IoT-1003-1

智慧路燈系統資安標準-

第一部：一般要求

V1.0

行動應用資安聯盟

中華民國 110 年 6 月

目錄

引言

物聯網應用興起帶動科技產業轉型，物聯網產品如雨後春筍般湧現，而近年來國際上透過物聯網產品進行網路攻擊的事件屢見不鮮，國內數家網通設備大廠的產品也深受其害。經濟部工業局體認物聯網產業之資訊與網路安全的防護已刻不容緩，因此，自 2017 年起，率先鳴起制定物聯網產業資安標準的第一槍，開始推動我國物聯網產業資安規範與制定標準，打造我國安全的聯網產業生態系統。

隨著物聯網與雲端運算技術的廣泛應用，在經濟部工業局發展智慧城市計畫與能源局擴大補助 LED 路燈計畫的帶動下，路燈燈桿上開始附加各種感測器，透過其連網功能將收集到的環境資料及照明狀態回傳雲端分析，進而衍生出智慧路燈系統。而智慧路燈為奠定智慧城市的基石，美國、阿根廷、新加坡、荷蘭、英國、丹麥與台灣等國家已布建許多具規模的城市場域。根據 2016 年 Philip 市場調查報告指出，全球路燈市場規模約 3 億盞，目前全球具備聯網功能的路燈平均每年複合成長率達 16%；IEK 預估 2020 年全球智慧路燈市場規模達 34.3 億美元。台灣在各地方政府投入的智慧路燈公共工程的帶領下，單以桃園為例，於 2019 年起將再投入 56 億台幣建置智慧路燈基礎建設。在帶來節能與生活便利的同時，伴隨而來的網路攻擊對資訊安全與隱私造成極大的威脅，如 2017 年美國駭客透過網路控制感測器與控制器，發動攻擊控制德州達拉斯 156 座警報器大作等公共安全隱憂。

有鑑於此，數位發展部數位產業署致力推動更藉由參照國際物聯網相關資安標準/規範，如 Open Web Application Security Project (OWASP) Top IoT Vulnerabilities[1]及 CNS 15652 智慧照明系統標準[2]等，制定了 IoT-1003-1 智慧路燈系統資安標準-第一部：一般要求(以下簡稱本標準)，與 IoT-1003-2 智慧路燈系統資安標準-第二部：智慧照明，為智慧路燈相關產業建立資訊安全指引。透過資安標準提升產品與公共服務的資訊安全，使我國智慧路燈輸出於國際市場上站穩出口大國地位。

本標準針對智慧路燈系統上相關應用的裝置制定資安標準，包括智慧路燈系統中的監控閘道器、附掛設備與監控伺服器，制定 IoT-2003 測試規範作為 IoT-1003 標準提供驗證之基準與測試方法。

本標準引用 CNS 15652-1「智慧照明系統－第 1 部：系統功能」之智慧照明系統組成元件，與智慧照明系統架構。

智慧路燈系統由後台監控伺服器、燈桿閘道器及燈桿附掛設備組成，後台監控伺服器負責蒐集、監控及操作燈桿附掛設備，燈桿閘道器作為燈桿附掛設備與後台資料傳輸之出入口，燈桿附掛設備即透過燈桿上預留之標準化接口，附掛在燈桿上提供智慧城市相關應用之物聯網設備。

智慧路燈系統包含智慧照明、氣象站與影像監控等子系統，可用來蒐集如日照、空氣品質、溫溼度及路況等資訊，各子系統將蒐集之照明與環境資料，傳送至支援 Wi-Fi、ZigBee 或 Wi-SUN 等聯網傳輸技術的燈桿閘道器，可藉由如網狀骨幹網路(Mesh)等的網路技術連接，再透過燈桿閘道器經由光纖、NB-IoT 或 3G/4G 與後台監控伺服器連接，提供相關單位即時監控與管理；而智慧路燈子系統之燈桿附掛設備，可能具備遠距無線傳輸網路功能，可直接與後端伺服器及場域內其他設備串聯成網路。如下圖 1 所示。

智慧路燈子系統中，可能採用具有邊緣運算功能之閘道器，可將感測器蒐集的資料分析處理後，再回傳至後端，以降低網路頻寬問題，亦能經由蒐集之資料，在本地端預先處理並即時預判，減少後端伺服器工作負擔。

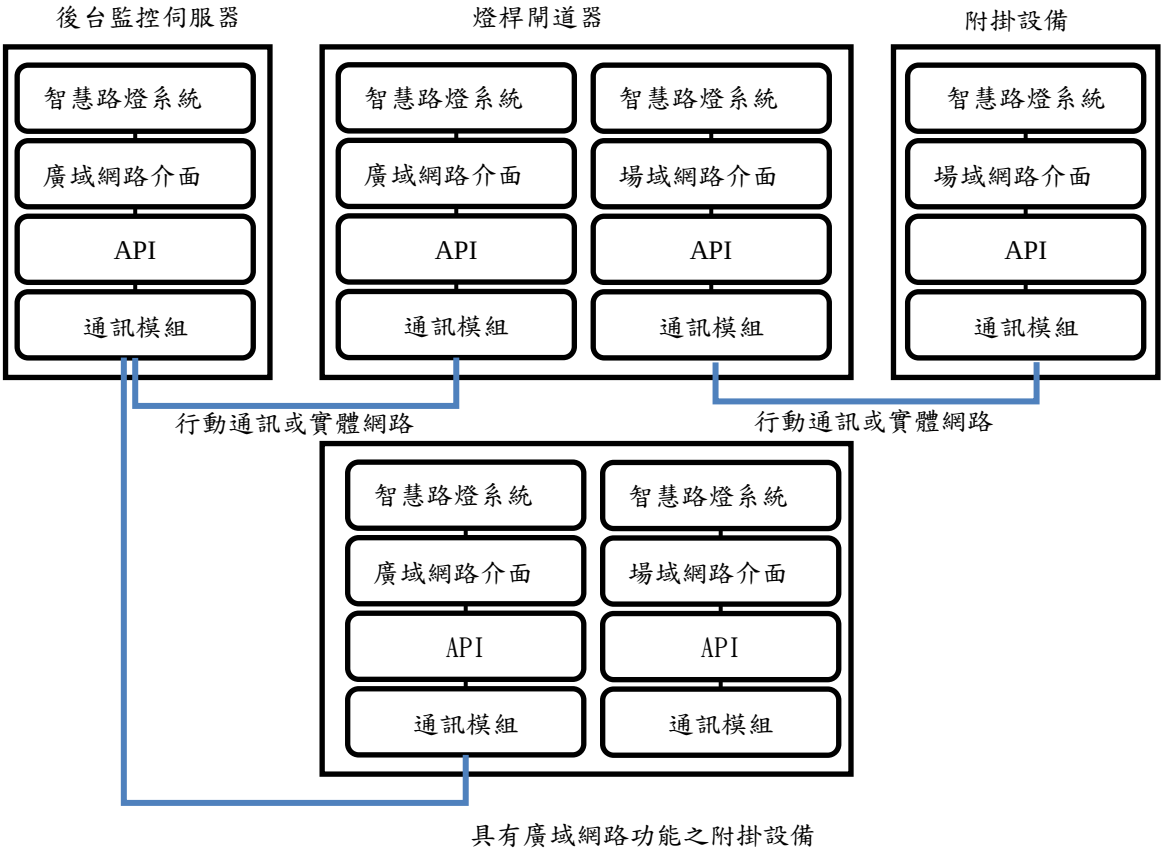
後台監控伺服器
智慧路燈系統
廣域網路介面
API
通訊模組
燈桿閘道器
智慧路燈系統
廣域網路介面
API
通訊模組
智慧路燈系統
場域網路介面
API
通訊模組
附掛設備
智慧路燈系統
場域網路介面
API
通訊模組
行動通訊或實體網路
行動通訊或實體網路
智慧路燈系統
廣域網路介面
API
通訊模組
智慧路燈系統
場域網路介面
API
通訊模組
具有廣域網路功能之附掛設備

