

# 從生態系看充電樁之資通安全保護

主講人：查士朝

國立臺灣科技大學 資訊管理系      教授兼系主任  
資通安全研究與教學中心 主任



# 大綱



充電樁的資安風險

目前充電樁的資安規範與缺口

從設備的資安到維運時的資安考量

結論



## 充電樁的資安風險

目前充電樁的資安規範與缺口

從設備的資安到維運時的資安考量

結論

## 雖然歐美開始在討論電動車是否環保的議題，但應該還是很可觀

- EEI (Edison Electronic Institute) 在 2022 年預估，到 2030 年，美國電動車將到達 264,000,000 輛
- Grand View Research 在 2022 年預估，到 2030 年，美國電動車相關骨幹的市場規模將達到 24,000,000,000 美金

🏠 > 日報 > 工商時報 >

### 美2032年電動車普及目標 砍半

2024.04.09 / 03:00 / 工商時報 顏嘉南

---

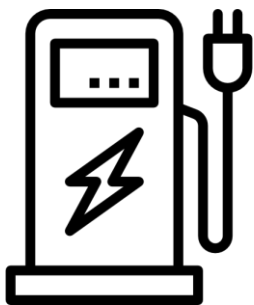
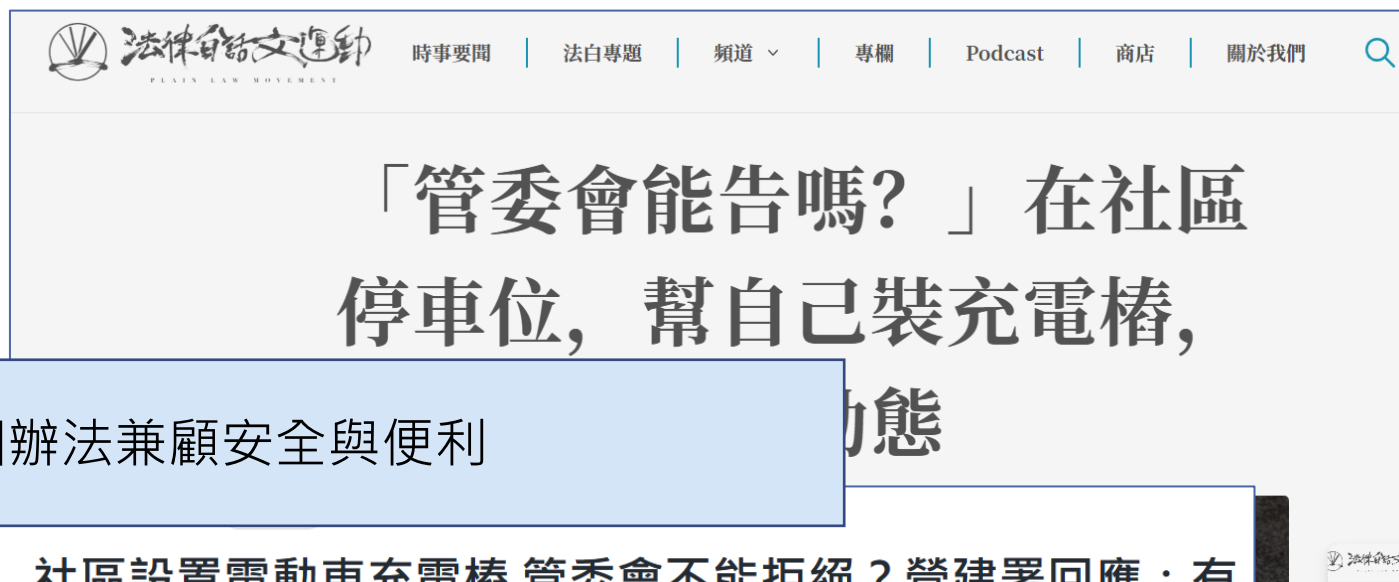
 拜登內閣頒布史上最嚴格的汽車廢氣排放標準，但也對汽車產業做出巨大讓步，將2032年前的電動車普及率目標幾乎對砍至35%，給予業者更多時間讓燃油車退場，意味著美國轉型至電動車將比預期耗費更多時間。

<https://www.ctee.com.tw/news/20240409700118-439901>

# 充電樁的安全問題目前有許多爭議

<https://plainlaw.me/posts/can-the-committee-sue>



## 社區設置電動車充電樁 管委會不能拒絕？營建署回應：有先決條件



徐筱嵐

2022年6月16日



隨著電動車日漸增多，社區內是否設置充電樁，引發正反兩面不同爭議，日前傳出，內政部營建署曾宣稱若無正當理由，管委會不得拒絕。營建署表示，《公寓大廈管理條例》修正版本的優先評估電動車充電系統設置，以基於確保用電安全與消防安全的前提下，尊重社區自治與公眾利益的決定，「並非不得拒絕」。

<https://tw.news.yahoo.com/%E7%A4%BE%E5%8D%80%E8%A8%AD%E7%BD%AE%E9%9B%BB%E5%8B%95%E8%BB%8A%E5%85%85%E9%9B%BB%E6%A8%81-%E7%AE%A1%E5%A7%94%E6%9C%83%E4%B8%8D%E8%83%BD%E6%8B%92%E7%B5%95-%E7%87%9F%E5%BB%BA%E7%BD%B2%E5%9B%9E%E6%87%89-%E6%9C%89%E5%85%88%E6%B1%BA%E6%A2%9D%E4%BB%B6-120200440.html>

# 建築物附屬停車空間電動車輛充電使用安全指引

## 法規資訊(體驗新版植根法律網)

法規名稱：建築物附屬停車空間電動車輛充電使用安全指引

時間：中華民國113年4月18日

所有條文

編章節

條文檢索

歷史沿革

相關令函

相關判解

制定依據

所有條文

一、為因應建築物附屬停車空間電動車輛充電使用，提升其設置及使用安全，特訂定本指引。

二、本指引適用對象為設有電動車輛充電設備（樁）之室內停車場或建築物依法附設之室內停車空間。

本指引用詞，依國家標準、商品檢驗法、車輛型式安全審驗管理辦法、用戶用電設備裝置規則、電業法、台灣電力股份有限公司（以下簡稱台電公司）營業規章、建築技術規則及各類場所消防安全設備設置標準用詞定義之規定。

三、建築物附屬停車空間設置之充電設備（樁），應依下列規定辦理：

（一）電動車輛充電設備（樁）之產品安全規範

電動車輛充電設備（樁）產品安全應符合國家標準要求；電動車輛充電設備（樁），應取得經濟部標準檢驗局之商品檢驗或產品驗證，確保安全。

（二）車輛型式安全審驗管理辦法

三、建築物附屬停車空間設置之充電設備（樁），應依下列規定辦理：

（一）電動車輛充電設備（樁）之產品安全規範

電動車輛充電設備（樁）產品安全應符合國家標準要求；電動車輛充電設備（樁），應取得經濟部標準檢驗局之商品檢驗或產品驗證，確保安全。

（二）車輛型式安全審驗管理辦法

..... (略)

（三）電業法

依據電業法第三十二條及用戶用電設備檢驗辦法第三條規定，住戶設置充電設備（樁）應向公用售電業（台電公司）申請，並經輸配電業（台電公司）檢驗合格時，方得接電。

（四）用戶用電設備裝置規則

經濟部已於用戶用電設備裝置規則第六章「特殊設備及設施」第五節訂有「電動車輛充電系統」規範充電系統之配線方法、設備構造、控制與保護等事宜，作為電器承裝業施工依據。

（五）台電公司營業規章

• 用戶向台電公司辦理充電設備（樁）用電申請，應委由電機技師或合法登記電器承裝業辦理設計及施工，並於申請前先將設計資料送經台電公司審查通過後興工，依照設置者申請用電容量及供電方式，台電公司會評估區域負載情形及饋線容量裕度，適時加裝供電變壓器，以提供充電設施所需電源。

• 用戶於竣工後向台電公司申報竣工，台電公司將依規定進行審查及檢驗送電。

（六）各類場所消防安全設備設置標準

建築物附屬停車空間應依各類場所消防安全設備設置標準第十八條規定就水霧、泡沫、乾粉、二氧化碳滅火設備選擇設置，或依場所風險屬性選設自動撒水設備，提升初期火災自動滅火功效。

## TAF充電設備(充電樁)測試實驗室認證要求及現況

### TAF 認可3家充電設備(充電樁)測試實驗室

#### 一、充電設備測試技術法規及自願性產品驗證制度(VPC)

經濟部標準檢驗局於2022年1月13日公告，修訂將電動車充電設備(充電樁)相關產品納入自願性產品驗證制度(VPC)，保障電動車使用者充電權益。隨著我國國家標準(CNS)修訂公布後，國內實驗室可依國家標準執行測試，且政府設置公共充電設備時，也可循相關設置使用需求選擇適用充電規格，預期將有助於提升充電設備品質、維護民眾使用安全，同時推動電動車相關產業發展。本會配合國家重要政策目標之推動，已於今(111)年一月著手規劃相關認證制度及資源之建立，以利服務國內測試實驗室之認證需求。

- 交流充電設備的充電樁，安規必須滿足CNS 15511-1(110年版)電動車輛傳導式充電系統 - 第1部之一般要求，電磁相容性必須滿足 CNS 15511-21-2(110年版)電動車輛傳導式充電系統-第21-2部電動車輛以傳導式連接至交流/直流電源的要求之非車載電動車輛充電系統的電磁相容要求，其充電槍頭及纜線必須滿足CNS 15700-1(106年版) 電源端插頭、電源端插座、車輛端插頭及車輛端插座 - 電動車輛傳導式充電 - 第1 部之一般要求及CNS 15700-2(110年版) 電源端插頭、電源端插座、車輛端插頭及車輛端插座 - 電動車輛傳導式充電 - 第2部針對交流刀片及導電嘴配件之尺度相容性及互換性的要求。
- 直流複合式充電設備的充電樁，安規必須滿足CNS 15511-1(110年版) 電動車輛傳導式充電系統 - 第1部的一般要求、CNS 15511-21-2(110年版) 電動車輛傳導式充電系統 - 第21-2部之電動車輛以傳導式連接至交流/直流電源的要求 - 非車載電動車輛充電系統的電磁相容要求及CNS 15511-23 (110年版) 電動車輛傳導式充電系統 - 第23部電動車輛直流充電站之要求，電磁相容必須滿足CNS 15511-21-2(110年版) 電動車輛傳導式充電系統 - 第21-2部之電動車輛以傳導式連接至交流/直流電源的要求 - 非車載電動車輛充電系統的電磁相容要求。
- 直流充電樁與電動車直流充電控制用數位通訊要求必須滿足CNS 15511-24(110年版) 電動車輛傳導式充電系統 - 第24 部電動車輛直流充電站與電動車輛間充電控制用數位通訊之要求，其充電槍頭及纜線必須滿足CNS 15700-1(106年版) 電源端插頭、電源端插座、車輛端插頭及車輛端插座 - 電動車輛傳導式充電 - 第1 部之一般要求、CNS 15700-3(110年版) 電源端插頭、電源端插座及車輛端耦合器 - 電動車輛傳導式充電 - 第3部之直流及交直流綜合型端子與接觸導管類型車輛端耦合器之尺度相容性及互換性要求及CNS 15700-3-1(110年版) 電源端插頭、電源端插座、車輛端插頭及車輛端插座 - 電動車輛傳導式充電 - 第3-1部之使用熱管理系統之直流充電用車輛端插頭、車輛端插座及纜線組要求。

[CS 29.120.30; 43.120]

## 中華民國國家標準

## C N S

### 電動車輛傳導式充電系統－ 第 3 部：安全要求

### Electric vehicle conductive charging system – Part 3: Safety requirements

CNS 15511-3:2021  
C4524-3

中華民國 100 年 10 月 25 日制定公布  
Date of Promulgation:2011-10-25

中華民國 110 年 3 月 25 日修訂公布  
Date of Amendment:2021-03-25

本標準非經經濟部標準檢驗局同意不得翻印

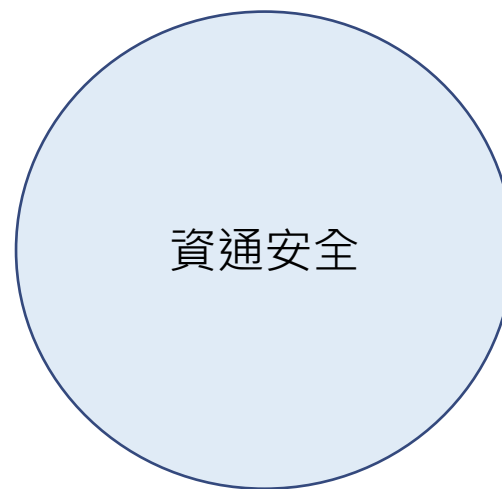
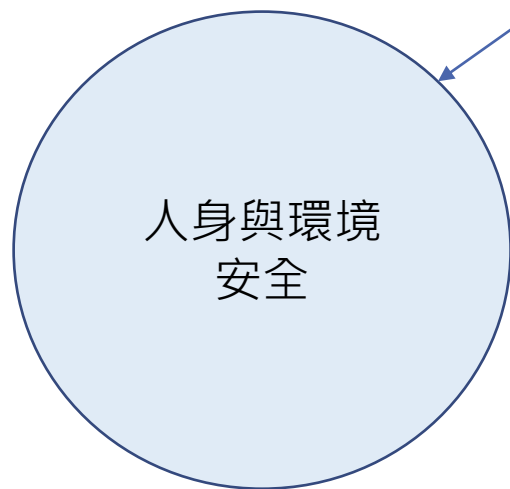


