檔　　號：

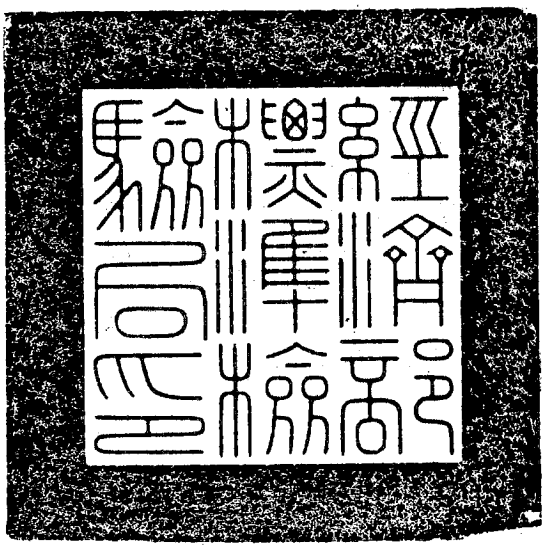
保存年限：

經濟部標準檢驗局　公告

發文日期：中華民國109年12月30日

發文字號：經標六字第10960030980號

附件：「太陽光電變流器及監視單元資安檢測技術規範」



主旨：公告「太陽光電變流器及監視單元資安檢測技術規範」，並自即日生效。

依據：「自願性產品驗證實施辦法」第四條第三項。

公告事項：如附「太陽光電變流器及監視單元資安檢測技術規範」。

局長 連錦漳

裝

訂

線

太陽光電變流器及監視單元資安檢測技術規範 (109 年 12 月版)

(Technical Specification for Security Testing of PV Inverters and Monitoring Units)

1. 適用範圍與目的

本規範適用於具有自主調控功能之太陽光電變流器(PV Inverter)，及資料傳輸指向網際網路(Internet)上特定伺服器或資料庫之監視單元(monitoring unit)產品。

本規範所定的方法與要求，目的在確認太陽光電變流器及監視單元具有基礎資安防護能力，包含(1)實體資安(2)系統資安(3)通訊資安(4)身分鑑別等四個資安構面，以確保產品資訊安全。

2. 引用標準

下列標準之全部或部份，為本規範引用之相關文件，有加註年份時僅適用該版本，未加註時則適用該文件最新版次(包含任何修訂)。

IEC 62443-1-1:2009	Industrial communication networks-Network and system security-Part 1-1: Terminology, concepts and models.
IEC 62443-4-2:2018	Security for industrial automation and control system, Part 4-2: Technical security requirements for IACS components.
NIST 2018 v1.1	Framework for improving critical infrastructure cybersecurity
NIST Aug, 2019	Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources
CTIA V1.1 Jun, 2019	CTIA Cybersecurity Certification Test Plan for IoT Devices.
ISA SSA-420 V 3.2	System Security Assurance-Vulnerability Identification Testing Specification.
CNS 16120-1:2019	影像監控系統安全－第 1 部：一般要求事項
CNS 16132-1:2020	影像監控系統安全測試方法－第 1 部：一般要求事項
CNS 15426-2:2003	太陽光電系統用電源轉換器之安全性－第 2 部：變流器之個別要求

3. 用語與定義

3.1 變流器 (Inverter)

將直流電流改變為單相或多相交流電流的電能轉換器，可內嵌或外接監視單元接受遠端監視或遠端操控。

3.2 本體單元 (Main unit)

本規範定義係變流器不包括監視單元之部分稱之。

3.3 監視單元 (Monitoring unit)

監視單元可內嵌於變流器，亦可為獨立於變流器外之介面或裝置。
監視單元具有資料擷取器(data logger)與閘道器(gateway)功能，可採擷一台或多台變流器本體單元之資訊，如直交流電壓、電流、功率等相關參數，並將擷取資訊經由網際網路協定，透過乙太網路實體線路、無線網路(WiFi)或行動通訊(GPRS)等將資料傳輸至雲端伺服器，以達成遠端監視或操控太陽光電變流器之目的。

3.4 嵌入式裝置 (Embedded device)

為控制、監視或輔助運作設備及機器的裝置，可嵌入於完整之硬體或機械設備，以微處理器或微控制器為核心，用於執行較固定的少數程序，如需變更程序，需透過外部介面進行更新。

3.5 主機式裝置 (Host device)

具備作業系統(operation system, OS)如 Microsoft Windows 或 Linux 等 OS 的通用設備，能夠安裝並執行來自不同供應商的一項或多項軟體應用程式。

3.6 工業通訊協定 (Industrial communication protocol)

於本規範中，工業通訊協定係指變流器與監視單元之間採用之通訊協定，如 Modbus/RTU 或 Modbus/TCP 等。

3.7 網際網路協定 (Internet Protocol Suite, IPS)

網際網路的基礎通訊架構，或稱 TCP/IP，包含傳輸控制協定(Transmission

Control Protocol, TCP)與網際網路協定(IP)，TCP/IP 提供了點對點連結的機制，將資料應該如何封裝、定址、傳輸、路由以及在目的地如何接收，都加以標準化。

3.8 管理系統 (Management system)

