IoT-1007-1

感測裝置資安標準

-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

政府為更有效率的提前防範與因應災情，投入民生公共物聯網計畫，建構了與民眾生活息息相關的「空氣品質」、「地震」及「水資源」領域的物聯網監測平台，在此政策的推動下，國內相關業者逐漸發展成環境感測物聯網生態產業鏈。在此同時，布建在外的感測裝置 [3.1] 便面臨了可能成為駭客攻擊跳板的機會，例如，2018 年發生駭客利用賭場大廳魚缸的聯網溫度感測裝置的漏洞當中繼站，入侵賭場資料庫，竊取豪客名單的個資外洩事件。

為預防類似攻擊事件發生，及助民生公共物聯網相關感測裝置提升資安品質，在數位發展部數位產業署支持下，本標準基於國際工控資安標準 IEC 62443 及歐盟資安標準 ETSI EN 303 645，針對諸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、水位計等感測裝置制定資安標準，以緩解感測裝置所面臨的資安威脅，作為開發商、整合商等作為產品開發設計、組裝階段資安導入之參考標準。

1. 適用範圍

本標準之適用範圍為環保署、水利署、氣象局、國震中心、園區/建築物管理中心等，用以監測民眾生活相關環境資料所使用的感測裝置，包括但不限於智慧聯網地震儀、水位計、空氣品質等感測裝置，如下圖所示。

本標準規範感測裝置之資安要求，惟下列項目不在本標準適用範圍內：

- 非採用聯網功能之感測裝置，與監測站之大型環境感測設備。
- 電信網路與感測物聯網平台之間網路傳輸安全。
- 網路設備與感測物聯網平台/監控記錄主機之間網路傳輸安全。
- 網路設備、感測物聯網平台及監控記錄主機。