圖 1 智慧路燈系統架構

1. 適用範圍

本系列標準適用於智慧路燈及其附掛具有聯網功能之智慧城市相關應用。智慧路燈是由後台監控伺服器、燈桿閘道器及燈桿附掛設備所組成，如下圖 2 所示。本標準定義了智慧路燈系統網路安全基本要求、後台監控伺服器安全要求及燈桿閘道器特定資安要求。其中網路安全基本要求共有七大構面：

- 身分識別、鑑別、權限控管
- 資料機密性與完整性
- 系統完整性
- 軟韌體更新
- 警示與紀錄
- 已知漏洞安全
- 軟體應用程式

本標準作為智慧路燈產業之系統整合商、設備商與軟體開發商於開發階段，落實網路安全功能之要求基準，進而在產品架構與產品設計中達到安全風險控制。

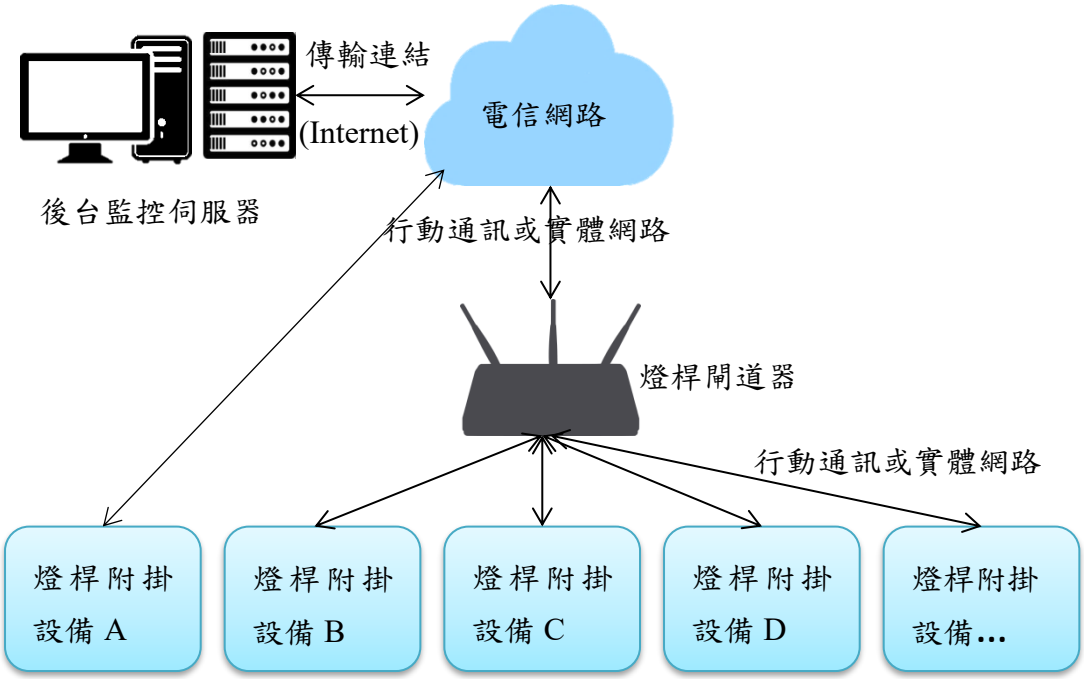

圖 2 適用範圍示意圖

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

[2] CNS 15652-1：2013 智慧照明系統– 第 1 部：系統功能

3. 用語及定義

「CNS 15652：2013 智慧照明系統-第 1 部：系統功能」之用語定義，及下列用語與定義適用於本標準。

3.1 智慧路燈系統(Intelligent Streetlight System)

立於公共街道、園區或公園內的智慧公共照明設施，於其燈桿附加感測器、攝影機等智慧城市相關物聯網應用設備，可視為智慧城市的基礎設施。能依據感測器收集當地的環境資訊供後端分析，提供政府機關可以遠端即時監控及管理。

3.2 後台監控伺服器(Monitoring and Control Server)

經由光纖、NB-IoT 或 3G/4G 等與燈桿閘道器連接，傳送控制指令至燈桿附掛設備或感測器，並蒐集各設備回傳之環境資料，提供相關單位即時監控與管理。

3.3 燈桿附掛設備(Streetlight Attached Equipment)

泛指獨立運作，具有實體之物件，透過燈桿預留之接口附掛於智慧路燈上，可接受指令以執行各種功能之物聯網設備。例如，智慧照明或影像監控裝置等。

3.4 燈桿閘道器(Streetlight Gateway)

安裝於智慧路燈上，作為燈桿附掛設備與後台監控伺服器資料傳輸之出入口，用於將燈桿附掛設備採集之日照、水位、路況等環境資訊，匯集傳送至後台監控伺服器，及負責將後台監控伺服器發送之控制或查詢指令派送至各燈桿附掛設備。亦有具邊緣運算功能之燈桿閘道器，可將燈桿附掛設備蒐集之資料，預先分析處理後，再回傳至後端的後台監控伺服器。

3.5 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。

3.6 國家弱點資料庫(National Vulnerabilities Database)

係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。

3.7 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。

3.8 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)發展至第三版。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[7]。

3.9 嚴重性等級(Severity Rating)

係指漏洞評分系統之評比分數，皆有其對應之嚴重性等級，分別是 0 分為無(None)嚴重性、0.1-3.9 分為低(Low)嚴重性、4.0-6.9 分為中(Medium)嚴重性、7.0-8.9 分高(High)嚴重性及 9.0-10.0 為重大(Critical)嚴重性。

3.10 異常狀況(Abnormal Conditions)

係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，當發生如夜晚時段的關燈請求、相同路段或區域中的感測器回報資料差異過大等異常事件。

3.11 安全敏感性資料(Secure Sensitive Data)

本標準之安全敏感性資料是指，在伺服器或產品應用程式運作時，於裝置及其附屬儲存媒介建立、儲存或傳輸之資訊，包括通行碼、金鑰等系統運行所需之機敏資料，而該資訊之洩漏有對系統或產品造成損害及攻擊之虞，例如，登入後台監控伺服器關閉照明等危及社會安全事件。

3.12 安全敏感功能(Secure Sensitivity Functions)

泛指智慧路燈系統中，須經授權方能操作產品或系統之功能。例如，開關燈桿附掛設備或更新韌體。

3.13 隱私(Privacy)

主要依「個人資料保護法」[4]上定義之所有得以直接或間接方式識別該個人之資料，包括但不限於智慧路燈系統之系統管理人員與協力廠商工班人員之個人資料：自然人之姓名、出生年月日、國民身分證統一編號、聯絡方式、國際行動產品識別碼(International Mobile Equipment Identity, IMEI)、國際行動用戶識別碼(International Mobile Subscriber Identity, IMSI)、人臉特徵點(Facial Landmark)及其他得以直接或間接方式識別該個人之資料。

3.14 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，如後台管理者、維修人員。

3.15 通行碼(Password)

係指一組能讓使用者使用系統或以識別使用者身分之字元串，包括本機儲存資料加密檔案密碼、自身帳號及密碼、遠端網路服務帳號及密碼。

3.16 預設通行碼(Default Password)

係指產品出廠預先設定好的通行碼，即在用戶初次將其連上網路，且在未更改任何設定的情況下，用以登入智慧路燈設備之通行碼。

3.17 加密(Encryption)

係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。

3.18 安全事件紀錄(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，本標準之安全事件即指使用者登入系統、使用者操作關燈等的行為。

3.19 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：目前常見之實作通訊協定為安全套接層(Secure Sockets Layer, SSL)和傳輸層安全性(Transport Layer Security, TLS)。