再生能源監控系統之核心，具有伺服功能及資料庫管理功能，提供不同之使用者存取合理資料之授權機制。部份管理系統除可接收資料外，亦可下達指令變更變流器或監視單元之工作狀態，或進行遠端軟/韌體更新作業。管理系統之資訊安全不在本規範納測範疇，惟管理系統對使用者帳號之管理能力及是否具遠端軟韌體更新等功能，亦會納入檢測之考量。

3.9 共同脆弱性及曝露 (Common Vulnerabilities and Exposures, CVE)

由美國非營利組織 MITRE Corporation 所屬之 National Cybersecurity FFRDC 所營運維護脆弱性管理計畫，針對每一資安脆弱性項目給予全球認可之唯一共通編號。

3.10 共同弱點列舉 (Common Weakness Enumeration, CWE)

由美國非營利組織 MITRE Corporation 所屬之 National Cybersecurity FFRDC 所營運維護之軟體弱點分類系統。

3.11 共同脆弱性評分系統(Common Vulnerability Scoring System, CVSS)

依資安脆弱性之特點與影響進行評分之系統。由美國國家基礎建設諮詢委員會負責研究(National Infrastructure Advisory Council, NIAC)，現轉由資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)發展，目前為第 3 版。

3.12 共同弱點評分系統(Common Weakness Scoring System, CWSS)

依軟體弱點之特點與影響進行評分之系統，為 CWE 系統之一部分。

3.13 角色(Role)

可指派予使用者或群組(人員、軟體程序或裝置)之一組關聯行為、權限及義務，如賦予工程師群組內之每一人員相同之權限與義務。

3.14 最少權限(Least privilege)

依據使用者(人員、軟體程序或裝置)被分派之責任與功能，授予所需最低權限之基本原則。

3.15 聯邦資訊處理標準第 140 號(Federal Information Processing Standards 140, FIPS 140)

聯邦資訊處理標準(FIPS)為美國聯邦政府制定除軍事機構外，所有政府機構及政府承包商所引用之標準。FIPS 140 係密碼模組安全需求標準，目前 FIPS 140-2 的規範是國際上業界所公認的密碼學模組標準。

3.16 識別與鑑別(Identify and authentication)

「識別」為使用者對其身分之宣稱;「鑑別」係對使用者所宣稱身分之查證。識別符(identifier)係可對作出判定或聲明身分之個體進行識別之符號型樣，如使用者帳號(account)；鑑別符(authenticator)係用以確認個體身分之方法，如通行碼(password)、指紋或感應磁卡等。

3.17 通行碼(Password)

用以鑑別身分或查證存取授權之字元串(字母、數字及其他符號)。

4. 系統架構：

太陽光電變流器及監視單元之資料傳輸架構及測試範疇如圖 1 所示，測試範圍包括「變流器本體單元」與「監視單元」等 2 種測試單元，如圖 1 紅色實線框處。對資料傳輸及管理系統等則有部份附加的資安要求，如圖 1 藍色虛線框處。

