不支援透過網路服務進行登入工具掃描，利用韌體掃描工具執行韌體掃描。

(h) 測試結果

(1) 作業系統、網路服務無檢測出美國國家漏洞資料庫評分 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：產品不支援作業系統。

5.5.1.3 測試作業系統與網路服務是否存在 CVSS v3 評分為 7.0 分以上之常見資安漏洞

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.5.1.3

(b) 安全等級

2 級

(c) 測試資料

(1) 產品 IP 位址。

(2) 產品應保持出廠預設環境狀態。

(3) 產品之系統管理者帳號和通行碼。

(d) 測試目的

驗證產品之作業系統與網路服務是否存在已知 CVSS v3 高資安風險的漏洞。

(e) 測試條件

(1) 產品支援作業系統。

(2) 產品支援網路服務。

(3) 若產品不支援透過網路服務進行登入工具掃描，則廠商應提供與送測相同版本且未加密之測試用韌體，作為測試查驗使用。

(f) 測試佈局

如圖 3。

(g) 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。

(3) 設定產品的 IP 位址及系統管理者帳號和通行碼。

(4) 對產品執行工具掃描。

(5) 若產品不支援透過網路服務進行登入工具掃描，利用韌體掃描工具執行韌體掃描。

(h) 測試結果

(5) 作業系統、網路服務無檢測出美國國家漏洞資料庫評分 CVSS v3 為 7.0 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。

(6) 通過：(1)項結果符合。

(7) 不通過：(1)項結果不符合。

(8) 不適用：產品不支援作業系統。

5.6 資源可用性測試

檢視產品有關資源可用性之送審資料是否符合 IoT-100x-1 之安全要求，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 儲存空間滾動機制測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.6.1.1

(b) 安全等級

2 級

(c) 測試資料

(1) 廠商應提供產品儲存空間配置、容量偵測與覆蓋等滾動(Log rotation)機制之技術說明文件，作為測試依據。

(2) 若產品不支援滾動機制，廠商應提供儲存容量不足警戒值設定及警示與紀錄功能及其操作說明文件，作為測試依據。

(3) 產品應提供管理者權限之帳號和通行碼，作為測試查驗使用。

(d) 測試目的

驗證產品是否具備處理儲存空間不足等異常狀況之功能。

(e) 測試條件

(1) 產品之感測資料儲存於產品儲存空間，例如:記憶體。

(2) 產品支援生成之安全事件日誌儲存於產品儲存空間。

(f) 測試佈局

如圖 3。

(g) 測試方法

(1) 啟動產品偵測功能。

(2) 根據說明文件，操作將感測資料填充至儲存空間，直到達到產品設定之儲存空間不足。

(3) 檢視產品之感測資料是否可持續正常記錄。

(4) 若產品支援生成安全事件日誌且儲存於產品儲存空間，根據說明文件，執行將安全事件日誌檔填充至儲存空間，直到達到產品設定之儲存空間不足。

(5) 檢視產品之安全事件日誌是否可持續正常記錄。

(6) 若產品不支援滾動機制，根據操作說明文件，設定容量不足警戒值並將儲存空間填充至達到產品容量不足警戒值。

(7) 檢視產品是否有相應的警示與紀錄。

(h) 測試結果

(1) 產品之感測資料到達儲存空間不足時，產品應仍可正常運作且具備滾動機制；或儲存容量不足時，產品應有安全事件紀錄並發出警示。

(2) 若產品支援生成安全事件日誌，產品之安全事件日誌到達儲存空間不足時，產品應仍可正常運作且具備滾動機制；或儲存容量不足時，產品應有安全事件紀錄並發出警示。。

(3) 產品儲存空間達到容量不足警戒值時，產品應產生安全事件日誌及發出警示。若產品不支援安全事件日誌警示功能時，可透過環境面設置與部署，例如：透過其他相連設備。若以環境面安全部署，廠商應在產品之使用說明書或資安指引中註明產品於現場佈建時額外部署的軟硬體設備，並說明建議部署的軟硬體設備類型。