3.20 控制場域(Control Field)

受後台監控伺服器監控之場地，包含至少 1 個以上直接受燈桿閘道器控制之燈桿附掛設備。

3.21 廣域網路(Wide Area Network, WAN)

泛指可跨越廣大範圍進行通訊之網路連接方式，包含網際網路或私人架設專線所建構之網路。例如，行動網路(5G、LTE)、光纖網路、NB-IoT 等。

3.22 場域網路(Field Area Network, FAN)

泛指一特定區域內，連結燈桿閘道器與各種燈桿附掛設備之網路，燈桿附掛設備如照明單元、感測器及自動控制設備等。場域網路可使用各種通訊實體介質及協定進行實作，例如無線網路(Zigbee、Sub-G、WiFi)、同軸電纜或雙絞線。亦可混合使用不同種類之通訊實體介質及協定。本標準之場域網路不包含使用 PLC 電力線之環境。

3.23 前向安全(Forward Secrecy, FS)

係指萬一通行碼或金鑰在某個時間點不慎洩露，過往的通訊依然是安全，不會因此而洩露過去的通信數據。

3.24 遠端證明(Remote Attestation)

係指透過憑證機制，通常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。

3.25 日誌滾動(Log Rotate)

日誌滾動是指系統管理中一個自動化歸檔過期日誌文件的過程，每次增加新日誌文件時，舊日誌文件名後面的數字就會增加，當舊日誌文件後面的數字超過設定臨界值時，可以被刪除或者存到他處來釋放儲存空間。日誌滾動提供了一個有效的方法來限制日誌文件的大小，同時保留近期的日誌用於分析。

3.26 身分鑑別因子(Authentication Factor)

用於認證或驗證實體身分的一個資訊或過程，包括：金鑰、密碼等。

3.27 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。

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

本標準為智慧路燈系統之共通安全要求，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)警示與紀錄(6)已知漏洞安全、(7)軟體應用程式，及後台監控伺服器安全要求的安全構面(8)資源可用性、(9)隱私保護及(10)雲端平台安全；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相依性，須依循章節 5 至 7 節之技術規範內容。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，例如，安全要求項目所面臨資安風險低、安全技術實現複雜度高時，則安全等級較高；面臨資安風險高、安全技術實現複雜度低時，則安全等級較低。產品須應先通過較低安全等級之測試，始可進行進階等級之測試。

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	3 級
5.標準規範-物聯網設備安全基本要求				
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 5.1.1.4 5.1.1.5	-	5.1.1.6
	5.1.2 權限管控	5.1.2.1 5.1.2.2	-	-
	5.1.3 通行碼鑑別	5.1.3.1 5.1.3.2 5.1.3.3	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 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	5.2.1.2	-
	5.2.2 傳輸資料保護	5.2.2.1	5.2.2.2	-
5.3 系統完整性	5.3.1 實體入侵防護	-	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 5.4.1.4	5.4.1.3	-
5.5 警示與紀錄	5.5.1 日誌檔與警示	5.5.1.1 5.5.1.2 5.5.1.3 5.5.1.4 5.5.1.5	-	-
5.6 已知漏洞安全	5.6.1 作業系統與網路服務	5.6.1.1	5.6.1.2	-
	5.6.2 網路服務連接埠	5.6.2.1	-	-
5.7 軟體應用程式	5.7.1 應用程式安全	5.7.1.1 5.7.1.2	-	-
6. 標準規範-後台監控伺服器				
6.1 身分識別、鑑別、權限控管要求	6.1.1 鑑別機制	6.1.1.1 6.1.1.2 6.1.1.4	-	6.1.1.3 6.1.1.5
	6.1.2 權限控管	6.1.2.1 6.1.2.2	-	-
	6.1.3 通行碼鑑別	6.1.3.1 6.1.3.4 6.1.3.5 6.1.3.6	-	6.1.3.2 6.1.3.3
6.2 資料機密性與完整性	6.2.1 安全敏感性資料儲存	6.2.1.3	6.2.1.1 6.2.1.4	6.2.1.2
	6.2.2 傳輸資料保護	6.2.2.1 6.2.2.2	6.2.2.3	-
6.3 警示與紀錄	6.3.1 日誌檔與警示	6.3.1.1 6.3.1.2 6.3.1.3 6.3.1.4 6.3.1.5	-	-
6.4 已知漏洞安全	6.4.1 作業系統與網路服務	6.4.1.1	-	-
	6.4.2 網路服務連接埠	6.4.2.1	-	-
6.5 軟體應用程式	6.5.1 網頁管理介面安全	6.5.1.1 6.5.1.2	-	-
6.6 資源可用性	6.6.1 備份	6.6.1.1 6.6.1.2	-	-
6.7 隱私保護	6.7.1 隱私保護能力	6.7.1.2 6.7.1.3	6.7.1.1	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
6.8 雲端平台安全	6.8.1 雲端安全要求	-	-	6.8.1.1
7. 標準規範-燈桿閘道器安全特殊要求				
7.1 身分識別、鑑別、權限控管	7.1.1 鑑別機制	7.1.1.1	-	-
	7.1.2 權限管控	-	-	-
	7.1.3 通行碼鑑別	7.1.3.1	-	7.1.3.2 7.1.3.3
7.2 資料機密性與完整性	7.2.1 安全敏感性資料儲存	-	7.2.1.2	7.2.1.3
	7.2.2 傳輸資料保護	-	-	-
7.3 系統完整性	7.3.1 實體入侵防護	-	7.3.1.2	7.3.1.3
7.4 軟韌體更新	7.4.1 更新安全	-	-	-
7.5 警示與紀錄	7.5.1 日誌檔與警示	-	-	-
7.6 已知漏洞安全	7.6.1 作業系統與網路服務	-	-	-
	7.6.2 網路服務連接埠	-	-	-
7.7 軟體應用程式	7.7.1 應用程式安全	-	-	-

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與授權相關機制，包括遠端指令管理介面、網頁管理介面等。

(b) 資料機密性與完整性：產品傳輸與儲存之資料應具有足夠安全之防護。

(c) 系統完整性：產品輕易被拆解與否、產品資料存儲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，視為實體安全要求的標的。

(d) 軟韌體更新：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) 警示與紀錄：產品日誌紀錄須有管理機制，且於發生安全事件須具有警示能力。

(f) 已知漏洞安全：產品之作業系統、網路服務應防止漏洞及具備安全機制。

(g) 軟體應用程式：產品之網頁管理介面應防止漏洞及具備安全機制。

(h) 資源可用性：後台監控伺服器須具備援安全機制。

(i) 隱私保護：後台監控伺服器須具有個人隱私的保護機制。

(j) 雲端平台安全：後台監控伺服器之雲端平台須達到國際資安標準之水準。

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，且每一安全要求分項包含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)技術實現複雜度之綜合考量，分為 1 級、2 級、3 級三個等級。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，適用於產品傳輸之資料為開放性資料，需要基本防護來避免產品成為駭客攻擊之跳板，且須保持中度的可用性。建議一般開放之區域使用，如公園、街道。

4.1.3.2 安全 2 級，適用於產品傳輸之資料為安全敏感性資料，需要進階防護來避免產品成為駭客攻擊之跳板，且須保持高度的可用性。建議具有中度管制區域使用，如私人公司園區。

4.1.3.3 安全 3 級，適用於產品傳輸之資料為機密性資料，需要花費較大成本來嚴格防護產品成為駭客攻擊之跳板，且須持續維持不可中斷。建議具有高度管制區域使用。

5. 標準規範-物聯網設備安全基本要求

本節詳盡載明智慧路燈之物聯網設備安全基本要求，為滿足安全功能應採取的共通方法，所有智慧路燈系統系列產品應符合本節中所有安全基本要求。其中，燈桿閘道器除須符合本章節之基本要求外，亦須符合 7. 燈桿閘道器特殊要求之規定；後台監控伺服器須符合 6. 標準規範-後台監控伺服器。