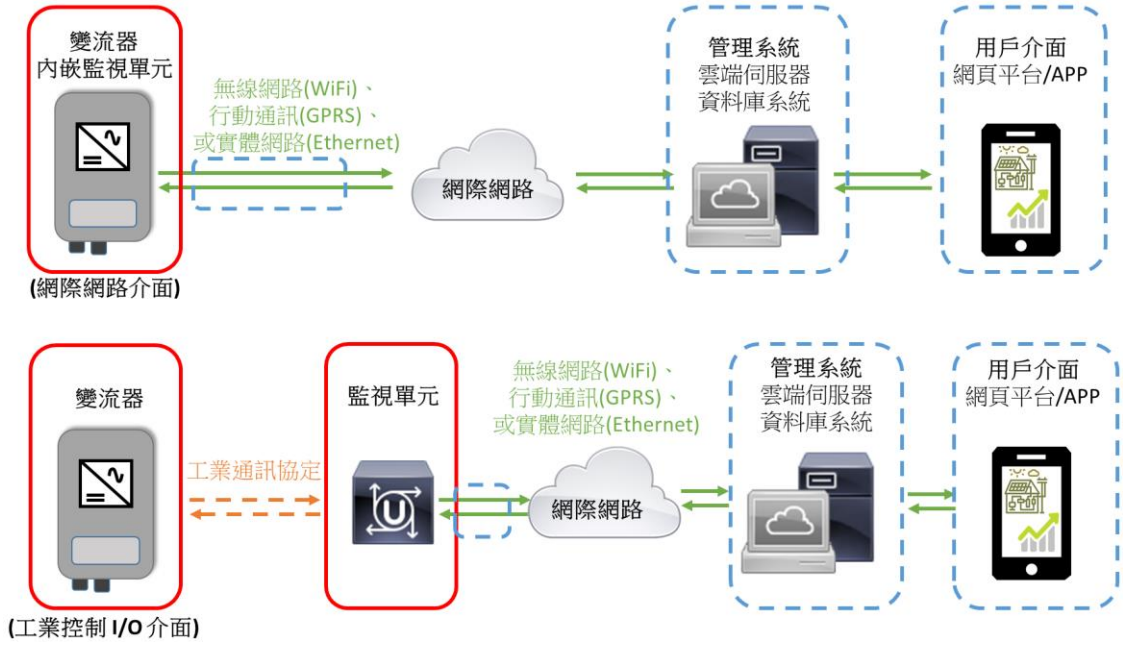


圖 1：變流器及監視單元之資料傳輸架構及測試範疇示意圖

5. 安全構面及資安等級：

5.1 安全構面

本規範以實體資安、系統資安、通訊資安與身分鑑別等構面來檢視產品之資訊安全程度，如表 1 所示，說明如下：

5.1.1 實體資安：產品應建立拆除障礙並應關閉非必要之實體埠，以降低駭客透過實體介面入侵或竄改資料的風險。

5.1.2 系統資安：產品之作業系統、應用程式或軟/韌體及所儲存之資料等，應具備足夠之資安防護。

5.1.3 通訊資安：產品之通訊應採已知最佳實踐方式架構，對敏感性資料之傳輸，應予以加密保護，以確保通訊資安。

5.1.4 身分鑑別：對每個可存取產品介面均須確立識別、鑑別與授權機制，以防止人員存取未經授權之資料或進行權限外之操作。

5.2 資安等級：

本規範將各項資安要求區分為 2 階資安等級，1 級之預期效果為防止無心之操作誤會、不成熟之攻擊行為或無足夠資源之蓄意攻擊行為；2 級則預期能防止蓄意且有資源之攻擊行為。對於資安等級之說明，整理於表 1；各資安要求列於表 2，其相應之國際標準條目，彙整於附件 1。

表 1 變流器及監視單元資安等級說明

資安等級	說明	備考
1 級	防止無心之操作誤會或不成熟之攻擊行為，或防止攻擊者無足夠資源之蓄意攻擊行為。	變流器本體及監視單元之基礎資安要求。
2 級	防止蓄意且有資源之攻擊行為。	進階資安要求。

表 2 變流器本體及監視單元資安要求與資安等級一覽表

測試單元	資安構面	資安要求	資安等級	
			1 級	2 級
1.本體單元	1.1 實體資安	1.1.1 實體防護		V
	1.2 系統資安	1.2.1 軟/韌體更新機制	V	V
		1.2.2 軟/韌體安全性評估		V
	1.3 身分鑑別	1.3.1 人機介面身分鑑別(實體)	V	V
		1.3.2 人機介面身分鑑別(無線)	V	V
2.監視單元	2.1 實體資安	2.1.1 實體防護		V
		2.1.2 最小實體介面要求	V	V
	2.2 系統資安	2.2.1 已知脆弱性掃描	V	V
		2.2.2 軟/韌體更新機制	V	V
		2.2.3 軟/韌體安全性評估	V	V
		2.2.4 機敏資料保護	V	V
		2.2.5 惡意程式防護		V
		2.2.6 帳戶管理	V	V
		2.2.7 事件日誌	V	V
		2.2.8 事件日誌之儲存容量與效期		V
	2.3 通訊資安	2.3.1 最小通訊埠要求	V	V
		2.3.2 動態資料加密保護	V	V
		2.3.3 動態資料加密保護-進階		V
		2.3.4 封包流量與指向分析	V	V
	2.4 身分鑑別	2.4.1 人員使用者識別與鑑別	V	V
		2.4.2 通行碼強度(長度基礎)	V	V
		2.4.3 通行碼輸入頻次限制	V	V
		2.4.4 預設通行碼變更機制	V	V

