IoT-1007-2

感測裝置資安標準

-第二部：智慧聯網地震儀

V1.0

行動應用資安聯盟

中華民國 111 年 12 月

目錄

引言

全球感測器市場穩定成長，亞太地區在近年來已發展為感測器應用最大的市場，經濟部於數年前大舉號召我國電子大廠搶攻全球感測器市場，在供需齊備、雙管齊下的政策推動下，國內相關業者逐漸發展成智慧感測物聯網生態產業鏈。根據工研院產科國際研究所資料[(1)]顯示，2022 年台灣的感測模組產值達新台幣 2299.73 億元，預估 2023 年產值達新台幣 2419.69 元，2022 至 2023 年年成長率逾 5%。

在此同時，我國為了監測水文、地震和空氣品質，於全台各處設置感測裝置，布建在外的感測裝置便面臨可能成為駭客攻擊跳板的機會，例如，2018 年美國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。諸如此類的資安事件，未來勢必仍不會間斷，甚至發生更嚴重的攻擊。

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，在數位發展部數位產業署的支持下，針對與民眾生活息息相關的智慧聯網地震儀與水位計等防災預測感測器，基於國際工控資安標準 IEC 62443-4-2 及歐盟資安標準 ETSI EN 303 645，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。

1. 適用範圍

本標準之適用範圍為用於探測、收集區域地震資料的智慧聯網地震儀產品，其組成係由感測組件、控制器(包括但不限於微控制器 MCU、處理器 CPU)及通訊模組所構成。產品設置在包括但不限於建築物、交通建設、井下等處，偵測之地震資料可透過網路傳輸傳送至地震預警系統，地震預警相關應用，例如：民生公共物聯網、中央氣象局、國家地震中心監測平台及建築物管理中心等。智慧聯網地震儀之適用範圍，如下圖所示。