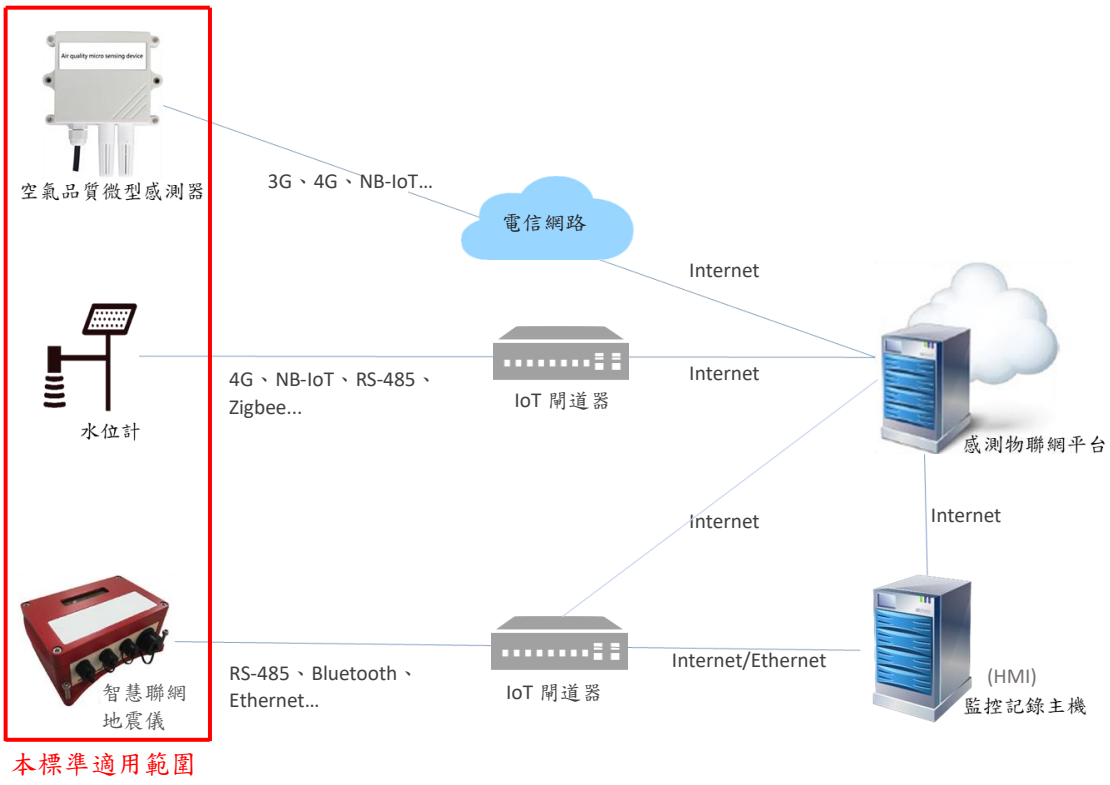

圖 1 感測物聯網架構示意圖

2. 引用標準

以下引用標準係本標準必要參考文件。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。

[1] IEC 62443-4-2-2019 **Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components**

[2] ETSI EN 303 645 V2.1.1(2020-06) **Cyber Security for Consumer Internet of Things: Baseline Requirements**

3. 用語及定義

下列用語及定義適用於本標準。

3.1 感測裝置(sensing devices)

本標準係指能夠從其周圍環境獲取偵測數據的物聯網裝置，例如：溫度、光、聲音、壓力、震動方向、流體速度等類型之裝置，以即時監測環境數據為目的，且能將感測資料透過網路回傳至感測物聯網平台(如 3.2 所述)，提供監管單位與民眾查詢。

3.2 感測物聯網平台(Sensing data platform)

指建置於雲端之環境感測裝置數據收集中心，其可能內含數據資料儲存、裝置管理、介面管理、通訊管理、裝置偵測等功能，提供 API 等介面作為國家、地方政府、其他機構或企業作為數據分析或資料展示等應用介接使用。例如，行政院環保署環境感測物聯網平台、水利署水資源物聯網平台、民生公共物聯網資料服務平台等。

3.3 智慧聯網地震儀(Seismometer)

本標準係指用於探測、收集區域地震資料的感測裝置，其由感測組件、控制器(包括但不限於微控制器 MCU、處理器 CPU)、及通訊模組所組成。例如：布建於建築物、交通建設、井下等處，可透過網路傳輸將收集之地震資料傳送至地震預警系統，包括但不限於民生公共物聯網、中央氣象局、國家地震中心或建築物管理中心。

3.4 水位計(Level sensors)

本標準係指偵測、收集即時水位、流速等資訊的感測裝置，其由感測組件、控制器(包括但不限於微控制器 MCU、處理器 CPU)及通訊模組所組成。例如：布建於河川、水庫、下水道等處，透過網路傳輸將收集之水位、流量等資料傳送至如各地方政府或水資源物聯網等的管理平台。

3.5 安全敏感性資料(Security-sensitive data)

指與設備或服務之安全性相關的資料，例如通行碼、金鑰等系統運行所需之機敏資料，或產品運用於特殊、機敏之應用情境所收集、利用、處理之感測資料等。例如：當產品透過 OTA 更新韌體時，如果更新伺服器發送之憑證金鑰遭惡意人士竄改，可能造成更新失敗或安裝了帶有惡意程式之韌體。

3.6 預設通行碼 (Default password)

係指產品出廠預先設定好的通行碼，即在使用者初次將產品連上網路，且在未更改任何設定的情況下，用以登入感測裝置之通行碼。

3.7 最小權限(Least privilege)

係一種資訊安全的概念，以使每個使用者都獲得該使用者執行其任務所需之最低存取資源和授權。

3.8 國家弱點資料庫(National Vulnerability Database, NVD)[(2)]

指美國國家標準技術研究所(National Institute of Standards and Technology, NIST)提供的美國國家弱點資料庫，負責常見弱點與漏洞(如 3.9 所述)之資料的發布及更新。

3.9 常見弱點與漏洞(Common Vulnerabilities and Exposures, CVE)

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

3.10 通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)

使用 IT 漏洞的特點與影響進行評分，由美國資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)發展至第 3.1 版[(3)]。包括威脅所造成損害的嚴重性、資安漏洞的可利用程度與攻擊者不當運用該漏洞的難易度，都被列入評比。評比從 0 分到 10 分，0 代表沒有弱點，而 10 則代表最高風險。

