IoT-2007-3

感測裝置資安測試規範

-第三部：水位計

V1.0

行動應用資安聯盟

中華民國 111 年 12 月

目錄

引言

為防範針對前端感測裝置的攻擊事件，與避免因駭客攻擊而中斷預測防災系統之運行，針對與民眾生活息息相關的智慧聯網地震儀與水位計之防災預測感測器，制定感測裝置之資安產業標準，著重可用性與感測裝置之資安防護能力，並藉以引導業者將資安設計概念導入感測產品中。

本測試規範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

本規範適用於感測物聯網中的水位計，如下圖 1 所示。

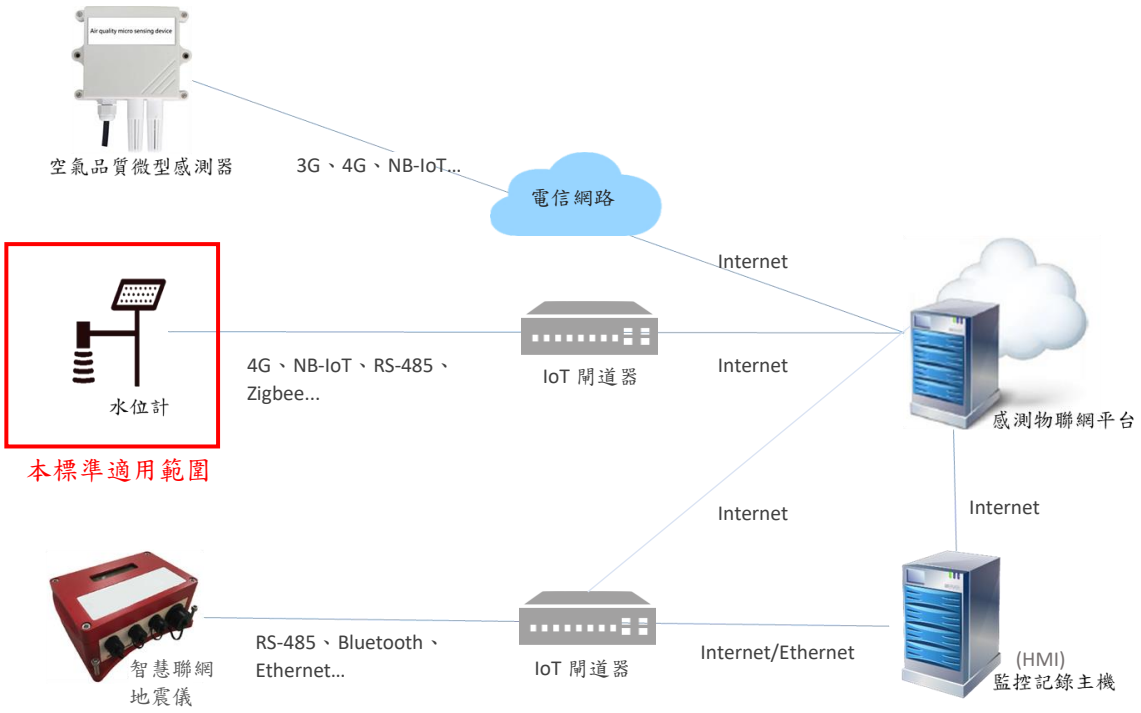

圖 1 適用範圍示意圖

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] IoT-100x-3 v1.0 感測裝置資安標準-第三部：水位計

3. 用語及定義

「IoT-100x-3 感測裝置資安標準-第三部：水位計」所規定之用語及定義適用於本規範。

3.1 電磁相容性(Electro Magnetic Compatibility，EMC)

係指產品在其電磁環境下能正常運作，且不會對其他設備產生電磁干擾的能力。國際上已有針對各環境下之電磁相容性發布相關標準與認證，其包括電磁干擾(Electromagnetic interference)與電磁耐受性(Electromagnetic susceptibility)，例如: IEC EN 61000、CNS13803 等。