6. 資安要求與檢測方式

廠商於測試前需填具自檢表，並提供各測試項目之自我檢查、相關說明及相應之佐證資料，自檢表格式如附件 2。

針對變流器與監視單元之測試佈局如圖 2 所示。

變流器本體之各項資安要求與檢測方式列於第 6.1 節，如表 3 所示。

監視單元之各項資安要求與檢測方式列於第 6.2 節，如表 4 所示。

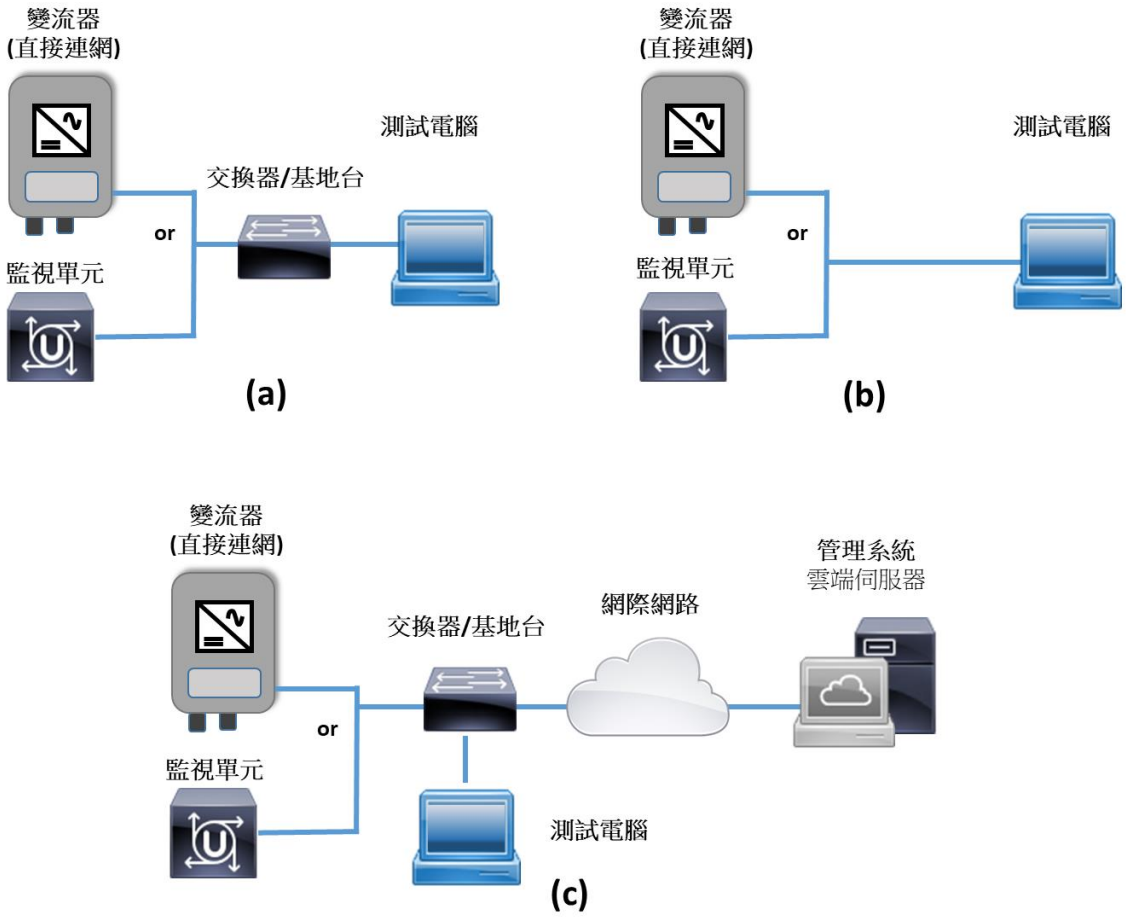


圖 2：測試佈局示意圖

圖 2 說明如下：

(a) 待測物與測試電腦處同一網域，透過交換器/基地台相互連接。

(b) 待測物提供網路存取點，測試電腦直接與之連接。

(c) 待測物連接至網際網路並與測試電腦處於同一網域，測試電腦可透過交換器/基地台監聽待測物之封包。

變流器資安檢測工具安裝於測試電腦，包括安裝弱點掃描工具、靜態程式碼分析工具、網路偵測工具與網路封包偵錄工具等。

6.1 變流器本體之資安要求與檢測方式

表 3 變流器本體單元之資安要求與檢測方式

資安要求	說明	檢測方式	紀錄	備考
1.1.1 實體防護	變流器本體應建立外殼拆除障礙或保有實體遭拆解之紀錄	目視變流器本體之外殼是否為一體成型、或具實體鎖、或採防拆螺絲，以建立拆除障礙。或以一次性貼紙張貼於外殼可拆處，以保有實體遭拆解之紀錄。	1.符合 2.不符合	目視檢查。
1.2.1 軟/韌體更新機制	變流器之軟/韌體在更新前需驗證軟/韌體之完整性與來源可信任	1. 變流器核心功能相關之軟/韌體應有更新機制，以修補漏洞或擴充功能，廠商應提供以下項目： (1)可更新之軟/韌體清單 (2)軟/韌體更新保護機制說明文件 (3)更新軟/韌體之操作程序 (4)可供更新之檔案 (5)具更新權限之帳戶 2. 依廠商提供更新檔案、具更新權限之帳戶與操作程序說明進行軟/韌體更新，應可成功更新且不會造成產品被重置為預設狀態(檢視登入帳號、系統時間、事件日誌等是否被重置)，否則判為不符合。 3. 對廠商提供之軟/韌體檔案進行修改，或以其他來源之軟/韌體對該產品進行更新，應有查覺軟/韌體錯誤之機制，否則判為不符合。本體單元應能拒絕錯誤軟/韌體之更新，或顯示更新失效而回復更新前之狀態或進入待機狀態，以保護電力穩定。	1.符合 2.不符合	依廠商提供之更新機制，或如測試佈局圖 2 (a)~(c)合宜者。

1.2.2 軟/韌體安全性評估	變流器之軟/韌體之程式碼應進行靜態分析確認資安弱點	1. 廠商應提供於 1.2.1 測試項目中進行軟/韌體更新之程式源碼(source code)做為安全性評估之標的。 2. 對標的檔案進行靜態程式碼弱點分析。分析工具應可視別共同弱點(CWE)或共同脆弱性(CVE)並比對弱點或脆弱性評分系統(CWSS/CVSS)以進行等級判定。 3. 若測得具共同弱點/脆弱性(CWE/CVE)編號之漏洞，且其CWSS/CVSS 分數大於等於 7 (或嚴重等級為 High 或 Critical 者)，廠商應能提供合理管控措施並說明之，否則本項不符合。	1.符合 2.不符合	受測方提供軟/韌體源碼，以測試電腦進行測試。
1.3.1 人機介面身分鑑別(實體)	透過實體人機介面(如顯示面板與按鍵)存取/操作變流器，應有權限管理與鑑別機制	1. 未採用實體人機介面之產品，或實體人機介面僅具資料查詢與顯示功能，本項可申明為不適用。 2. 廠商應提供實體人機介面鑑別機制、存取方式與操作權限之說明，並提供可通過鑑別之鑑別符(如通行碼、感應磁扣等)。 3. 以步驟 2 提供之鑑別符，應能通過鑑別並存取裝置，確認操作權限與廠商說明相符，則本項符合。 4. 若未經鑑別而可以對變流器本體進行電力相關參數變更(如改變輸出電壓、頻率等)，則本測項不符合。為確保人員或產品安全相關之切斷開關則不在此限。	1.符合 2.不符合 3.不適用	依實際狀況進行檢測。
1.3.2 人機介面身分鑑別(無線)	對透過無線之人機介面(如透過藍芽)存取/操作變流器，應有權限管	1. 未採用無線人機介面之產品，或無線人機介面僅具資料查詢與顯示功能，則此項目可申明為不適用。 2. 廠商應提供無線人機介面鑑別機制、存取方式與操作權限之說明，並提供可通過鑑別之鑑別符。	1.符合 2.不符合 3.不適用	依實際狀況進行檢測。