3.11 加密(Encryption)

指為了避免資訊的洩漏，明文資訊透過數學演算法進行改變，使原來的明文資訊變成不可讀而達到保密之目的。

3.12 安全通道(Security tunnel)

為網際網路通訊端點與端點(End-to-End)間，並達到資料隱密性及完整性所建立之通道，例如：目前常見之實作安全套接層協定 (Secure Sockets Layer, SSL)和傳輸層安全性(Transport Layer Security, TLS)。

3.13 安全區域 (Secure domain, Secure world)

係指與正常作業環境隔離出的區域，僅用於執行安全性相關操作，如：加解密、金鑰管理、完整性檢查，並供敏感性資料保存用。

3.14 安全事件日誌 (Security event log)

係指記錄每個稽核規則所定義的活動，用以察覺威脅或攻擊事件的發生，本文之安全事件包括但不限於使用者登入、連線失敗、資源達警戒值等行為。

3.15 關鍵基礎設施(Critical Infrastructure, CI)

係指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。根據國家關鍵基礎設施領域分類(111 年 3 月 30 日修正版)，我國現行關鍵基礎設施分為八大主領域，分別為能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區。

3.16 關鍵金鑰 (Critical security key)

係指產品專用以確保完整性與真實性所使用的金鑰，若洩露或修改可能危及產品的安全性。

4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

本標準為感測裝置之共通安全要求，安全等級總表如表 1 所示，第一欄為安全構面，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；第二欄為安全要求分項，係依各安全構面設計對應之安全要求分項；第三欄為安全等級，按各安全要求分項之驗證結果，作為安全等級評估標準。本安全等級總表各欄的關連性，須依循本節 5.1 至 5.6 之技術規範內容。

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 安全要求等級總表

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	-

4.1.1 安全構面：

(a) 身分識別、鑑別、授權：溝通介面須確保鑑別、鑑別與授權相關機制，包括遠端指令管理介面、通訊協定等應具有一定防護能力，避免遭受蓄意人士入侵。

(b) 資料機密性與完整性：產品傳輸與儲存之資料應具備足夠的安全保護，避免遭受有心人士惡意竄改。

(c) 系統完整性：產品啟動階段，對於韌體、軟體及作業系統是否經過竄改或植入惡意程式，應具備防禦能力，視為實體安全要求的標的。

(d) 更新安全：產品之作業系統及韌體版本更新服務及韌體程式設計等，須具備足夠安全防護。

(e) 已知漏洞安全：產品應防止作業系統、網路服務存在已知安全漏洞。

(f) 資源可用性：產品之資源管理應預防造成服務中斷，並在安全事件發生時具備記錄功能。

4.1.2 安全要求分項：

依安全構面所設計對應之安全要求要項，其中每一安全要求分項包含一個或一個以上之安全要求。

4.1.3 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，分為安全等級 1 級和 2 級二個等級。其對應之列即其所應符合的安全要求分項，安全等級級數的大小代表安全等級的高低，欲符合較高等級之進階安全要求必須先滿足較低安全等級之必要安全要求。

4.1.3.1 安全 1 級，適用產品傳輸之資料為開放性資料(經所屬單位評估許可，開放在使用範圍內存取)，防護目標為無特定目的及動機之駭客攻擊，以避免成為攻擊跳板。

4.1.3.2 安全 2 級，適用產品具有安全敏感功能且資料傳輸須確保完整性，需要防護針對安全敏感性資料作有特定目的及動機之駭客攻擊，以避免成為攻擊跳板，並維持產品可用性。

5. 一般要求

本節詳盡載明感測裝置需要滿足之全功能應採取之方法，感測裝置產品依 4.1.3 節所述，滿足本節之安全要求。

5.1 身分鑑別、識別、授權

5.1.1 鑑別機制

5.1.1.1 每個產品應有一組唯一的識別碼。(1 級)

5.1.1.2 產品之所有介面應具備身分鑑別機制。(1 級)

5.1.1.3 產品之身分鑑別所使用之預設安全敏感性資料(例:通行碼、金鑰)皆須相異；抑或首次成功取得產品存取之授權，須強制更改預設通行碼。(1 級)