# 目前比較著重在人身與環境安全 (Safety)

作業科技 (Operational technology, OT)：包括與實體環境互動的可程式化系統與裝置  
— NIST SP 800-82r3

因為會和實體環境互動，  
所以要避免發生意外事件  
而影響到外界

減少外界威脅利用到弱點  
而發生意外事件



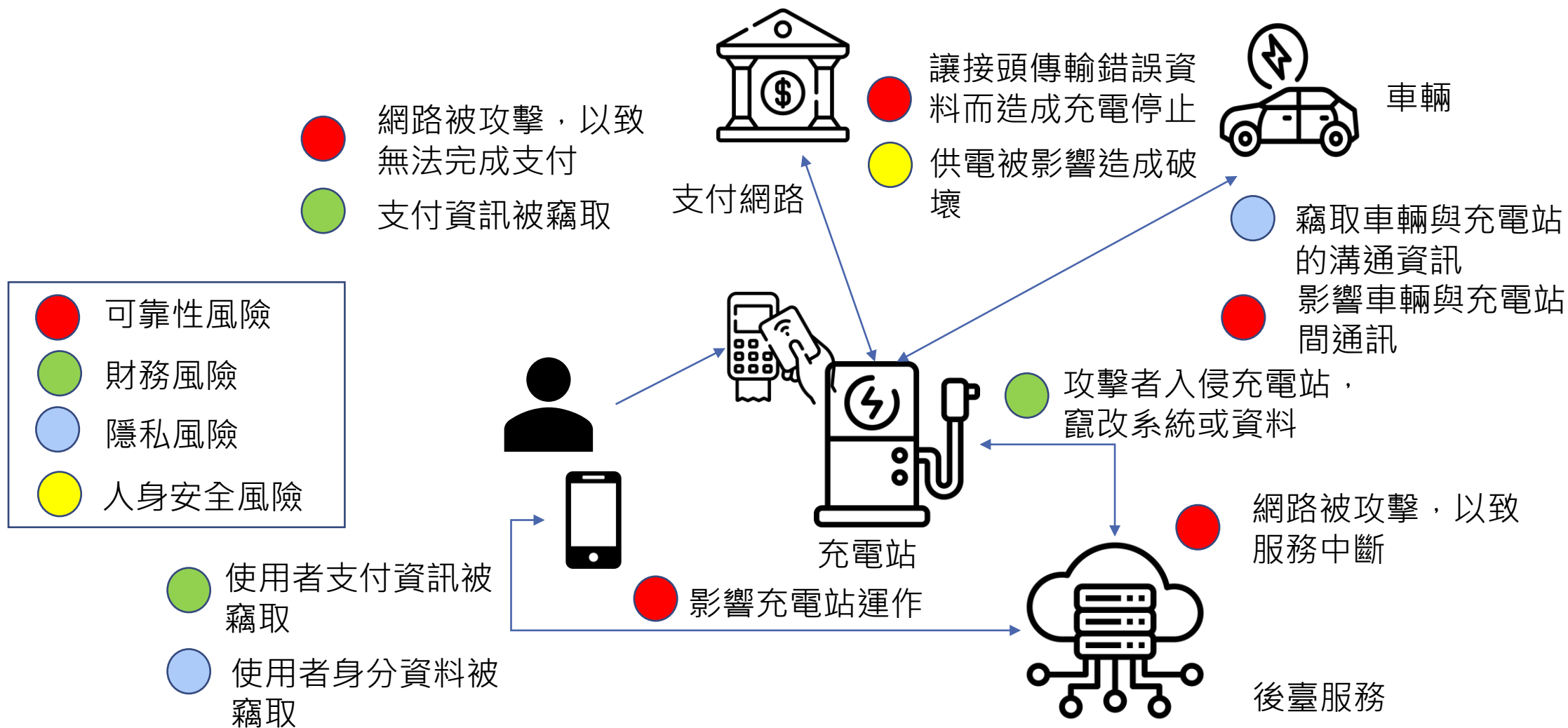


## 充電樁理所當然會有人身與環境安全議題，但是也有資訊安全議題

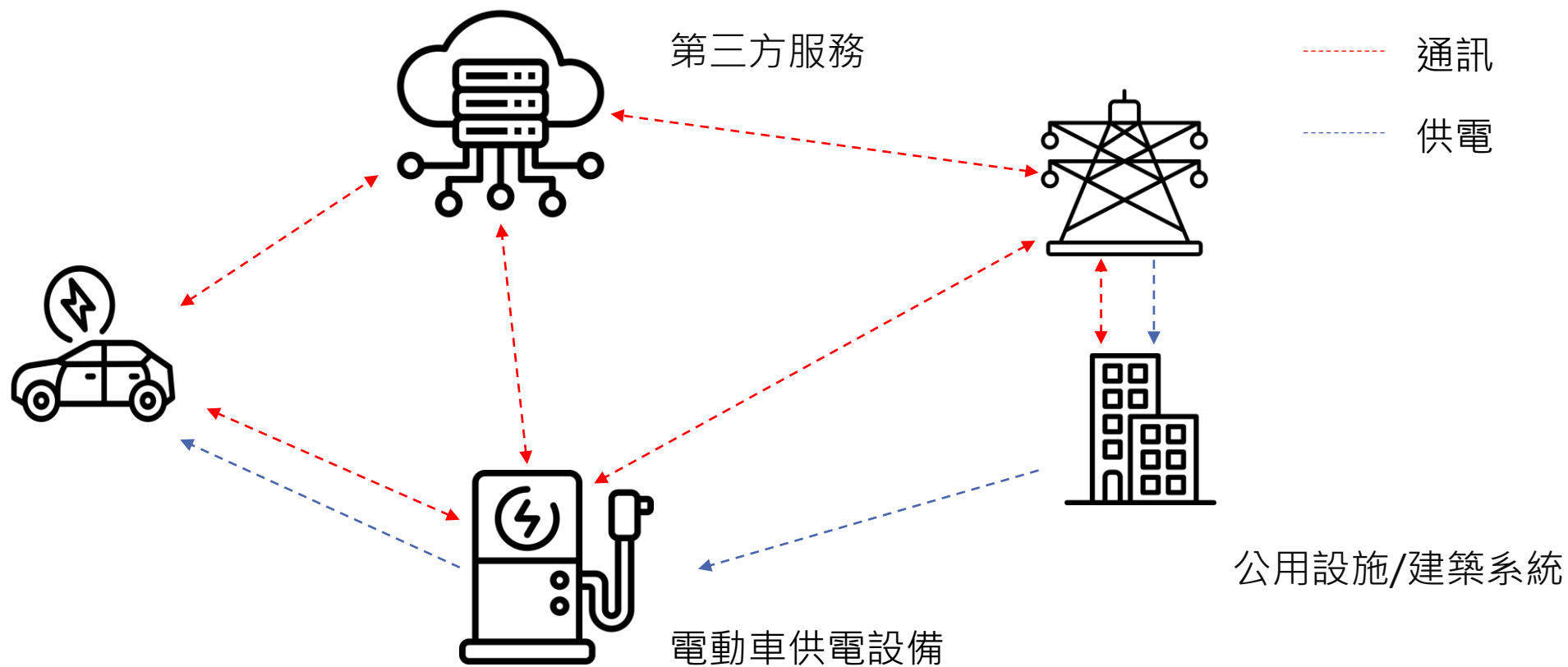
可靠性風險 (Reliability Risk)	系統不能提供服務，間歇供電，或是其他被攻擊者控制而造成對供電穩定性的影響
隱私風險 (Privacy Risk)	使用者資料被竊取或被未經授權存取等，而造成隱私受到侵害的風險
財務風險 (Financial Risk)	造成充電者或充電服務提供者財務損失的風險
人身安全風險 (Safety Risk)	造成人員或骨幹受到損害的風險

EPRI (Electric Power Research Institute), Cybersecurity Platform and Certification Framework Development for Extreme Fast Charging (XFC)- Integrated Charging Ecosystem, Technical Report, 2023

# EPRI 的技術報告中所列出的充電站資通安全風險



# 充電樁的安全會和整個生態系的資通安全與人身安全相關





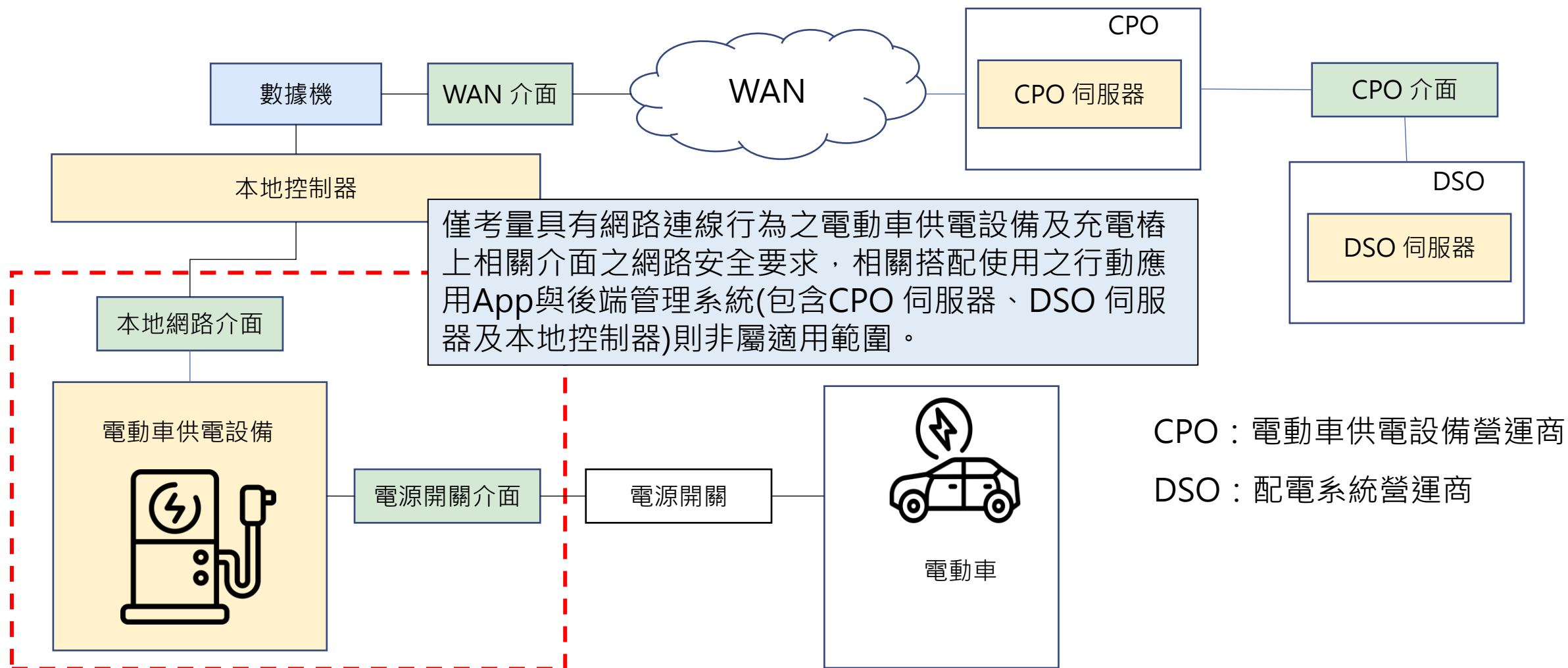
充電樁的資安風險

目前充電樁的資安規範與缺口

從設備的資安到維運時的資安考量

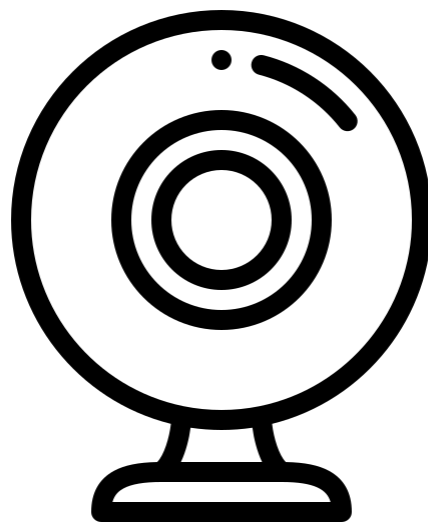
結論

# 電動車供電設備資訊安全檢測技術規範



實體安全	對供電設備實體介面的防禦要求	第一級
系統安全	包括安全日誌與阻斷式服務攻擊等的系統防禦能力要求	防止操作疏失之安全問題， 並能防禦未具備足夠資源攻擊者之攻擊行為
韌體更新	對於韌體版本與更新服務等的安全要求	第二級
通訊安全	對於傳輸資料的安全要求	可防禦具備足夠資源攻擊者 之攻擊行為
身分鑑別與授權 機制安全	對供電設備介面的身分鑑別與存取控制 要求，以防止未經授權之操作	

在介紹細節之前，請在腦海裡想像如果這標準套到網路攝影機





## 6.1 實體安全

採用 Security by Design 的最佳實務，最小權限是其中考量，對到IEC 62443-3-3 SR 7.7 也可以

編號	要求	對應標準	等級 1	等級 2
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	CNS 62443-4-1 SD-4	○	○
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	IEC 62443-3-3 SR 1.2	○	○
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記錄。	IEC 62443-4-2 SR 3.11、IEC 62443-4-2 EDR3.11	○	○

實體性篡改抵抗與偵測

控制系統要有能力去識別與鑑別所有存取的元件與裝置 =?

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)。

## 6.2 設備強化

系統使用通知：在使用系統前要有訊息通知？

SR2.8事件可稽

SR7.3 - 控制系統備份？

最小權限

編號	要求	對應標準	等級 1	等級 2
6.2.1	電動車供電設備應刪除不需要的應用程式			
6.2.1.1	電動車供電設備僅使用最小需要的通訊埠	IEC 62443-3-3 SR 7.7	○	○
6.2.1.2	電動車供電設備僅使用最小需要的通訊埠	IEC 62443-3-3 SR 7.7		
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。	IEC 62443-4-2 SR 1.12	○	○
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。	IEC 62443-3-3 SR 2.11 RE 1	○	○
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。	IEC 62443-3-3 SR 3.3		○

SR 6. 當發現事件時，能通知有關單位事件的發生與相關證據，並及時採取矯正動作，以因應資安違規行為

SR3.3 - 資安功能查證？

## 6.2 設備強化 (續)

避免服務拒絕 (Denial of Service) 攻擊

編號	要求	對應標準	等級 1	等級 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 分以上或嚴重性等級評比為以上者。	CNS 62443-4-1 SVV-3、CNS 62443-4-1 DM-3	○	○
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。	IEC 62443-3-3 SR 7.1		○
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。	IEC 62443-3-3 SR 7.4		○

SR7.3 - 控制系統備份

SR7.4 - 控制系統的還原與重建

## 6.3 韌體更新

SR 4.1資訊機密性

SR 3.10 (1)嵌入式裝置應在安裝之前，驗核任何軟體更新或升級的真確性與完整性

支援更新

SR 7.4 控制系統的還原與重建

編號	要求	對應標準	等級 1	等級 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。	IEC 62443-4-2 CR 3.10	○	○
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。	IEC 62443-3-3 SR 7.4	○	○
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。	CNS 62443-4-1 SUM-4		○
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。	IEC 62443-4-2 CR 1.2	○	○
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。	CNS 62443-4-1 SUM-4	○	○

每個元件要能識別自己並能被其他裝置所鑑別？

安全更新派送

## 6.4 通訊安全

SR4.1 - 資訊機密性  
SR 4.3 - 密碼學技術之使用

一般都是支援哪些版本

編號	要求	對應標準	等級 1	等級 2
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。	IEC 62443-3-3 SR 4.1、 IEC 62443-3-3 SR 4.3	○	○
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。	IEC 62443-4-2 FR 5	○	○
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。	IEC 62443-4-2 CR 4.1	○	○
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 SP800-131A 規定之同等或以上強度的加密演算法。	IEC 62443-4-2 CR 1.7		○

以密碼為基礎之鑑別之強度？

? SR 5. 對控制系統進行分割，以限制不必要的資料流。

## 6.5 身分鑑別與授權機制安全

EDR2.13 - 避免使用實體診斷與測試介面

NDR 1.13- 要監控與控制從非信任網路的存取

SR1.1, SR1.2

編號	要求	對應標準	等級 1	等級 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。	IEC 62443-3-3 SR 1.2	○	○
6.5.1.2	電動車供電設備應具備身分鑑別機制。	IEC 62443-4-2 EDR 2.13 、NDR 1.13	○	○
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。	IEC 62443-4-2 SR 1.5	○	○
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。	IEC 62443-3-3 SR 1.7		○
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。	IEC 62443-3-3 SR 3.8		○
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。	IEC 62443-3-3 SR 1.11		○

鑑別器管理

連線完整性

登錄失敗處理

Source: 電動車供電設備資訊安全檢測技術規範



## 6.5 身分鑑別與授權機制安全 (續)

NDR 5.2 RE(1) 區域  
邊界保護:全部拒絕，  
例外允許

編號	要求	對應標準	等級 1	等級 2
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。	CNS 62443-4-1 SG-6	○	○
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。	IEC 62443-3-3 SR 5.2 RE 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。	IEC 62443-3-3 SR 2.1	○	○
6.5.3.3	電動車供電設備應允許定義新的角色。	IEC 62443-3-3 SR 2.1 RE 2		○

