TAICS

TAICS TS-0036 v1.0 : 2020

空氣品質微型感測裝置資安標準

Cybersecurity standard 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標準

Cybersecurity standard for air quality micro sensing devices

出版日期: 2020/11/26

終審日期: 2020/11/09

誌謝

本標準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

此標準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

本標準由經濟部工業局支持研究制定。

目錄

前言

本標準係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業標準。

本標準並未建議所有安全事項，使用本標準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。

本標準之部分內容，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

隨著全球環保意識提升，對於空氣品質的關注程度跟著增加，國民對於居住環境的品質重視程度也跟過往大相逕庭，其中又以空氣污染的環保議題最為受到廣泛重視與討論。行政院環保署故而針對空氣品質，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，更提供各主管基於污染熱區的觀察與監測。有鑑於此，環保署自 2017 年起在相關場域，布建空氣品質微型感測裝置進行監測，至 2020 年預計布建達 10,200 個空氣品質微型感測裝置。

從 Markets & Markets 市場研究指出，氣體感測器市場預計將從 2019 年的 10 億美元，到 2024 年擴大到 14 億美元。市場在 2019 年至 2024 年間，預測將以年複合成長率 (CAGR) 6.4%的年複合成長率快速成長。但由於我國空氣感測組件仍以仰賴國外進口為主，在感測裝置研發上亦大多由國外廠商領導市場；因此，行政院前瞻基礎建設-數位建設-建構民生公共物聯網計畫大力扶植國內空氣品質物聯網產業，同時帶動空氣品質感測裝置產業發展，藉以將我國產業自主研發產品開拓國際市場。

然而，近幾年層出不窮的資安事件說明物聯網產品儼然已成為駭客攻擊重點目標，在物聯網攻擊案例中，針對感測裝置的攻擊時有所聞，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，竊取豪客的名單，個資遭洩漏事件；攻擊者利用聲波、電磁波、電信訊號等外部信號欺騙感測裝置讀取不準確的數據等報導，未來勢必會出現類似或更嚴重的攻擊。

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，由於感測裝置具備網路連接功能，相關的安全性問題也隨之而來，此外， 空氣品質微型感測裝置透過行動網路或NB-IoT 等無線通訊技術與其他智慧家電串聯，若缺乏足夠的網路安全機制，一旦遭入侵將嚴重影響用戶隱私安全與服務使用安全；空氣品質微型感測裝置應用上可能面臨產品供應商利用感測裝置暗藏後門，竊取或洩漏機敏資料回傳至非法伺服器等。空氣品質微型感測裝置為智慧城市治理中發揮環境監控的重要端點設備，當遭受駭客利用進行 DoS 攻擊，恐釀成癱瘓城市治理運作。

本標準制定之目的為協助環保署與各地方政府相關單位，增進其所布建之空氣品質物聯網感測裝置之資安防護能力，並藉此引領空氣品質微型感測裝置與其相關物聯網應用廠商導入資安防護設計概念與技術。

1. 適用範圍

本標準規定空氣品質微型感測裝置之資訊安全要求。空氣品質微型感測裝置由微控制器(MCU)、感測組件、網路傳輸模組/裝置所組成，目的為即時監測空氣品質，由空氣品質微型感測裝置將偵測之感測資料透過網路回傳至空氣品質物聯網運算營運平台，提供環保監管單位與民眾查詢各地空氣品質狀態，如下圖 1 所示。至於電信網路與空氣品質物聯網運算營運平台間之網路傳輸安全、空氣品質物聯網運算營運平台則不在本標準規範之範圍。

