TAICS

TAICS TS-0027-2 v1.0 : 2019

智慧路燈系統資安標準
－第二部：智慧照明

Intelligent Streetlight System Cybersecurity Standard
- Part 2: Intelligent Lighting

2019/12/06

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

智慧路燈系統資安標準-

第二部：智慧照明

Intelligent Streetlight System Cybersecurity Standard

- Part 2: Intelligent Lighting

出版日期: 2019/12/06

終審日期: 2019/11/27

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：安華聯網科技股份有限公司 洪光鈞 總經理

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 副主任

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 組長

TC5 物聯網資安工作組：財團法人資訊工業策進會 賴怡伶、劉濬銘

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、台灣德國萊因技術監護顧問股份有限公司、安華聯網科技股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣電子檢驗中心、財團法人資訊工業策進會、財團法人電信技術中心、國立交通大學、優力國際安全認證有限公司。

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、台達電子工業股份有限公司、台灣 LED 照明產業聯盟、台灣飛樂喜萬年有限公司、光宇股份有限公司、安謀國際科技股份有限公司、威力工業網絡股份有限公司、思納捷科技股份有限公司、研揚科技股份有限公司、神通資訊科技股份有限公司、國立雲林科技大學、晶復科技股份有限公司、億光電子工業股份有限公司。

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交通及環境資料回傳雲端分析，進而衍生出智慧路燈照明系統。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照明路燈公共工程及億光、光寶、台達電等大廠的帶領下，單以台北市為例，過去每年路燈照明電費約 3 億元，路燈升級後電費已降至 1.7 億。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 2016 年白帽駭客發現透過 ZigBee 的 Touchlink 控制系統的漏洞，利用 Philips 智慧燈泡更新韌體時植入蠕蟲發動 DDoS 攻擊，成功掌控城市路燈並癱瘓城市照明。

有鑑於此，本系列標準針對智慧路燈系統上相關應用的裝置制定資安標準，包括智慧路燈上的照明監控閘道器與照明設備。制定 TAICS TS-0028 系列測試規範作為 TAICS TS-0028 系列標準提供驗證之基準與測試方法，TAICS TS-0027 系列共有二部標準，包括「TAICS TS-0027-1 智慧路燈系統資安標準-第一部：一般要求」、「TAICS TS-0027-2 智慧路燈系統資安標準-第二部：智慧照明系統」(以下簡稱本標準)。

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。

智慧照明系統包含 1 個主要照明監控伺服器、1 個以上之照明控制場域，每個照明控制場域包含 1 個以上之照明監控閘道器，透過 NB-IoT 或 3G/4G 等網路傳輸方式與照明監控伺服器建立連接；照明控制場域應包含至少 1 個受控制的照明設備，藉由 ZigBee、Sub-G 或 Wi-Fi 等傳輸方式與照明監控閘道器建立一個網狀骨幹網路(Mesh)或其他網路技術連接。如下圖 1 所示。