?帳號管理指引

授權落實

權限映射(permission mapping)到角色



## 對於國內標準建立的一般性建議

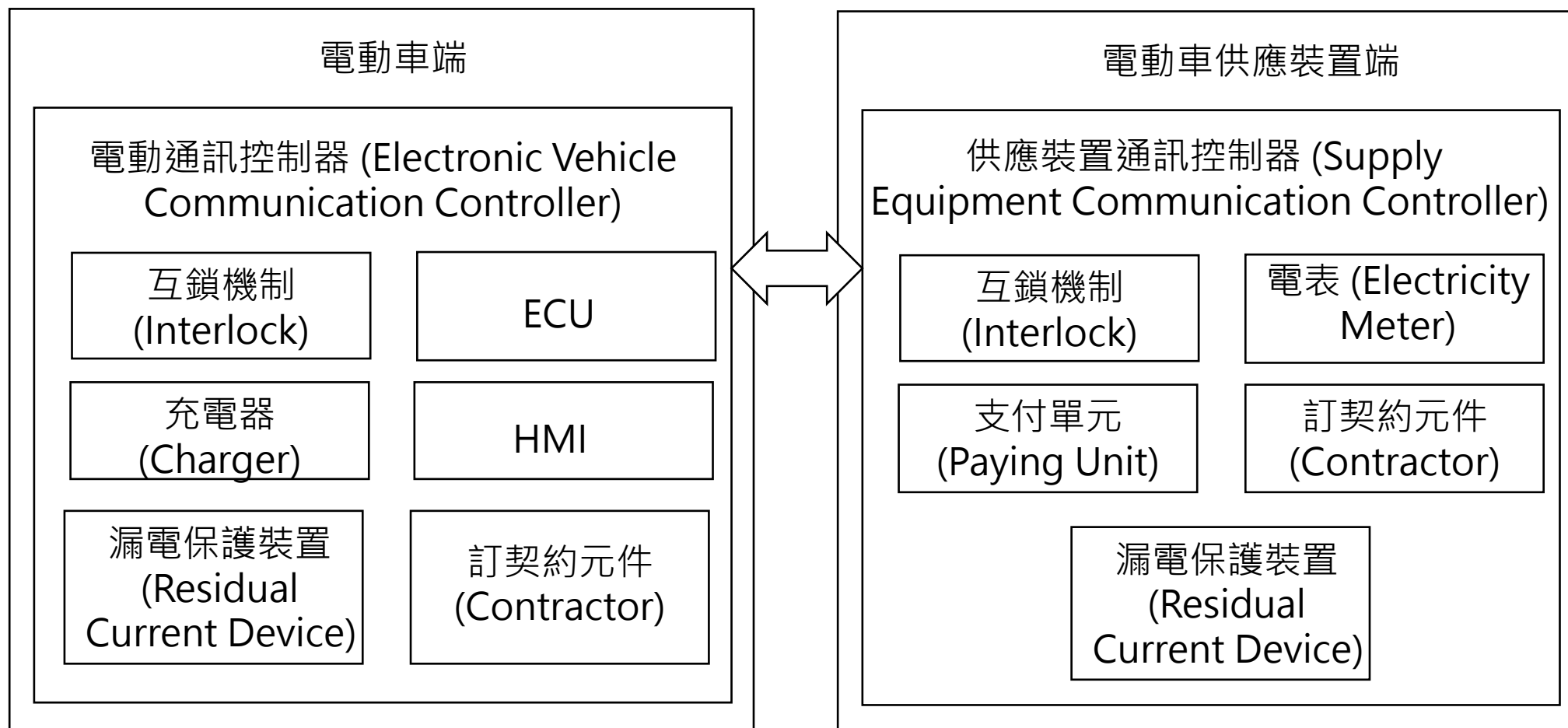
應該要能夠反映不同  
裝置的特色

不要把檢測單位都當  
能開天眼

不要整天找人背書，  
講了建議又敷衍

# ISO 15118 當中的主要元件

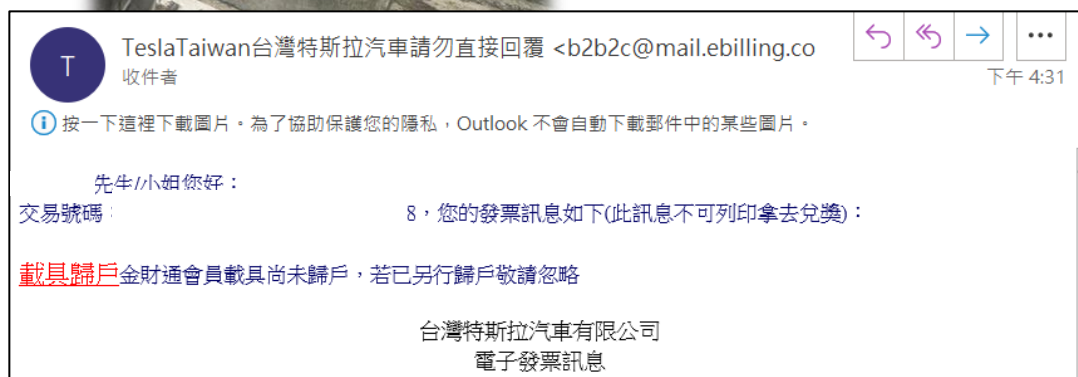
道路車輛 – V2G通訊介面 (Road vehicles - Vehicle to grid communication interface)



# 充電介面的鑑別機制－運作方式 (PnC 與 EIM 模式)



PnC



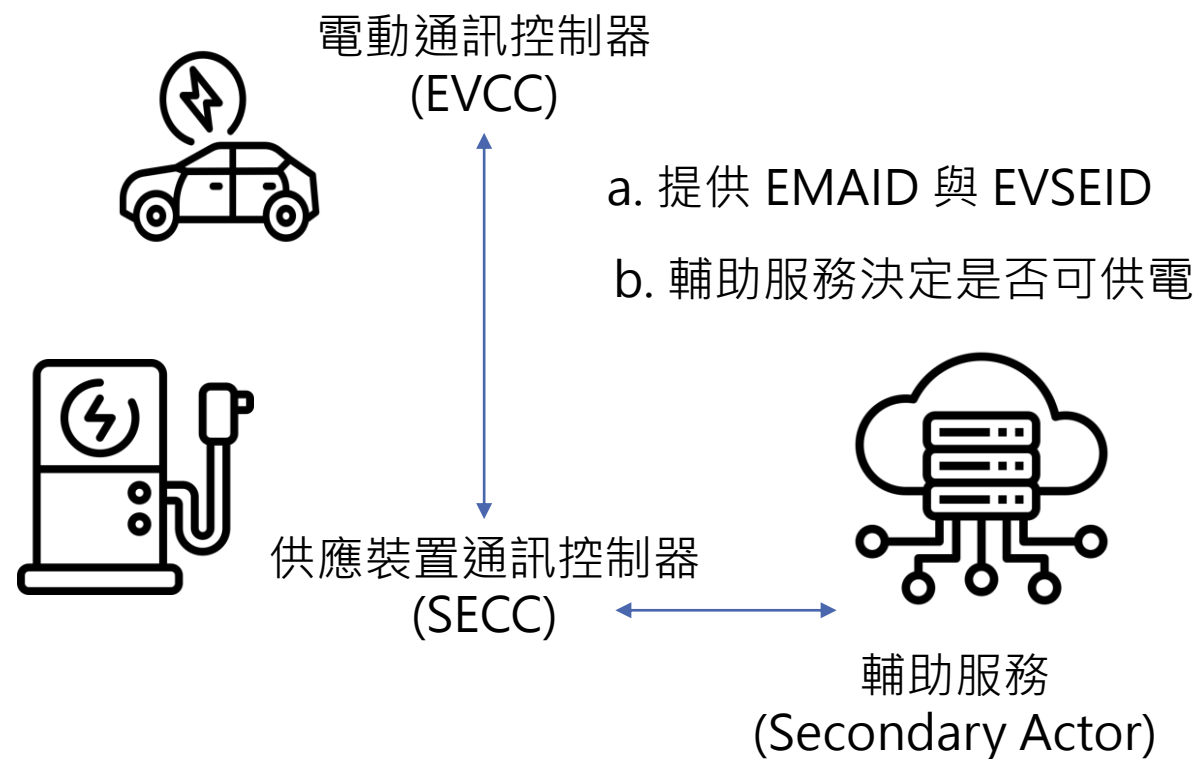
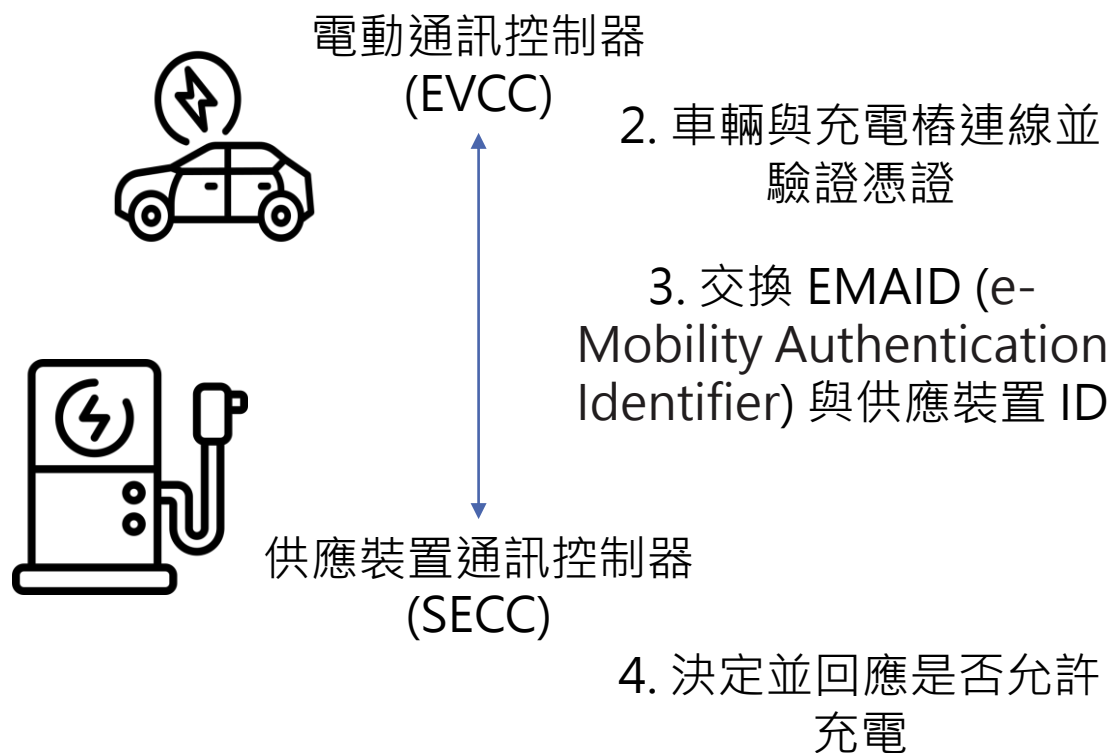
EIM



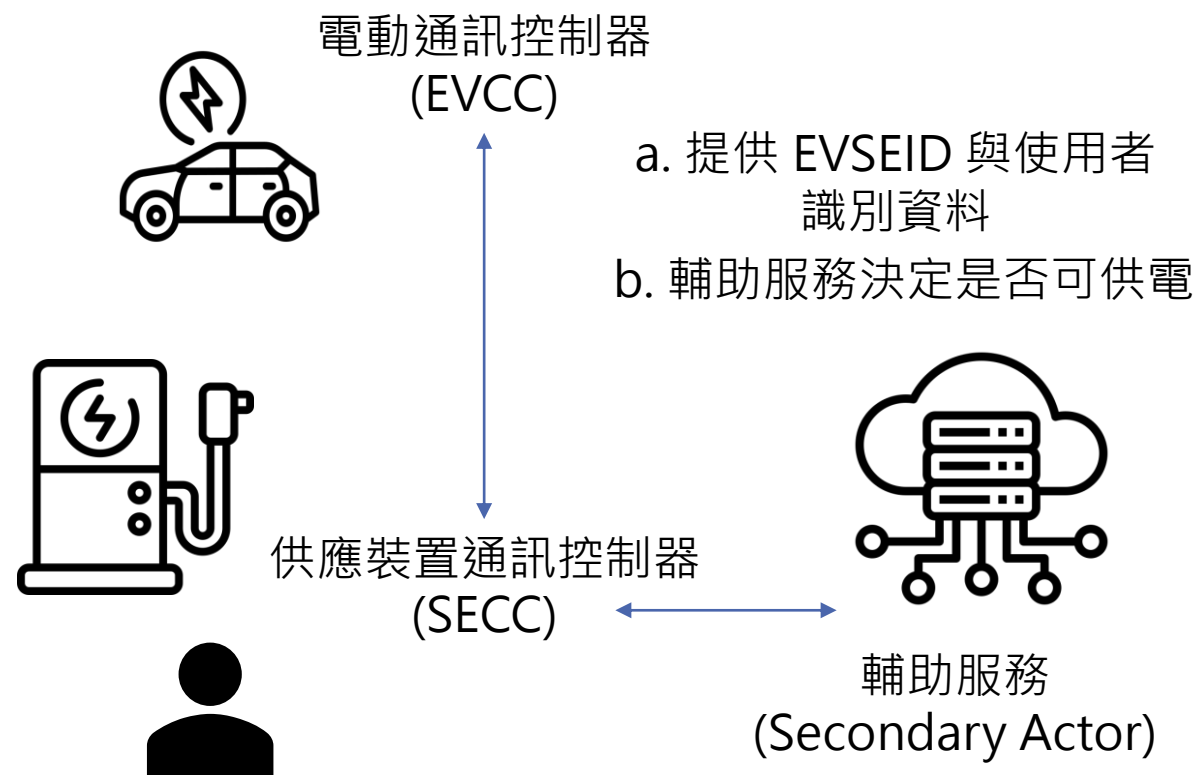
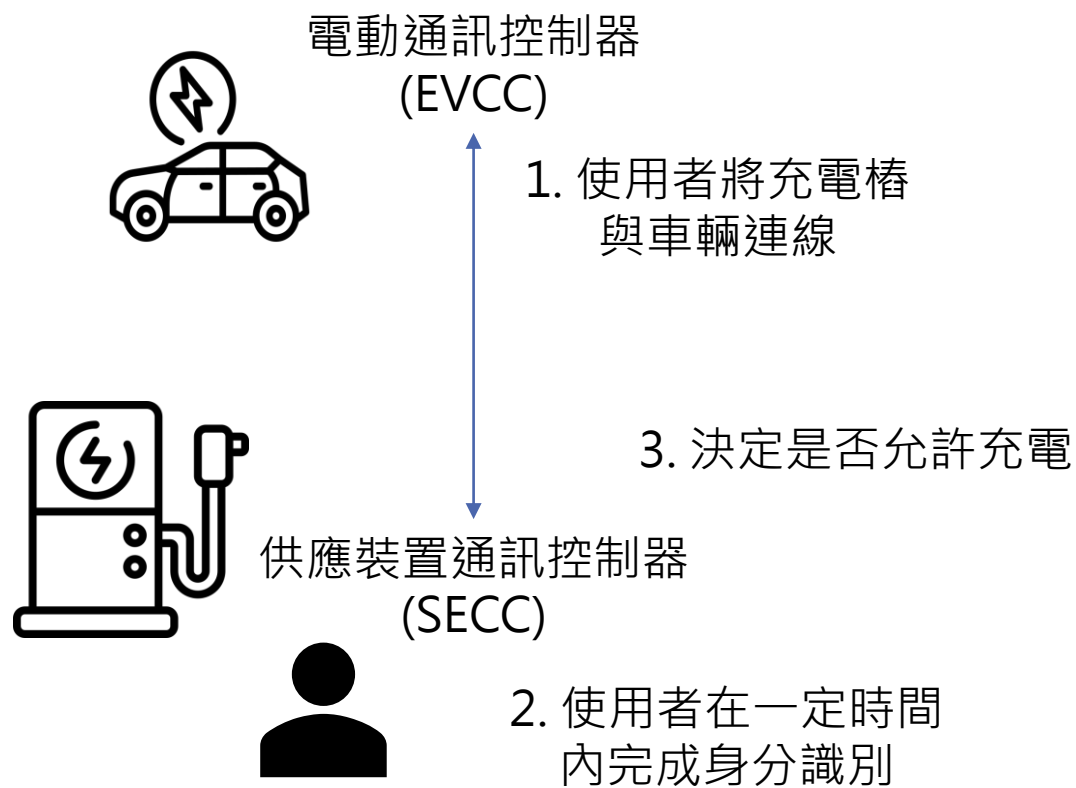
# PnC (Plug and Charge) 模式