	理與鑑別機制	3. 以步驟 2 提供之鑑別符,應能通過鑑別並存取裝置,確認操作權限與廠商說明相符，則本項符合。 4. 若此無線介面採預設之通行碼做為鑑別符,宜有強制使用者更新通行碼之機制,若否,則此預設通行碼不得為： (1) 可公開可取得之資訊(如登載於產品說明書內)。 (2) 公認之弱通行碼型式，如：與帳號相同、採常見預設通行碼或單詞(ex. admin, root, password)、 重複字元。(ex. kkkkk)、低於 8 碼之純數字組合、鍵盤按鍵順序組合(ex. qwerty)等。		

6.2 監視單元之資安要求與檢測方式

表 4 監視單元之資安要求與檢測方式

資安要求	說明	檢測方式	紀錄	備考
2.1.1 實體防護	監視單元應建立外殼拆除障礙	目視監視單元之外殼，應為一體成型、或具實體鎖或設計於可上鎖之箱體內、或採防拆螺絲搭配一次性貼紙，以建立拆除障礙。	1.符合 2.不符合	目視檢查。
2.1.2 最小實體介面要求	應將監視單元上非必要之實體介面(如 USB 埠、RJ45 埠、SD card 插槽等) 移除或預設為關閉，以減少可能被攻擊之途徑	1. 廠商提供文件說明實體介面之目的及相關保護措施。目視產品外觀並清點實體介面應與廠商說明文件相符，否則此項判為不符合。 2. 如存有非必要之實體介面未移除、則應預設關閉或採實體保護,否則此項判為不符合。	1.符合 2.不符合	書審及目視檢查。

2.2.1 已知脆弱性掃描	監視單元不應存在風險等級較高之已知脆弱性	1. 使用弱點識別工具對產品進行弱點掃描，脆弱性識別應依共同脆弱性評分系統(CVSS)進行判定。 2. 若測得具共同脆弱性及曝露(CVE)編號之漏洞，且其 CVSS 分數大於等於 7 (或嚴重等級為 High 或 Critical 者)則本項不符合。 3. 若帶有中等級之脆弱性，廠商應能提供合理管控措施，否則本項不符合。	1.符合 2.不符合	測試佈局如圖 2 (a)或(b)。
2.2.2 軟/韌體更新機制	監視單元之軟/韌體在更新前需驗證軟/韌體之完整性與來源可信任	1. 監視單元核心功能相關之軟/韌體應有更新機制，以修補漏洞或擴充功能，廠商應提供以下項目： (1)可更新之軟/韌體清單 (2)軟/韌體更新保護機制說明文件 (3)更新軟/韌體之操作程序 (4)可供更新之檔案 (5)具更新權限之帳戶 2. 依廠商提供更新檔案、具更新權限之帳戶與操作程序說明進行軟/韌體更新，應可成功更新且不會造成產品被重置為預設狀態(檢視登入帳號、系統時間、事件日誌等是否被重置)，否則判為不符合。 3. 對廠商提供之軟/韌體檔案進行修改，或以其他來源之軟/韌體對該產品進行更新，應有查覺軟/韌體錯誤之機制，否則判為不符合。	1.符合 2.不符合	依廠商提供之更新機制，或如測試佈局圖 2 (a)~(c)合宜者。
2.2.3 軟/韌體安全性評估	監視單元之軟/韌體程式碼應進行靜態分析確認資安弱點	1. 廠商應提供於 2.2.2 測試項目中進行軟/韌體更新之檔案程式源碼(source code)做為安全性評估之標的。 2. 對標的檔案進行靜態程式碼分析。分析工具應可視別共同弱點(CWE)或共同脆弱性(CVE)並比對弱點或脆弱性評分系統(CWSS/CVSS)以進行等級判定。	1.符合 2.不符合	受測方提供軟/韌體源碼，以測試電腦進行測試。