本標準為智慧聯網地震儀之資安要求，惟下列項目不在本標準適用範圍內：

- 非採用聯網功能之地震儀。
- 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。

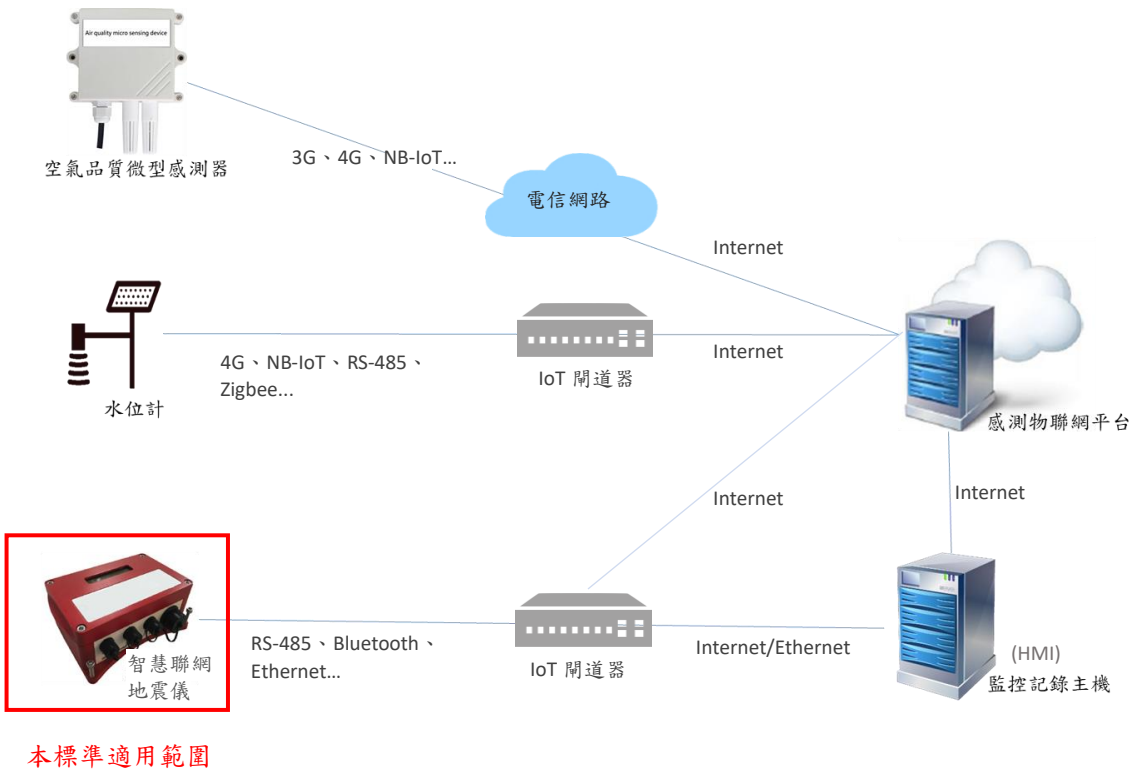

圖 1 適用範圍示意圖

標準適用說明：

- 智慧聯網地震儀產品皆須依循 IoT-100x-1「感測裝置資安標準-第一部：一般要求」標準規範及本標準所載明之標準規範。

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] 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」所述及下列用語及定義適用於本標準。

3.1 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，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。

3.2 遠端證明(Remote attestation)

係指系統用以驗證前端產品身分的方法，通常透過憑證機制與公鑰加密結合，來保證發出的資訊只能被發出證明要求的電腦或設備讀取，而非其他竊聽者。

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

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(必要要求)與 2 級(進階要求)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	5.1.1.2	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	5.2.2.3
	5.2.3 密碼演算法之使用	-	-
5.3 系統完整性	5.3.1 系統安全	-	5.3.1.2
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	-	-
	5.6.2 警示與記錄	-	5.6.2.2

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：

IoT-100x-1 之第 4.1.2 節之規定適用於本標準。

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

智慧聯網地震儀產品為滿足安全功能，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」標準規範及本節所載明之標準規範。

5.1 身分鑑別、識別、授權

5.1.1 鑑別機制

5.1.1.1 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.1.1 節之要求。

5.1.1.2 鑑別過程與鑑別錯誤訊息不應顯露出合法使用者帳號與通行碼。(1 級)

5.1.1.3 產品應具備遠端證明(Remote Attestation)功能，使產品向管理平台證明自身的合法性。(2 級)

5.1.2 權限控管

5.1.2.1 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.1.2 節之要求。

5.1.3 通行碼鑑別

5.1.3.1 產品之通行碼安全強度設定原則，應符合國際標準規範或資安產業慣例之通行碼規定。(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 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.2.1 節之要求。

5.2.2 資料傳輸

5.2.2.1 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.2.2 節之要求。

5.2.2.2 產品應確保感測資料傳輸的完整性。(1 級)

5.2.2.3 產品應確保偵測之感測資料的完整性與正確性。(2 級)

5.2.3 密碼演算法之使用

5.2.3.1 產品須依循 IoT-1000x-1 感測裝置資安標準-第一部：一般要求第 5.2.3 節之要求。

5.3 系統完整性

5.3.1 系統安全

5.3.1.1 產品須依循 IoT-1000x-1 感測裝置資安標準-第一部：一般要求第 5.3.1 節之要求。

5.3.1.2 產品產生的時間戳應具備與系統時間同步的功能，例如網路時間協定(NTP)、全球衛星定位(GPS)。(2 級)

5.4 更新安全

5.4.1 軟韌體更新

5.4.1.1 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.4.1 節之要求。

5.5 已知漏洞安全

5.5.1 作業系統與網路服務

5.5.1.1 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.5.1 節之要求。

5.6 資源可用性

5.6.1 資源管理

5.6.1.1 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.6.1 節之要求。

5.6.2 警示與記錄

5.6.2.1 產品須依循 IoT-100x-1 感測裝置資安標準-第一部：一般要求第 5.6.1 節之要求。

5.6.2.2 產品發生安全事件時應有警示功能。(2 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]
5.1.1.2	D7P1(O)* - 強制使用強密碼	CR1.10 - Authenticator feedback	-
5.1.1.3	D2P1 - 使用相互認證	CR1.2 - Software process and device identification and authentication CR1.2RE(1) - Unique identification and authentication	-
5.1.3.1	D7P1(O)* - 強制使用強密碼	-	-
5.2.2.2	-	-	-
5.2.2.3	-	-	-
5.3.1.2	-	CR2.11RE(1) - Time synchronization	-
5.6.2.2	D5P2* - 異常通報機制	-	-

(*部分對應)

參考資料

(1) Sensing Taiwan 行不行，智動化 Smart Auto，https://smartauto.ctimes.com.tw/DispArt-tw.asp?O=HK63Q0ZVXPGARASTDT&U=OFTV

(2) 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

(3) NIST 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

(4) 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

(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