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 除錯或測試用之遠端指令介面如: SSH 或 Telnet 等，須關閉或存取須經過身分鑑別。

5.1.1.2 產品需具備身分鑑別機制，包括管理介面、通訊協定、API，且該身分鑑別機制應能防止重送攻擊。

5.1.1.3 確保每台產品金鑰之唯一性，以降低金鑰外洩可能引發之資安風險。

5.1.1.4 每個產品應有一組唯一的識別碼。

5.1.1.5 產品必須驗證相連裝置所發送之憑證是否為受信任之憑證。

5.1.1.6 燈桿閘道器、燈桿附掛設備應支援向後台監控伺服器證明自身合法性之遠端證明(Remote Attestation)功能。

5.1.2 權限管控

5.1.2.1 產品的存取權限須控管包括管理介面、通訊協定、API，應切割成數個使用者角色，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。

5.1.2.2 管理介面之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。

5.1.3 通行碼鑑別

5.1.3.1 廠商所生產之產品，其設定預設通行碼都須相異；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。

5.1.3.2 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼長度至少大於 8 個字元。

5.1.3.3 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼中之字元必須符合下列四種字元中的三種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字 (0 到 9)；4.非英文字母字元 (例如： !、$、#、%)。

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 產品所儲存的安全敏感性資料，須經授權之使用者始可存取。

5.2.1.2 產品所儲存之通行碼、加解密用之金鑰(不含非對稱加密用之公鑰)不應明文儲存，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。

5.2.2 傳輸資料保護

5.2.2.1 產品之身分鑑別因子應加密傳輸，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。

5.2.2.2 資料傳輸須加密，以確保資料之機密性、正確性及完整性，若走 TLS 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)。

5.3 系統完整性

5.3.1 實體入侵防護

5.3.1.1 預設不應透過實體介面存取產品作業系統之除錯模式，或該實體介面之存取須通過身分鑑別。

5.4 軟韌體更新

5.4.1 更新安全

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

5.4.1.2 產品之更新路徑須加密，以確保韌體之機密性、正確性及完整性，若走 TLS 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)。

5.4.1.3 韌體檔案須加密保護以確保機密性，且須採用 FIPS 140-2 Annex A [6] 所核可之加密演算法；抑或是產品韌體之程式碼與安裝檔內其它檔案中，不應存在明文或可被解密回復之安全敏感性資料，與未宣告之相連伺服器 IP 和 URL。

5.4.1.4 產品之系統版本不應降回舊版本，避免舊版漏洞遭利用。

5.5 警示與紀錄

5.5.1 日誌檔與警示

5.5.1.1 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 日誌紀錄中不應存在明文或可被還原回復之安全敏感性資料。

5.5.1.3 產品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。

5.5.1.4 產品之事件日誌檔須具備日誌滾動(log rotate)機制。

5.5.1.5 產品之網頁介面、遠端指令控制介面、應用程式介面、實體介面發生使用者登入系統安全事件時，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。

5.6 已知漏洞安全

5.6.1 作業系統與網路服務

5.6.1.1 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。

5.6.1.2 產品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 CVSSv3 嚴重性等級評比為高風險。

5.6.2 網路服務連接埠

5.6.2.1 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用的網路服務而被侵入的可能性，且廠商須於產品文件中標註必須啟用之網路服務，避免未宣告之網路服務被開啟。

5.7 軟體應用程式

5.7.1 應用程式安全

5.7.1.1 產品之網站服務(web service)不應存在 OWASP 所揭露之網站 10 大資安風險[8]，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。

5.7.1.2 移除應用程式的超級使用者權限，避免因應用程式被攻陷而導致整個系統權限被取得。

6. 標準規範-後台監控伺服器

本節詳盡載明智慧路燈系統之後台監控伺服器的標準規範，為滿足安全功能應採取的方法，後台監控伺服器產品應符合本節之安全要求。

6.1 身分識別、鑑別、權限控管要求

6.1.1 鑑別機制

6.1.1.1 管理介面之身分鑑別錯誤訊息不應顯露出合法使用者名稱。

6.1.1.2 產品需具備身分鑑別機制，包括管理介面、通訊協定、API，且該身分鑑別機制應能防止重送攻擊。

6.1.1.3 後台監控伺服器管理介面之身分鑑別機制須採用多因子鑑別或 FIDO 身分鑑別同等或以上之強身分鑑別機制，增加身分偽造之難度。

6.1.1.4 產品必須驗證相連裝置所發送之憑證是否為受信任之憑證。

6.1.1.5 在智慧路燈系統應具備遠端證明(Remote Attestation)功能，使燈桿閘道器、燈桿附掛設備向後台監控伺服器證明自身合法性。

6.1.2 權限控管

6.1.2.1 產品的存取權限須控管包括管理介面、通訊協定、API，應切割成數個使用者角色，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。

6.1.2.2 管理介面之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。

6.1.3 通行碼鑑別

6.1.3.1 產品在登入通行碼的設計上須有輸入頻率及次數的限制，即：

(a) 最高五次嘗試登入失敗即鎖定帳戶。

(b) 在一定時間內須鎖定帳戶。

(c) 至少經過一定時間，始可將失敗的登入嘗試計數器重設為零次。

6.1.3.2 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼含使用者帳戶名稱全名中，不能包含 3 個以上之連續字元。

6.1.3.3 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼須執行歷程記錄。

6.1.3.4 廠商所生產之產品，其設定預設通行碼都須相異；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。

6.1.3.5 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼長度至少大於 8 個字元。

6.1.3.6 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼中之字元必須符合下列四種字元中的三種，1.英文大寫字元(A 到 Z)；2.英文小寫字元(a 到 z)；3.十進位數字(0 到 9)；4.非英文字母字元(例如：!、$、#、%)。

6.2 資料機密性與完整性

6.2.1 安全敏感性資料儲存

6.2.1.1 產品須提出金鑰管理程序，以確保金鑰管理的品質。

6.2.1.2 安全敏感性資料須存放於產品的安全區域(Security Domain)，從正常作業環境中隔離。

6.2.1.3 產品所儲存的安全敏感性資料，須經授權之使用者始可存取。

6.2.1.4 產品所儲存之通行碼、加解密用之金鑰(不含非對稱加密用之公鑰)不應明文儲存，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。

6.2.2 傳輸資料保護

6.2.2.1 後台監控伺服器應確認附掛於燈桿上設備所傳送過來資料的完整性。

6.2.2.2 產品之身分鑑別因子應加密傳輸，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。

6.2.2.3 資料傳輸須走加密，以確保資料之機密性、正確性及完整性，若走 TLS 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)。

6.3 警示與紀錄

6.3.1 日誌檔與警示

6.3.1.1 須具備安全事件紀錄，確實記錄使用者的存取行為，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。

6.3.1.2 日誌紀錄中不應存在明文或可被還原回復之安全敏感性資料。

6.3.1.3 產品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。

6.3.1.4 產品之事件日誌檔須具備日誌滾動(log rotate)機制。

6.3.1.5 產品發生安全事件時，須具備主動告警機制，包括回報管理者或推播警示、告警等訊息。

6.4 已知漏洞安全

6.4.1 作業系統與網路服務

6.4.1.1 後台監控伺服器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。

6.4.2 網路服務連接埠

6.4.2.1 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用的網路服務而被侵入的可能性，且廠商須於產品文件中標注必須啟用之網路服務，避免未宣告之網路服務被開啟。

6.5 軟體應用程式

6.5.1 網頁管理介面安全

6.5.1.1 產品之網站服務(web service)不應存在 OWASP 所揭露之網站十大資安風險[8]，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。