5.1.1.4 產品應確保每一台關鍵金鑰之唯一性。(2 級)

5.1.2 權限控管

5.1.2.1 產品之所有介面應具備權限控管，區分之角色所需之權限控制與廠商所宣告的一致，且遵守最小權限的原則(Least privilege)。(1 級)

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 產品所儲存之安全敏感性資料不應明文儲存，而保護資料的加密方式應依據 5.2.3.1 項之加密演算法要求。(1 級)

5.2.1.2 韌體檔案不應置於公開存取之位置，晶片中的韌體須加密保護以確保機密性，不得存在明文或可被解密回復之安全敏感性資料且須採用 5.2.3.1 所核可之同等或以上強度的加密演算法。(1 級)

5.2.1.3 安全敏感性資料應存放於產品的安全區域，與正常作業環境隔離。(2 級)

5.2.2 資料傳輸

5.2.2.1 產品之安全敏感性資料傳輸應透過安全通道，而安全通道的通道加密方式應依據 5.2.3.1 項之加密演算法要求。(1 級)

5.2.2.2 產品於傳輸過程中應鑑別所接收指令的完整性。(1 級)

5.2.2.3 產品之感測資料傳輸應透過安全通道，而安全通道的通道加密方式應依據 5.2.3.1 項之加密演算法要求。(2 級)

5.2.2.4 產品於傳輸過程中應鑑別接收指令來源身分的真實性，如使用加密演算法應依據 5.2.3.1 項之要求。(2 級)

5.2.3 密碼演算法之使用

5.2.3.1 產品所使用之密碼演算法應根據國際公認 NIST SP 800-140Cr1 [(4)]所核可的同等或以上等級之密碼演算法。(1 級)

5.3 系統完整性

5.3.1 系統安全

5.3.1.1 產品於啟動階段應確保韌體、軟體的完整性。(2 級)

5.4 更新安全

5.4.1 軟韌體更新

5.4.1.1 產品須具備韌體更新機制，且即使發生更新失敗時，系統能回復正常運作。(1 級)

5.4.1.2 產品之軟/韌體應具備安全更新功能，更新之安全功能包括但不限於防止安裝舊版本(非關鍵基礎設施環境所設置之產品)、加密傳輸符合 5.2.3.1 之加密演算法、更新傳輸走安全通道。(1 級)

5.4.1.3 產品應在更新安裝前驗證任何軟韌體更新檔的真實性和完整性。(1 級)

5.5 已知漏洞安全

5.5.1 作業系統與網路服務

5.5.1.1 產品啟用之功能與網路服應為提供產品必要服務之所需。(1 級)

5.5.1.2 產品之作業系統與網路服務(Network Service)，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為重大風險。(1 級)

5.5.1.3 產品之作業系統與網路服務(Network Service)，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。(2 級)

5.6 資源可用性

5.6.1 資源管理

5.6.1.1 產品之儲存空間(包括安全事件日誌及感測裝置資料)應具備滾動(Log rotation)機制，或儲存容量達警戒值時，應有安全事件紀錄並發出警示。(2 級)

5.6.2 警示與記錄

5.6.2.1 產品應提供與安全相關的日誌記錄功能，安全事件日誌應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。(1 級)

附錄 A
(參考)
技術要求事項與各標準規範對照表

本標準	對應標準規範		
要求事項	民生公共物聯網資通安全要求 V3	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.1.1.1	-	CR1.2RE(1) - Unique identification and authentication	-
5.1.1.2	D3P2(O)* - 使用防火牆與 VPN(遠端登入:身分鑑別機制) D5P1-實體存取限制	CR1.1 - Human user identification and authentication	5.5-4 - Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.
5.1.1.3	D7P1(O)* - 強制使用強密碼 D7P3* - 密鑰管理的職責分離	CR1.5A - support the use of initial authenticator content. CR1.5B - support the recognition of changes to default authenticators made at installation time.	5.1-1 - Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
5.1.1.4	D6P2(O)* - 運用對稱或非對稱金鑰保護 D6P3(O)* - 合適的密鑰管理 D7P3* - 密鑰管理的職責分離	-	5.4-4 - Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.
5.1.2.1	D7P2 - 限制遠端對安全網路的存取 D2P4(O) - 適當的身分管理 D9P3* - 限制對日誌之存取 D5P4 - 防竄改機制 D7P3* - 密鑰管理的職責分離	CR2.1 - Authorization enforcement	-