0. 供應商提供憑證

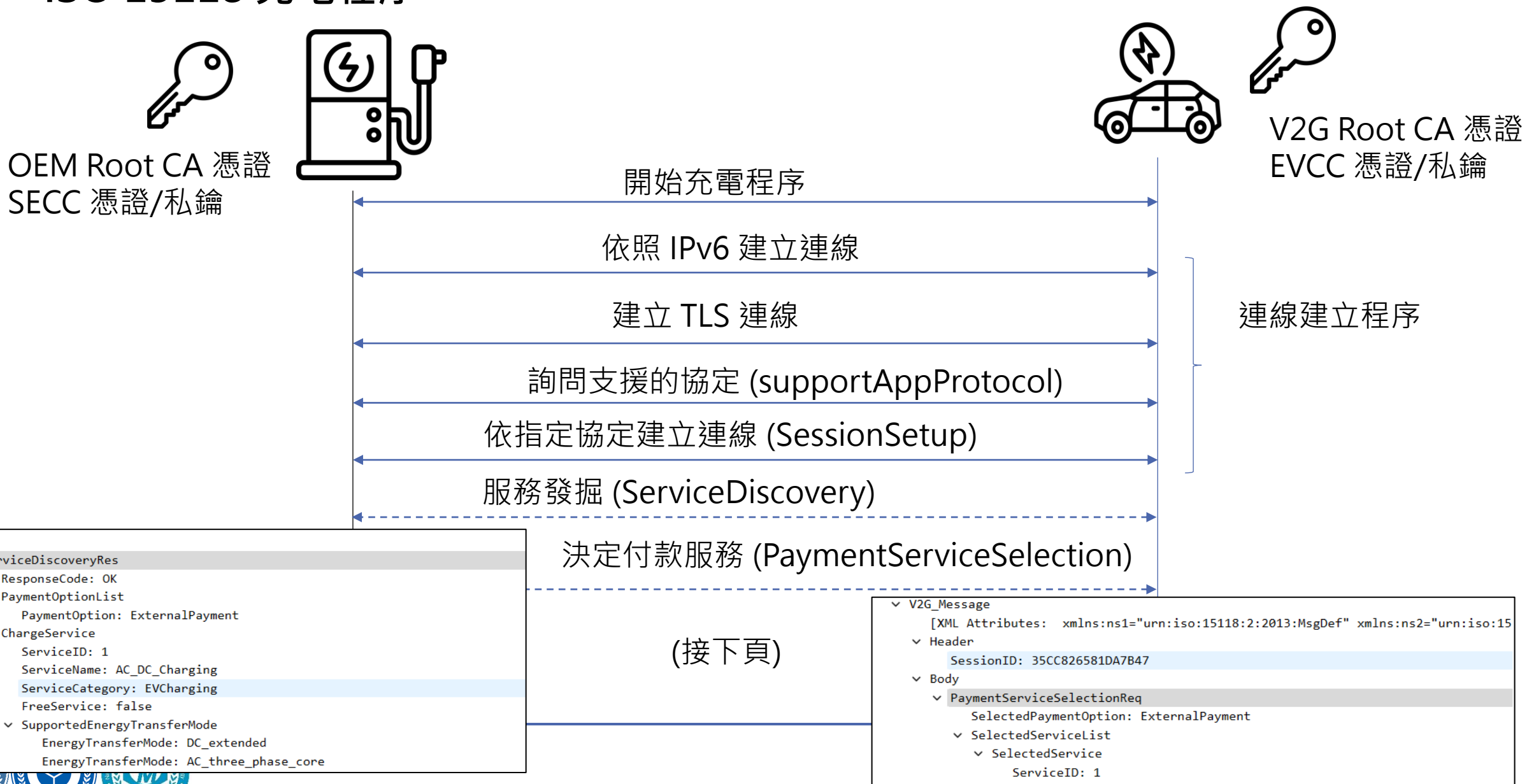
1. 使用者將充電樁  
與車輛連線



# EIM (External Identification Mode) 模式

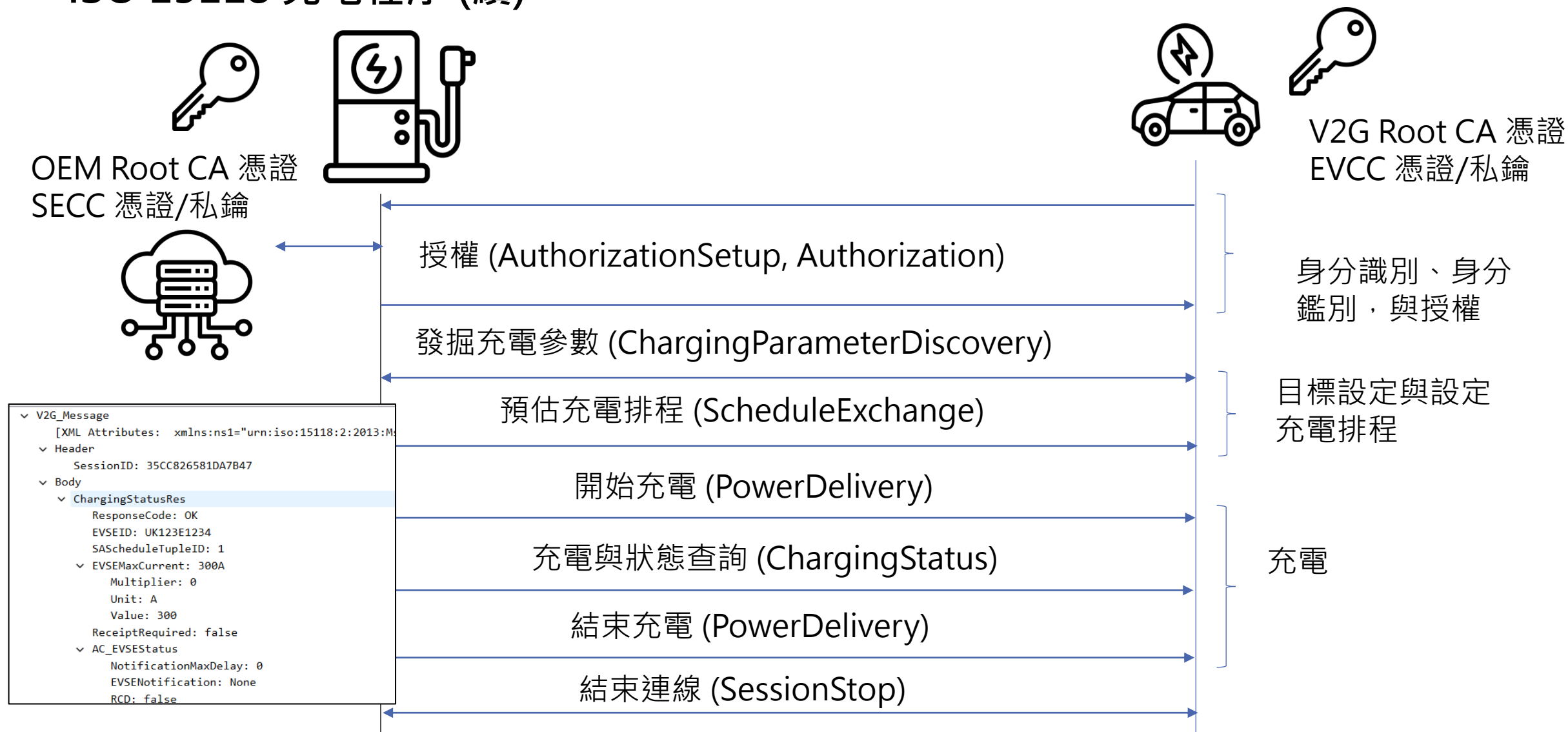


# ISO 15118 充電程序



(接下頁)

# ISO 15118 充電程序 (續)



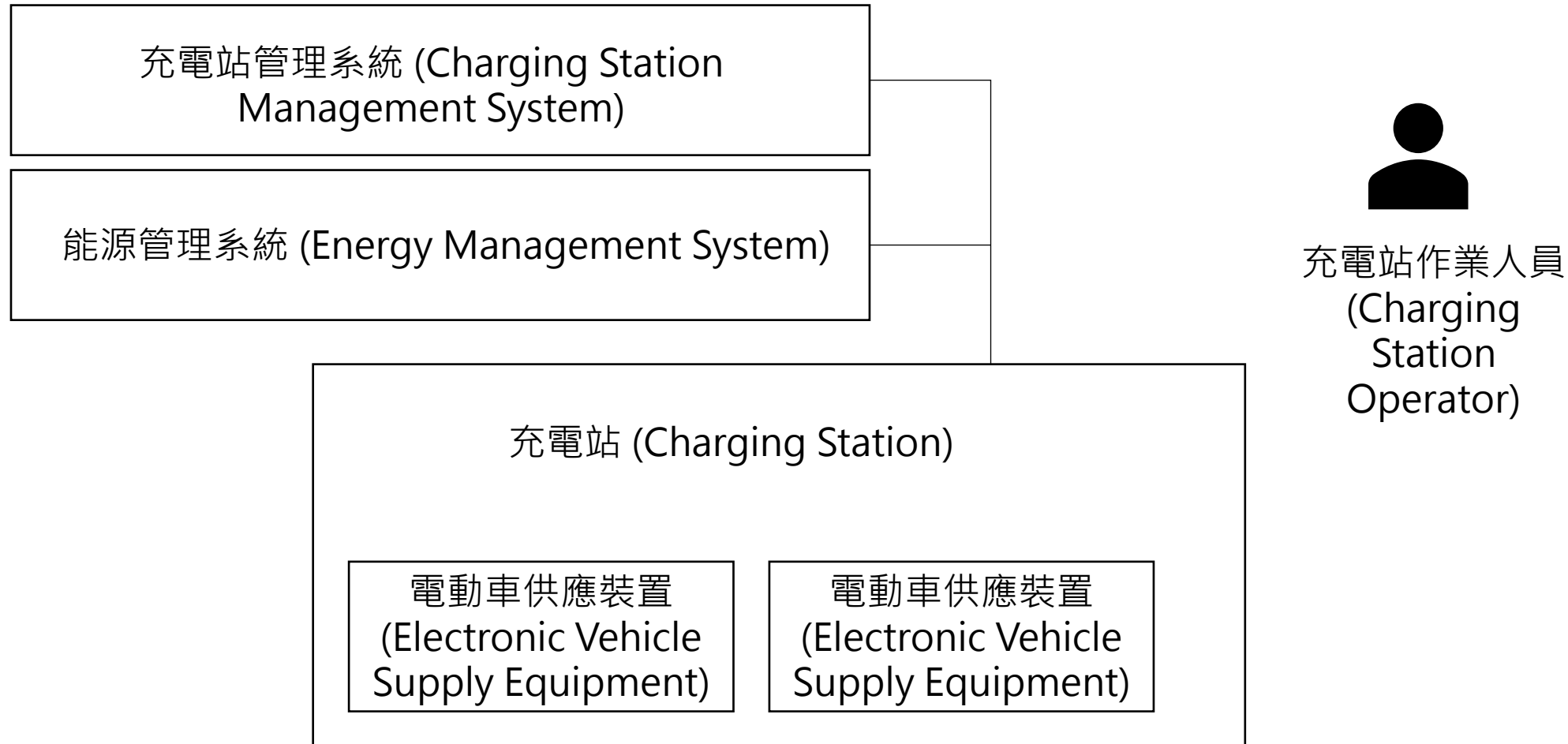


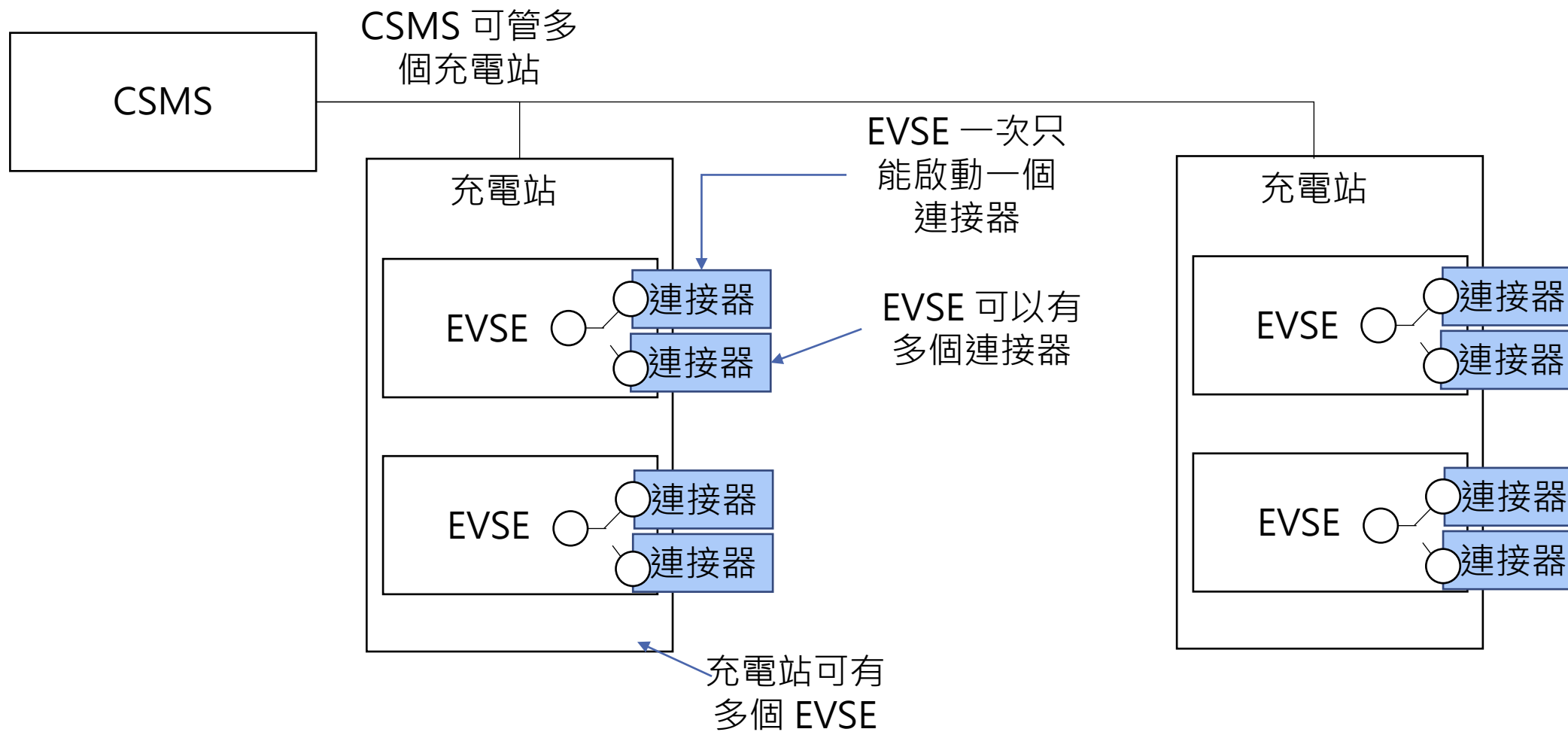
# 模擬器的資料傳輸範例

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (SAP)	98	supportedAppProtocolRes
2	1.109950	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	108	SessionSetupReq
3	1.144160	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	125	SessionSetupRes
4	2.157244	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ServiceDiscoveryReq
5	2.194613	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	130	ServiceDiscoveryRes
6	3.066816	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	110	PaymentServiceSelectionReq
7	3.105869	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	108	PaymentServiceSelectionRes
8	3.807652	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	AuthorizationReq
9	3.837493	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	109	AuthorizationRes
10	4.487213	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	126	ChargeParameterDiscoveryReq
11	4.572591	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	419	ChargeParameterDiscoveryRes
12	5.467347	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	123	PowerDeliveryReq
13	5.502729	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	111	PowerDeliveryRes
14	6.129068	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ChargingStatusReq
15	6.194229	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	129	ChargingStatusRes
16	6.964419	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ChargingStatusReq
17	7.008645	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	129	ChargingStatusRes
18	7.584344	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ChargingStatusReq
19	7.627003	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	129	ChargingStatusRes
20	8.163629	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ChargingStatusReq
21	8.193553	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	129	ChargingStatusRes
22	8.800739	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ChargingStatusReq
23	8.833433	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	129	ChargingStatusRes
24	9.370772	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ChargingStatusReq
25	9.441140	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	129	ChargingStatusRes
26	9.900129	fe80::68a9:c954:b5fb:8ab	fe80::77f8:c2ce:49c1:140e	V2GMSG (ISO-2 ?)	107	ChargingStatusReq
27	9.936767	fe80::77f8:c2ce:49c1:140e	fe80::68a9:c954:b5fb:8ab	V2GMSG (ISO-2 ?)	129	ChargingStatusRes