		3. 若測得具共同弱點/脆弱性(CWE/CVE)編號之漏洞，且其CWSS/CVSS 分數大於等於 7 (或嚴重等級為 High 或 Critical 者)，廠商應能提供合理管控措施並說明之，否則本項不符合。		
2.2.4 機敏資料保護	監視單元儲存之機敏資料應受到保護	1. 機敏資料包括但不限於身分鑑別資訊(如使用者帳號、通行碼)及含有使用者隱私之資料，廠商應提供自定義之機敏資料說明。若監視單元內無儲存機敏資料，則本項可聲明為不適用。 2. 廠商應說明對機敏資料之保護方式，如將機敏資料加密，或置於需要特殊權限方能存取之資料路徑。 3. 驗證廠商之保護說明：以沒有特殊權限的一般帳戶登入並嘗試存取機敏資料，如未能成功存取，則本項符合。	1.符合 2.不符合 3.不適用	書審並依實際狀況確認佐證資訊。測試佈局圖 2 (a)~(c)合宜者。
2.2.5 惡意程式防護	監視單元應防止來源不明、未授權或已知含有惡意程式的軟/韌體被安裝或被執行	1. 若監視單元為嵌入式裝置則通過測試項目 2.2.2、2.2.3，此項次即符合。 2. 若監視單元為主機裝置，除第 1 條所述之通過要件外，應採取合宜措施防範惡意程式碼(例：針對病毒、蠕蟲、特洛伊木馬程式及間諜軟體)並提供說明，以書面審查判定本項是否符合。	1.符合 2.不符合	書審並依實際狀況確認佐證資訊。測試佈局圖 2 (a)~(c)合宜者。
2.2.6 帳戶管理	監視單元應提供人員使用者至少二階層(如管理員及一般使用者)以上之存取權	1. 廠商應就所有人員使用者可存取產品之途徑提供說明。 2. 基於使用者角色之差異，應至少需有二階層以上之存取權限，且應符合最少權限原則。 3. 人員使用者可存取監視單元之介面可能存在於本地端或遠端(管理系	1.符合 2.不符合	書審並依實際狀況確認佐證資訊。測試佈局圖 2

	限，以利分級管理，或經由管理系統之支援達成此項要求	統)，帳戶管理要求可於任一端實踐之。 4. 廠商應就步驟 1~3 所述提出書面說明，以審閱判斷是否符合要求。 5. 廠商應提供測試用帳戶。登入較低權限之帳號，並嘗試存取需較高權限之資料或需較高權限之操作。若能成功登入且無法存取需較高權限之資料或無法進行需較高權限之操作，則本項符合。 6. 廠商得申明「最低權限使用者」(如僅具閱覽展示資訊之權限)，此等使用者得採用較弱之識別與鑑別程序。惟此等「最低權限使用者」不應授予存取 2.2.4 所列之機敏資料(除該使用者本身之帳號或隱私資訊)之權限、不應授予如 1.2.1 及 2.2.2 所述進行軟/韌體更新之權限、不應授予於遠端控制變流器之行為之權限且不應授予修改變流器電力相關參數之權限。		(a)~(c)合宜者。
2.2.7 事件日誌	監視單元應具備事件日誌功能，或經由管理系統之支援達成此項要求	1. 事件日誌可存在於監視單元(本地端)或管理系統(遠端)內。 2. 事件日誌應至少包含：軟/韌體更新紀錄、緊急/異常事件及遠端控制事件(如有遠端控制功能)，且每一事件應可由紀錄中辨識事件時間、事件種類與誘發事件之來源身分(可能為人員或設備)。 3. 廠商應提供存取事件日誌之操作程序說明，並提供具權限之帳號。登入具權限之帳號並存取並瀏覽事件日誌，確認有符合步驟 2 之要求，否則判為不符合。 4. 登入較低權限之帳號，應無法刪除或	1.符合 2.不符合	書審並依實際狀況確認佐證資訊。測試佈局圖 2 (a)~(c)合宜者。

		修改事件日誌，否則判為不符合。		
2.2.8 事件日誌之儲存容量與效期	廠商應能預期監視單元或管理系統之事件日誌之儲存容量與效期	1. 廠商應提供事件日誌保存方式與預期儲存時間之說明。 2. 廠商應說明對產品之事件日誌保存期限之需求及原因，且步驟 1 之預期儲存時間應高於此需求。 3. 廠商應說明事件日誌儲存量瀕臨或超過其儲存空間時之應對方式(如定期將事件日誌上傳管理系統，而不會一直累積於監視單元內)，並確保不會造成監視單元故障。 4. 審閱上述說明文件，確認廠商均能提出合理說明，則本項符合。	1.符合 2.不符合	書審並依實際狀況確認佐證資訊。測試佈局圖 2 (a)~(c)合宜者。
2.3.1 最小通訊埠要求	監視單元不應存在未知之網路埠	1. 廠商應說明其產品開通之通訊埠與開通原因，啟用之通訊埠應符合最少權限原則。若存在非必要之通訊埠或未能提供說明者，本項為不符合。 2. 將產品與測試電腦連接，啟用具網路埠掃描功能之工具，對產品執行 TCP 埠、UDP 埠及埠 0 之掃描。 3. 比對掃描結果是否與廠商說明一致，若內容相符，則本項為符合。	1.符合 2.不符合	書審及測試，測試佈局圖 2 (a)或(b)。
2.3.2 動態資料加密保護	應對透過監視單元傳輸之機敏資料進行加密保護	1. 機敏資料之定義請參考測試項目 2.2.4。 2. 將監視單元連接至網際網路並與測試電腦處於同一網域，持續以測試電腦監聽/側錄往來監視單元之封包。 3. 側錄期間，依廠商之操作說明，登入帳戶並對監視單元進行存取動作。 4. 檢視側錄之封包，應無法查看到機敏資料未經加密之明文，否則本項次為不符合。	1.符合 2.不符合 3.不適用	測試佈局圖 2 (c)。
2.3.3 動態資料加密保護–進階	監視單元與管理系統間之資料傳輸	1. 由廠商提供監視單元與管理系統間資料傳輸所採用加密方式之說明與佐證資料，其加解密用金鑰的保密機	1.符合 2.不符合	書審及測試，測試佈局