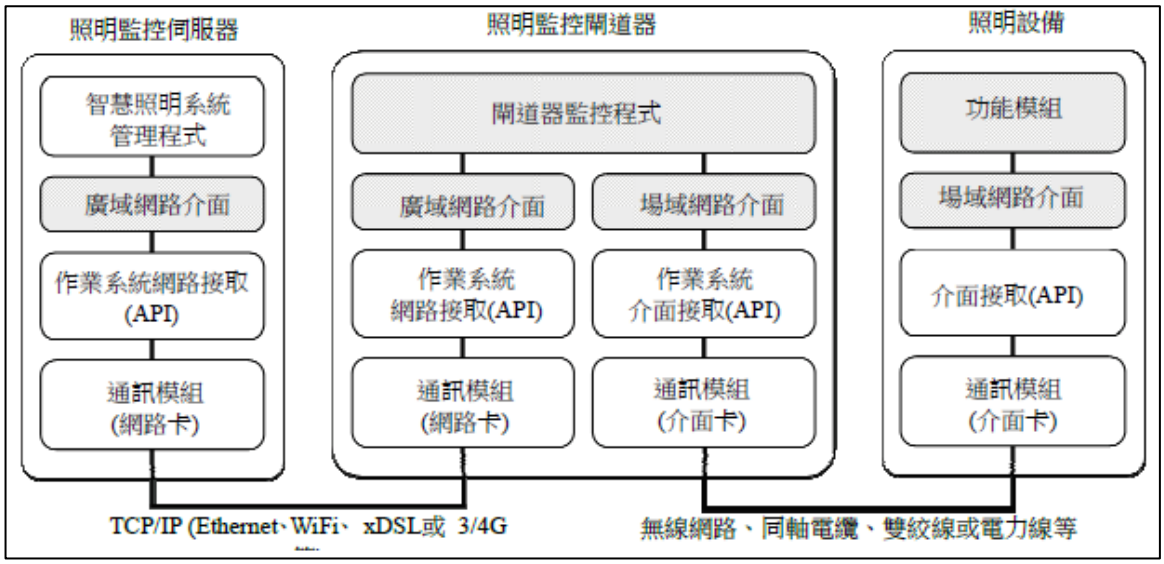

圖 1 智慧照明系統架構

圖片來源：CNS 15652-1

由於智慧照明產業技術隨科技發展日新月異，圖 1 照明設備與監控伺服器間之傳輸方式可區分為三種類型，分別為介接廣域網路介面與場域網路介面型式的照明監控閘道器、僅具備場域網路介面的照明設備，及直接透過廣域網路介面通訊的照明設備。

1. 適用範圍

本系列標準適用於智慧照明系統，智慧照明是由照明監控伺服器、照明監控閘道器及照明設備所組成，如下圖 2 所示。本標準自七個構面定義了智慧照明系統網路安全要求：

- 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

本標準作為智慧照明產業之系統整合商、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。

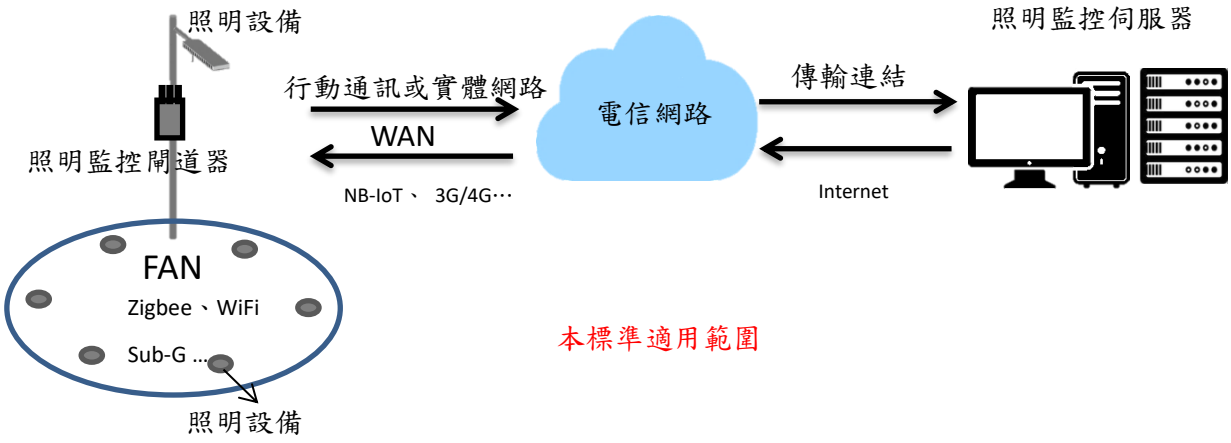

圖 2 適用範圍示意圖

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 智慧照明系統(Intelligent Lighting System)

可依人體或被照物等需求自動調控色溫、亮度等相關因子，以塑造最舒適之照明環境。因此，此系統藉由感測與控制之量測資訊，可挑選最佳視覺之照明或最適合人體生理之照明，同時亦可搭配遠端遙控系統以進行相關之監控及控制。

3.2 照明監控伺服器(Lighting Control and Monitoring Server)

提供智慧照明系統之監測資料記錄及人員遠端控制功能之伺服器，足以對網路點進行管控與資料收發，以及執行運作之軟體程式，負責管理者登入與邏輯應用程式執行等作業，例如：系統維護、故障偵錯、資料查詢及設備監控等應用。

3.3 照明設備(Lighting Equipment)