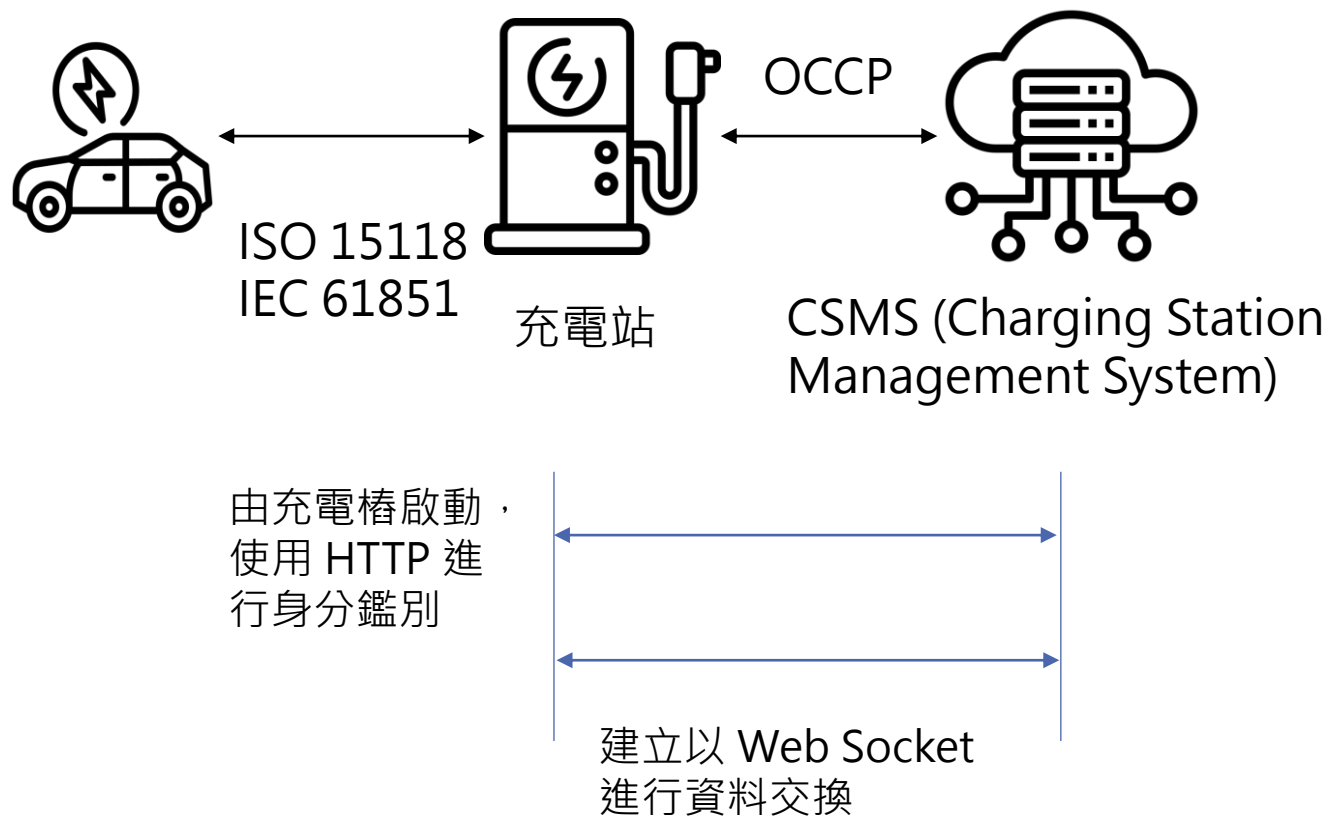
現在想想看有沒有可能車對充電樁，或充電樁對車進行攻擊

# OCPP 主要針對充電站管理系統與充電站間的互動





# OCPP (Open Charge Point Protocol)



## A. 安全

- 更新充電站密碼
- 更新充電站憑證 (由 CSMS 要求)
- 更新充電站憑證 (由充電站要求)
- 安全事件通知 (由充電站要求)
- 更新充電站安全檔案

## B. 提供

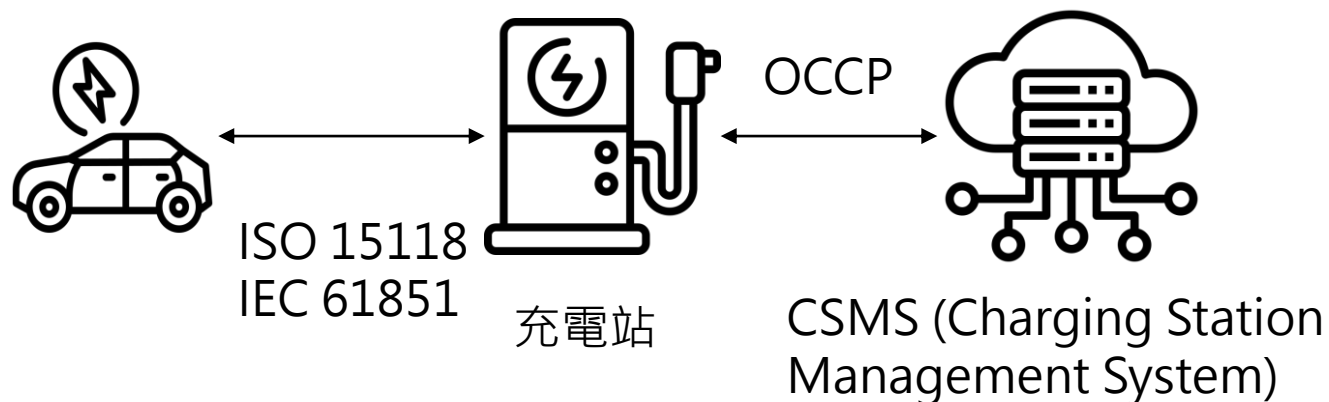
- 充電站開機與離線處理
- 充電站設定
- 充電站重置 (Reset)

## C. 授權 (例如決定是否可以供電或是停止供電)

## D. 管理充電站本地授權清單

由 Open Charge Alliance 訂定

# OCPP (Open Charge Point Protocol) (續)



由充電樁啟動，  
使用 HTTP 進  
行身分鑑別



E. 充電交易 (起始/結束交易、更新交易狀況等)

F. 遠端控制

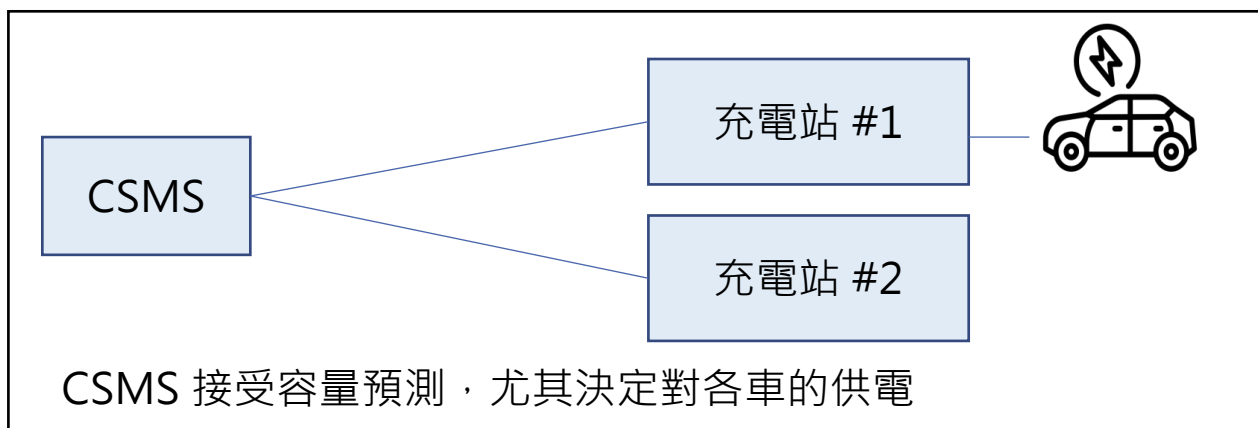
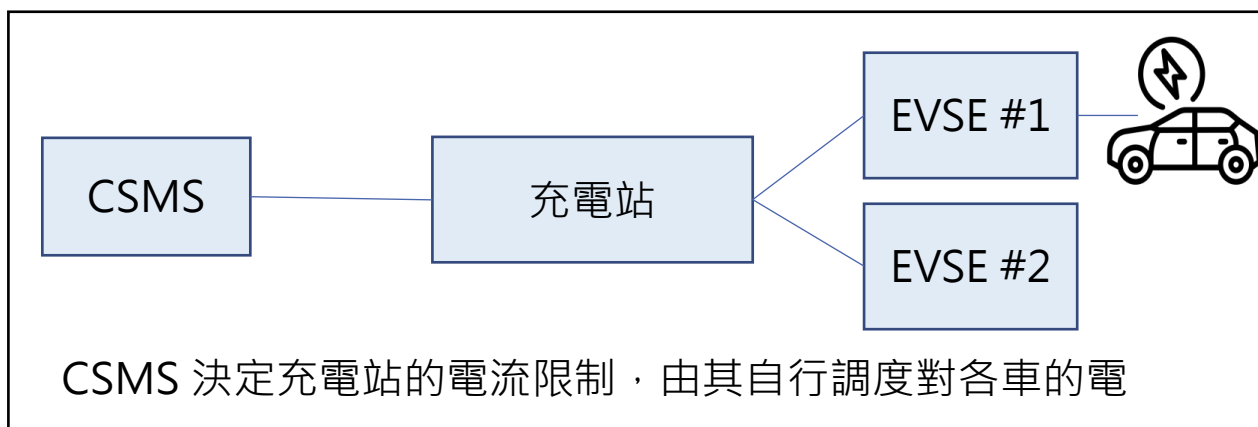
- 遠端起始交易
- 遠端終止交易
- 遠端解鎖
- 遠端驅動訊息

G. 可用性管理

- 狀態通知
- Heartbeat
- 停用或啟用充電樁置
- 在未妥善連接前禁止充電

H. 預約/取消預約

# OCPP (Open Charge Point Protocol) (續)



CSMS 透過本地控制器，去授權其管理充電站群組的供電

I. 提供價目表與充電成本資訊

J. 儀表數值

- 交易相關數值
- 依時間呈現數值
- 衡量參數設定

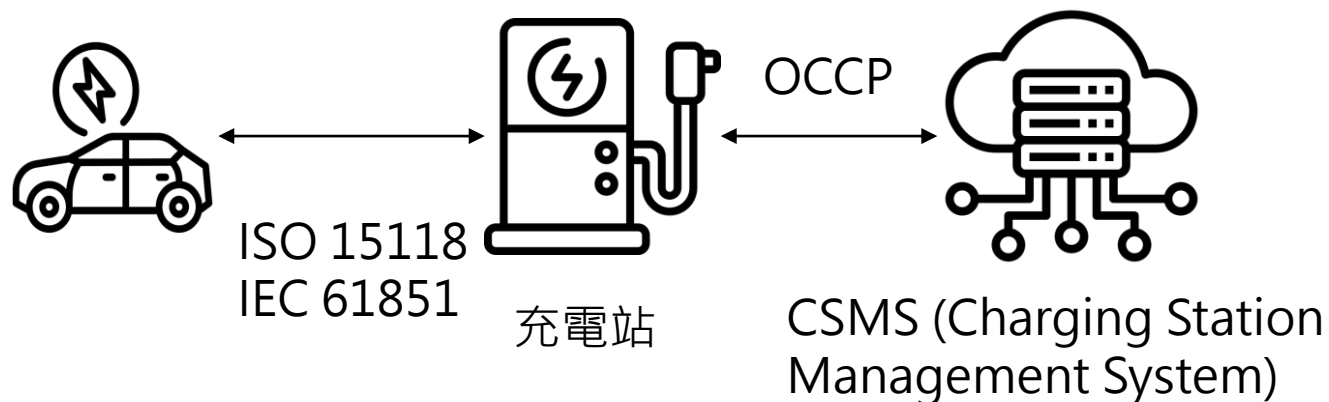
K. 智慧充電

- 內部負載平衡
- 集中式智慧充電
- 本地智慧充電
- 基於外部智慧充電訊號

充電站接受外部能源管理系統進行調整



# OCPP (Open Charge Point Protocol) (續)



由充電樁啟動，  
使用 HTTP 進  
行身分鑑別



L. 韌體管理與更新

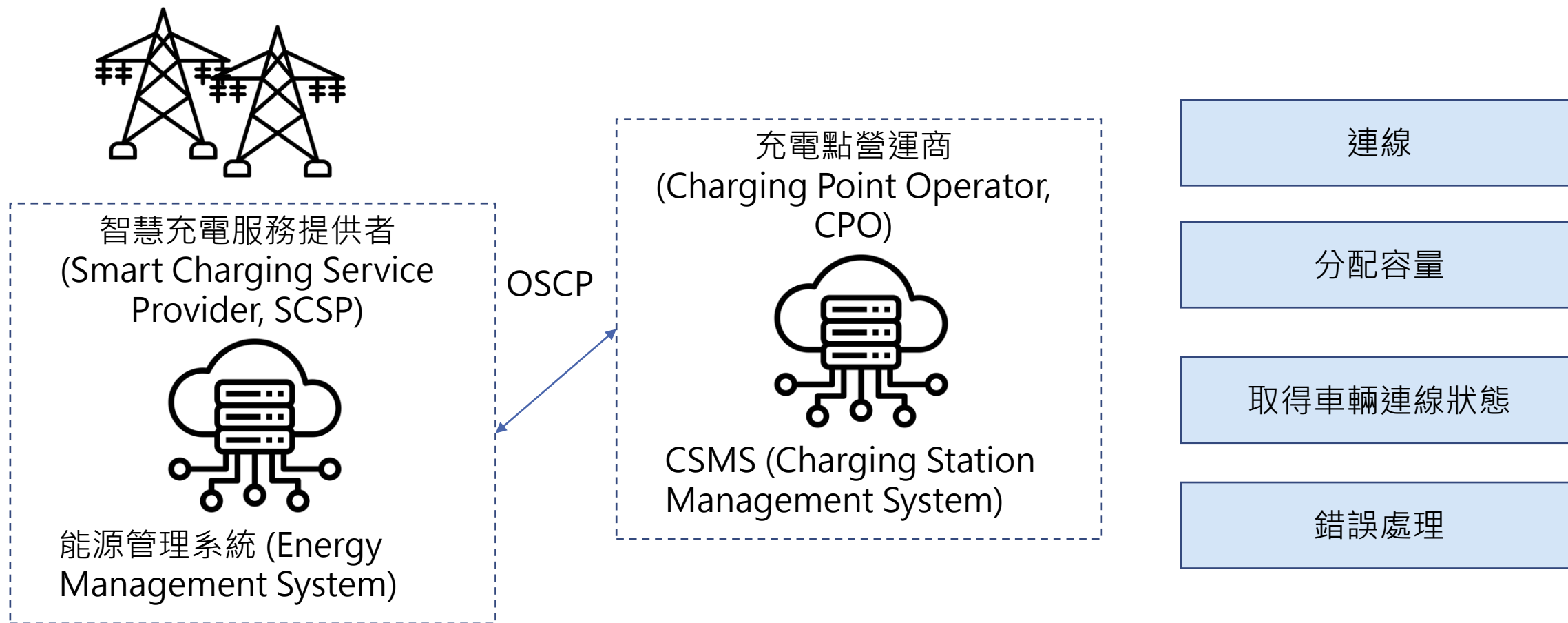
M. ISO 15118 憑證管理

N. 診斷

- 取得 Log 資訊
- 取得監控報告
- 監控機制管理

那 OCPP 有沒有可能被攻擊的地方？

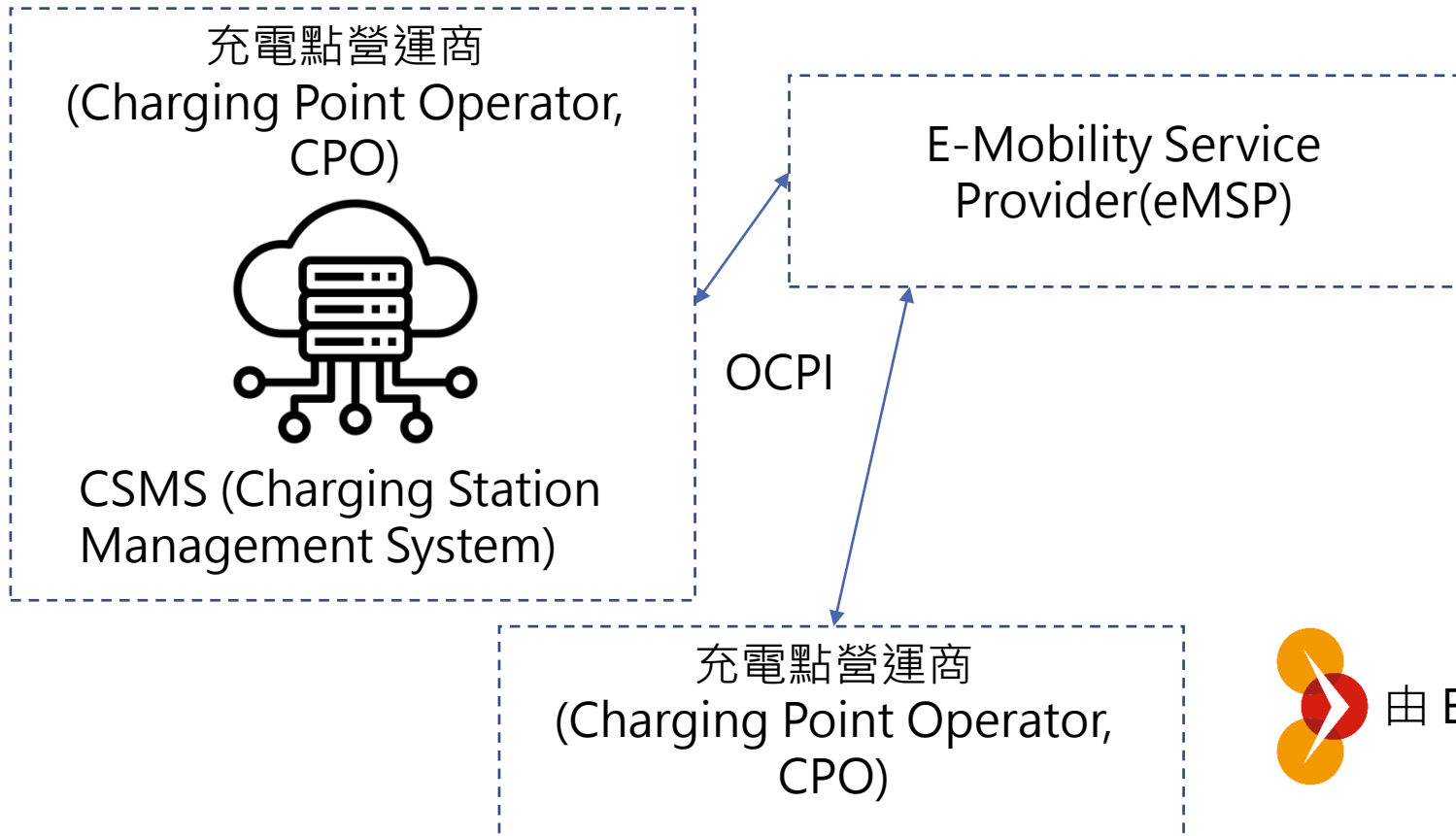
# OSCP (Open Smart Charging Protocol)