本標準適用對象為氣體感測裝置模組開發商、設備商及服務整合商，使其於開發階段及產品上線前，落實網路安全功能之要求基準，進而在產品中達到安全風險控制。

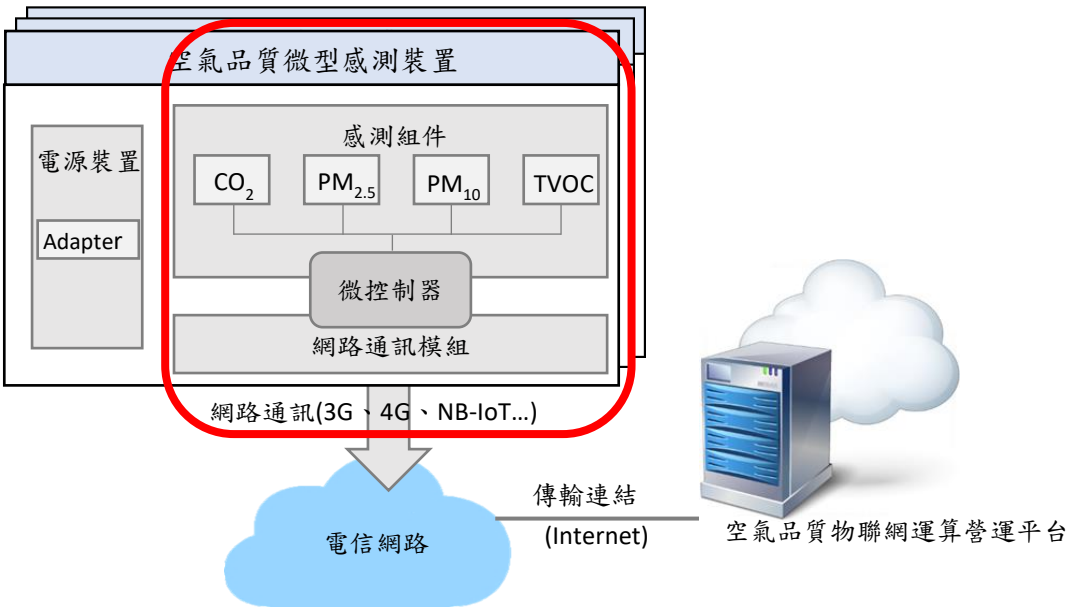

圖 1 適用範圍示意圖

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 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components

[2] NIST SP 800-140C, CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759

3. 用語及定義

下列用語與定義適用於本標準。

3.1 空氣品質微型感測裝置(Air quality micro sensing devices)

指符合低成本、重量輕且體積小、操作不需訓練、提供連續或接近連續的數據採集、數據可直接由設備或網頁方式呈現之特性(參見附錄 B 所述)，產品設置之區域與方式為可輕易卸除、移動之簡易型空氣感測裝置。

3.2 空氣品質物聯網運算營運平台(Air quality IoT computing and operating platform)

指建置於雲端之空氣品質感測裝置數據收集中心，內含有數據資料儲存、裝置管理、介面管理、通訊管理、裝置偵測等功能，提供 API 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、民生公共物聯網資料服務平台、LASS 環境感測器網路系統等。

3.3 感測組件(Sensing unit)

泛指空氣品質微型感測裝置中，用以偵測周圍環境的空氣品質數據之元件。例如，CO_2 模組、PM2.5 模組、VOCs 模組等。

3.4 不可否認性(Non-repudiation)

確保網路交易的雙方無法否認曾進行過的交易、或通訊參與的雙方皆無法否認曾進行資料傳輸或接收訊息。

3.5 國家弱點資料庫(National Vulnerabilities Database, NVD)

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[5]，負責常見弱點與漏洞(如 3.7 所述)之資料的發布及更新。

3.6 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。

3.7 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[7]。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。

3.8 異常狀況(Abnormal conditions)

指產品運作情形出現超出系統合理運行機制範圍之行為或狀況。例如，空氣品質微型感測裝置回傳感測資料之頻率，超出空氣品質物聯網運算營運平台之限制(例：每3分鐘須回傳一次) 已持續一段時間等異常事件。

3.9 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。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。

3.10 安全敏感功能(Secure sensitivity functions)

泛指對於空氣品質微型感測裝置須經授權方能操作產品之功能。例如，關閉感測裝置。

3.11 管理者(Administrator)

具更改作業系統、控制介面、功能應用程式之權限人員，如維修人員、平台專案管理者。

3.12 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。

3.13 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，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)。

4. 安全等級

安全等級係為降低或消弭裝置之資訊安全威脅，透過最適之安全組合，確保裝置達到安全之要求。

4.1 安全等級概述

本標準為空氣品質微型感測裝置之共通安全要求，安全要求總表如表 1 所示，第一欄為安全構面，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；第二欄為安全要求分項，依各安全構面設計之對應安全要求項目；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，本安全要求總表各欄位的關聯性，須依循章節 5 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，分為 1 級、2 級二個等級。裝置須應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 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	-