	應採用符合 FIPS 140-2 要求之密碼模組進行資料保護	制應採用符合 FIPS 140-2 要求之密碼模組。 2. 審閱廠商提供之資料以確認符合本測試項目要求。		圖 2 (c)。
2.3.4 封包流量與指向分析	監視單元連接網路時不應對未宣告的 IP 進行封包傳遞	1. 廠商應宣告監視單元預期會連結之伺服器 IP 位址及其他可能位置。並提供合理數據流量之說明資料。 2. 將監視單元連接至網際網路並與測試電腦處於同一網域，持續以測試電腦監聽/側錄往來監視單元之封包至少 24 小時。 3. 檢查側錄之封包，其目的地位址應與廠商自我宣告後台伺服器連線目的地之 IP/DNS 相符，否則本項不符合。 4. 檢視側錄之封包流量，如有發現異常流量而廠商無法說明，則此項不符合。	1.符合 2.不符合	書審及監聽封包，測試佈局圖 2 (c)。
2.4.1 人員使用者識別與鑑別	監視單元對人員使用者應予識別與鑑別	1. 廠商應就測項 2.2.6 步驟 1 列出之所有人員使用者可存取產品之途徑，提供使用者識別與鑑別機制之說明。 2. 審閱廠商說明，並進行人員使用者登入，檢驗識別與鑑別機制是否符合廠商說明。	1.符合 2.不符合	依廠商提供之存取機制說明，測試佈局如圖 2 (a)~(c)合宜者。
2.4.2 通行碼強度(長度基礎)	若採通行碼做為鑑別機制，則通行碼應有長度要求，以防止被暴力破解	1. 依測項 2.2.6 與 2.4.1，除廠商特意申明之最低權限使用者，餘人員使用者若以通行碼做為鑑別機制，則其通行碼應有長度要求。 2. 若通行碼為人員使用者自行定義，則不應限定通行碼為固定長度(如限定僅能輸入 4 碼)，否則本項不符合。 3. 若採用預設通行碼而未強制使用者更新，則此預設通行碼不得為：	1.符合 2.不符合 3.不適用	書審及操作檢視，測試佈局如圖 2 (a)~(c)合宜者。

		(1) 可公開可取得之資訊(如登載於產品說明書內)。 (2) 公認之弱通行碼型式，如：與帳號相同、採常見預設通行碼或單詞(ex. admin, root, password)、 重複字元。(ex. kkkkk)、低於 8 碼之純數字組合、鍵盤按鍵順序組合(ex. qwerty)等。 4. 檢視廠商說明並進行相應帳號登入操作，驗證通行碼要求與廠商說明相符，則本項符合。		
2.4.3 通行碼輸入頻次限制	採通行碼做為鑑別機制，應有通行碼輸入次數之限制，以防止被暴力破解	1. 依測項 2.2.6 與 2.4.1，除廠商特意申明之最低權限使用者，餘人員使用者若以通行碼做為鑑別機制，則其通行碼輸入錯誤容許次數應為 5 次(含)以下，超過容許之登入次數時，介面應有重置或時間間隔鎖定機制。 2. 依廠商提供之測試帳號及通行碼登入產品，應能成功登入。後以錯誤之通行碼再登入，應登入失敗，且超過通行碼輸入錯誤容許次數後，應有重置或時間間隔鎖定機制，否則此測項不符合。	1.符合 2.不符合 3.不適用	書審及操作檢視，測試佈局如圖 2 (a)~(c)合宜者。
2.4.4 預設通行碼變更機制	人員使用者之初次鑑別若採公開取得之預設通行碼，則使用者首次登入後，應有要求預設通行碼變更之機制	1. 依測項 2.2.6 與 2.4.1，除廠商特意申明之最低權限使用者，餘人員使用者若採可公開取得之帳號或通行碼(如標示於產品說明書內)，應有強制使用者更新之機制。若無可公開取得之帳號與通行碼，本項可申明為不適用。 2. 依可公開取得之帳號及/或通行碼登入產品，應能成功登入。 3. 首次登入成功後，組件或系統應要求更改預設通行碼，且對通行碼之要求符合通行碼長度要求，否則本項不符	1.符合 2.不符合 3.不適用	書審及操作檢視，測試佈局如圖 2 (a)~(c)合宜者。