由 Open Charge Alliance 訂定

有沒有可能透過 OCPP 攻擊 CSMS 之後，進一步攻擊 EMS？

# OCPI (Open Charge Point Interface)

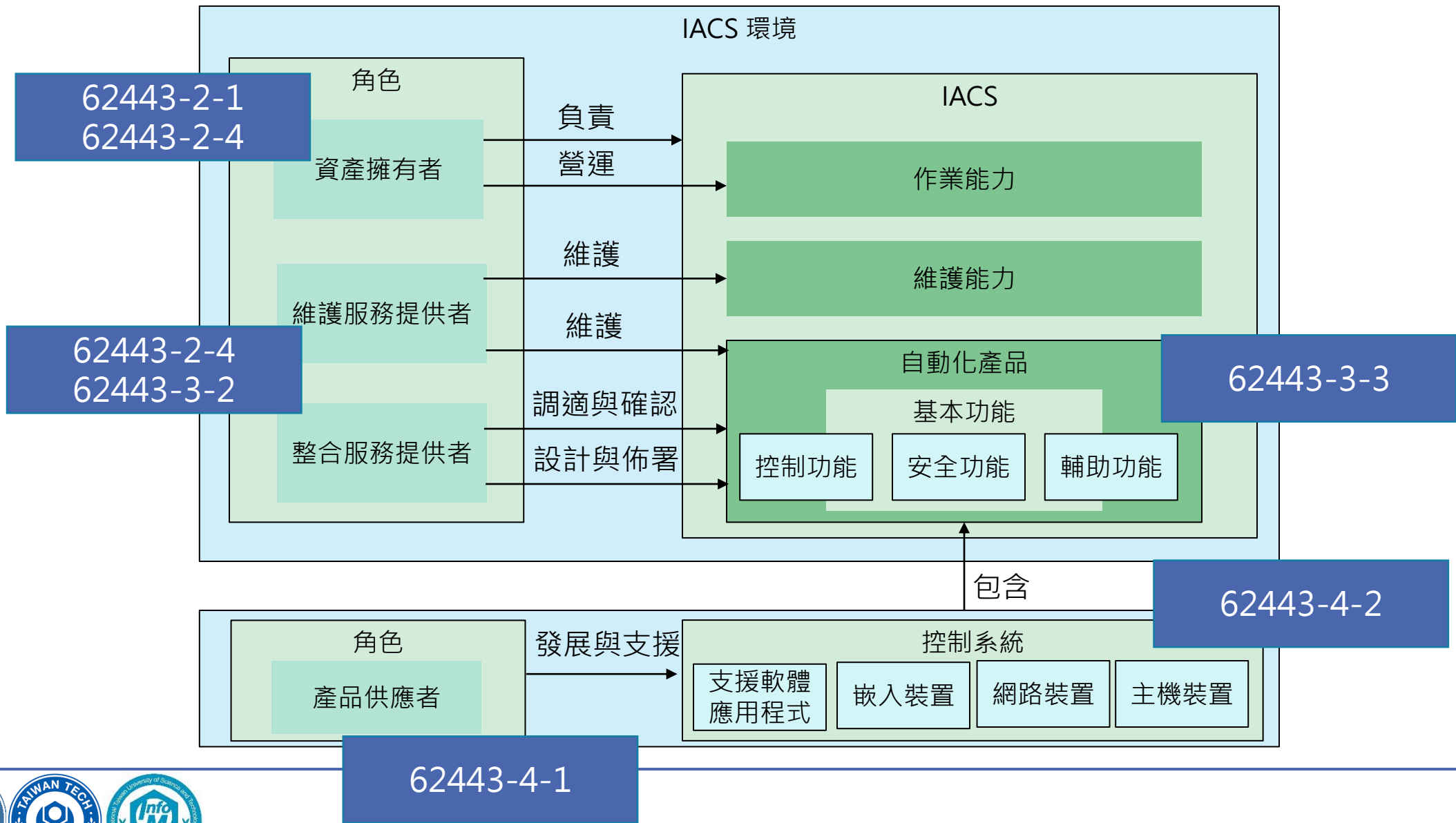


由 EVRoaming Foundation 制定

我們可以用 IEC 62443-3-3 來定義充電樁安全要求嗎？

# ISA/IEC 62443

一般	62443-1-1	62443-1-2	62443-1-3	62443-1-4	
	概念與模型	主要用語與縮寫	系統安全符合性指標	安全生命週期與使用案例	
政策與程序	62443-2-1	62443-2-2	62443-2-3	62443-2-4	62443-2-5
	IACS 資產擁有者 安全管理制度需求	IACS 保護等級	IACS 環境的更新管理	IACS 方案 供應商需求	IACS 資產管理 者實作指引
技術	62443-3-1	62443-3-2	62443-3-3		
	供 IACS 的 安全技術	安全風險評估與系統設計	系統安全需求與安全等級		
組成	62443-4-1	62443-4-2			
	產品發展需求	IACS 組成之技術安全需求			





## IEC 62443-3-3 中工控場域資訊安全的 7 項基本要求

基礎	相關流程例
FR1 – 識別和認證控制 (Identification and Authentication Control, IAC)	用戶認證和授權
FR2 – 使用控制 (Use Control, UC)	角色和責任的執行
FR3 – 系統完整性 (System Integrity, SI)	檔案變更的管理
FR4 – 資料保密性 (Data Confidentiality, DC)	使用加密技術
FR5 – 限制資料流 (Restrict Data Flow, RDF)	網路分段
FR6 – 及時回應事件 (Timely Response to Event, TRE)	稽核日誌
FR7 – 資源可用性 (Resource Availability, RA)	系統備份與恢復

# 資訊安全等級(Security Level)


一般做認證大多選擇  
這二個等級之一

定義的安全等級 (Security Levels Defined, SLs)	
SL 0	無需特定要求或安全保護 (No specific requirements or security protection necessary)
SL 1	Protection against casual or coincidental violation 防止偶然或偶然的違規行為
SL 2	能避免使用簡單方法、低度資源、一般技術，與低動機人員所引發的未經授權資訊揭露 (Protection against intentional violation using simple means with low resources, generic skills and low motivation)
SL 3	能避免使用複雜方法、中度資源、有 IACS 特殊技術，與中度動機人員所引發的未經授權資訊揭露 (Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation)
SL 4	能避免使用複雜方法、豐沛資源、有 IACS 特殊技術，與高度動機人員所引發的未經授權資訊揭露 (Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation)

# FR1 - 在進行存取前，能夠透過身分鑑別的方式，確認存取者的身分

			SL1	SL2	SL3	SL4	
功能要求	SR1.1 - 人員用戶之識別與鑑別	要提供使用者鑑別能力					
		增項1：唯一的識別與鑑別					
		增項2：用於所有介面之多重因子鑑別					
	SR1.2 - 軟體程序與裝置之識別與鑑別	要能夠識別軟體與裝置					
		增項1：唯一的識別與鑑別					
	SR1.3 - 帳戶管理	要提供帳號管理功能					
	SR1.4 - 識別碼管理	要能夠發給與管理識別碼					
	SR1.5 - 鑑別器管理 (像是 Token、金鑰等)	提供鑑別器的管理功能					
		增項 1：供鑑別器之硬體安全機制					
	SR1.6 - 無線存取管理 (參考 NDR 1.6)	要能夠識別會透過無線存取的使用者					
	SR 1.7 - 以密碼為基礎之 鑑別之強度	要能夠強制要求密碼的長度					
		增項 1：人員用戶之密碼產生與生命週期限制					
		增項 2：用於所有用戶(人員、軟體程序或裝置)之密碼生命週期限制					





















































  

		SL1	SL2	SL3	SL4
NDR1.6 - 無線存取管理	限制無線網路存取				
	增項1：用戶的唯一的識別與鑑別				

# FR1 - 在進行存取前，能夠透過身分鑑別的方式，確認存取者的身分 (續)

			SL1	SL2	SL3	SL4	
功能要求	SR1.8 - 公開金鑰基礎設施憑證	要按照最佳實務運行 PKI 機制			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SR1.9 - 以公開金鑰為基礎之鑑別之強度	憑證驗證與金鑰的使用要符合最佳實務 增項 1：供公開金鑰鑑別之硬體安全機制			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SR1.10 - 對鑑別之回饋	身分鑑別程序避免暴露太多資訊			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SR 1.11 - 登錄嘗試失敗	紀錄失敗的登入操作			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SR 1.12 - 系統使用通知	提供系統使用須知			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SR 1.13 – 經由不受信賴網路之存取	限制從未信任網路的存取			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	SR 1.14 – 以對稱金鑰為基礎之鑑別之強度	使用對稱式金鑰時要滿足最佳實務 增項 1：供對稱金鑰之硬體安全機制			<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## FR2 - 落實對於鑑別身份用戶(人員、軟體程序或裝置)所分派的權限，以限制其對組件行使之要求，並監視此等權限使用

功能要求			SL1	SL2	SL3	SL4	
	SR2.1 - 授權落實	要按照最小需求與分工原則進行授權					
		增項 1：強制執行所有用戶(人員、軟體程序與裝置)之授權					
		增項 2：權限映射(permission mapping)到角色					
		增項 3：管理者 (Supervisor) 重設權限					
		增項 4：雙重核准					
	SR2.2 - 無線使用控制	要採用最佳實務進行無線存取授權					
	SR2.3 - 對於可攜式與行動裝置之使用控制	限制可攜式媒體的使用					
	SR2.4 - 行動碼 (參考SAR 2.4、EDR 2.4、HDR 2.4、NDR 2.4)	限制行動碼的使用					
	SR2.5 - 連線鎖	一段時間後要進行連線鎖定					
	SR2.6 - 遠端連線終止	遠端連線時間限制					
	SR2.7 - 並行連線控制	能夠限制同時的連線數					
	SR2.8 - 事件可稽	紀錄事件以便之後稽核					
	SR2.9 - 儲存稽核能力	要提供足夠的空間以儲存紀錄					
		增項 1：達到稽核記錄儲存能力臨界值時發出警告					

		SL1	SL2	SL3	SL4
HDR2.4 - 行動碼	限制行動程式碼的執行				
	增項 1：行動碼真確性檢查				

**FR2 - 落實對於鑑別身份用戶(人員、軟體程序或裝置)所分派的權限，以限制其對組件行使之要求，並監視此等權限使用 (續)**

			SL1	SL2	SL3	SL4
功能要求	SR2.10 - 對稽核處理失效之回應	紀錄失效時要能夠做警報				
		紀錄產生時要有時間				
	SR2.11 - 時戳	增項 1：時間同步				
		增項2：保護時間源之正確性				
	SR2.12 - 不可否認性	要能夠證明使用者進行的活動				
		增項 1：所有用戶的不可否認性				
SR2.13 - 實體性診斷與測試介面之使用 (參考EDR 2.13、HDR 2.13、NDR 2.13)						

			SL1	SL2	SL3	SL4
HDR2.13 - 避免使用實體診斷與測試介面	對於實體診斷與測試界面的限制					
	增項 1：主動監視					






# FR3 - 系統應確保元件之完整性與正確性，防止未經授權的操弄或修改

			SL1	SL2	SL3	SL4			
功能要求	SR3.1 - 通訊正確性	保護傳輸資料的正確性	●	●	○	○	○	○	○
		增項 1：通訊鑑別			○	○	○		○
	SR3.2 - 惡意程式碼之防範 (參考SAR 3.2、EDR 3.2、HDR 3.2、 NDR 3.2)	對於惡意程式的預防							
	SR3.3 - 資安功能查證	對於安全功能的驗證	●	●	○	○	○	○	○
		增項 1：正常操作期間之資安功能查證							○
		避免軟體與資訊被竄改	●	●	○	○	○	○	
	SR3.4 - 軟體與資訊正確性	增項 1：軟體與資訊之真確性(Authenticity)			○	○	○	○	
		增項 2：違反完整性之自動通知					○	○	
	SR3.5 - 輸入驗核	對輸入資料要進行檢查	●	●	○	○	○	○	○
	SR 3.6 – 輸出結果之確認 (Deterministic Output)	對輸出資料要進行檢查	●	●	○	○	○	○	
SR3.7 - 錯誤處理	能夠發現錯誤並進行處理	●	●	○	○	○	○	○	
SR3.8 - 連線完整性	要能拒絕不正確的連線	●	●		○	○	○	○	
SR3.9 - 稽核資訊之保護	保護稽核紀錄避免被竄改	●	●		○	○	○		
	增項 1：一次性寫入媒體的稽核記錄						○		

		SL1	SL2	SL3	SL4
HDR3.2 - 惡意程式碼之防範	對於惡意程式的防範	○	○	○	○
	增項 1：報告保護程式的版本		○	○	○














## FR3 - 系統應確保元件之完整性與正確性，防止未經授權的操弄或修改 (續)

		SL1	SL2	SL3	SL4
SR3.10 - 支援更新 (參考EDR 3.10、HDR 3.10、NDR 3.10)	 	功能要求			
SR3.11 - 實體性篡改抵抗與偵測 (參考EDR 3.11、HDR 3.11、NDR 3.11)					
SR3.12 - 提供產品供應商之信賴根源 (root of trust) (參考EDR 3.12、HDR 3.12、NDR 3.12)					
SR3.13 - 供應資產擁有者之信賴根源 (root of trust) (參考EDR 3.13、HDR 3.13、NDR 3.13)					
SR3.14 - 啟動程序之完整性 (參考EDR 3.14、HDR 3.14、NDR 3.14)					
		SL1	SL2	SL3	SL4
HDR3.10 - 支援更新	提供更新功能	○	○	○	○
	增項 1：更新真確性與完整性		○	○	○
HDR3.11 - 實體性篡改抵抗與偵測	能夠對實體性竄改進行偵測		○	○	○
	增項1：通報篡改意圖			○	○
HDR3.12 - 提供產品供應商之信賴根源 (root of trust)	要提供供產品供應商識別的機制		○	○	○
HDR3.13 - 供應資產擁有者之信賴根源 (root of trust)	要提供供資產擁有者識別的機制		○	○	○
HDR3.14 - 啟動程序之完整性	要確保啟動程序沒被竄改	○	○	○	○
	增項1：啟動程序之真確性		○	○	○
































## FR4 - 確保在傳輸中資料和儲存資料之機密性，以防止未經授權的揭露

				SL1	SL2	SL3	SL4		
功能要求	SR4.1 - 資訊機密性	保護機密資訊避免未經授權存取	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
		要提供資料抹除功能	 		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
	SR4.2 - 資訊持續性	增項 1：共享記憶體資源的抹除				<input type="radio"/>	<input type="radio"/>		
		增項 2：抹除查證				<input type="radio"/>	<input type="radio"/>		
	SR4.3 - 密碼學技術之使用	使用業界認可的演算法與金鑰長度	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
















# FR5 - 對控制系統進行分割，以限制不必要的資料流

與環境  
有關


























功能要求

			SL1	SL2	SL3	SL4	
與環境 有關	SR5.1 - 網路隔離 (Network Segmentation)	提供網路分割能力					
	SR5.2 - 區域邊界保護 (參考 NDR 5.2)	對跨邊界的通訊進行監控與防護					
	SR5.3 - 一般目的的人對人通訊之限制 (參考 NDR 5.3)	限制人與人間的通訊					
	SR 5.4 - 應用程式分區(Application partitioning)	將應用程式分區					
			SL1	SL2	SL3	SL4	
功能要求	在區域邊界進行監控與防護						
	增項1：全部拒絕，允許例外						
	增項2：孤島模式						
	增項3：失效關閉 (Fail Close)						
	NDR5.3 - 一般目的的人對人通訊之限制	限制一般目的的人對人通訊					

# FR6 - 當發現事件時，能通知有關單位事件的發生與相關證據，並及時採取矯正動作，以因應資安違規行為

功能要求					SL1	SL2	SL3	SL4	
SR 6.1 - 稽核日誌可存取性	要讓有權限的人能夠讀到唯讀的日誌								
	增項 1：透過 API，提供程序化的日誌存取								
與環境有關	SR6.2 - 持續監視								
	持續監控各安全機制的效能								

# FR7 - 確保元件的可用性，防止基本服務的降級或無法被存取

功能要求			SL1	SL2	SL3	SL4		
	SR7.1 - 避免服務拒絕(Denial of Service)攻擊	提供遭受 DoS 攻擊的降級模式	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	 
		增項 1：透過限速等方式管理通訊負載		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
	SR7.2 - 資源管理	限制對安全功能資源的使用以避免資源耗竭	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
		提供備份功能	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
	SR7.3 - 控制系統備份	增項 1：備份完整性查證		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
		增項 2：自動備份			<input type="radio"/>	<input type="radio"/>		
	SR7.4 - 控制系統的還原與重建	要能利用備份進行還原	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	 
	SR 7.5 - 緊急電源	提供緊急電源		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
	SR 7.6 網路與安全組態之設定	提供安全組態設定指引	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
		增項 1：機器可讀取的當前資安設定報告				<input type="radio"/>	<input type="radio"/>	
	SR7.7 - 使用最小功能(Least Functionality)	只能使用最小需要功能	 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	 
	SR7.8 - 控制系統元件財產目錄	提供元件盤點功能	 		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	



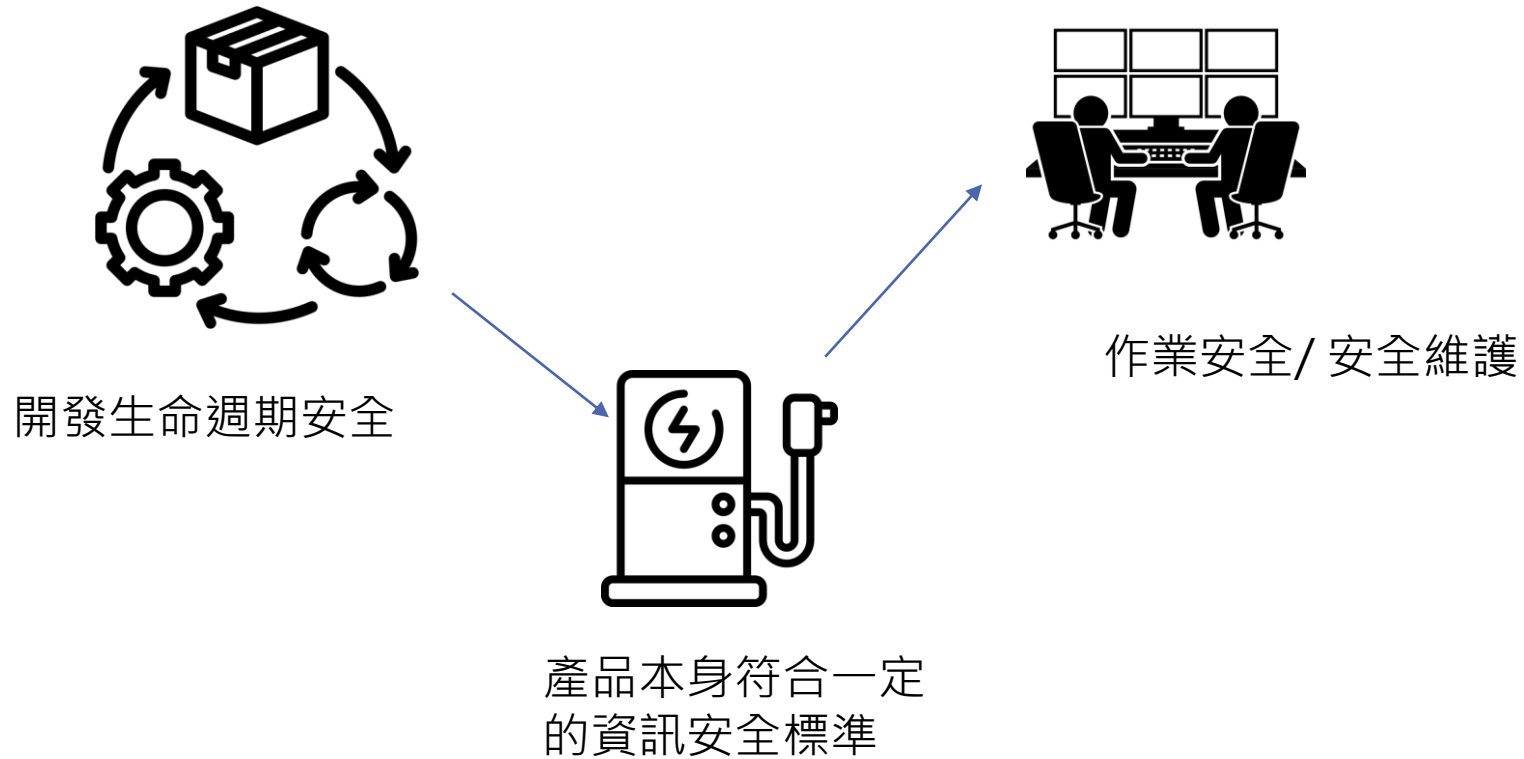
充電樁的資安風險

目前充電樁的資安規範與缺口

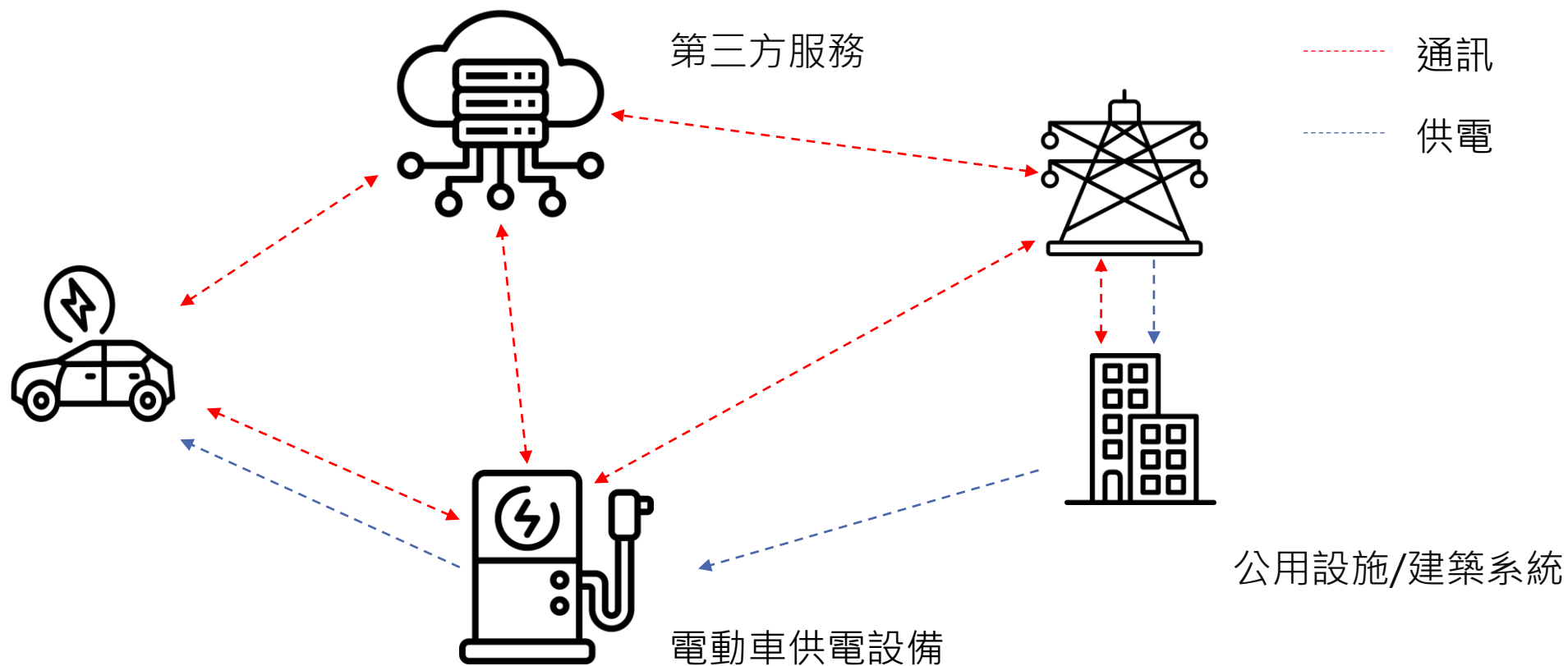
從設備的資安到維運時的資安考量

結論

# 產品安全與實地運作安全



# NIST IR 8473 針對整個快速充電生態系



# NIST IR 8473 的目的

透過安全通訊來達成可靠的效能

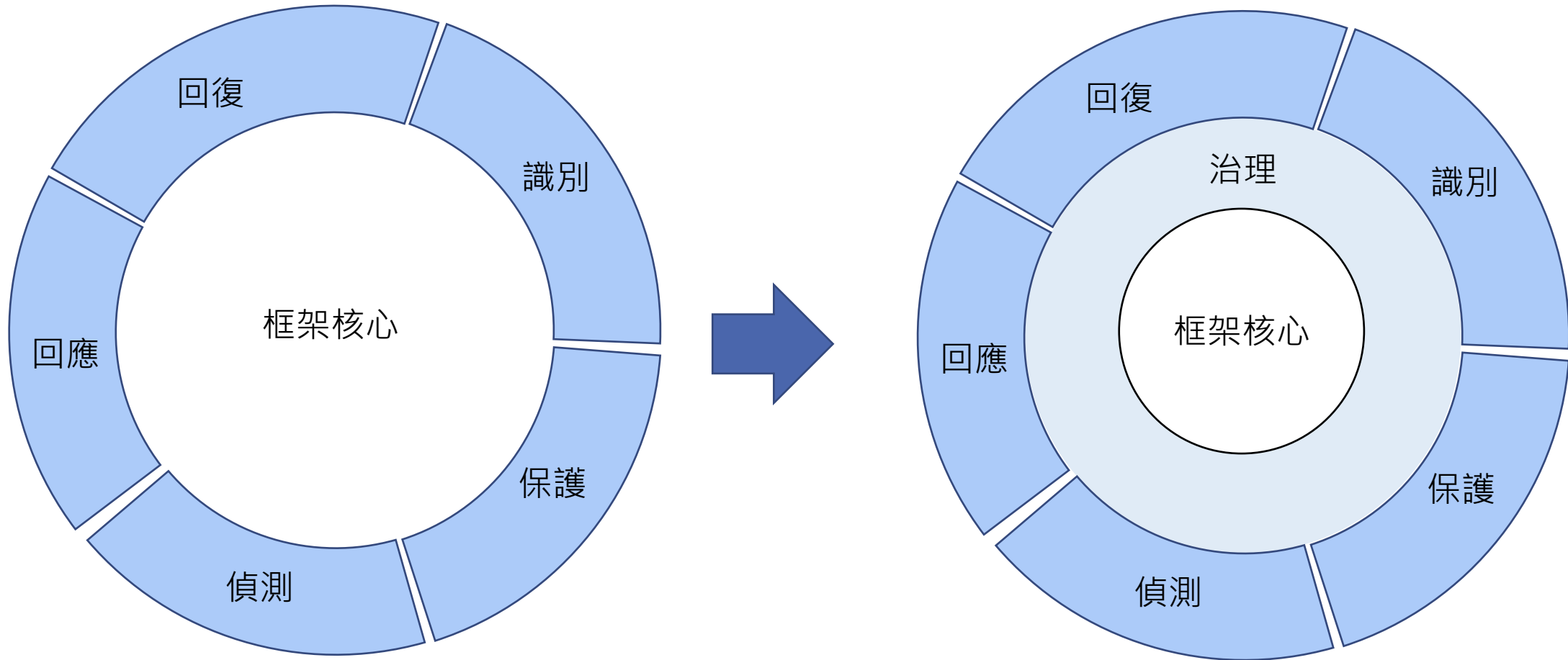
維護骨幹的安全與韌性

建立與維護各方間的信任關係

在面對攻擊時，仍能持續運作



# NIST IR 8473 還是基於 NIST CSF 1.1



# 充電站在識別功能的要求

- 資產管理 (Asset Management, AM)

- ★ AM-1：盤點充電站相關的實體裝置與系統 (SR 7.8)
- ★ AM-2：盤點軟體平台與應用程式，並且維持更新 (SR 7.8)
- ★ AM-3：將組織的通訊與資料流進行對應，並且限制對於充電站的通訊
- AM-4：將外部資訊系統分類，如公用設施、建築系統，或第三方服務等
- AM-5：依照不同種類的充電站，按照資源的重要性與價值進行排序
- ★ AM-6：指派人員的資安角色與責任，而充電站製造商要考慮到產品的後續維運

確保元件安全

限制連線

識別相關單位與  
定義責任

- 企業環境 (Business Environment, BE)

- ★ BE-1：識別充電站在供應鏈中的角色，如生產者、EV 資料使用者，通訊工具提供者等
- BE-2：了解充電站在關鍵基礎設施的角色，並且掌握服務中斷的影響
- BE-3：了解充電站製造商、擁有者，與維運者在資安與作業上的要求，並將要求排序
- BE-4：充電站的製造商、擁有者，與維運者要知道其在生態系當中的重要性
- BE-5：充電站製造商應考量到產品的韌性要求

## 充電站在識別功能的要求 (續)

- 治理 (Governance, GV)

- ★ GV-1：在生態系中，要有一致性的資安政策與程序
- ★ GV-2：要考慮到資訊安全的角色與責任，並且與其他單位相校準
- ★ GV-3：盤點法規上對資安的要求
- ★ GV-4：在治理與風險管理程序中考慮到資通安全風險

識別相關單位與  
定義責任

- 風險評估 (Risk Assessment)

- ★ RA-1：識別與紀錄資產弱點，像是未被控管的連接埠、實體安全不足、不正確的韌體，過時的系統等
- ★ RA-2：從資訊分享社群接收威脅情資
- ★ RA-3：內外部的威脅被識別與紀錄
- ★ RA-4：識別對企業的衝擊與可能性
- ★ RA-5：使用威脅、弱點、衝擊，與可能性來計算風險
- ★ RA-6：有識別風險回應並做排序

執行安全檢查

## 充電站在識別功能的要求 (續)

- 風險管理 (Risk Management, RM)

- ★ • RM-1：有建立風險管理程序，並被利害關係人同意，利害關係人包括合作夥伴、供應商，與相關機構
- ★ • RM-2：組織的可容忍風險值被決定且清楚表示
- ★ • RM-3：組織有將可容忍風險值通知生態系中相關的其他角色

- 供應鏈風險管理 (Supply Chain Risk Management)

- ★ • SC-1：要針對充電樁的關鍵元件，進行供應鏈資通安全風險管理程序
- ★ • SC-2：要用供應鏈資通安全風險管理程序，去評估供應商與第三方的資訊系統、元件，與服務，但要考量到有些元件可能相對選擇較少
- ★ • SC-3：在與供應商或第三方單位簽約時，要求其達到資通安全目標，以滿足組織的供應鏈風險管理計畫
- ★ • SC-4：透過稽核確認供應商或第三方單位有符合相關要求 (SR 6.1)
- ★ • SC-5：確認供應商或第三方單位的回應與回復活動有符合相關要求 (SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4)

執行安全檢查

# 充電站在保護功能的要求

- 身分管理、身分鑑別，與存取控制 (Identity Management, Authentication and Access Control, AC)
  - ★ • AC-1：對於授權使用者與裝置的身分與驗證資訊之發放、管理、驗證、註銷，與稽核等，皆有妥善程序 (SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9)
  - ★ • AC-2：對資產的實體存取要被管理與保護。充電站像是電池儲存機制 (Battery Energy Storage System, BESS)、網路通訊設備，交易機制都需要特別被考量
  - ★ • AC-3：遠端存取管理 (SR 1.13, SR 2.6)
  - ★ • AC-4：存取授權有滿足最小需求原則與分工原則 (SR 2.1)
  - ★ • AC-5：有保護網路正確性 (SR 3.1, SR 3.8)
  - ★ • AC-6：身分資訊有被驗證，並且有綁定驗證資訊，而在互動時有檢驗 (SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1)
  - ★ • AC-7：使用者、裝置，與其他資產，有被採用與交易風險相襯的方式進行身分鑑別 (SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10)
- 教育訓練與宣導 (Awareness and Training, AT)
  - AT-1：每個員工必須被告知資通安全的責任，並進行訓練
  - AT-2：特權使用者了解其角色與責任
  - AT-3：第三方利害關係人了解其資安的角色與責任
  - AT-4：資深高階經理人了解其資安的角色與責任
  - AT-5：實體與資通安全人員，了解其角色與責任

使用者與  
權限管理

## 充電站在保護功能的要求 (續)

- 資料安全 (Data Security, DS)

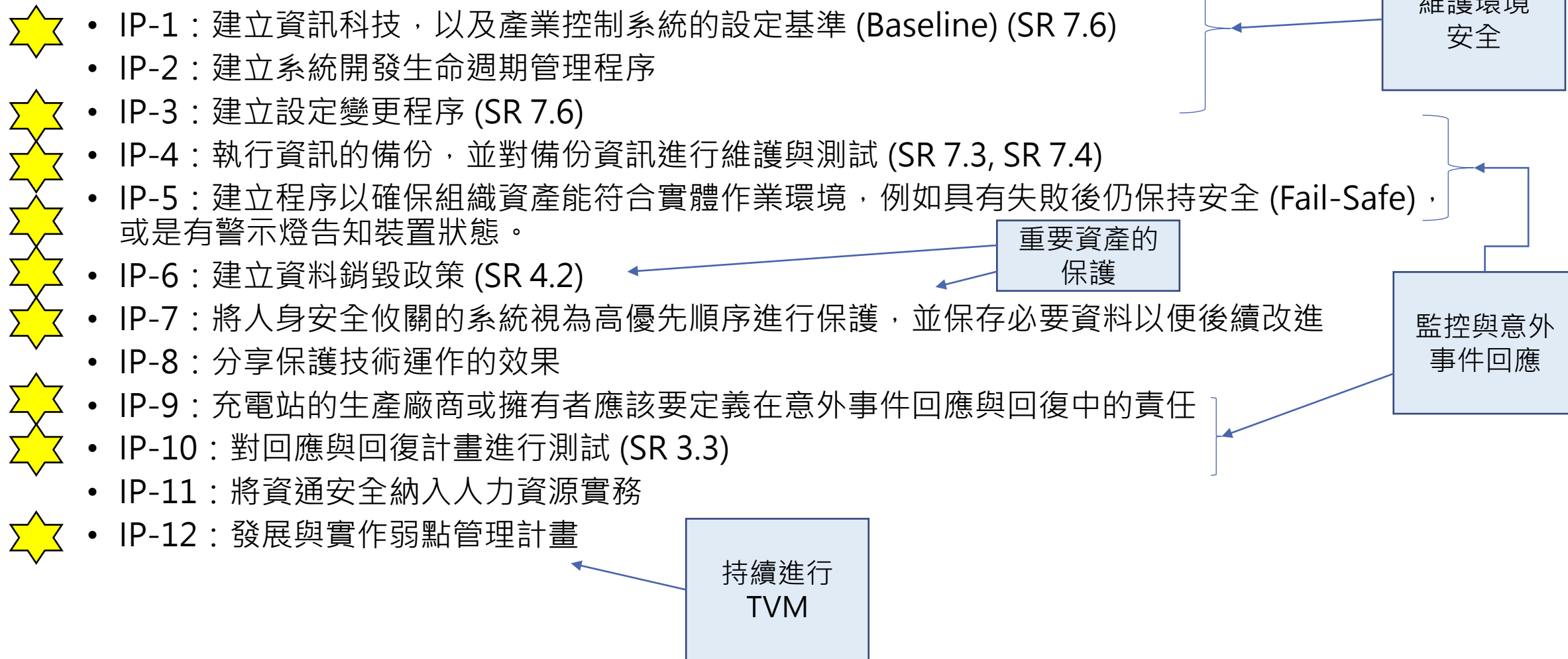
- ★ DS-1：靜態資料 (Data-at-Rest, DAR) 的保護 (SR 3.4, SR 4.1)
- ★ DS-2：資料傳輸 (Data-in-Transit, DIT) 的保護 (SR 3.1, SR 3.8, SR 4.1, SR 4.2)
- ★ DS-3：資產在移除、轉移，和拋棄的過程中都有被管理 (SR 4.2)
- ★ DS-4：建立適當的容量以確保可獲得性 (SR 7.1, SR 7.2)
- ★ DS-5：保護 EV 所有人與付款資訊，避免被外洩 (SR 5.2)
- ★ DS-6：驗證軟體、硬體，與資訊的正確性 (SR 3.1, SR 3.3, SR 3.4, SR 3.8)
- ★ DS-7：將開發、測試，與生產環境分開
- ★ DS-8：驗證硬體機制的正確性，例如驗證人身安全 (Safety) 保護系統的正确運作

執行安全  
檢查

維護環境  
安全

## 充電站在保護功能的要求 (續)

- 資訊保護與處理 (Information Protection and Processes, IP)





## 充電站在保護功能的要求 (續)

- 維護 (Maintenance, MA)

- ★ MA-1：對於充電站資產的維護與維修有進行紀錄，並且只可透過被核可的工具進行
- ★ MA-2：對於充電站資產遠端維護必須有經過核可與紀錄，並能避免未經授權存取

- 保護技術 (Protective Technology, PT)

- ★ PT-1：建立政策，以定義要使用的稽核紀錄，之後按程序執行紀錄，並進行審查 (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12)
- ★ PT-2：定義可攜式媒體的保護政策，並依照政策限制其使用 (SR 2.3)
- ★ PT-3：將最小權限原則整合到設定管理系統中，以確保充電站只提供基本功能 (SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7)
- ★ PT-4：保護控制系統網路的通訊 (SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6)
- ★ PT-5：建立在正常狀態與異常狀態下確保韌性的機制 (SR 7.1, SR 7.2)

使用者與  
權限管理

重要資產的  
保護

維護環境  
安全

監控與意外  
事件回應



# 充電站在偵測功能的要求

監控與意外  
事件回應

- 異常與事件(Anomalies and Events, AE)

- ★ AE-1：建立與管理使用者網路作業與期待資料流的基準
- ★ AE-2：對偵測到的事件進行分析，以發現其目標和方法 (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2)
- ★ AE-3：從多個來源或感應器中收集資料並建立關聯 (SR 6.1)
- ★ AE-4：決定事件的衝擊
- ★ AE-5：建立意外事件警報的門檻

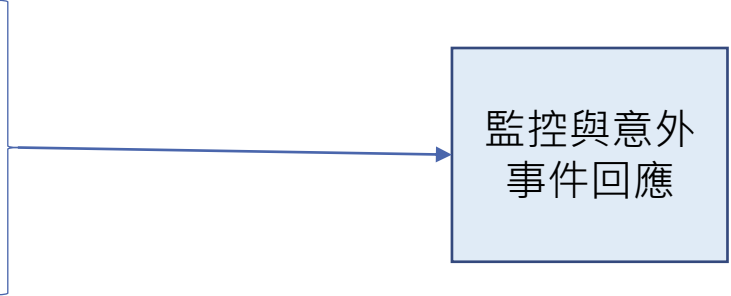
- 安全持續監控 (Security Continuous Monitoring, CM)

- ★ CM-1：監控網路以發現可能的資通安全事件 (SR 6.2)
- ★ CM-2：由實體環境的硬體狀態，去發現可能的資通安全事件
- ★ CM-3：監控使用者行為，以發現可能的資通安全事件 (SR 6.2)
- ★ CM-4：偵測惡意程式碼 (SR 3.2)
- ★ CM-5：偵測未經授權的行動程式碼 (SR 2.4)
- ★ CM-6：偵測外部服務提供者的活動，如遠端連線的嘗試、設定變更，與軟體更新等，以發現可能的資通安全事件
- ★ CM-7：透過監控以發現未經授權的人員、裝置、連線，與執行的軟體
- ★ CM-8：執行弱點掃描

執行安全檢查

## 充電站在偵測功能的要求 (續)

- 偵測程序 (Detection Processes, DP)
  - ★ DP-1：定義偵測的角色與責任，以確保可究責性
  - ★ DP-2：偵測活動符合所有適用的需求
  - ★ DP-3：偵測程序有被測試 (SR 3.3)
  - ★ DP-4：偵測的事件資訊有被妥善的傳遞 (SR 6.1)
  - ★ DP-5：偵測程序有被持續改善



監控與意外  
事件回應

# 充電站在回應功能的要求

- 分析 (Analysis, AN)

- ★ AN-1：依據偵測系統的通知進行調查 (SR 6.1)
- ★ AN-2：了解意外事件的衝擊
- ★ AN-3：執行鑑識 (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1)
- ★ AN-4：意外事件被按照回應計畫分類
- ★ AN-5：建立從組織內外接收弱點並進行回應的程序

監控與意外  
事件回應

- 溝通 (Communications, CO)

- CO-1：人員知道在活應作業當中的角色
- CO-2：依照既有的規定，一致性的對意外事件進行報告
- CO-3：依照回應計畫分享資訊
- CO-4：依照回應計畫與利害關係人溝通
- CO-5：自願對外界進行資訊分享，以便外部利害關係人了解資安事件狀況

持續進行  
TVM

## 充電站在回應功能的要求 (續)

- 改善 (Improvements, IM)

- ★ • IM-1：將從事件中學習的經驗納入回復計畫

- ★ • IM-2：更新回應策略

- 減輕 (Mitigation, MI)

- ★ • MI-1：限制意外事件發生後的影響 (SR 5.1, SR 5.2, SR 5.4)

- ★ • MI-2：減輕意外事件可能帶來的影響

- ★ • MI-3：管理新發現的弱點，使其風險可被接受

- 回應規劃 (Response Planning, RP)

- ★ • RP-1：因應意外事件，在過程中或事後執行回應計畫

監控與意外  
事件回應

持續進行  
TVM

# 充電站在回復功能的要求

- 溝通 (Communications, CO)
  - CO-1：管理公共關係
  - CO-2：在意外事件後修復聲譽
  - CO-3：對內外利害關係人與高階主管團隊溝通回復活動

- 改善 (Improvements, IM)

- ★ • IM-1：從過去的經驗中學習並調整回復計畫

- ★ • IM-2：更新回復策略

- 回復規劃 (Recover Planning, RP)

- ★ • RP-1：在意外事件發生後執行回復計畫

監控與意外  
事件回應



充電樁的資安風險

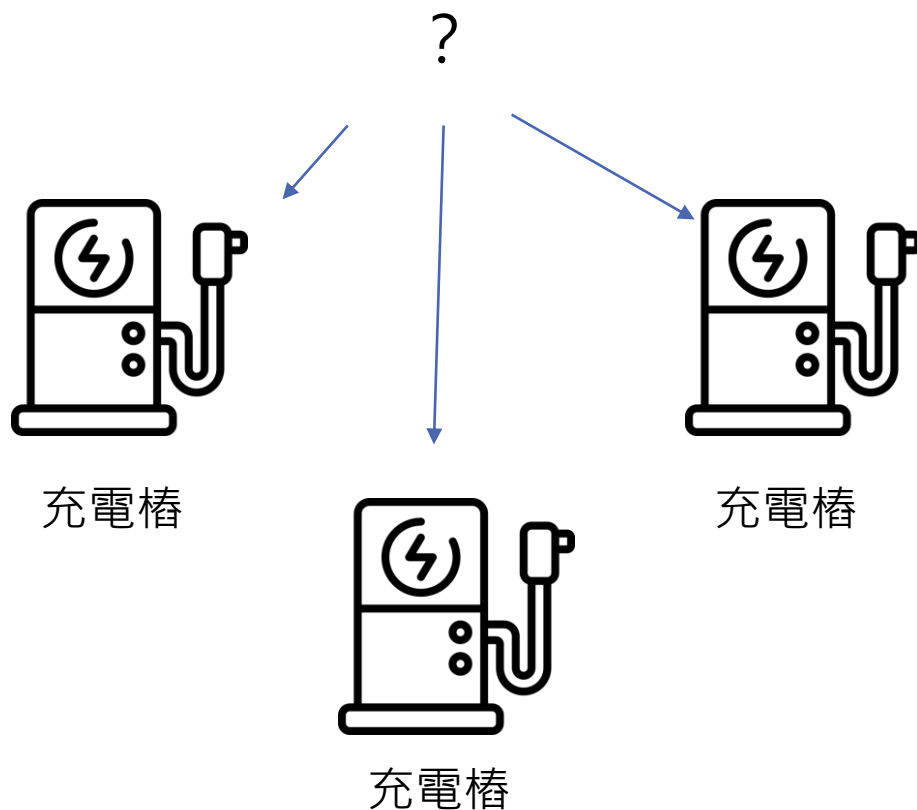
目前充電樁的資安規範與缺口

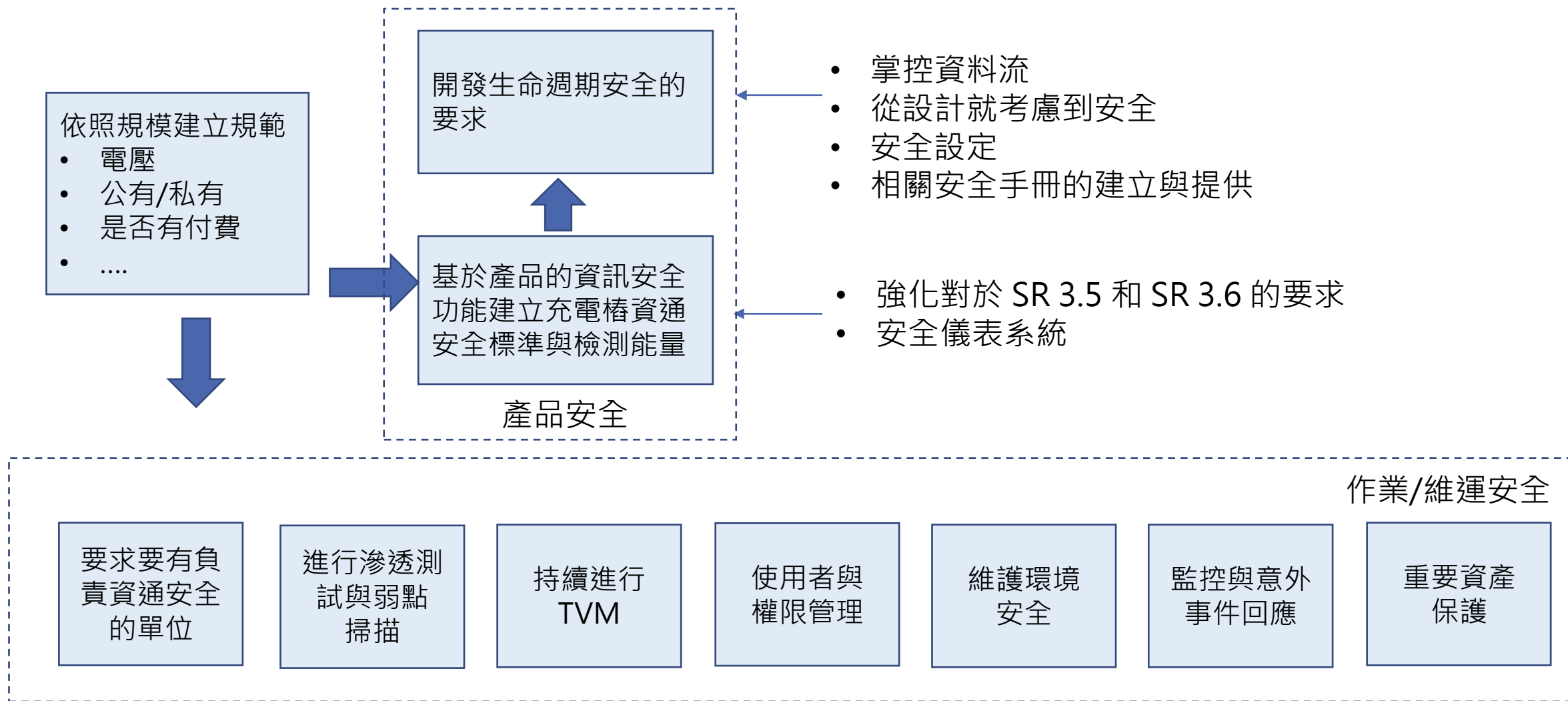
從設備的資安到維運時的資安考量

結論

## 結論

- 隨著電動車的數量增長，充電樁的需求也隨之增加，但是若未考慮到人身與環境安全，則推動時就會受到影響
- 目前我國的充電樁安全標準，較偏重於人身與環境安全
  - 充電樁具有 OT 的特性，可能因為資通安全問題，而造成人身與環境安全問題
- 雖然有「電動車供電設備資訊安全檢測技術規範」，但是還是多半只著重於充電樁產品本身的安全性
- 充電樁會特別需要考慮和電動車以及電力系統連線的安全性
- 除了應具備有一定的安全功能外，也應該要考慮到作業/維運安全
- 應該要有一個單位，按照資通安全維護標準，去維護充電樁安全







謝謝各位的聆聽