本標準	對應標準規範		
要求事項	民生公共物聯網資通安全要求 V3	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.2.1.1	D4P2(O) - 保護資料之傳輸，使用及儲存 D6P1 - 使用業界公認的加密方式	CR4.1A - provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported.	-
5.2.1.2	D4P2(O) - 保護資料之傳輸，使用及儲存 D6P1 - 使用業界公認的加密方式	-	-
5.2.1.3	D4P2(O) - 保護資料之傳輸，使用及儲存	-	-
5.2.2.1	D4P2(O) - 保護資料之傳輸，使用及儲存 D6P1 - 使用業界公認的加密方式	CR4.1A - provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported.	-
5.2.2.2	D4P1(O) - 啟用資料加密	CR3.1 - Communication integrity	-
5.2.2.3	D4P1(O) - 啟用資料加密(資料評估) D4P2(O) - 保護資料之傳輸，使用及儲存 D6P1 - 使用業界公認的加密方式	CR4.1A - provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported.	-
5.2.2.4	D6P1 - 使用業界公認的加密方式 D6P2(O)* - 運用對稱或非對稱金鑰保護	CR3.1RE(1) - Communication authentication	5.3-10(partial) - Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.
5.2.3.1	D6P1 - 使用業界公認的加密方式	CR 4.3 - Use of cryptography	5.1-3(partial) - Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage. 5.5-1(partial) - The consumer IoT device shall use best practice cryptography to communicate securely. 5.3-7(partial) - The device

本標準	對應標準規範		
要求事項	民生公共物聯網資通安全要求 V3	IEC 62443-4-2[1]	ETSI EN 303 645[2]
			shall use best practice cryptography to facilitate secure update mechanisms.
5.3.1.1	D1P1 - 使用安全的數位簽章(安全啟動) D1P3 - 確保更新的完整性	NDR3.14 - Integrity of the boot process	-
5.4.1.1	D7P4 - 保持軟體/韌體更新	NDR3.10 - Support for updates	5.3-1 - All software components in consumer IoT devices should be securely updateable. 5.3-8 - Security updates shall be timely.
5.4.1.2	D6P1 - 使用業界公認的加密方式 D7P4* - 保持軟體/韌體更新	-	5.3-2 - When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.
5.4.1.3	D1P3 – 確保更新的完整性	NDR3.10RE(1) - Update authenticity and integrity	5.3-9 - The device should verify the authenticity and integrity of software updates. 5.3-10(partial) - Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.
5.5.1.1	D3P1 - 連接最小化	CR7.7 - Least functionality	5.6-1 - All unused network and logical interfaces shall be disabled.
5.5.1.2	D10P2 - 進行安全檢測	-	-
5.5.1.3	D10P2 - 進行安全檢測	-	-
5.6.1.1	D8P3 - 監控及偵測容量使用情況	CR2.9RE(1)(partial) - Warn when audit record storage capacity threshold reached	-
5.6.2.1	D2P3 - 記錄登入失敗日誌	CR2.8 - Auditable events	-

本標準	對應標準規範		
要求事項	民生公共物聯網資通安全要求 V3	IEC 62443-4-2[1]	ETSI EN 303 645[2]
	D3P3(O) - 記錄連線授權失敗日誌 D4P3(O) - 記錄存取機敏資料 D5P3 - 異常日誌紀錄		

(*部分對應)

參考資料

(1) 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

(2) NIST, National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing

(3) FIRST, Common Vulnerability Scoring System version 3: Specification Document, https://www.first.org/cvss/specification-document

(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) 民生公共物聯網資通安全要求 第三版，https://ci.taiwan.gov.tw/uploads/民生公共物聯網資通安全要求 (第三版)_1090701 科會辦公告版.pdf

版本修改紀錄

版本	時間	摘要