安全構面	安全要求分項	安全等級	
		1 級	2 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 5.5.1.2	-
5.6 資源可用性	5.6.1 資源管理	-	5.6.1.1

4.1.1 安全構面：

(a) 身分識別、鑑別、權限控管：溝通介面須確保鑑別、授權及權限控管相關機制，包括遠端指令管理介面、通訊協定等，應具備一定防護能力，避免遭受蓄意人士入侵。

(b) 資料機密性與完整性：裝置傳輸與儲存之資料應具有足夠安全之防護，避免遭受蓄意人士入侵。

(c) 系統完整性：裝置是否輕易地被拆解、裝置資料儲存與測試用連接埠的處置，或執行開機時，對於韌體、驅動程式及作業系統是否經過授權使用，應具備一定防護能力，視為實體安全要求的標的。

(d) 韌體更新：裝置之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：裝置之系統、網路服務應防止漏洞及具備即時檢視漏洞之安全機制。

(f) 資源可用性：裝置之資源管理應預防造成服務中斷。

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)資料保護程度之綜合考量，分為安全等級 1 級、安全等級 2 級二個等級，其中第 2 級包含對第 1 級之所有資安要求。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，欲符合較高等級之安全要求必須先滿足較低安全等級要求。

4.1.3.1 安全 1 級，適用裝置傳輸之資料為開放性資料，需要防護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，適用裝置具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，並維持裝置可用性。

5. 標準規範

本節詳盡載明空氣品質微型感測裝置為滿足安全功能應採取的方法，空氣品質微型感測裝置應符合本節中所有安全基本要求。

5.1 身分識別、鑑別、權限控管要求

5.1.1 鑑別機制

5.1.1.1 每個裝置應有一組唯一的識別碼。

5.1.1.2 裝置之所有介面應具備身分鑑別機制，包括實體、通訊 API，且該身分鑑別機制應能防止重送攻擊。

5.1.1.3 裝置應確保每一台金鑰之唯一性。

5.1.2 權限管控

5.1.2.1 裝置之所有介面應具備權限控管，包括管理介面、通訊 API 等，應切割成數個使用者角色，必須遵守最小權限原則(Least Privilege)，例如：一般使用者與系統管理者等，確保裝置之角色權限與裝置文件所宣告的相符。

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 裝置所儲存之安全敏感性資料應加密儲存，而保護資料的加密方式須採用 NIST SP 800-140C[6]所核可之同等或以上強度的加密演算法。

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，且須採用 NIST SP 800-140C 所核可之同等或以上強度的加密演算法；晶片中的韌體不

得存在於未宣告之相連伺服器 IP 和 URL，且不得存在明文或可被解密回復之安全敏感性資料。

5.2.1.3 安全敏感性資料應存放於裝置的安全區域，與正常作業環境隔離。

5.2.2 傳輸資料保護

5.2.2.1 裝置應驗證由空氣品質物聯網運算營運平台所傳送指令之完整性，而驗證資料完整性的方式須採用 NIST SP 800-140C 所核可之同等或以上強度的雜湊演算法。

5.2.2.2 裝置與空氣品質物聯網運算營運平台間安全敏感性資料的傳輸應走安全通道，且安全通道版本應符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密(Forward Secrecy)，此外裝置必須驗證空氣品質物聯網運算營運平台所發送之憑證是否為受信任根憑證機構(Root Certification Authority; Root CA)所發行。

5.2.2.3 裝置與空氣品質物聯網運算營運平台間之感測裝置資料傳輸應走安全通道，且安全通道版本應符合「TLS v1.2 同等或以上版本」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)，此外裝置必須驗證空氣品質物聯網運算營運平台所發送之憑證是否為受信任根憑證機構所發行；或裝置應支援空氣品質物聯網運算營運平台驗證資料來源鑑別性(Authenticity)之功能，而數位簽章的演算法須採用 NIST SP 800-140C 所核可之同等或以上強度的數位簽章演算法。