6.5.1.2 移除應用程式的超級使用者權限，避免因應用程式被攻陷而導致整個系統權限被取得。

6.6 資源可用性

6.6.1 備份

6.6.1.1 後台監控伺服器應提供備份能力，以確保失效或錯誤設置時可以恢復正常狀態。

6.6.1.2 後台監控伺服器應提供在開始恢復系統之前驗證備份檔案的完整性。

6.7 隱私保護

6.7.1 隱私保護能力

6.7.1.1 應提供傳輸加密功能予隱私資料傳輸。

6.7.1.2 隱私資料須被授權的個體始可存取。

6.7.1.3 後台監控伺服器之隱私政策宣告，須符合世界經濟合作暨發展組織(OECD)個資保護基本原則[9]。

6.8 雲端平台安全

6.8.1 雲端安全要求

6.8.1.1 後台監控伺服器之雲端安全須符合 ISO 27017[10]或 CSA STAR[11]國際雲端資安標準之規定。

7. 標準規範-燈桿閘道器安全特殊要求

本節詳盡載明智慧路燈系統之燈桿閘道器的安全特殊要求，為滿足安全功能應採取的方法，燈桿閘道器產品應符合第 5 節物聯網設備基本要求與本節之安全要求。

7.1 身分識別、鑑別、權限控管要求

7.1.1 鑑別機制

7.1.1.1 管理介面之身分鑑別錯誤訊息不應顯露出合法使用者名稱。

7.1.2 權限管控

7.1.2.1 產品須依循第 5.1.2 節之要求。

7.1.3 通行碼鑑別

7.1.3.1 產品在登入通行碼的設計上須有輸入頻率及次數的限制，即：

(a) 最高五次嘗試登入失敗即鎖定帳戶。

(b) 在一定時間內須鎖定帳戶。

(c) 至少經過一定時間，始可將失敗的登入嘗試計數器重設為零次。

7.1.3.2 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼含使用者帳戶名稱全名中，不能包含 3 個以上之連續字元。

7.1.3.3 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼須執行歷程記錄。

7.2 資料機密性與完整性

7.2.1 安全敏感性資料儲存

7.2.1.1 產品須依循第 5.2.1 節之要求。

7.2.1.2 產品須提出金鑰管理程序，以確保金鑰管理的品質。

7.2.1.3 安全敏感性資料須存放於產品的安全區域(Security Domain)，從正常作業環境中隔離。

7.2.2 傳輸資料保護

7.2.2.1 產品須依循第 5.2.2 節之要求。

7.3 系統完整性

7.3.1 實體入侵防護

7.3.1.1 產品須依循第 5.3.1 節之要求。

7.3.1.2 預設不應透過除錯埠(UART、JTAG)萃取產品韌體，或從晶片中被萃取出之韌體不應存在可識別之安全敏感性資料。

7.3.1.3 產品應支援安全啟動(Secure Boot)功能，不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。

7.4 軟韌體更新

7.4.1 更新安全

7.4.1.1 產品須依循第 5.4.1 節之要求。

7.5 警示與紀錄

7.5.1 日誌檔與警示

7.5.1.1 產品須依循第 5.5.1 節之要求。

7.6 已知漏洞安全

7.6.1 作業系統與網路服務

7.6.1.1 產品須依循第 5.6.1 節之要求。

7.6.2 網路服務連接埠

7.6.2.1 產品須依循第 5.6.2 節之要求。

7.7 軟體應用程式

7.7.1 應用程式安全

7.7.1.1 產品須依循第 5.7.1 節之要求。

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)
智慧路燈系統安全需求之緩解對策

根據本標準之適用範圍定義智慧路燈系統資產列表，如下表 B.1 所示。

表 B.1 智慧路燈系統資產列表

資產名稱	敘述
實體層	監控燈桿閘道器之機板、外殼、(COM port 或 USB 接口)。
作業系統	控制燈桿閘道器軟、硬體模組，包括或不包括檔案系統(File System)之核心軟體(如 Windows、Linux)。 後台監控伺服器之核心軟體。
OTA 更新	透過無線網路接收軟體、組態安裝及設定。
韌體	燒錄在燈桿閘道器中的儲存媒介，對於燈桿閘道器正常運作必要之軟體。
組態檔	定義作業系統及軟體運作方式之重要設定檔(如伺服器 IP、port 設定、自動更新等)。
安全事件紀錄(logs)	記錄系統安全、異常事件或使用者操作的資料。
安全敏感性資料與功能	使用者通行碼、帳號密碼及路燈控制。
通訊協定	Wi-Fi、LTE、NB-IoT 等 WAN 端的通訊，與 Sub-G、ZigBee、Wi-SUN 等 LAN 端的通訊。
網站服務(Web Service)	使燈桿閘道器、燈桿附掛設備及後台監控伺服器之間能夠溝通互動。

根據上述步驟所識別之智慧路燈系統的資產，經過分析定義出其衍生之常見資安威脅，鏈結其所危害之資產，如下列說明：

(1) 實體層

燈桿閘道器實體埠介面遭存取，竄改設定，導致資料遭竊取或安全敏感性資料外洩，成為惡意程式植入入口。

(2) 作業系統

燈桿監控閘道器及後台監控伺服器利用已知作業系統漏洞，植入惡意程式，取得控制權等操作。

(3) OTA(Over-the-Air)更新

燈桿閘道器及燈桿附掛設備更新之韌體，未經授權或安全通道傳送更新，造成韌體遭竄改或植入惡意程式。

(4) 韌體

韌體本身可能存在未經修補之已知資安漏洞。

(5) 組態檔

燈桿閘道器或後台監控伺服器之作業系統，可能存在未經修補之已知資安漏洞。

燈桿閘道器或後台監控伺服器之作業系統所儲存之安全敏感性資料，未經保護加密遭竊取利用，突破身份驗證機制。

(6) 安全事件紀錄

安全事件紀錄資料中可能以明文顯示或可被還原回復之安全敏感資料，而產生相應的資安漏洞，使駭客有機可乘。

(7) 安全敏感性資料與功能

燈桿閘道器與後台監控伺服器間所傳輸之安全敏感性資料，未設定存取權限，造成未經認證授權執行事件發生。

後台監控伺服器對燈桿閘道器及燈桿附掛設備之安全敏感性功能操作，如未對使用者進行角色與權限鑑別，可能造成重要功能遭誤啟動之情事。

傳輸資料過程中，遭受攔截並偽造資料回傳，使後台監控伺服器錯誤判斷關閉所有道路照明造成危險；或可能受到駭客發動 DDoS 及偽造控制指令的中間人攻擊等攻擊事件。

(8) 通訊協定

利用已知的傳輸通訊協定漏洞，駭客可能假冒管理者登入後台監控伺服器，取得控制權。

利用已知的無線個人區域網路漏洞，可能網路設定可能遭竄改，或發動重送攻擊癱瘓照明控制場域。

(9) 網路服務

透過後台監控伺服器的已知網路服務漏洞，駭客可能將惡意程式碼注入到網頁，藉由發動注入攻擊，取得後台監控伺服器之安全敏感檔案或後台監控伺服器的控制權。

根據識別之資產可能遭遇的威脅建立威脅模型，將威脅嚴重程度以 CVSS v3 所定義的風險評估因子進行評比，擬定各威脅之緩解對策，如下表 B.2 所示。

表 B.2 威脅模型分析表

威脅	資產	嚴重等級	緩解對策
實體介面入侵	安全敏感性資料	Medium	增加外殼破解難度 移除實體介面 實體介面身分鑑別
Firmware dump	安全敏感性資料	Medium	
接入裝置遭偽冒	燈桿閘道器	High	安全啟動
已知作業系統漏洞利用	作業系統	High ~ Critical	已知漏洞檢查
已知網路服務漏洞利用	網路服務	High ~ Critical	已知漏洞檢查
工程後門	燈桿閘道器 燈桿附掛設備 後台監控伺服器	Critical	最小化網路服務
韌體遭竄改/植入惡意程式	韌體	High	韌體簽章 韌體更新走安全通道
韌體 hardcode 安全敏感性資料	韌體	Medium	韌體加密 源碼掃描
DDoS 殭屍機	燈桿閘道器燈桿附掛設備 後台監控伺服器	High	已知漏洞檢查 未知漏洞檢查 警示與安全事件紀錄
挖礦殭屍機	燈桿閘道器 燈桿附掛設備 後台監控伺服器	High	已知漏洞檢查 未知漏洞檢查 警示與安全事件紀錄
勒索病毒	後台監控伺服器	Critical	備份
無線個人區域網路漏洞利用	燈桿閘道器 燈桿附掛設備	High ~ Critical	已知漏洞檢查、身分鑑別、權限控管、閒置逾時、正確的組態設定