泛指獨立運作，具有實體之物件，可接受指令以執行各種功能之硬體。例如：照明單元、感測器及自動控制設備。

3.4 照明監控閘道器(Lighting Control Gateway)

安裝於照明控制場域之硬體設備，以及執行運作軟體程式，負責建立與照明監控伺服器之網路連接，接收來自照明監控伺服器之指令，並將指令轉送至目的照明設備，同時亦負責蒐集來自個別照明設備之狀態回報，並回傳至照明監控伺服器。

3.5 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。

3.6 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)發展至為第三版。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[6]。

3.8 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。

3.9 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。

3.10 安全敏感性資料(Secure Sensitivity 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，登入照明監控伺服器關閉照明等危及社會安全事件。

3.11 安全敏感功能(Secure Sensitive Function)

泛指智慧照明系統中，須經授權方能操作產品或系統之功能。例如，開關照明設備或更新韌體。

3.12 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，包括但不限於智慧照明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。

3.13 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，如監控伺服器管理者、維修人員。

3.14 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通行碼、自身帳號及通行碼、遠端網路服務帳號及通行碼。

3.15 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，用以登入照明監控設之通行碼。

3.16 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。

3.17 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、使用者操作全面關燈等的行為。

3.18 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)。

3.19 照明控制場域(Lighting Control Field)

受照明監控伺服器監控之場地，包含至少 1 個以上直接受照明監控閘道器控制之照明設備。

3.20 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。

3.21 場域網路(Field Area Network, FAN)

泛指一特定區域內，連結照明監控閘道器與各種照明設備之網路，照明設備如照明單元、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。

3.22 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。

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

本標準為智慧照明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)已知漏洞安全及(7)軟體應用程式，及照明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-照明設備				
5.1 身分識別、鑑別、權限控管	5.1.1 鑑別機制	5.1.1.2 5.1.1.3	-	-
	5.1.2 權限管控	-	-	-
	5.1.3 通行碼鑑別	5.1.3.2	-	5.1.3.3 5.1.3.4
5.2 資料機密性與完整性	5.2.1 安全敏感性資料儲存	-	5.2.1.2	5.2.1.3
	5.2.2 傳輸資料保護	-	-	-
5.3 系統完整性	5.3.1 實體入侵防護	-	5.3.1.2	5.3.1.3
5.4 軟韌體更新	5.4.1 更新安全	-	-	-
5.5 警示與紀錄	5.5.1 日誌檔與警示	-	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.6 已知漏洞安全	5.6.1 作業系統與網路服務	-	-	-
	5.6.2 網路服務連接埠	-	-	-
5.7 軟體應用程式	5.7.1 應用程式安全	-	-	-
6. 標準規範-照明監控伺服器				
6.1 身分識別、鑑別、權限控管要求	6.1.1 鑑別機制	-	-	-
	6.1.2 權限控管	-	-	-
	6.1.3 通行碼鑑別	-	-	-
6.2 資料機密性與完整性	6.2.1 安全敏感性資料儲存	-	-	-
	6.2.2 傳輸資料保護	-	-	-
6.3 警示與紀錄	6.3.1 日誌檔與警示	-	-	-
6.4 已知漏洞安全	6.4.1 作業系統與網路服務	-	-	-
	6.4.2 網路服務連接埠	-	-	-
6.5 軟體應用程式	6.5.1 網頁管理介面安全	-	-	-
6.6 資源可用性	6.6.1 備份	-	-	-
6.7 隱私保護	6.7.1 隱私保護能力	-	-	-
6.8 雲端平台安全	6.8.1 雲端安全要求	-	-	-
7. 標準規範-照明監控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	-	-	-
	7.1.2 權限管控	-	-	-
	7.1.3 通行碼鑑別	-	-	-
7.2 資料機密性與完整性	7.2.1 安全敏感性資料儲存	-	-	-
	7.2.2 傳輸資料保護	-	-	-
7.3 系統完整性	7.3.1 實體入侵防護	-	-	-
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、網路服務應防止資安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資安漏洞及具備安全機制。

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-照明設備

智慧照明系統為滿足安全功能，所有智慧照明系統之照明設備產品應須依循 TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」標準規範及本節所載明之標準規範。