5.2.2.4 裝置與空氣品質物聯網運算營運平台間之控制指令傳輸應走安全通道，且安全通道版本應符合「TLS v1.2 同等或以上版本」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)，此外裝置必須驗證空氣品質物聯網運算營運平台所發送之憑證是否為受信任根憑證機構所發行；或裝置應驗證由空氣品質物聯網運算營運平台所傳送之控制指令鑑別性，而數位簽章的演算法須採用 NIST SP 800-140C 所核可之同等或以上強度的數位簽章演算法。

5.3 系統完整性

5.3.1 安全啟動

5.3.1.1 裝置應具備安全啟動(secure boot)功能。

5.4 軟韌體更新

5.4.1 更新安全

5.4.1.1 裝置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。

5.4.1.2 裝置之更新路徑須通過安全通道，以確保韌體之機密性、正確性及完整性，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密(Forward Secrecy)。

5.5 已知漏洞安全

5.5.1 作業系統與網路服務

5.5.1.1 裝置啟用之功能與網路服務須為廠商提供必要服務之所需。

5.5.1.2 裝置之作業系統與網路服務，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。

5.6 資源可用性

5.6.1 資源管理

5.6.1.1 裝置之儲存空間(包括安全事件紀錄及感測裝置數據)應具備滾動(Log Rotation)機制。

附錄 A
(規定)
安全通道版本使用要求

係指超文本傳輸協定結合安全套接層協定(SSL)或傳輸層安全性協定(TLS)，建立安全通道以保護傳輸中資料不被竊取之技術，然而安全套接層協定在 2014 年 10 月由 Google 指出其資訊安全漏洞，宣布將全面禁用，所以已經完全由傳輸層安全性協定取代安全套接層協定，但傳輸層安全性協定 1.0 存在可以降級到安全套接層協定 3.0 的功能，使得傳輸層安全性協定 1.0 同樣不被信任，因此目前本標準應使用的版本為：

傳輸層安全性協定 v1.2 同等或以上之版本。

附錄 B
(參考)
空氣品質微型感測裝置定義

空氣品質微型感測裝置之定義，係依據我國行政院環保署之空氣品質監測設備分類，與美國國家環境保護局之低成本感測裝置屬性，參考來源如下：

(a) 行政院環境保護署空氣品質監測網：

(1) 國家監測站、智慧城鄉感測點及學校民間感測裝置的差異
(https://airtw.epa.gov.tw/CHT/Encyclopedia/AirSensor/AirSensor_2.aspx)

(b) 美國國家環境保護局(EPA)：

(1) How to Evaluate Low-Cost Sensors by Collocation with Federal Reference Method Monitors
(https://www.epa.gov/air-research/instruction-guide-and-macro-analysis-tool-evaluating-low-cost-air-sensors-collocation)

(2) Sensor Evaluation Report
(https://cfpub.epa.gov/si/si_public_record_report.cfm?Lab=NERL&TIMSType=&count=10000&dirEntryId=277270&searchAll=&showCriteria=2&simpleSearch=0&startIndex=10001)

附錄 C
(參考)
空氣品質微型感測裝置安全需求之緩解對策

根據本標準之適用範圍定義空氣品質微型感測裝置資產列表，如下表 C. 1 所示。

表 C. 1 空氣品質微型感測裝置資產列表

資產名稱	敘述
實體	實體為組成裝置的各組件，包括控制機板、感測組件、除錯介面、儲存裝置、電源裝置。
韌體	燒錄在裝置或感測組件中的程式，為空氣品質微型感測裝置正常運作之必要軟體。
安全敏感性資料與功能	身分驗證、使用者帳號通行碼及控制指令。
通訊協定	有線網路或無線網路(WiFi、行動網路、藍牙或 NB-IoT)

根據上述步驟所識別之空氣品質微型感測裝置之資產項目，經分析定義出其衍生之常見資安威脅，透過下列說明各資產與其資安威脅之關聯。

(c) 實體

(1) 控制機板：控制機板被有心人士加入惡意晶片，透過惡意晶片發動攻擊，透過回傳感測資料功能傳送惡意程式至空氣品質物聯網運算營運平台，以取得平台控制權監控或竊取敏感資料。