		合。 4. 首次登入成功而被要求更改通行碼時，仍採預設通行碼做設定，若可成功設定，則本項為不符合。		

附件 1：本規範與國際標準關聯對應表

測試單元	資安構面	資安要求	國際標準		
			IEC 62443-4-2	CTIA IoT test plan	TAICS TS-0014-1
1.變流器本體單元	1.1 實體資安	1.1.1 實體防護	CR 3.11	N/A	5.1.3.1
	1.2 系統資安	1.2.1 軟/韌體更新機制	CR 3.10	3.5 3.6	5.2.3.2
		1.2.2 軟/韌體安全性評估	IEC 62443-4-1 SI-1		
	1.3 身分鑑別	1.3.1 人機介面身分鑑別(實體)	CR 1.1	3.3	5.4.1.1
		1.3.2 人機介面身分鑑別(無線)	CR 1.1	3.3	5.4.1.1
2.監視單元	2.1 實體資安	2.1.1 實體防護	CR 3.11	N/A	5.1.3.1
		2.1.2 最小實體介面要求	CR 7.7	N/A	5.1.1.1
	2.2 系統資安	2.2.1 已知脆弱性掃描	SSA-420	N/A	5.2.1.1 5.2.5.1
		2.2.2 軟/韌體更新機制	CR 3.10	3.5 3.6	5.2.3.2
		2.2.3 軟/韌體安全性評估	IEC 62443-4-1 SI-1		
		2.2.4 機敏資料保護	CR 4.1	5.15	5.2.4.1 5.2.4.2
		2.2.5 惡意程式防護	CR 3.2	4.12	N/A

		2.2.6 帳戶管理	CR 1.3	3.4	5.4.3.1
		2.2.7 事件日誌	CR 2.8	4.7	5.2.7.1 5.2.7.2
		2.2.8 事件日誌之儲存容量與效期	CR 2.9	N/A	5.2.7.3
	2.3 通訊資安	2.3.1 最小通訊埠要求	CR 7.7	N/A	5.2.2.1
		2.3.2 動態資料加密保護	CR 4.3	4.8	5.3.1.1
		2.3.3 動態資料加密保護-進階	CR 1.8 CR 4.3	4.8 5.14	5.3.1.1 5.3.1.2
		2.3.4 封包流量與指向分析	FR 5	N/A	N/A
	2.4 身分鑑別	2.4.1 人員使用者識別與鑑別	CR 1.1	3.3	5.4.3.1
		2.4.2 通行碼強度(長度基礎)	CR 1.7	3.2	5.4.2.2
		2.4.3 通行碼輸入頻次限制	CR 1.11	3.2	5.4.2.4
		2.4.4 預設通行碼變更機制	CR 1.5	3.2	5.4.2.1

附件 2：廠商自我檢查表

變流器本體單元廠商自我檢查表

基本資訊			
申請者：		填表日期：	
變流器是否具備內嵌式監視單元？		□是　請額外填寫監視單元廠商自我檢查表 □否 (請提供佐證資料)	

產品名稱	資安要求	資安等級	自我檢查	附加說明或佐證
變流器本體單元	1.1.1 實體防護	2	□符合 □不符合	(欄位不足可自行拉伸，或以註解方式將資訊顯示於本表末欄。)
	1.2.1 軟/韌體更新機制	1	□符合 □不符合	
	1.2.2 軟/韌體安全性評估	2	□符合 □不符合	
	1.3.1 人機介面身分鑑別(實體)	1	□符合 □不符合 □不適用	
	1.3.2 人機介面身分鑑別(無線)	1	□符合 □不符合 □不適用	
*佐證資料：				
(若說明欄格位不足時,可以附註方式將必要資訊呈現於此欄位,本欄位不限格式、可自行延伸。)				

監視單元廠商自我檢查表

基本資訊			
申請者：		填表日期：	
監視單元			
樣品樣態：	□ Smart Dongle □ Data logger/ PV Gateway/Data Recorder □ 工業電腦+軟體程式 □其他		
監視單元是否可控制、修訂變流器本體單元之電力相關參數或遠端執行本體單元之軟/韌體更新？		□是 □否 (請提供佐證資料)	

產品名稱	資安要求	資安等級	自我檢查	附加說明或佐證
監視單元	2.1.1 實體防護	2	□符合 □不符合	
	2.1.2 最小實體介面要求	1	□符合 □不符合	
	2.2.1 已知脆弱性掃描	1	□符合 □不符合	
	2.2.2 軟/韌體更新機制	1	□符合 □不符合	
	2.2.3 軟/韌體安全性評估	1	□符合 □不符合	
	2.2.4 機敏資料保護	1	□符合 □不符合	
	2.2.5 惡意程式防護	2	□符合 □不符合	
	2.2.6 帳戶管理	1	□符合 □不符合	
	2.2.7 事件日誌	1	□符合 □不符合	

	2.2.8 事件日誌之儲存容量/效期	2	□符合 □不符合	
	2.3.1 最小通訊埠要求	1	□符合 □不符合	
	2.3.2 動態資料加密保護	1	□符合 □不符合 □不適用	
	2.3.3 動態資料加密保護-進階	2	□符合 □不符合	
	2.3.4 封包流量與指向分析	1	□符合 □不符合	
	2.4.1 人員使用者識別與鑑別	1	□符合 □不符合	
	2.4.2 密碼強度(長度基礎)	1	□符合 □不符合 □不適用	
	2.4.3 密碼輸入頻次限制	1	□符合 □不符合 □不適用	
	2.4.4 預設密碼變更機制	1	□符合 □不符合 □不適用	
*佐證資料：				
(若說明欄格位不足時,可以附註方式將必要資訊呈現於此欄位,本欄位不限格式、可自行延伸。)				