5.1 身分識別、鑑別、權限控管

5.1.1 鑑別機制

5.1.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.1.1 節之要求。

5.1.1.2 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。

5.1.1.3 安全敏感性功能操作於異常情況下需經過身分鑑別。

5.1.2 權限管控

5.1.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－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 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.1.3 節之要求。

5.1.3.2 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 5 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 0 次

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

5.1.3.4 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。

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 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.2.1 節之要求。

5.2.1.2 產品須提出金鑰管理程序，以確保金鑰管理的品質。

5.2.1.3 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。

5.2.2 傳輸資料保護

5.2.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.2.2 節之要求。

5.3 系統完整性

5.3.1 實體入侵防護

5.3.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.3.1 節之要求。

5.3.1.2 晶片中的韌體必須無法被解析。

5.3.1.3 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。

5.4 軟韌體更新

5.4.1 更新安全

5.4.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.4.1 節之要求。

5.5 警示與紀錄

5.5.1 日誌檔與警示

5.5.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.5.1 節之要求。

5.6 已知漏洞安全

5.6.1 作業系統與網路服務

5.6.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.6.1 節之要求。

5.6.2 網路服務連接埠

5.6.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.6.2 節之要求。

5.7 軟體應用程式

5.7.1 應用程式安全

5.7.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 5.7.1 節之要求。

6. 標準規範-照明監控伺服器

本節詳盡載明智慧照明系統之照明監控伺服器的標準規範，為滿足安全功能應採取的方法，照明監控伺服器產品依循 TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」之「6. 標準規範-後台監控伺服器」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 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.1.1 節之要求。

6.1.2 權限控管

6.1.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.1.2 節之要求。

6.1.3 通行碼鑑別

6.1.3.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.1.3 節之要求。

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 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.2.1 節之要求。

6.2.2 傳輸資料保護

6.2.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.2.2 節之要求。

6.3 警示與紀錄

6.3.1 日誌檔與警示

6.3.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.3.1 節之要求。

6.4 已知漏洞安全

6.4.1 作業系統與網路服務

6.4.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.4.1 節之要求。

6.4.2 網路服務連接埠

6.4.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.4.2 節之要求。

6.5 軟體應用程式

6.5.1 網頁管理介面安全

6.5.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.5.1 節之要求。

6.6 資源可用性

6.6.1 備份

6.6.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.6.1 節之要求。

6.7 隱私保護

6.7.1 隱私保護能力

6.7.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.7.1 節之要求。

6.8 雲端平台安全

6.8.1 雲端安全要求

6.8.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 6.8.1 節之要求。

7. 標準規範-照明監控閘道器安全特殊要求

本節詳盡載明智慧照明系統之照明監控閘道器的標準規範，為滿足安全功能應採取的方法，照明監控閘道器產品依循 TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」之「7. 標準規範-燈桿閘道器安全特殊要求」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 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.1.1 節之要求。

7.1.2 權限管控

7.1.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.1.2 節之要求。

7.1.3 通行碼鑑別

7.1.3.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.1.3 節之要求。

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 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.2.1 節之要求。

7.2.2 傳輸資料保護

7.2.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.2.2 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 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.3.1 節之要求。

7.4 軟韌體更新

7.4.1 更新安全

7.4.1.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.4.1 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 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.5.1 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 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.6.1 節之要求。

7.6.2 網路服務連接埠

7.6.2.1 產品須依循 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.6.2 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 TAICS TS-0027-1 「智慧路燈系統資安標準－第一部：一般要求」第 7.7.1 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)
智慧照明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照明系統資產列表，如下表 B.1 所示。

表 B.1 智慧照明系統資產列表

資產名稱	敘述
實體層	監控閘道器之機板、外殼、(COM port 或 USB 接口)。
作業系統	控制閘道器軟、硬體模組，包括或不包括檔案系統(File System)之核心軟體(如 Windows、Linux)。 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	燒錄在照明監控閘道器中的儲存媒介，對於照明監控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、帳號通行碼及照明控制。
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)	使照明監控閘道器、照明設備及照明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照明系統的資產，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