(2) 感測組件：透過於布建地點利用電磁波、聲波等訊號、建置高溫、高腐蝕環境，欺騙空氣感測組件偵測數值，導致設備回報異常或提供民眾及執法單位錯誤的空氣品質資訊。

(3) 除錯介面：透過實體埠更新偽造韌體或竄改感測資料，導致偵測空氣品質資料錯誤，導致環保執法稽查不當。

(4) 儲存裝置：透過破壞空氣品質微型感測裝置外殼，竊取儲存裝置(例如，內建記憶體、記憶卡)資料造成暫存感測資料丟失，或設備功能異常。

(5) 電源裝置：破壞電源裝置(例如，與路燈共用電力)造成空氣品質微型感測裝置關機無法運作。

(d) 韌體

韌體本身可能存在未經修補之已知資安漏洞；韌體遭竄改植入惡意程式，安裝至各空氣品質微型感測裝置後，可能導致所有空氣品質微型感測裝置遭駭客控制與監聽，回傳已被惡意變造的感測資料，造成空氣品質資料展示平台顯示的資訊錯誤。

(e) 安全敏感性資料與功能

空氣品質微型感測與空氣品質物聯網運算營運平台進行身分驗證時，恐遭攔截竄改，或竄改空氣品質物聯網運算營運平台發送之控制指令等，發動 DoS 攻擊，癱瘓系統運作。

(f) 通訊協定

駭客利用已知通訊協定漏洞，潛入傳送通道監聽身分認證和回傳的資料，利用假冒空氣品質微型感測裝置，回傳偽造的感測資料，導致某地區的空氣品質呈現錯誤資訊，影響民眾出門判斷或環保稽查單位獲取假資訊造成執法失當。

根據識別之資產可能遭遇的威脅建立威脅模型，以 ETSI TVRA v5.2.3[(1)]所定義的風險評估方法進行評量。首先，將威脅對於資產的影響嚴重程度，程度分為 Low、Medium 和 High 三級；接著以發動一次攻擊所需的時間(Time)、攻擊者的專業度(Expertise)、對資產熟悉程度(Knowledge)、發動攻擊的機會(Opportunity)、與攻擊所使用的工具專業度(Equipment)進行潛在攻擊的可能性(likelihood of attack)的識別；最後，資產影響程度(Asset Impact)與發動攻擊的強度(Intensity)進行風險等級劃分。完成的威脅分析結果，如下表 C. 2 所示，其中風險等級定義如下：

(a) Critical: 供應商和用戶的主要利益受到威脅，應最大程度的降低風險。

(b) Major: 對相關資產的威脅可能會發生，儘管其影響不太可能是致命的，但應該確實處理風險，並通過適當緩解對策來將風險最小化。

(c) Minor: 造成較小風險的資安威脅，根本不需要採取緩解對策。

表 C. 2 威脅分析表

ID	威脅	弱點	不良的後果	風險等級
T-I-01	Stored data analysis	1. 儲存中安全敏感資料未加密 2. 日誌存有安全敏感資料	1.儲存中的密碼未經過 hash 處理，且/或金鑰未經過加密，權限控管不當，一旦作業系統層被入侵，敏感資料外洩，將遭受更嚴重的攻擊 2.日誌資料中有安全敏感資料被顯示出來	Critical
		韌體 hardcode 敏感資料	韌體放在公眾可取得，或者是可以從 flash 中萃取出來，該韌體又 hardcode 敏感資料造成敏感資料外洩，將遭受更進一步的駭客攻擊	Critical
T-I-02	Authentication factor leakage	認證因子明文傳輸	認證時，相關身分認證因子，例如: 密碼、憑證，會因為傳輸通道沒有加密而導致敏感資料可被有心人士擷取	Critical
T-I-03	Traffic analysis	傳輸中的敏感資料未加密	裝置傳送出的空品資料被監聽，進一步分析，未來可能遭受駭客進一步攻擊	Major
T-I-04	Secret stolen	不必要的功能/服務沒有關掉	裝置存在不必要功能/服務，導致機密資料外洩，例如，偷傳資料回惡意伺服器、偷裝監視器，回傳敏感區域之監控影像	Critical
T-M-01	1. fabrication of data	接收端或通訊 API 沒有驗證資料的完整性及鑑別性	裝置送往資料中心的資料被竄改，廠商可藉此避開法律責任，例如: 將 PM 2.5 濃度調降	Critical
	2. Replay/MITM control message	接收端或通訊 API 沒有驗證控制訊息來源的鑑別性、或未鑑別傳送控制訊息者身分	將先前側錄的控制訊息重送至裝置，或中途攔截訊息加以竄改、或植入預期外的值，再送至裝置，使裝置執行預料外之動作，例如:關機、重開機	Critical

ID	威脅	弱點	不良的後果	風險等級
T-M-02	Masquerade as IoT device	裝置本身未驗裝載韌體的完整性及鑑別性，裝置的實體和遠端通訊介面也沒有身分認證機制	1. 重新燒錄帶有 malware 的韌體，或從實體/遠端通訊介面入侵，取得管理者權限，可以控制該合法機器，執行任意動作 2. 在另一台 IoT 裝置載入合法韌體，複製認證因子，偽造另一台同型機種	Critical
T-M-03	Storage tampering	儲存中之敏感資料未驗證完整性、未有權限控管	儲存中之 sensor 資料被竄改，廠商可藉此避開法律責任，例如: 將 PM 2.5 濃度調降	Critical
T-M-04	Transduction attacks	無辨識感測數據異常，無異常事件處理措施，例: 失效控制、異常處理	感測組件偵測到的空氣品質數值超出範圍或感測數據差異太大，誤導民眾與環保稽查	Minor
T-R-01	Denial of transmission	無資安事件日誌、無資安事件警示功能	合法的 sensor 發送惡意和惡作劇的資料，或者被植入 malware，事後無數位證據證實是由該 sensor 發送	Major
T-D-01	Power outage	欠缺備援電源	惡意斷電或停電導致感測裝置關機	Critical
T-D-02	1. Injection of false messages 2. Message saturation	1. 無封包過濾功能 2. sensor 可用資源不足	大量的非法訊息被送入，導致正確的接收訊息被碰撞掉，或者系統忙著處理那些垃圾訊息，導致系統資源被耗盡，因此存取接收訊息、IoT 裝置內部資源不能	Critical
T-D-03	Radio Jamming	無線傳輸容易被干擾	射頻干擾，導致訊息無法收送	Critical
T-D-04	Overflow the record store	無限制儲存空間、或循環再利用	日誌儲存空間不足，可能導致功能喪失或資料異常，甚至機器 crash	Major

根據上述步驟，識別空氣品質微型感測裝置的資產與資安威脅，排除非適用範圍所定義之資產衍生的威脅，透過威脅分析衍生出空氣品質微型感測裝置之緩解對策(即資安需求)，詳見表 C. 3。

表 C. 3 安全需求緩解對策表

ID	威脅	緩解對策	風險等級(原)	風險等級(緩解後)
T-I-01	Stored data analysis	5.2.1.1 裝置所儲存之安全敏感性資料應加密儲存，而保護資料的加密方式須採用 NIST SP 800-140C[6]所核可之同等或以上強度的加密演算法。 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，且須採用 NIST SP 800-140C 所核可之同等或以上強度的加密演算法；亦或是晶片中的韌體，不應存在未宣告之相連伺服器 IP 和 URL，與明文或可被解密回復之安全敏感性資料。	Critical	Minor
		5.2.1.3 安全敏感性資料應存放於裝置的安全區域，與正常作業環境隔離。	Critical	Minor
T-I-02	Authentication factor leakage	5.2.2.3 裝置與空氣品質物聯網運算營運平台間安全敏感性資料的傳輸應走安全通道，且安全通道版本應符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)，此外裝置必須驗證空氣品質物聯網運算營運平台所發送之憑證是否為受信任根憑證機構所發行。	Critical	Minor
T-I-04	Secret stolen	5.6.1.1 裝置啟用之功能與網路服務須為廠商提供必要服務之所需。	Critical	Minor
T-M-01	1. fabrication of data 2. Injection of false messages	5.2.2.1 裝置應支援空氣品質物聯網運算營運平台驗證資料完整性之功能，而驗證資料完整性的方式須採用 NIST SP 800-140C 所核可之同等或以上強度的雜湊演算法。	Critical	Minor