4. 測試項目分級

本節依據「IoT-100x-3 感測裝置資安標準-第三部：水位計」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)、2 級(進階安全要求)二個等級，產品須先通過 1 級安全等級之測試，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	5.1.1.2	5.1.1.3
	5.1.2 權限控管	-	-
	5.1.3 通行碼鑑別	5.1.3.1	-
5.2 資料機密性與完整性	5.2.1 安全敏感性資料儲存	-	-
	5.2.2 資料傳輸	-	5.2.2.2
	5.2.3 密碼演算法之使用	5.2.3.2	-
5.3 系統完整性	5.3.1 系統安全	-	-
5.4 更新安全	5.4.1 軟韌體更新	-	-
5.5 已知漏洞安全	5.5.1 作業系統與網路服務	-	-
5.6 資源可用性	5.6.1 資源管理	5.6.1.2	-
	5.6.2 警示與記錄	-	5.6.2.2

5. 資安測試規範

水位計為滿足安全功能應依不同級別依循 IoT 100x-1「感測裝置資安標準 第一部：一般要求[1]」測試規範及本節所載明之測試規範。

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-3 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 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.1.1 節。

5.1.1.2 身分鑑別訊息測試

(a) 網頁介面

(1) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.1.1.2

(2) 安全等級

1 級

(3) 測試資料

(i) 產品使用者帳號與通行碼。

(ii) 產品使用說明文件，例如：產品使用手冊。

(4) 測試目的

驗證身分鑑別過程與鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件

產品應支援網頁管理介面。

(6) 測試佈局

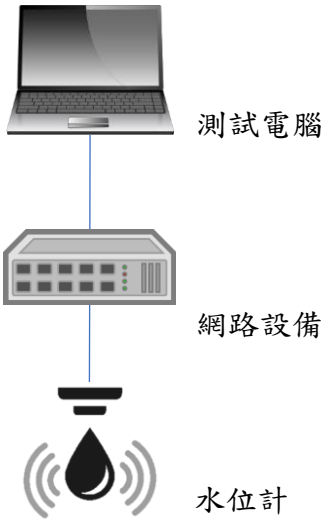

圖 2 測試示意圖

(7) 測試方法

(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) 輸入已存在的使用者帳號，及輸入錯誤的通行碼。

(iv) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(v) 輸入不存在的使用者帳號和通行碼。

(vi) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(8) 測試結果

(i) 身分鑑別過程中所輸入通行碼的呈現不以明碼顯示，例如：以符號(＊或●等)顯示。

(ii) 身分鑑別錯誤訊息所顯示的資訊不能被推斷出使用者帳號或通行碼，例如：「使用者帳號不存在」、「通行碼錯誤」此類資訊是不被允許的。

(iii) 通過：(i)(ii)項結果皆符合。

(iv) 不通過：(i)(ii)項結果不符合其一。

(v) 不適用：產品不支援網頁管理介面。

(b) 實體介面

(1) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.1.1.2

(2) 安全等級

1 級

(3) 測試資料

產品使用者帳號與通行碼。

(4) 測試目的

驗證身分鑑別過程與鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件

(i) 產品支援實體管理介面。

(ii) 廠商應提供實體介面之連接方式，例如:產品使用手冊，作為測試依據。

(6) 測試佈局

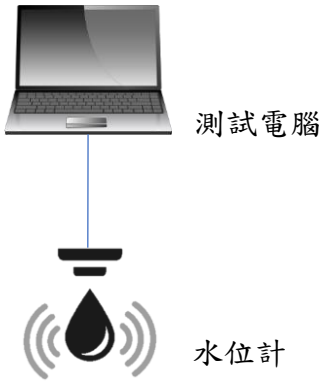

圖 3 測試示意圖

(7) 測試方法

(i) 若產品支援 UART，根據說明文件將測試電腦連接產品之 UART。

(ii) 透過 UART 埠存取作業系統之除錯模式。

(iii) 輸入產品已存在的使用者帳號，及輸入錯誤的通行碼。

(iv) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(v) 輸入不存在的使用者帳號和通行碼。

(vi) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(vii) 若產品支援 JTAG，根據說明文件將測試電腦連接產品之 JTAG。

(viii)透過 JTAG 埠存取作業系統之除錯模式。

(ix) 重複步驟(iii)~(vi)。

(x) 若產品支援 USB，根據說明文件將測試電腦連接產品之 USB。

(xi) 透過 USB 埠存取作業系統之除錯模式。

(xii) 重複步驟(iii)~(vi)。

(8) 測試結果

(i) 身分鑑別過程中所輸入通行碼的呈現不以明碼顯示，例如：以符號(＊或●等)顯示。

(ii) 身分鑑別錯誤訊息所顯示的資訊不能被推斷出使用者帳號或通行碼，例如：「使用者帳號不存在」、「通行碼錯誤」此類資訊是不被允許的。

(iii) 通過：(i)(ii)項結果皆符合。

(iv) 不通過：(i)(ii)項結果不符合其一。

(v) 不適用：產品不支援實體管理介面。

(c) 遠端指令介面

(1) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.1.1.2

(2) 安全等級

1 級

(3) 測試資料

(i) 產品使用者帳號與通行碼。

(ii) 產品使用說明文件，例如：產品使用手冊。

(4) 測試目的

驗證身分鑑別過程與鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件

產品支援遠端指令介面。

(6) 測試佈局

如圖 2。

(7) 測試方法

(i) 將測試電腦連接產品。

(ii) 根據產品使用說明，開啟遠端指令介面。

(iii) 輸入產品已存在的使用者帳號，及輸入錯誤的通行碼。

(iv) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(v) 輸入不存在的使用者帳號和通行碼。

(vi) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(8) 測試結果

(i) 身分鑑別過程中所輸入通行碼的呈現不以明碼顯示，例如：以符號(＊或●等)顯示。

(ii) 身分鑑別錯誤訊息所顯示的資訊不能被推斷出使用者帳號或通行碼，例如：「使用者帳號不存在」、「通行碼錯誤」此類資訊是不被允許的。

(iii) 通過：(i)(ii)項結果皆符合。

(iv) 不通過：(i)(ii)項結果不符合其一。

(v) 不適用：產品不支援遠端指令介面。

(d) API 介面

(1) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.1.1.2

(2) 安全等級

1 級

(3) 測試資料

(i) 產品使用者帳號與通行碼。

(ii) 產品使用說明文件，例如：產品使用手冊。

(4) 測試目的

驗證身分鑑別過程與鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件

產品支援 API 介面。

(6) 測試佈局

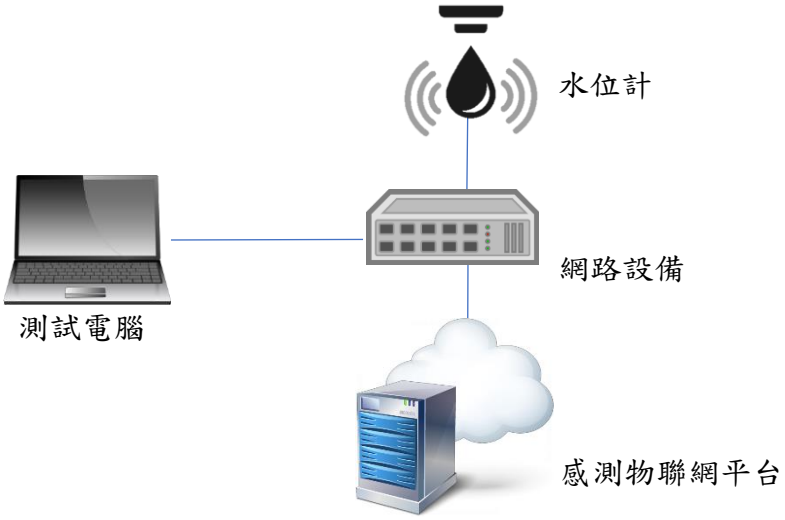

圖 4 測試示意圖

(7) 測試方法

(i) 將測試電腦與感測物聯網平台連結在同一區域網路中。

(ii) 將產品連結感測物聯網平台。

(iii) 根據產品使用說明，開啟遠端指令介面。

(iv) 輸入產品已存在的使用者帳號，及輸入錯誤的通行碼。

(v) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(vi) 輸入不存在的使用者帳號和通行碼。

(vii) 檢視身分鑑別輸入過程及鑑別錯誤訊息。

(8) 測試結果

(i) 身分鑑別過程中所輸入通行碼的呈現不以明碼顯示，例如：以符號(＊或●等)顯示。

(ii) 身分鑑別錯誤訊息所顯示的資訊不能被推斷出使用者帳號或通行碼，例如：「使用者帳號不存在」、「通行碼錯誤」此類資訊是不被允許的。

(iii) 通過：(i)(ii)項結果皆符合。

(iv) 不通過：(i)(ii)項結果不符合其一。