照明監控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

照明監控閘道器及照明監控伺服器利用已知作業系統，植入惡意程式，取得控制權等操作。

(3) OTA(Over-the-Air)更新

照明監控閘道器及照明設備更新之韌體，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

照明監控閘道器或照明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。

照明監控閘道器或照明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，突破身分驗證機制。

(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

照明監控閘道器與照明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。

照明監控伺服器對照明監控閘道器及照明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，使照明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照明監控伺服器，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

透過照明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，取得照明監控伺服器之安全敏感檔案或照明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	Severity	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	照明監控閘道器	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	照明監控閘道器 照明設備 照明監控伺服器	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	照明監控閘道器 照明設備 照明監控伺服器	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	照明監控閘道器 照明設備 照明監控伺服器	High	已知漏洞檢查 未知漏洞檢查 警示與安全事件紀錄

威脅	資產	Severity	緩解對策
勒索病毒	照明監控伺服器	Critical	備份
無線個人區域網路漏洞利用	照明監控閘道器 照明設備	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
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	
通行碼破解	所有介面	High ~ Critical	無預設通行碼 通行碼強度
注入攻擊	照明監控伺服器 照明設備 照明監控閘道器	Medium	傳輸加密 安全通道
隱私外洩	照明監控伺服器	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，識別智慧照明系統的資產與資安威脅，透過威脅模型分析衍生出智慧照明系統之資安需求，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 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)
	5.1.1.3 安全敏感性功能操作於異常情況下需經過身分鑑別。	V			
5.1.3 通行碼鑑別	5.1.3.2 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			通行碼破解、DDoS 殭屍機、挖礦殭屍機、偽造感測器資料、控制指令(MITM、replay)
	5.1.3.3 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	
	5.1.3.4 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	

安全要求內容		1 級	2 級	3 級	可能遭遇攻擊模式 (風險等級)
5.2.1 安全敏感性資料儲存	5.2.1.2 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)
	5.2.1.3 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	
5.3.1 實體入侵防護	5.3.1.2 晶片中的韌體必須無法被解析。		V		實體介面入侵(Medium)
	5.3.1.3 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	

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	
	OWASP IoT Top 10[1]	IEC 62443-4-2[3]
5.1.1.1	-	-
5.1.1.2	I7 Insecure Mobile Interface Ensuring user accounts can not be enumerated using functionality such as password reset mechanisms	CR 1.10–認證者回饋 Authenticator feedback
5.1.1.3	I2 Insufficient Authentication/Authorization Ensuring re-authentication is required for sensitive features	CR 1.1–使用者識別及認證 Human user identification and authentication
5.1.2.1	-	-
5.1.3.1	-	-
5.1.3.2	I1 Insecure Web Interface Ensuring account lockout after 3 -5 failed login attempts I2 Insufficient Authentication/Authorization Ensuring that the strong passwords are required Ensuring options are available for configuring password controls I8 Insufficient Security Configurability Ensuring the ability to force strong password policies	CR 1.11–失敗的嘗試登錄 Unsuccessful login attempts
5.1.3.3		CR 1.7–通行碼身分認證的強度 Strength of password-based authentication
5.1.3.4		CR 1.7–通行碼身分認證的強度 Strength of password-based authentication
5.2.1.1	-	-
5.2.1.2	-	CR 1.9–公鑰認證的強度 Strength of public key authentication
5.2.1.3	I8 Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit I2 Insufficient Authentication/Authorization Ensuring credentials are properly protected	-
5.2.2.1	-	-
5.3.1.1	-	-
5.3.1.2	-	CR 3.11 - 實體竄改防止及偵測 Physical tamper resistance and detection
5.3.1.3	I9 Insecure Software/Firmware Implement the secure boot if possible (chain of trust)	CR 3.14 - 開機程序的完整性 Integrity of boot process
5.4.1.1	-	-
5.5.1.1	-	-
5.6.1.1	-	-
5.6.2.1	-	-
5.7.1.1	-	-

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 智慧照明系統-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) First, Common Vulnerability Scoring System v3.0 Specification, https：//www.first.org/cvss/specification-document

(7) 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

(8) TAICS TS-0027-1 v0.9:2019 智慧路燈系統資安標準-第一部：一般要求

版本修改紀錄

版本	時間	摘要
v1.0	2019/12/06	出版

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw