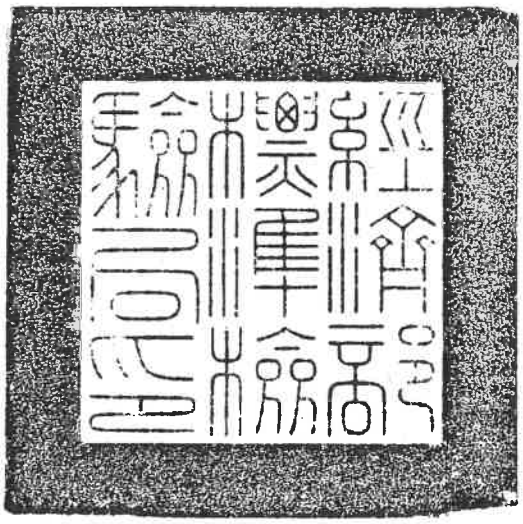
文號：1113051534

檔　　號：

保存年限：

經濟部標準檢驗局　公告

發文日期：中華民國111年8月2日
發文字號：經標三字第11130006550號
附件：電動車供電設備資訊安全檢測技術規範



裝

主旨：公告「電動車供電設備資訊安全檢測技術規範」，並自即日生效。

訂

依據：「自願性產品驗證實施辦法」第四條第三項。

公告事項：「電動車供電設備資訊安全檢測技術規範」（如附件）。

局長連錦漳

線

電動車供電設備資訊安全檢測技術規範

1. 電動車供電系統架構

圖 1 為電動車(Electric Vehicle, EV)供電系統基本架構示意圖，其中電動車供電設備(Electric Vehicle Supply Equipment, EVSE)為電動車提供電力；電動車供電設備營運商(Charge Point Operators, CPO)為負責營運電動車供電設備之廠商，主要可記錄電動車充電量、識別並允許電動車使用者充電等功能；配電系統營運商(Distribution System Operators, DSO)以自有配電網路發展分散式電力調控，推動電動車供電設備普及之營運商，主要確保供電設備供電穩定，以及記錄電動車充電量；虛線表示實體電力線的連接；實線則表示各介面的連接。

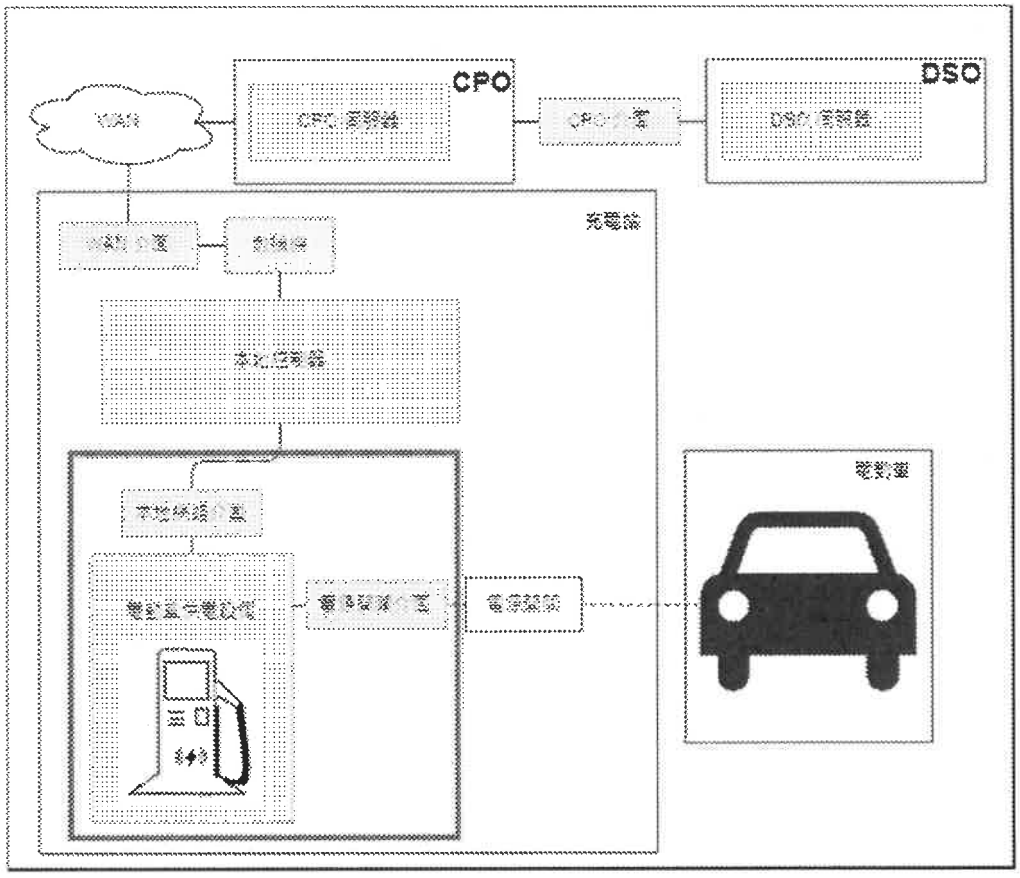


圖 1 電動車供電系統基本架構示意圖

2. 適用範圍

本技術規範之適用範圍如圖 1 中的電動車供電設備、本地網路介面及電源開關介面所示，即僅考量具有網路連線行為之電動車供電設備及充電樁上相關介面之網路安全要求，相關搭配使用之行動應用 App 與後端管理系統(包含 CPO 伺服器、DSO 伺服器及本地控制器)則非屬適用範圍。

本技術規範所規定的資訊安全要求，目的在確認電動車供電設備具有基礎資訊安全防護能力，包含：(1)實體安全、(2)系統安全、(3)韌體更新、(4)通訊安全、(5)身分鑑別與授權機制安全，以確保電動車供電設備之資訊安全。

3. 引用標準

下列標準之全部或部分，為本技術規範引用之相關文件，有加註年分時僅適用該版本，未加註時則適用該文件之最新版次(包含任何修訂)。

CNS 62351-2	電力系統管理及關聯資訊交換–資料及通訊安全–第 2 部：詞彙
IEC 62351-5：2013	Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 5: Security for IEC 60870-5 and Derivatives
IEC 62351-7：2017	Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 7: Network and System Management (NSM) Data Object Models
IEC 62351-9：2017	Power systems Management and Associated Information Exchange – Data and Communi-

	cations Security – Part 9: Cyber Security Key Management for Power System Equipment
IEC 62443-3-3：2013	Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels
CNS 62443-4-1	工業自動化及控制系統之安全性 – 第 4-1 部：產品開發生命週期之安全要求事項
IEC 62443-4-2：2019	Security for Industrial Automation and Control Systems – Part 4-2: Technical Security Requirements for IACS Components
ENCS EV-301：2019	EV Charging Systems Security Requirements
FIPS PUB 140-2 Annex A：2021	Security Requirements for Cryptographic Modules
NIST SP 800-52 Revision 2：2019	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
NIST 800-140C：2021	CMVP Approved Security Functions
NIST 800-131A：2019	Transitioning the Use of Cryptographic Algorithms and Key Lengths
UL 2900-1：2017	Software Cybersecurity for Network-Connectable Products, Part 1：General Requirements

4.用語及定義

4.1 電動車 (Electric Vehicles, EVs)

指在道路上使用，且由可充電蓄電池、燃料電池、太陽光電組列或其他方式提供電力至電動機，作為主要動力之電動車。

4.2 電動車充電站(EV Charging Station)

連接供電網路之電動車供電設備的定置部分。

4.3 電動車供電設備(EV Supply Equipment, EVSE)

提供專用功能，自固定之電氣設施或供電網路供應電能至電動車進行充電之設備或設備的組合。

4.4 電動車充電系統(EV Charging System)

完整的系統包括電動車供電設備及依充電目的之要求對電動車供應電能的功能。

4.5 交流電動車充電站(AC EV Charging Station)

供應電動車交流電之電動車充電站。

4.6 交流電動車供電設備(AC EV Supply Equipment)

供應電動車交流電之電動車供電設備，且其額定供電電壓在 1,000 Vac 以下。

4.7 直流電動車充電站(DC EV Charging Station)

供應電動車直流電之電動車充電站。

4.8 直流電動車供電設備(DC EV Supply Equipment)

供應電動車直流電之電動車供電設備，且其額定供電電壓在 1,500 Vdc 以下。

4.9 鑑別符(Authenticator)

用以確認個體身分之方法，如通行碼(password)、指紋或感應磁卡

等。

4.10 電動車供電設備營運商(Charge Point Operators, CPO)

泛指負責營運電動車供電設備之廠商。

4.11 充電(Charging)

調節經由交流或直流供電網路提供電壓及/或電流所需之所有功能，以確保供應 RESS 電能。

4.12 密碼套件(Cipher Suite)

係指使用於安全通道(Secure Sockets Layer / Transport Layer Security, SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分驗證、加密、訊息鑑別碼(Message Authentication Code, MAC)及金鑰交換演算法。

4.13 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，針對每一資訊安全脆弱性項目給予全球認可之唯一共通編號。

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

依資訊安全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)發起，現由美國資訊安全事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)提供的脆弱性評分系統，以衡量軟體脆弱性的特徵及嚴重性進行評分，目前為第 3.1 版。

4.15 阻斷服務攻擊(Denial-of-Service Attack, DoS Attack)

使目標資訊系統的網路或計算資源耗盡，導致服務暫時中斷或停止，

讓使用者無法正常存取，例：洪水攻擊(Flooding)。

4.16 配電系統營運商(Distribution System Operators, DSO)

以自有配電網路發展分散式電力調控，推動電動車供電設備普及之營運商。

4.17 本地控制器(Local Controller)

泛指電動車供電設備的控制中心，負責處理電動車充電站的所有資料。

4.18 開放式充電點協定(Open Charge Point Protocol, OCPP)

一種電動車供電設備與後端管理系統(包含 CPO 伺服器、DSO 伺服器及本地控制器)間的應用層通訊協定，目的在讓後端管理系統可與不同製造商的電動車供電設備互相通訊。

4.19 通行碼(Password)

指一組能讓使用者使用系統或用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。

4.20 個人資料(Personally Identifiable Information)

依「個人資料保護法」第 2 條第 1 款定義為自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

4.21 重送攻擊(Replay Attack)

指一種網路攻擊手法，透過惡意重複或拖延正常的資料傳輸而實施。

4.22 敏感性資料(Sensitive Data)

指洩漏時可能對使用者造成損害之資料，包括但不限於個人資料、

通行碼、金鑰或地理位置等。此等資料依使用者行為於供電設備及其附屬儲存媒體之建立、儲存或傳輸。

5.安全構面與資訊安全要求

5.1 安全構面

本技術規範包含電動車供電設備之實體安全、系統安全、韌體更新、通訊安全，以及身分鑑別與授權機制安全等構面，說明如下：

(a) 實體安全：電動車供電設備的實體介面需有一定防禦能力，包含當系統故障時期。電動車供電設備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。

(b) 系統安全：確保系統的防禦能力，包含安全日誌功能、可抵禦阻斷服務攻擊等。

(c) 韌體更新：電動車供電設備之韌體版本更新服務等，須具備足夠安全防護。電動車供電設備之作業系統、應用程式或韌體及所儲存之資料等，亦應具備足夠之資訊安全防護。

(d) 通訊安全：電動車供電設備與傳輸之資料應具有足夠安全之防護，避免遭受蓄意人士入侵。電動車供電設備之通訊應採已知最佳實踐方式架構，對敏感性資料之傳輸，亦應加密保護，以確保通訊安全。

(e) 身分鑑別與授權機制安全：對每個可存取電動車供電設備介面均須建立識別、鑑別與授權機制，以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，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 資訊安全等級

本技術規範將各項資訊安全要求等級依(1)相關資安風險高低、(2)技術實現複雜度綜合考量，分為 1 級、2 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。對於資訊安全等級之說明，整理於表 1。

表 1 電動車充電供電設備資訊安全等級說明

資訊安全等級	說明	備考
1 級	防止無心之操作誤會、不成熟之攻擊行為或攻擊者無足夠資源之蓄意攻擊行為。	電動車供電設備之基礎資訊安全要求。
2 級	防止蓄意且有資源之攻擊行為。	電動車供電設備之進階資訊安全要求。

5.3 安全構面與要求概述

安全構面與要求如表 2 所示，第 1 欄為安全構面，包含：(1)實體安全、(2)系統安全、(3)韌體更新、(4)通訊安全、(5)身分鑑別與授權機制安全；第 2 欄為安全要求，係依第 1 欄安全構面設計之對應安全要求；第 3 欄為安全要求項目，須依循第 6 節所規定內容。各資訊安全要求相應之標準規範要求事項對照表，彙整於附錄 A。

5.4 資安要求檢測方式

屬適用範圍之電動車供電設備於測試前，需填具自我檢查表，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，自我檢查表格式如附件一。針對電動車供電設備之資安要求與檢測方式，如附件二所示。

表 2　安全構面與資訊安全要求總表

安全構面	資訊安全要求	安全要求項目	資訊安全等級	
			1 級	2 級
6.1 實體安全	6.1.1 實體介面最小化要求	6.1.1.1	V	V
	6.1.2 防止實體操作	6.1.2.1	V	V
		6.1.2.2	V	V
6.2 系統安全	6.2.1 設備強化	6.2.1.1	V	V
		6.2.1.2	V	V
	6.2.2 事件日誌	6.2.2.1	V	V
		6.2.2.2		V
		6.2.2.3	V	V
		6.2.2.4		V
	6.2.3 作業系統與網路服務	6.2.3.1	V	V
		6.2.3.2		V
	6.2.4 敏感性資料備份	6.2.4.1		V
6.3 韌體更新	6.3.1 更新安全	6.3.1.1	V	V
		6.3.1.2	V	V
		6.3.1.3		V
	6.3.2 安全版本	6.3.2.1	V	V
		6.3.2.2	V	V
6.4 通訊安全	6.4.1 傳輸資料保護	6.4.1.1	V	V
		6.4.1.2		V
		6.4.1.3		V
		6.4.1.4	V	V
	6.4.2 敏感性資料儲存	6.4.2.1	V	V
		6.4.2.2		V
6.5 身分鑑別與授權機制安全	6.5.1 身分鑑別	6.5.1.1	V	V
		6.5.1.2	V	V
		6.5.1.3	V	V
		6.5.1.4		V
		6.5.1.5		V
		6.5.1.6		V
	6.5.2 帳戶管理	6.5.2.1	V	V
	6.5.3 存取控制	6.5.3.1	V	V
		6.5.3.2	V	V
		6.5.3.3		V

6. 資訊安全要求

本節詳盡載明電動車供電設備為滿足安全功能應採取的方法，電動車供電設備應符合本節中所有資訊安全基本要求。

6.1 實體安全

6.1.1 實體介面最小化要求

6.1.1.1 電動車供電設備應將不需使用的介面及序列埠移除。

6.1.2 防止實體操作

6.1.2.1 能夠識別對電動車供電設備之實體操作行為與供電設備之狀態。

6.1.2.2 電動車供電設備本體應建立外殼拆除障礙或保有實體遭拆解之紀錄。

6.2 系統安全

6.2.1 設備強化

6.2.1.1 電動車供電設備應刪除不需要的應用程式。

6.2.1.2 電動車供電設備僅使用最小需要的通訊埠。

6.2.2 事件日誌

6.2.2.1 電動車供電設備應具安全日誌功能並紀錄事件。

6.2.2.2 電動車供電設備應支援安全日誌異地備份功能。

6.2.2.3 電動車供電設備應具備時間同步機制。

6.2.2.4 電動車供電設備發生使用者異常登入安全事件時，應具備主動告警機制，包括回報管理者或推播警示、告警及供電設備識別碼編號等訊息。

6.2.3 作業系統與網路服務

6.2.3.1 電動車供電設備之作業系統與網路服務，不應存在美國國家弱點資料庫所公開的常見弱點與脆弱性資料 CVE，且共同脆弱性評分系統 CVSS 最新版本之分數評比 7 分以上或嚴重性等級評比

為高(High)以上者。

6.2.3.2 電動車供電設備應具有抵禦阻斷服務攻擊的能力，避免電動車供電設備因資源耗盡或收到錯誤訊息時，導致長時間無法使用。

6.2.4 敏感性資料備份

6.2.4.1 電動車供電設備應提供敏感性資料備份功能。

6.3 韌體更新

6.3.1 更新安全

6.3.1.1 電動車供電設備應支援更新功能。

6.3.1.2 電動車供電設備進行韌體更新時，即使發生更新失敗，系統應仍能回復正常運作。

6.3.1.3 電動車供電設備之韌體更新，其韌體應具保護機制，使韌體之程式碼無法被解析；若採安全通道進行更新，則安全通道版本及密碼套件應符合附錄 B 之要求。

6.3.2 安全版本

6.3.2.1 電動車供電設備的韌體版本應受管制。

6.3.2.2 廠商應能提供每個韌體的加密雜湊值作為韌體版本之追溯管控。

6.4 通訊安全

6.4.1 傳輸資料保護

6.4.1.1 敏感性資料應加密傳輸，若採安全通道進行傳輸，其版本及密碼套件應符合附錄 B 的要求。

6.4.1.2 電動車供電設備應清楚提供通訊協定版本。

6.4.1.3 電動車供電設備應設定允許連線的協定版本最小值，拒絕與舊版本的協定連線。

6.4.1.4 電動車供電設備連接網路時，不應對未宣告的 IP 進行封包傳輸。

6.4.2 敏感性資料儲存

6.4.2.1 電動車供電設備所儲存之敏感性資料應加密儲存。

6.4.2.2 電動車供電設備所儲存之敏感性資料其加密方式應採用符合 FIPS PUB 140-2 Annex A 、NIST SP 800-140C 或 NIST SP 800-131A 規定之同等或以上強度的加密演算法。

6.5 身分鑑別與授權機制安全

6.5.1 身分鑑別

6.5.1.1 每一台電動車供電設備都應有一組識別碼並受管制。

6.5.1.2 電動車供電設備應具備身分鑑別機制。

6.5.1.3 使用者之初次鑑別若採公開取得之預設通行碼，則各產品之預設通行碼應相異，或於首次登入後，應有強制使用者變更預設通行碼之機制。

6.5.1.4 對於身分鑑別所使用之通行碼強度應有一定規則之要求，以避免被輕易破解並遭不當利用。

6.5.1.5 進行遠端操控電動車供電設備時，應具防止重送攻擊之機制。

6.5.1.6 若使用者在多次登入電動車供電設備失敗後，電動車供電設備將臨時或永久拒絕該使用者的請求，登入次數與時間應可設定。

6.5.2 帳戶管理

6.5.2.1 電動車供電設備不得包含常見預設帳戶。

6.5.3 存取控制

6.5.3.1 電動車供電設備應能設置白名單僅允許特定主機可存取。

6.5.3.2 電動車供電設備應提供人員至少二階層以上之存取權限。

6.5.3.3 電動車供電設備應允許定義新的角色。

附錄 A
(參考)
標準規範要求事項對照表

安全要求項目	IEC 62351 系列	IEC 62443 系列	其他相關資訊安全規範
6.1.1.1		CNS 62443-4-1 SD-4	ENCS EV-301 OP10-CS
6.1.2.1		IEC 62443-3-3 SR 1.2	
6.1.2.2		IEC 62443-4-2 CR 3.11、IEC 62443-4-2 EDR3.11	ENCS EV-301 PH3-CS
6.2.1.1		IEC 62443-3-3 SR 7.7	
6.2.1.2		IEC 62443-3-3 SR 7.7	
6.2.2.1		IEC 62443-4-2 CR 1.12	
6.2.2.2			ENCS EV-301 OP5-CS
6.2.2.3		IEC 62443-3-3 SR 2.11 RE 1	
6.2.2.4		IEC 62443-3-3 SR 3.3	ENCS EV-301 OP4-CS
6.2.3.1		CNS 62443-4-1 SVV-3 、CNS 62443-4-1 DM-3	ENCS EV-301 OP11-CS
6.2.3.2		IEC 62443-3-3 SR	ENCS EV-301

		7.1、IEC 62443-4-2 CR 7.1	CM5-CS
6.2.4.1		IEC 62443-3-3 SR 7.4	
6.3.1.1		IEC 62443-4-2 CR 3.10、IEC 62443-4-2 EDR 3.10、IEC 62443-4-2 NDR 3.10	
6.3.1.2		IEC 62443-3-3 SR 7.4	
6.3.1.3	IEC 62351-5 5.4.10	CNS 62443-4-1 SUM-4	
6.3.2.1		IEC 62443-4-2 CR 1.2	
6.3.2.2		CNS 62443-4-1 SUM-4	
6.4.1.1	IEC 62351-5 5.4.10	IEC 62443-3-3 SR 4.1、IEC 62443-3-3 SR 4.3	
6.4.1.2	IEC 62351-7 5.4		
6.4.1.3			NIST SP 800-52 Revision 2
6.4.1.4		IEC 62443-4-2 FR 5	
6.4.2.1		IEC 62443-4-2 CR 4.1	
6.4.2.2		IEC 62443-4-2 CR 1.7	FIPS PUB 140-2 Annex A、NIST

			SP 800-140C 、NIST SP 800-131A
6.5.1.1	IEC 62351-5 7.2.8.4 、IEC 62351-7 5.10.2	IEC 62443-3-3 SR 1.2	
6.5.1.2		IEC 62443-4-2 EDR 2.13、IEC 62443-4-2 NDR 1.13	
6.5.1.3		IEC 62443-4-2 CR 1.5	
6.5.1.4		IEC 62443-3-3 SR 1.7 、IEC 62443-4-2 CR 1.7	UL 2900-1 8.3(b)、8.3(c)
6.5.1.5		IEC 62443-3-3 SR 3.8 、IEC 62443-4-2 CR 3.8	ENCS EV-301 CM1-CS
6.5.1.6		IEC 62443-3-3 SR 1.11 、IEC 62443-4-2 CR 1.11	
6.5.2.1		CNS 62443-4-1 SG-6	
6.5.3.1		IEC 62443-3-3 SR 5.2 RE 1	
6.5.3.2		IEC 62443-3-3 SR 2.1 、IEC 62443-4-2 CR 2.1	
6.5.3.3		IEC 62443-3-3 SR 2.1 RE 2	

附錄 B
(規定)
安全通道版本及密碼套件使用要求

指超文件傳輸協定(HTTP)結合安全接套層協定(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；然而安全接套層協定在 2014 年 10 月由 Google 指出其資訊安全脆弱性，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接套層協定。但傳輸層安全性協定 v1.0 同樣不被信任，因此目前本技術規範應使用的版本為：傳輸層安全性協定 v1.2 同等或以上之版本。

以下為各版本安全通道(TLS)可選用之密碼套件：

- TLSv1.2
  - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256

附件一

電動車供電設備自我檢查表

基本資訊			
申請者		填表日期	
商品名稱		廠牌	

1.測試時，是否有其他配合之營運商？

□是，營運商為：

□否

2.產品是否具有遠端操控功能?

□是，請說明遠端操控功能之用途：eg 軟韌體更新、故障維修、

□否

3. 產品是否支援開放式充電點協定(OCPP)?

□是，OCPP 版本： eg V1.6、V 2.0

□否，其他：

產品名稱	安全要求	安全要求項目	資安等級	自我檢查	附加說明或佐證
電動車供電設備	6.1.1 實體介面最小化要求	6.1.1.1	1	□符合 □不符合	
	6.1.2 防止實體操作	6.1.2.1	1	□符合 □不符合	
		6.1.2.2	1	□符合 □不符合	
	6.2.1 設備強化	6.2.1.1	1	□符合 □不符合	
		6.2.1.2	1	□符合 □不符合	
	6.2.2 事件日誌	6.2.2.1	1	□符合 □不符合	
		6.2.2.2	2	□符合	

				□不符合	
		6.2.2.3	1	□符合 □不符合	
		6.2.2.4	2	□符合 □不符合	
	6.2.3 作業系統與網路服務	6.2.3.1	1	□符合 □不符合	
		6.2.3.2	2	□符合 □不符合	
	6.2.4 敏感性資料備份	6.2.4.1	2	□符合 □不符合	
	6.3.1 更新安全	6.3.1.1	1	□符合 □不符合	
		6.3.1.2	1	□符合 □不符合	
		6.3.1.3	2	□符合 □不符合	
	6.3.2 安全版本	6.3.2.1	1	□符合 □不符合	
		6.3.2.2	1	□符合 □不符合 □不適用	
	6.4.1 傳輸資料保護	6.4.1.1	1	□符合 □不符合	
		6.4.1.2	2	□符合 □不符合	
		6.4.1.3	2	□符合 □不符合	
		6.4.1.4	1	□符合 □不符合	

	6.4.2 敏感性資料儲存	6.4.2.1	1	□符合 □不符合	
		6.4.2.2	2	□符合 □不符合	
	6.5.1 身分鑑別	6.5.1.1	1	□符合 □不符合	
		6.5.1.2	1	□符合 □不符合	
		6.5.1.3	1	□符合 □不符合	
		6.5.1.4	2	□符合 □不符合	
		6.5.1.5	2	□符合 □不符合	
		6.5.1.6	2	□符合 □不符合 □不適用	
	6.5.2 帳戶管理	6.5.2.1	1	□符合 □不符合	
	6.5.3 存取控制	6.5.3.1	1	□符合 □不符合	
		6.5.3.2	1	□符合 □不符合	
		6.5.3.3	2	□符合 □不符合	
*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。）					

附件二

電動車供電設備之資安要求與檢測方式

資安要求	說明	檢測方式	結果	等級
6.1.1 實體介面最小化要求	6.1.1.1 電動車供電設備應將不需使用的介面及序列埠移除。	1. 廠商應提供文件說明實體介面之目的及相關保護措施。 2. 檢視待測物外觀並清點實體介面，其結果應與廠商之說明文件相符，否則本項不符合。 3. 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，否則本項不符合。	1.符合 2.不符合	1
6.1.2 防止實體操作	6.1.2.1 能夠識別對電動車供電設備之實體操作行為與供電設備之狀態。	1. 廠商應提供相關文件，說明待測物具備其實體操作行為與供電狀態之告知機制(如螢幕顯示或語音告知方式呈現)。 2. 檢視待測物之告知機制應與廠商所附文件一致。	1.符合 2.不符合	1
	6.1.2.2 電動車供電設備本體應建立外殼拆除障礙或保有實體遭拆解之紀錄。	檢視待測物之外殼，應一體成形、或具實體鎖、或設計於可上鎖之箱體內、或採防拆螺絲、或使用一次性貼紙，以建立拆除障礙。	1.符合 2.不符合	1
6.2.1 設備強化	6.2.1.1 電動車供電設備應	1. 廠商應提供相關文件，說明待測物中所安裝之應用程式清單	1.符合 2.不符合	1

	刪除不需要的應用程式。	及其作用，以及如何進入系統查詢應用程式之操作方法；若操作設有權限，亦應提供具該權限之帳號與鑑別符。 2. 依據廠商所提供之說明文件對待測物進行操作，若其應用程式與清單所載不一致，則本項不符合。		
	6.2.1.2 電動車供電設備僅使用最小需要的通訊埠。	1. 廠商應說明待測物開通之通訊埠與開通原因。 2. 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，則本項不符合。 3. 將待測物與測試電腦連接，啟用具網路埠掃描功能之工具，對待測物執行 TCP 埠、UDP 埠及埠 0 之掃描。 4. 比對掃描結果應與廠商說明一致，否則本項不符合。	1.符合 2.不符合	1
6.2.2 事件日誌	6.2.2.1 電動車供電設備應具安全日誌功能並紀錄事件。	1. 安全日誌可存在於待測物（本地端）或遠端內。 2. 安全日誌應至少包含： (1)韌體更新紀錄 (2)緊急/異常事件 (3)實體介面存取及遠端遙控事件（如有遠端控制功能） 且每一事件應可由紀錄中辨	1.符合 2.不符合	1

		識事件時間、事件種類與誘發事件之來源身份（可能為人員或設備）。 3. 安全日誌之存取應設有權限管理。廠商應說明存取安全日誌之操作方式，並提供具存取權限之帳號與鑑別符。 4. 檢視安全日誌，其內容應符合第 2 點之要求，否則本項不符合。		
	6.2.2.2 電動車供電設備應支援安全日誌異地備份功能	1. 廠商應說明觸發日誌紀錄之事件。 2. 依說明觸發數個事件，事件應被紀錄於安全日誌中，且該日誌應可儲存於異地。 3. 廠商應提供存取異地安全日誌之操作方式，以及測試用帳號與鑑別符。 4. 查詢第 2 點所觸發之事件皆確實登載於日誌中；若無法提供測試用帳號與鑑別符，則廠商應提供資料，佐證所觸發之事件皆登載於日誌中。	1.符合 2.不符合	2
	6.2.2.3 電動車供電設備應具備時間同步機制。	1. 廠商應提供設定同步校時之操作方式；若操作設有權限，亦應提供具該權限之帳號與鑑別符。 2. 依說明設定同步校時後，應	1.符合 2.不符合	1

		能顯示正確時間。		
	6.2.2.4 電動車供電設備發生使用者異常登入安全事件時，應具備主動告警機制，包括回報管理者或推播警示、告警及供電設備識別碼編號等訊息。	1. 廠商應提供自定義異常登入安全事件之說明。異常登入安全事件包含但不限於： (1) 輸入通行碼超過頻次限制。 (2) 非白名單上之主機嘗試進行遠端登入。 2. 廠商應說明待測物發生異常登入安全事件時的告警機制。 3. 觸發異常登入安全事件，並檢視待測物之告警機制，其結果應與廠商說明一致，否則本項不符合。	1.符合 2.不符合	2
6.2.3 作業系統與網路服務	6.2.3.1 電動車供電設備之作業系統與網路服務，不應存在美國國家弱點資料庫所公開的常見弱點與脆弱性資料 CVE，且共同脆弱性評分系統 CVSS 最新版本之分數評比 7 分以上或嚴重性等	1. 使用弱點識別工具對待測物進行弱點掃描，脆弱性識別應依共同脆弱性評分系統（CVSS）進行判定。 2. 若測得共同脆弱性及暴露（CVE）編號之漏洞，且其 CVSS 最新版本之分數大於等於 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	1

	級評比為高(High)以上者。			
	6.2.3.2 電動車供電設備應具有抵禦阻斷服務攻擊的能力，避免電動車供電設備因資源耗盡或收到錯誤訊息時，導致長時間無法使用。	1. 廠商應提供資料佐證待測物具備抵禦阻斷服務攻擊之能力。 2. 針對待測物進行阻斷服務攻擊，則待測物所提供之服務於攻擊期間應能正常運作。	1.符合 2.不符合	2
6.2.4 敏感性資料備份	6.2.4.1 電動車供電設備應提供敏感性資料備份功能	1. 待測物之敏感性資料應具備異地備份之功能。 2. 廠商應敘述備份之方式並提供備份操作說明；若操作設有權限，亦應提供具該權限之帳號與鑑別符。 3. 依據廠商之操作說明應可成功備份敏感性資料。	1.符合 2.不符合	2
6.3.1 更新安全	6.3.1.1 電動車供電設備應支援更新功能。	1. 待測物核心功能之韌體應有更新機制，以修補漏洞或擴充功能，且更新行為應設有權限管理。廠商應提供以下項目： (1) 可更新之韌體清單 (2) 韌體更新保護機制說明文件	1.符合 2.不符合	1

		(3) 更新韌體之操作程序 (4) 可供更新之檔案 (5) 具更新權限之帳戶與識別符 2. 依廠商所提供之項目，待測物應可成功更新其韌體。		
	6.3.1.2 電動車供電設備進行韌體更新時，即使發生更新失敗，系統應仍能回復正常運作。	1. 對廠商提供之韌體檔案進行修改，或以其他來源之韌體對待測物進行更新，應有查覺韌體錯誤並拒絕更新之機制，否則本項不符合。 2. 遇有更新中斷之情形（如斷開電源或通訊連線），待測物應能回復更新前之狀態或進入待機狀態。待測物重新完成更新後應能正常運作。	1.符合 2.不符合	1
	6.3.1.3 電動車供電設備之韌體更新，其韌體應具保護機制，使韌體之程式碼無法被解析；若採安全通道進行更新，則安全通道版本及密碼套件應符合附錄 B 之要求。	1. 若待測物不具備更新能力則本項不符合。 2. 若待測物之韌體採安全通道進行更新，則安全通道版本及密碼套件應合於附錄 B 之要求，否則本項不符合。 3. 若待測物非採安全通道進行韌體更新，則韌體應加密保護，或無法經由反組譯解出韌體之明文程式碼。	1.符合 2.不符合	2

6.3.2 安全版本	6.3.2.1 電動車供電設備的韌體版本應受管制。	1. 廠商應提供資料佐證韌體版本之序號受有管制（如：序號編碼方式、序號清單管制文件）。 2. 廠商應提供查詢待測物韌體版本資訊之操作說明，而操作後所查得之版本應與廠商所提供之資料相符。	1.符合 2.不符合	1
	6.3.2.2 廠商應能提供每個韌體的加密雜湊值作為韌體版本之追溯管控。	1. 韌體若採安全通道方式進行更新，則本項可申明為不適用。 2. 廠商應提供韌體版本與其加密雜湊值對照表，並置於網站上或使用者可取得之處。 3. 依廠商所述之方式加密韌體後，所得加密雜湊值應與對照表一致，否則本項不符合。	1.符合 2.不符合 3.不適用	1
6.4.1 傳輸資料保護	6.4.1.1 敏感性資料應加密傳輸，若採安全通道進行傳輸，其版本及密碼套件應符合附錄 B 的要求。	1. 建立待測物之網路通道，並進行相關操作以觸發待測物之網路行為。 2. 廠商應提供針對敏感性資料傳輸加密之機制。 3. 查看傳輸具敏感性資料之網路封包，其應受加密保護；若採用安全通道進行傳輸，則安全通道版本及密碼套件應符合附錄 B 之要求。	1.符合 2.不符合	1
	6.4.1.2 電動	檢視廠商提供之相關證明或說明	1.符合	2

	車供電設備應清楚提供通訊協定版本。	文件是否符合本項之要求。	2.不符合	
	6.4.1.3 電動車供電設備應設定允許連線的協定版本最小值，拒絕與舊版本的協定連線。	1. 廠商應提供連線協定版本最小值之設定方式。 2. 經設定後，以低於最小值之協定版本與待測物連線，待測物應拒絕之，否則本項不符合。	1.符合 2.不符合	2
	6.4.1.4 電動車供電設備連接網路時，不應對未宣告的IP進行封包傳輸。	1. 廠商應宣告待測物預期會連結之伺服器 IP 位址及其他可能位置。 2. 將待測物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待測物之封包至少 24 小時。 3. 檢查側錄之封包，其目的地位址應與廠商所宣告之內容相符，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，則本項不符合。	1.符合 2.不符合	1
6.4.2 敏感性資料儲存	6.4.2.1 電動車供電設備所儲存之敏感性資料應加密儲存。	1. 敏感性資料包括但不限於金鑰、憑證、關鍵數據、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	1.符合 2.不符合	1

		敏感性資料之說明。 2. 敏感性資料儲存於待測物時，應先進行加密。廠商應提供說明佐證待測物具備該保護機制，並提供存取敏感性資料之方式及路徑。 3. 嘗試存取敏感性資料，其內容應為密文之形式，否則本項不符合。		
	6.4.2.2 電動車供電設備所儲存之敏感性資料其加密方式應採用符合FIPS PUB 140-2 Annex A 、NIST SP 800-140C 或NIST SP 800-131A 規定之同等或以上強度的加密演算法。	1. 廠商應提供待測物所儲存之敏感性資料加密保護演算法作為審查依據。 2. 依廠商提供之演算法及密鑰對敏感性資料進行加密，所得結果應與儲存於待測物中之敏感性資料密文一致；廠商若無法提供密鑰，則應提供資料佐證之。	1.符合 2.不符合	2
6.5.1 身分鑑別	6.5.1.1 每一台電動車供電設備都應有一組識別碼並受管制。	1. 廠商應提供資料佐證待測物之識別碼受有管制（如：識別碼編碼方式、識別碼清單管制文件）。 2. 廠商應提供查詢待測物識別碼之操作方式。	1.符合 2.不符合	1

		3. 依操作檢視其識別碼，該識別碼應與廠商提供之佐證資料相符。		
	6.5.1.2 電動車供電設備應具備身分鑑別機制	1. 待測物之存取（實體操作或遠端登入）及進入除錯模式(若具備除錯模式)應具備身分鑑別機制，且其鑑別符不可公開取得（預設通行碼除外）。 2. 廠商應提供存取待測物及進入除錯模式之操作方式。 3. 待測物於存取及進入除錯模式時，應能要求身份鑑別，並於通過鑑別後得進行相應之操作。	1.符合 2.不符合	1
	6.5.1.3 使用者之初次鑑別若採公開取得之預設通行碼，則各產品之預設通行碼應相異，或於首次登入後，應有強制使用者變更預設通行碼之機制	1. 審閱產品之預設通行碼設計文件，檢視產品是否存在相同之預設通行碼，若相異則本項符合。 2. 若存有相同之產品預設通行碼，則首次登入成功後，系統應要求更改預設通行碼，否則本項不符合。 3. 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。	1.符合 2.不符合	1
	6.5.1.4 對於身分鑑別所使	1. 若通行碼為人員使用者自行定義，則通行碼之複雜性要	1.符合 2.不符合	2

	用之通行碼強度應有一定規則之要求，以避免被輕易破解並遭不當利用。	求應符合下列最小需求：(A)不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元；(B)長度至少為 8 個字元；(C)包含下列 4 種字元中的 3 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：!、$、#、%) 2. 檢視廠商說明並進行相應帳號登入操作，若通行碼要求與廠商說明相符，則本項符合。		
	6.5.1.5 進行遠端操控電動車供電設備時，應具防止重送攻擊之機制。	1. 以廠商提供之測試用帳號與鑑別碼登入待測物，側錄待測物與遠端主機間之通訊封包，並擷取其交談識別碼。 2. 登出帳號。 3. 將前步驟中之交談識別碼，透過測試工具執行重送攻擊，待測物應能拒絕之。	1.符合 2.不符合	2
	6.5.1.6 若使用者在多次登入電動車供電設備失敗後，電動車供電設備將臨時或永	1. 若待測物不以通行碼作為其身份鑑別之方式，則本項可申明為不適用。 2. 除廠商特意申明之「最低權限使用者」(如僅具閱覽展示資訊之權限)，其餘使用者之	1.符合 2.不符合 3.不適用	2

	久拒絕該使用者的請求，登入次數與時間應可設定。	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。 3. 依廠商提供之測試帳號及通行碼登入待測物，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，否則本項不符合。		
6.5.2 帳戶管理	6.5.2.1 電動車供電設備不得包含常見預設帳戶。	輸入常見預設帳號（root、admin、administrator、user、guest）於登入介面中，待測物應無法識別之。	1.符合 2.不符合	1
6.5.3 存取控制	6.5.3.1 電動車供電設備應能設置白名單僅允許特定主機可存取。	1. 廠商應提供相關文件，說明待測物設置白名單之操作方式。設定幾組主機之IP或MAC address於電動車供電設備之白名單。 2. 嘗試以非白名單內之IP或MAC address存取待測物，待測物應拒絕存取。	1.符合 2.不符合	1
	6.5.3.2 電動車供電設備應提供人員至少二階層以上之存取權限。	1. 待測物中應有至少二階層以上之使用者身分區別及其相應存取權限之設計，且應符合最少權限原則。 2. 廠商應就各階身分可存取待測物之途徑提供說明。	1.符合 2.不符合	1

		3. 使用者可存取待測物之介面可存在於本地端或遠端（管理系統），帳戶管理要求可於任一端實踐之。 4. 廠商應就第 1～3 點所述提出書面說明，以審閱判斷是否符合要求。 5. 廠商應說明各階身分權限行為之差異（如：低中高三階身分，低權限僅可瀏覽或查詢，中權限還可調整時間，高權限還可創建新角色），並應提供測試用帳戶。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進行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： (1) 存取敏感性資料（除該使用者本身之帳號或隱私資訊）之權限。 (2) 進行韌體更新之權限。		

		(3) 遠端控制行為之權限。		
	6.5.3.3 電動車供電設備應允許定義新的角色。	1. 廠商應提供文件，說明待測物創建新角色並設定其權限之方式；若上述操作設有權限，亦應提供具該權限之帳號與鑑別符。 2. 依操作應可於待測物上創建新角色及設定其權限，並能以該新角色成功登入設備及執行其權限行為。	1.符合 2.不符合	2