(v) 不適用：產品不支援 API 介面。

5.1.1.3 終端設備身分證明測試

(a) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.1.1.3

(b) 安全等級

2 級

(c) 測試資料

(1) 產品應提供與產品相連的管理平台，以供測試使用。

(2) 產品應提供身分證明機制之說明文件，作為審查依據。

(d) 測試目的

驗證管理平台與產品間是否具備身分證明機制。

(e) 測試條件

無。

(f) 測試佈局

如圖 2。

(g) 測試方法

(1) 審閱產品之身分證明機制說明文件。

(2) 根據說明文件，將產品與管理平台建立連線，並側錄封包。

(3) 檢視產品身分證明機制是否符合遠端證明設計。

(h) 測試結果

(1) 產品提供之說明文件足以證明產品具備身分證明之功能，且產品具有相應之功能。

(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 權限控管測試

5.1.2.1 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.1.2 節。

5.1.3 通行碼鑑別測試

5.1.3.1 通行碼強度測試

(a) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.1.3.1

(b) 安全等級

1 級

(c) 測試資料

管理者帳號、通行碼。

(d) 測試目的

驗證產品的通行碼安全強度是否符合國際標準規範或資安產業慣例之作法之通行碼規定。

(e) 測試條件

(1) 產品應支援通行碼鑑別機制。

(2) 產品應提供通行碼鑑別機制說明文件，並列出產品之不合法的通行碼設定規則，以作為審查依據。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱產品通行碼設定規則說明文件。

(2) 開啟產品管理介面，新建立帳號、通行碼，或變更現有帳號之通行碼。

(3) 嘗試輸入通行碼，例如:輸入連續字母(aaaaaa、1234abcd)。

(4) 檢視通行碼是否能成功建立或變更。

(h) 測試結果

(1) 產品之說明文件證實通行碼設定原則符合國際標準規範或資安產業慣例之通行碼規定，例如: NIST SP 800-63B[6]。

(2) 產品建立或變更通行碼失敗。

(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：產品不支援通行碼鑑別機制。

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-3 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 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.2.1 節。

5.2.2 資料傳輸測試

5.2.2.1 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.2.2 節。

5.2.2.2 電磁抗干擾能力測試

(a) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.2.2.2

(b) 安全等級

2 級

(c) 測試資料

(1) 廠商應提供產品定位與設置環境之宣告文件，例如:產品使用手冊等。

(2) 廠商應提供依產品建置環境所須滿足之電磁相容性(EMC)國際認驗證機構認可實驗室所核發檢測報告，作為審查依據。

(d) 測試目的

產品是否具備電磁抗干擾的能力。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審查廠商提供之產品電磁相容性檢測報告。