威脅	資產	嚴重等級	緩解對策
偽造感測器資料、 控制指令(重送攻擊)	所有介面	Critical	身分鑑別、權限控管、閒置逾時、安全通道、金鑰管理、信任憑證、安全敏感性功能存取控制
偽造感測器資料、 控制指令(MITM)	所有介面	High	
密碼破解	所有介面	High ~ Critical	無預設密碼 密碼強度
注入攻擊	後台監控伺服器 燈桿附掛設備 燈桿閘道器	Medium	傳輸加密 安全通道
隱私外洩	後台監控伺服器	High ~ Critical	已知漏洞檢查、未知漏洞檢查、傳輸加密
安全敏感性資料外洩 (儲存)	安全敏感性資料	Medium	資料加密、存取控制、身分鑑別、權限控管、閒置逾時
安全敏感性資料外洩 (傳輸)	安全敏感性資料	Medium	安全通道 資料加密

根據上述步驟，識別智慧路燈系統的資產與資安威脅，透過威脅模型分析衍生出智慧路燈系統之資安需求，詳見 5.標準規範。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級。安全等級 1 級為下表 B.3 積分之 5~6，安全等級 2 級為積分 4，安全等級 3 級為積分 2~3。

表 B.3 安全等級劃分

風險(Risk) 技術複雜度	**Critical** **(3)**	**High** **(2)**	**Medium~None** **(1)**
低 (3)	6	5	4
中 (2)	5	4	3
高 (1)	4	3	2

當安全要求項目所面臨資安風險低、安全技術實現複雜度高時，則安全等級較高，例如「安全敏感性資料須存放於產品的安全區域並從正常作業環境中隔離」，安全敏感性資料外洩之資安風險為中等程度，但本項目廠商所要實現安全保護的技術與成本較高，因此將安全等級列為 3 級。當面臨資安風險高、安全技術實現複雜度低時，則安全等級較低，例如「網路服務連接埠的安全要求」，工程後門所面臨的資安風險很高，但本項目的檢測手法及防護技術的複雜度很低，因此安全等級列為 1 級。

表 B.4 安全需求緩解對策表

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式(風險等級)
5.1.1 鑑別機制	5.1.1.2 產品需具備身分鑑別機制，包括管理介面、通訊協定、API，且該身分鑑別機制應能防止重送攻擊。	V			DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)資料遭竄改、中間人攻擊(MITM)
	5.1.1.1 除錯或測試用之管理介面如: SSH 或 Telnet 等，預設須關閉或存取須經過身分鑑別。	V			
	5.1.1.3 確保每台產品金鑰之唯一性，以降低金鑰外洩可能引發之資安風險。	V			
	5.1.1.4 每個產品應有一組唯一的識別碼。	V			
	5.1.1.5 產品必須驗證相連裝置所發送之憑證是否為受信任之憑證。	V			
	5.1.1.6 在智慧路燈系統應具備遠端證明(Remote Attestation)功能，使燈桿閘道器、燈桿附掛設備向後台監控伺服器證明自身合法性。			V	
5.1.2/ 7.1.2 權限管控	5.1.2.1 產品的存取權限須控管包括管理介面、通訊協定、API，應切割成數個使用者角色，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。	V			DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)
	5.1.2.2 管理介面之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。	V			
5.1.3 通行碼鑑別	5.1.3.1 廠商所生產之產品，其設定預設通行碼都須相異；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。	V			密碼破解、DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)
	5.1.3.2 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼長度至少大於 8 個字元。	V			

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式(風險等級)
	5.1.3.3 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼中之字元必須符合下列四種字元中的三種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十 進位數字 (0 到 9)；4.非英文字母字元(例如：!、$、#、%)。	V			
5.2.1/ 7.2.1 安全敏感性資料儲存	5.2.1.1 產品所儲存的安全敏感性資料，須經授權之使用者始可存取。	V			安全敏感性資料外洩(儲存)、偽造感測器資料、控制指令(MITM、replay)
	5.2.1.2 產品所儲存之通行碼、加解密用之金鑰(不含非對稱加密用之公鑰)不應明文儲存，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。		V		
5.2.2/ 7.2.2 傳輸資料保護	5.2.2.1 產品之身分鑑別因子應加密傳輸，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。	V			DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)、安全敏感性資料外洩(傳輸)
	5.2.2.2 資料傳輸須走安全通道，以確保資料之機密性、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)。		V		
5.3.1/ 7.3.1 實體入侵	5.3.1.1 預設不應透過實體介面存取產品作業系統之除錯模式，或該實體介面之存取須通過身分鑑別。		V		實體介面入侵(Medium)
5.4.1/ 7.4.1 更新安全	5.4.1.1 產品須具備軟韌體更新機制，且即使發生更新失敗時，系統能回復正常運作。	V			無法提供安全性更新、韌體遭竄改/植入惡意程式、韌體 hardcode 安全敏感性資料、已知作業系統漏洞
	5.4.1.2 產品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)。	V			
	5.4.1.3 韌體檔案須加密保護以確保機密性，且須採用 FIPS 140-2 Annex A [6] 所核可之加密演算法；抑或是產品韌體之程式碼與安裝檔內其它檔案中，不應存在明文或可被解密回復之安全敏感性資料，與未宣告之相連伺服器 IP 和 URL。		V		
	5.4.1.4 產品之系統版本不應降回舊版本，避免舊版漏洞遭利用。	V			
5.5.1/ 7.5.1 日	5.5.1.1 須具備安全事件紀錄，確實記錄使用者的存取行為，得以查核未授權或異常行為，	V			DDoS 殭屍機、挖礦殭屍機