ID	威脅	緩解對策	風險等級(原)	風險等級(緩解後)
		5.2.2.4 裝置與空氣品質物聯網運算營運平台間之感測裝置資料傳輸應走安全通道，且安全通道版本應符合「TLS v1.2 同等或以上版本」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)，此外裝置必須驗證空氣品質物聯網運算營運平台所發送之憑證是否為受信任根憑證機構所發行；或裝置應支援空氣品質物聯網運算營運平台驗證資料來源鑑別性(Authenticity)之功能，而數位簽章的演算法須採用 NIST SP 800-140C 所核可之同等或以上強度的數位簽章演算法。	Critical	Minor
T-M-01	MITM control message	5.2.2.2 裝置應驗證由空氣品質物聯網運算營運平台所傳送指令之完整性，而驗證資料完整性的方式須採用 NIST SP 800-140C 所核可之同等或以上強度的雜湊演算法。 5.2.2.5 裝置與空氣品質物聯網運算營運平台間之控制指令傳輸應走安全通道，且安全通道版本應符合「TLS v1.2 同等或以上版本」的要求，同時金鑰交換協議應支援前向保密(Forward Secrecy)，此外裝置必須驗證空氣品質物聯網運算營運平台所發送之憑證是否為受信任根憑證機構所發行；或裝置應驗證由空氣品質物聯網運算營運平台所傳送之控制指令鑑別性，而數位簽章的演算法須採用 NIST SP 800-140C 所核可之同等或以上強度的數位簽章演算法。	Critical	Minor

ID	威脅	緩解對策	風險等級(原)	風險等級(緩解後)
T-M-02	Masquerade as IoT device	5.1.2.1 裝置之所有介面應具備權限控管，包括管理介面、通訊協定、API，應切割成數個使用者角色，必須遵守最小權限原則(Least Privilege)，例如：一般使用者與系統管理者等，確保裝置之角色權限與裝置文件所宣告的相符。 5.1.1.2 裝置之所有介面應具備身分鑑別機制，包括實體、通訊 API，且該身分鑑別機制應能防止重送攻擊。 5.6.1.2 裝置之作業系統與網路服務，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。	Critical	Minor
		5.1.1.3 裝置應確保每一台金鑰之唯一性，以降低金鑰外洩可能引發之資安風險。 5.1.1.1 每個裝置應有一組唯一的識別碼。 5.2.2.4 裝置與空氣品質物聯網運算營運平台間之感測裝置資料傳輸應走安全通道，且安全通道版本應符合「TLS v1.2 同等或以上版本」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)，此外裝置必須驗證空氣品質物聯網運算營運平台所發送之憑證是否為受信任根憑證機構所發行；或裝置應支援空氣品質物聯網運算營運平台驗證資料來源鑑別性(Authenticity)之功能，而數位簽章的演算法須採用 NIST SP 800-140C 所核可之數位簽章演算法。	Critical	Minor
		5.2.1.3 安全敏感性資料應存放於裝置的安全區域，與正常作業環境隔離。 5.3.1.1 裝置應具備安全啟動(secure boot)功能。	Major	Minor

ID	威脅	緩解對策	風險等級(原)	風險等級(緩解後)
T-M-03	Storage tampering	5.1.1.2 裝置之所有介面應具備身分鑑別機制，包括實體、通訊 API，且該身分鑑別機制應能防止重送攻擊。 5.1.2.1 裝置之所有介面應具備權限控管，包括管理介面、通訊協定、API，應切割成數個使用者角色，必須遵守最小權限原則 (Least Privilege)，例如：一般使用者與系統管理者等，確保裝置之角色權限與裝置文件所宣告的相符。	Critical	Major
		5.2.1.3 安全敏感性資料應存放於裝置的安全區域，與正常作業環境隔離。	Critical	Minor
T-R-01	Denial of transmission	5.5.1.1 裝置須具備安全事件紀錄，得以查核未授權或異常行為，供後續查閱之用，且須具時間戳記與事件內容。 5.5.1.2 裝置之安全事件紀錄須具備權限控管機制，該安全事件紀錄檔不應允許未經授權的存取。 5.5.1.3 裝置發生安全事件時，須具備主動告警機制，包括回報管理者或推播警示、告警及設備識別碼編號等訊息。	Major	Minor
T-D-04	Overflow the record store	5.7.1.1 裝置之儲存空間(包括安全事件紀錄及感測裝置資料)應具備滾動(log rotate)機制。	Major	Minor

安全等級依據 ETSI TVRA 之風險分析結果，以(1)相關資安風險高低(Risk)、(2)安全技術實現複雜度(Cost benefit)作為安全等級的判斷因子，共分為 1 級、2 級、3 級三個等級，安全等級級數的大小代表安全等級的高低，等級越高則安全要求越嚴格。(本標準可接受的最低風險等級訂為 Minor)

安全等級越低可承受的資安風險越高，安全等級越高可承受的資安風險越低，因此緩解能力較差的安全要求可以擺放在較低的安全等級。若存在 2 個以上的資安需求可緩解同一資安風險，且安全技術實現複雜度相似，則應優先採用緩解能力較佳的安全要求。若存在 2 個以上的資安需求可緩解同一資安風險，且緩解能力相同，則採用安全

技術實現複雜度較低的安全需求會擺放在較低之安全等級；相反地，較高之安全技術實現複雜度的安全需求，應屬於較高之安全等級

附錄 D
(參考)
技術要求事項與各標準規範對照表

本標準與 IEC 62443-4-2、NISTIR 8259 之比對結果，如下表所示：

本標準要求	對應標準規範	
	IEC 62443-4-2[1]	NISTIR 8259(4)
5.1.1.1	CR 1.2–軟體進程及設備的識別及認證 Software process and device identification and authentication	Device Identification: The IoT device can be uniquely identified logically and physically.
5.1.1.2	CR 1.2–軟體進程及設備的識別及認證 Software process and device identification and authentication CR 3.8- Session 完整性 Session integrity	Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
5.1.1.3	CR 1.8–公鑰基礎結構憑證 Public key infrastructure certificates	-
5.1.2.1	CR 2.1–授權執行 Authorization enforcement CR 2.2-無線使用控制 Wireless use control	Device Configuration: The configuration of the IoT device’s software and firmware can be changed, and such changes can be performed by authorized entities only.
5.2.1.1	CR 1.5–身份認證碼管理 Authenticator management CR 1.9–公鑰認證的強度 Strength of public key authentication	Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
5.2.1.2	CR 4.3–密碼學的使用 Use of cryptography	-
5.2.1.3	-	-
5.2.2.1	CR 4.3–密碼學的使用 Use of cryptography	-
5.2.2.2	CR 4.3–密碼學的使用 Use of cryptography	-
5.2.2.3	CR 3.1–通訊完整性 Communication integrity CR 1.9–公鑰認證的強度 Strength of public key authentication	-

本標準要求	對應標準規範	
	IEC 62443-4-2[1]	NISTIR 8259(4)
5.2.2.4	CR 3.1–通訊完整性 Communication integrity CR 1.9–公鑰認證的強度 Strength of public key authentication	-
5.2.2.5	CR 3.1–通訊完整性 Communication integrity CR 1.9–公鑰認證的強度 Strength of public key authentication	-
5.3.1.1	CR 3.14 - 開機程序的完整性 Integrity of boot process	Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
5.4.1.1	CR 3.10–更新 Support for updates	-
5.4.1.2	CR 3.1–通訊完整性 Communication integrity	-
5.5.1.1	CR 7.6–網路及安全設定 Network and security configuration settings CR 7.7–最小功能性 Least functionality	-
5.5.1.2	-	-
5.6.1.1	CR 2.9–審計儲存容量 Audit storage capacity	-

參考資料

(1) ETSI TS 102 165-1 V5.2.3 (2017-10), CYBER; Methods and protocols;Part 1: Method and pro forma for Threat,Vulnerability, Risk Analysis(TVRA)

(2) ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things.

(3) IEC 62443-4-2-2018 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components.

(4) NISTIR 8259 Draft (2nd) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline.

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

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

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

(8) 空氣品質國家監測站、智慧城鄉感測點及學校民間感測器的差異表, https://airtw.epa.gov.tw/CHT/Encyclopedia/AirSensor/AirSensor_2.aspx

(9) EPA, Sensor Evaluation Report, https://cfpub.epa.gov/si/si_public_record_report.cfm?Lab=NERL&dirEntryId=277270

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