(h) 測試結果

(1) 根據產品提供之佐證資料足以證明產品通過之電磁相容性檢測，檢測報告符合其宣告之類別，例如:工業、科學、醫療設備之 CNS 13803 認證。

(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。

5.2.3 密碼演算法之使用測試

5.2.3.1 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.2.3 節。

5.2.3.2 無線網路傳輸安全機制設置測試

(a) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.2.3.3

(b) 安全等級：

1 級

(c) 測試資料

(1) 產品應保持出廠預設組態。

(2) 產品使用說明文件，例如：產品使用手冊。

(d) 測試目的

驗證產品是否具有安全的 Wi-Fi 通道保護設定。

(e) 測試條件

產品支援 Wi-Fi 功能。

(f) 測試佈局

如圖 2。

(g) 測試方法

(1) 將測試電腦連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具。

(3) 與產品建立連線，同時側錄傳輸封包。

(4) 依據側錄結果查驗傳輸是否採用 Wi-Fi 存取保護版本 v2(WPA 2)同等或以上版本。

(h) 測試結果

(1) 若受測產品具有 Wi-Fi 基地台(AP)能力時，Wi-Fi 預設加密模式為 Wi-Fi 存取保護版本 v2(WPA 2)同等或以上版本。

(2) 若受測產品僅能透過 Wi-Fi AP 連線時(使用者端角色)，則產品應支援相應之 WPA 版本。

(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：產品不支援 Wi-Fi 功能。

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-3 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 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.3.1 節。

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-3 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 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.4.1 節。

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-3 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 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.5.1 節。

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-3 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 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.6.1 節。

5.6.1.2 備援機制測試

(a) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.6.1.2

(b) 安全等級

1 級

(c) 測試資料

廠商應提供設置預防網路和電源中斷的備援機制運作之作法，及其環境面部署的說明文件。

(d) 測試目的

驗證產品是否設置因應網路、電源中斷的備援機制。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱預防網路和電源中斷備援機制書面文件。

(2) 根據說明文件，中斷產品網路，檢視產品運作情況。

(3) 中斷電源，檢視產品運作情況。

(h) 測試結果

(1) 產品備援機制或產品以環境面的部署應能使產品功能持續運作，例如：產品能繼續正常偵測並保存感測資料。

(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。

5.6.2 警示與記錄測試

5.6.2.1 測試依循「IoT-200x-1 感測裝置資安測試規範-第一部：一般要求」第 5.6.2 節。

5.6.2.2 警示功能測試

(a) 測試依據

「IoT-100x-3 感測裝置資安標準-第三部：水位計」之 5.6.2.2

(b) 安全等級

2 級

(c) 測試資料

(1) 廠商應提供產品之安全事件警示功能說明與操作方法之書面文件，並條列出觸發安全警示功能的安全事件，作為審查依據。

(2) 若產品須透過環境面部署(例如:連接其他設備)發出安全事件警示，廠商應提供此機制的設計與操作說明之書面文件作為審查依據，例如：產品之安全指引等。

(3) 廠商應提供與產品連接的管理平台或/及其他設備，以供測試使用。

(d) 測試目的

驗證產品發生安全事件時，產品是否有能力發出警示。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱廠商提供之警示功能說明文件。

(2) 根據操作方法書面文件，觸發產品安全事件。

(3) 確認產品是否發出警示。

(h) 測試結果

(1) 當產品發生安全事件時，產品應向管理平台或管理者發出警示。

(2) 若產品透過環境面部署以發出安全事件警示時，廠商提供之書面文件足以證實在產品具有安全事件警示功能。

(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。

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) IoT-100x-1 v1.0: 感測裝置資安標準 第一部：一般要求

(2) 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.

(3) 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.

(4) 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

(5) 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

(6) NIST SP 800-63 Rev.5: Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

版本修改紀錄

版本	時間	摘要