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式(風險等級)
誌檔與警示	供後續查閱之用，且須具時間戳記與事件內容。				
	5.5.1.2 日誌紀錄中不應存在明文或可被還原回復之安全敏感性資料。	V			
	5.5.1.3 產品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。	V			
	5.5.1.4 產品之事件日誌檔須具備日誌滾動(log rotate)機制。	V			
	5.5.1.5 產品發生安全事件時，須具備主動告警機制，包括回報管理者或推播警示、告警等訊息。	V			
5.6.1./ 7.6.1 作業系統與網路服務	5.6.1.1 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。	V			已知作業系統漏洞利用、已知網路服務漏洞利用、DDoS 殭屍機、挖礦殭屍機
	5.6.1.2 產品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。		V		
5.6.2/ 7.6.2 網路服務連接埠	5.6.2.1 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用的網路服務而被侵入的可能性，且廠商須於產品文件中標註必須啟用之網路服務，避免未宣告之網路服務被開啟。	V			工程後門
5.7.1/ 7.7.1 應用程式安全	6.7.1.1 產品之網站服務(web service)不應存在 OWASP 所揭露之網站十大資安風險[8]，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。	V			已知網站服務漏洞利用
	5.7.1.2 移除應用程式的超級使用者權限，避免因應用程式被攻陷而導致整個系統權限被取得。	V			
6.1.1 鑑別機制	6.1.1.1 管理介面之身分鑑別錯誤訊息不應顯露出合法使用者名稱。	V			DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式(風險等級)
	6.1.1.2 產品需具備身分鑑別機制，包括管理介面、通訊協定、API，且該身分鑑別機制應能防止重送攻擊。	V			控制指令(MITM、replay)
	6.1.1.3 後台監控伺服器管理介面之身分鑑別機制須採用多因子鑑別或 FIDO 身分鑑別同等或以上之強身分鑑別機制，增加身分偽造之難度。			V	
	6.1.1.4 產品必須驗證相連裝置所發送之憑證是否為受信任之憑證。	V			
	6.1.1.5 在智慧路燈系統應具備遠端證明(Remote Attestation)功能，使燈桿閘道器、燈桿附掛設備向後台監控伺服器證明自身合法性。			V	
6.1.2 權限控管	6.1.2.1 產品的存取權限須控管包括管理介面、通訊協定、API，應切割成數個使用者角色，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。	V			
	6.1.2.2 管理介面之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。	V			
6.1.3 / 7.1.3 通行碼鑑別	6.1.3.1/7.1.3.1 產品在登入通行碼的設計上須有輸入頻率及次數的限制，即： (a) 最高五次嘗試登入失敗即鎖定帳戶。 (b) 在一定時間內須鎖定帳戶。 (c) 至少經過一定時間，始可將失敗的登入嘗試計數器重設為零次。	V			密碼破解、DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)
	6.1.3.2/7.1.3.2 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼含使用者帳戶名稱全名中，不能包含 3 個以上之連續字元。			V	
	6.1.3.3 /7.1.3.3 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼須執行歷程記錄。			V	
	6.1.3.4 廠商所生產之產品，其設定預設通行碼都須相異；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。	V			
	6.1.3.5 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼長度至少大於 8 個字元。	V			

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式(風險等級)
	6.1.3.6 所有介面之通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼中之字元必須符合下列四種字元中的三種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十 進位數字 (0 到 9)；4.非英文字母字元 (例如： !、$、#、%)。	V			
6.2.1/ 7.2.1 安全敏感性資料儲存	6.2.1.1/7.2.1.2 產品須提出金鑰管理程序，以確保金鑰管理的品質。		V		安全敏感性資料外洩(儲存)、偽造感測器資料、控制指令(MITM、replay)
	6.2.1.2/7.2.1.3 安全敏感性資料須存放於產品的安全區域(Security Domain)，從正常作業環境中隔離。			V	
	6.2.1.3 產品所儲存的安全敏感性資料，須經授權之使用者始可存取。	V			
	6.2.1.4 產品所儲存之通行碼、加解密用之金鑰(不含非對稱加密用之公鑰)不應明文儲存，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。		V		
6.2.2 傳輸資料保護	6.2.2.1 後台監控伺服器應確認附掛於燈桿上設備所傳送過來資料的完整性與不可否認性。	V			DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)、安全敏感性資料外洩(傳輸)
	6.2.2.2 產品之身分鑑別因子應加密傳輸，而保護資料的加密方式須採用 FIPS 140-2 Annex A[6] 所核可之加密演算法。	V			
	6.2.2.3 資料傳輸須走安全通道，以確保資料之機密性、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)。		V		
6.3.1 日誌檔與警示	6.3.1.1 須具備安全事件紀錄，確實記錄使用者的存取行為，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。	V			
	6.35.1.2 日誌紀錄中不應存在明文或可被還原回復之安全敏感性資料。	V			
	6.3.1.3 產品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。	V			

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式(風險等級)
	6.3.1.4 產品之事件日誌檔須具備日誌滾動(log rotate)機制。	V			
	6.3.1.5 產品發生安全事件時，須具備主動告警機制，包括回報管理者或推播警示、告警等訊息。	V			
6.4.1. 作業系統與網路服務安全	6.4.1.1 後台監控伺服器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。	V			已知作業系統漏洞利用、已知網路服務漏洞利用、DDoS 殭屍機、挖礦殭屍機
6.4.2 網路服務連接埠	6.4.2.1 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用的網路服務而被侵入的可能性，且廠商須於產品文件中標注必須啟用之網路服務，避免未宣告之網路服務被開啟。	V			工程後門
6.5.1 網頁管理介面安全	6.5.1.1 產品之網站服務(web service)不應存在 OWASP 所揭露之網站 10 大資安風險[8]，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。	V			已知網站服務漏洞利用
	6.5.1.2 移除應用程式的超級使用者權限，避免因應用程式被攻陷而導致整個系統權限被取得。	V			
6.6.1 備份	6.6.1.1 後台監控伺服器應提供系統層級備份能力，以確保失效或錯誤設置時可以恢復正常狀態。	V			勒索病毒
	6.6.1.2 後台監控伺服器應提供在開始恢復系統之前驗證備份檔案的完整性。	V			
6.7.1 隱私保護能力	6.7.1.1 應提供安全通道功能予隱私資料傳輸。		V		-
	6.7.1.2 隱私資料須被授權的個體始可存取。	V			-
	6.7.1.3 後台監控伺服器之隱私政策宣告，須符合世界經濟合作暨發展組織(OECD)個資保護基本原則[9]。	V			-
6.8.1 雲端安全要求	6.8.1.1 後台監控伺服器之雲端安全須符合 ISO 27017[10]或 CSA STAR[11]國際雲端資安標準之規定。			V	-

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式 (風險等級)
7.1.1 鑑別機制	7.1.1.1 管理介面之身分鑑別錯誤訊息不應顯露出合法使用者名稱。	V			DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)資料遭竄改、中間人攻擊(MITM)
7.3.1 實體入侵	7.3.1.2 晶片中的韌體必須無法被解析。		V		韌體萃取
	7.3.1.3 產品應支援安全啟動(Secure Boot)功能，不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。			V	接入裝置遭偽冒

附錄 C
(參考)
技術要求事項與各標準規範對照表

表 C.1　本標準適用範圍之資安脆弱點/要求事項與標準規範對照表

本標準 要求事項	對應標準規範	
	IEC 62443-4-2[3]	NIST-Core IoT Cybersecurity Capabilities Baseline
5.1.1.1	-	-
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	Baseline 1 The IoT device can be identified both logically and physically.
5.1.1.3	CR 1.8–公鑰基礎結構憑證 Public key infrastructure certificates	-
5.1.1.4	CR 1.2–軟體進程及設備的識別及認證 Software process and device identification and authentication	Baseline 1 The IoT device can be identified both logically and physically.
5.1.1.5	CR 1.14-對稱式金鑰認證的強度 Strength of symmetric key authentication CR 3.3-安全功能認證 Security functionality verification	-
5.1.1.6	CR 1.2–軟體進程及設備的識別及認證 Software process and device identification and authentication CR 2.2-無線使用控制 Wireless use control	Baseline 1 The IoT device can be identified both logically and physically.
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	Baseline 3 Authorized users can securely change the IoT device's configuration, including restoration to a secure "default." Unauthorized changes to the IoT device's configuration can be prevented.
5.1.2.2	CR 2.6–遠端 Session 終止 Remote session termination	-
5.1.3.1	-	-
5.1.3.2	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.
5.1.3.3	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	
5.2.1.1	CR 2.1–授權執行 Authorization enforcement CR 4.1–資訊機密性 Information confidentiality	-
5.2.1.2	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	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.