(4) 通過：(1)(3)項結果符合其一，或(2)(3)項結果符合其一。

(5) 不通過：(1)(3)項結果皆不符合，或(2)(3)項結果皆不符合。

(6) 不適用：產品不支援感測資料儲存至產品之儲存空間。

(7) 不適用：產品不支援生成之安全事件日誌儲存於產品之儲存空間。

5.6.2 警示與記錄測試

5.6.2.1 安全事件日誌測試

(a) 測試依據

「IoT-100x-1 感測裝置資安標準-第一部：一般要求」之 5.6.2.1

(b) 安全等級

1 級

(c) 測試資料

(1) 廠商應提供與產品連接的管理平台或其他設備，以供測試使用。

(2) 廠商應提供書面文件以說明產品發生哪些安全事件及如何記錄安全事件，作為測試依據。

(3) 若是由管理平台或其他設備記錄安全事件，廠商應提供書面文件說明以何方式通知管理平台或其他設備進行安全事件的記錄，作為測試依據。

(d) 測試目的

驗證產品是否具備安全事件日誌功能。

(e) 測試條件

無。

(f) 測試佈局

如圖 2。

(g) 測試方法

(1) 情況 1：(產品具備安全事件日誌)

(i) 將測試電腦與產品連接。

(ii) 根據廠商提供之說明文件，觸發安全事件。

(iii) 根據產品使用說明，開啟相應之管理介面連接工具。

(iv) 瀏覽安全事件日誌。

(v) 確認日誌內容是否記載步驟(ii)的安全事件紀錄。

(vi) 檢視該日誌是否具有包括但不限於時間戳、來源(原始設備、軟體程序或使用者帳號)、類別、事件 ID 和安全事件結果。

(vii) 將產品重新開機，開啟相應之管理介面連接工具，瀏覽安全事件日誌。

(2) 情況 2：(由管理平台或其他設備記錄產品之安全事件日誌)

(i) 觸發設備所定義的安全事件。

(ii) 以系統管理者帳號和通行碼登入管理平台瀏覽安全事件日誌。

(iii) 或側錄傳送往管理平台或其他設備之封包，檢視傳送往管理平台或其他設備之安全事件日誌。

(h) 測試結果

(1) 產品具有安全事件日誌功能，或產品之安全指引/使用手冊闡明由管理平台或其他設備記錄安全事件日誌。

(2) 安全事件日誌或定期事件回傳的資料應包含但不限於時間戳(標示應符合 ISO 8601:2019[6]所規定含時區標示之格式)、來源(原始設備、軟體程序或使用者帳號)、類別、事件 ID 和安全事件結果。

(3) 重開機後之安全事件日誌仍可查詢。

(4) 通過：(1)~(3)項結果皆符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：無。

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.一、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)
相連之感測物聯網平台(IP)	民生公共物聯網 (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 B
(規定)
安全功能規格說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表 B.一、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。	
7. 預設組態設定	列出產品出廠預設之組態設定及其功能說明，或提供說明文件。	

參考資料

(1) IEC 62443-4-2-2019 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, https://webstore.iec.ch/publication/34421.

(2) ETSI EN 303 645 V2.1.1(2020-06) Cyber Security for Consumer Internet of Things: Baseline Requirements, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

(3) ETSI TS 103 701 V1.1.1(2021-08): Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements, https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

(4) SP 800-140C Rev. 1:2022 CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759, https://csrc.nist.gov/publications/detail/sp/800-140c/rev-1/final

(5) FIRST, Common Vulnerability Scoring System version 3.1: Specification Document, https://www.first.org/cvss/specification-document

(6) ISO 8601-1:2019 Date and time- Representations for information interchange, https://www.iso.org/standard/70907.html

(7) ISO 8601-1:2019/Amd 1:2022 Date and time - Representations for information interchange - Part 1: Basic rules - Amendment 1: Technical corrections

版本修改紀錄

版本	時間	摘要