本標準 要求事項	對應標準規範	
	IEC 62443-4-2[3]	NIST-Core IoT Cybersecurity Capabilities Baseline
5.2.2.1	CR 4.3–密碼學的使用 Use of cryptography	
5.2.2.2	CR 3.1–通訊完整性 Communication integrity	Baseline 6 The IoT device can use industryaccepted, standardized protocols for all layers of the device's transmissions.
5.3.1.1	~~CR 3.11 – 實體竄改防止及偵測~~ ~~Physical tamper resistance and detection~~(放 5.5.1.5) CR 2.13 - use of physical diagnostic and test interface	Baseline 12 The IoT device is designed to allow physical access to it to be controlled.
5.4.1.1	CR 3.10–更新 Support for updates	Baseline 2 The IoT device's software and firmware can be updated using a secure, controlled, and configurable mechanism.
5.4.1.2	CR 3.1–通訊完整性 Communication integrity	Baseline 6 The IoT device can use industryaccepted, standardized protocols for all layers of the device's transmissions.
5.4.1.3	CR 4.3–密碼學的使用 Use of cryptography	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.
5.4.1.4	CR 3.10–更新 Support for updates	-
5.5.1.1	CR 6.1–審計日誌可存取性 Audit log accessibility CR 6.2–持續監控 Continuous monitoring CR 2.11–時間戳 Timestamps CR 2.8-可審查事件 Auditable events CR 2.13 - use of physical diagnostic and test interface CR 3.9-審計訊息的保護 Protection of audit information	Baseline 7 The IoT device can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems.
5.5.1.2	-	-
5.5.1.3	CR 6.1–審計日誌可存取性 Audit log accessibility	Baseline 7 The IoT device can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems.
5.5.1.4	CR 2.9–審計儲存容量 Audit storage capacity	
5.5.1.5	CR 2.10–對審計處理失敗的回應 Response to audit processing failures CR 3.11 - 實體竄改防止及偵測 Physical tamper resistance and detection CR 3.3-安全功能認證 Security functionality verification (關燈那條)	-
5.6.1.1	~~NCR 3.2–惡意程式防護~~ ~~Malicious code protection~~	-

本標準 要求事項	對應標準規範	
	IEC 62443-4-2[3]	NIST-Core IoT Cybersecurity Capabilities Baseline
	~~CR 3.2 惡意代碼防衛~~ ~~Malicious code protection~~	
5.6.1.2		-
5.6.2.1	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	Baseline 11 The IoT device can enforce the principle of least functionality through its design and configuration.
5.7.1.1	-	Baseline 9 Information confirming the sources of all of the IoT devices's software, firmware, hardware, and services is disclosed and accessible.
5.7.1.2	-	-
6.1.1.1	CR 1.10–認證者回饋 Authenticator feedback	-
6.1.1.2	CR 1.2–軟體進程及設備的識別及認證 Software process and device identification and authentication	Baseline 1 The IoT device can be identified both logically and physically.
6.1.1.3	-	-
6.1.1.4	CR 1.9–公鑰認證的強度 Strength of public key authentication	-
6.1.1.5	CR 1.2–軟體進程及設備的識別及認證 Software process and device identification and authentication	Baseline 1 The IoT device can be identified both logically and physically.
6.1.2.1	CR 2.1–授權執行 Authorization enforcement	Baseline 3 Authorized users can securely change the IoT device's configuration, including restoration to a secure "default." Unauthorized changes to the IoT device's configuration can be prevented.
6.1.2.2	CR 2.6–遠端 Session 終止 Remote session termination	-
6.1.3.1	CR 1.11–失敗的嘗試登錄 Unsuccessful login attempts	-
6.1.3.2	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.
6.1.3.3	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	
6.1.3.4	-	-
6.1.3.5	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.
6.1.3.6	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	
6.2.1.1	CR 1.9–公鑰認證的強度 Strength of public key authentication	-
6.2.1.2	-	-
6.2.1.3	CR 2.1–授權執行 Authorization enforcement CR 4.1–資訊機密性 Information confidentiality	-

本標準 要求事項	對應標準規範	
	IEC 62443-4-2[3]	NIST-Core IoT Cybersecurity Capabilities Baseline
6.2.1.4	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	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.
6.2.2.1	CR 2.12-不可否認性 Non-repudiation CR 3.4–軟體及資訊完整性 Software and information integrity	Baseline 9 Information confirming the sources of all of the IoT device's software, firmware, hardware, and services is disclosed and accessible.
6.2.2.2	CR 4.3–密碼學的使用 Use of cryptography	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.
6.2.2.3	CR 3.1–通訊完整性 Communication integrity	~~Baseline 6.2~~ ~~Use of specific protocols should be verifiable by inspection.~~ ~~(沒有)~~
6.3.1.1	CR 6.1–審計日誌可存取性 Audit log accessibility CR 6.2–持續監控 Continuous monitoring CR 2.11–時間戳 Timestamps CR 2.13 - use of physical diagnostic and test interface	Baseline 7 The IoT device can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems.
6.3.1.2	-	-
6.3.1.3	CR 6.1–審計日誌可存取性 Audit log accessibility	Baseline 7 The IoT device can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems.
6.3.1.4	CR 2.9–審計儲存容量 Audit storage capacity	
6.3.1.5	CR 2.10–對審計處理失敗的回應 Response to audit processing failures	-
6.4.1.1	NCR 3.2–惡意程式防護 Malicious code protection CR 3.2–惡意代碼防衛 Malicious code protection	-
6.4.2.1	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	Baseline 11 The IoT device can enforce the principle of least functionality through its design and configuration.
6.5.1.1	CR 3.5-輸入認證 Input validation	Baseline 9 Information confirming the sources of all of the IoT devices's software, firmware, hardware, and services is disclosed and accessible.
6.5.1.2	-	-
6.6.1.1	CR 7.4–控制系統復原及重建 Control system recovery and reconstitution	-
6.6.1.2	CR 7.3–控制系統備份 Control system backup	-
6.7.1.1	-	-
6.7.1.2	-	-

本標準 要求事項	對應標準規範	
	IEC 62443-4-2[3]	NIST-Core IoT Cybersecurity Capabilities Baseline
6.7.1.3	-	-
6.8.1.1	-	-
7.1.1.1	CR 1.10–認證者回饋 Authenticator feedback	-
7.1.2.1	-	-
7.1.3.1	CR 1.11–失敗的嘗試登錄 Unsuccessful login attempts	-
7.1.3.2	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	Baseline 5 The IoT device can use cryptography to secure its stored and transmitted data.
7.1.3.3	CR 1.7–密碼身份認證的強度 Strength of password-based authentication	
7.2.1.1	-	-
7.2.1.2	CR 1.9–公鑰認證的強度 Strength of public key authentication	-
7.2.1.3	-	-
7.2.2.1	-	-
7.3.1.1	-	-
7.3.1.2	CR 3.11 - 實體竄改防止及偵測 Physical tamper resistance and detection	Baseline 12 The IoT device is designed to allow physical access to it to be controlled.
7.3.1.3	CR 3.14 - 開機程序的完整性 Integrity of boot process	-
7.4.1.1	-	-
7.5.1.1	-	-
7.6.1.1	-	-
7.6.2.1	-	-
7.7.1.1	-	-

參考資料

(1) Open Web Application Security Project(OWASP).org, Top IoT Vulnerabilities, https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

(2) CNS 15652-1：2013 智慧路燈系統-第 1 部：系統功能

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

(4) 個人資料保護法, Dec., 2015.

(5) National Institute of Standards and Technology(NIST), National Vulnerability Database, https：//nvd.nist.gov/vuln/full-listing

(6) National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions, available at URL: http://www.nist.gov/cmvp.

(7) First, Common Vulnerability Scoring System v3.0 Specification, https：//www.first.org/cvss/specification-document

(8) Open Web Application Security Project(OWASP).org, Top 10 -2017, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

(9) Organisation for Economic Co-operation and Development,OECD, The 2013 OECD Privacy Guidelines , http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

(10) ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

(11) CSA Security Trust Assurance and Risk (STAR), https://cloudsecurityalliance.org/star/

(12) NIST, Considerations for a Core IoT Cybersecurity Capabilities Baseline, https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf