智慧車聯網資安國際規範及應對措施

車輛中心 產業發展處 李佩蓉

隨著智慧車聯網技術的普及，資安需求成為汽車產業的關鍵議題。若系統遭遇駭客攻擊，可能影響汽車控制系統，對駕駛和乘客安構成威脅。為此，各國政府和企業加強相關政策與解決方案，確保車聯網的安全。本篇介紹智慧車聯網的國際規範及應對措施。

智慧車聯網的資安挑戰及聯合國法規

智慧車聯網核心在數據傳輸的即時性與安全性，相較傳統汽車更容易受到網路攻擊，聯合國在2020 年制定車輛網絡安全和軟體更新的兩項法規 UN R155、R156 (如表 1)，UN R155 規定製造商建立網路安全管理系統，涵蓋從設計、製造到供應鏈需防範安全威脅；R156 規範 OTA 軟體更新管理系統，防止駭客利用漏洞進行惡意更新。

上述法規 2021 年 1 月份生效，規定從 2024 年 7 月起，所有車型須通過標準，才能在歐盟、日本、南韓等會員國銷售，如 Porsche 原計畫 2024 年在歐洲推出 Macan 的燃油版與純電版，但因燃油版不符規定，於歐洲停售。

	UN R155 車輛網路安全管理系統	UN R156 軟體更新管理系統
規範	要求車輛製造商，建立「網絡安全管理系統(CSMS)」，確保車輛在生命周期的網路安全	針對 OTA，製造商需制定標準流程，確保軟體更新即時且安全進行，在更新過程減少風險
執行標準	ISO/SAE 21434，涵蓋道路車輛的 E/E(電汽及電子)系統概念、產品開發、生產、操作、維護與除役報廢	ISO 24089，軟體更新機制的安全框架，包含軟體開發基礎架構的安全性要求、軟體升級過程中的風險管控等

表 1，UNECE R155、R156 規範內容

資料來源：新聞媒體，車輛中心整理

國際汽車產業推動 SBOM 確保符合 UN R155 標準

因應智慧車輛資安需求，國際汽車產業推動軟體物料清單（SBOM），確保供應鏈中的軟體符合 UN R155。日本汽車業團體於 2024 年 7 月發布初版 SBOM，以降低供應鏈中軟體命名和規範不一帶來的風險，計畫在 2025 年 3 月推出正式版，目前 Toyota、Denso、Hitachi 等逾

百家日企加入 Japan Automotive ISAC 行列，同時與美國 Auto-ISAC 及歐洲車廠（如 Mercedes-Benz）合作。此外，歐盟於 2024 年 10 月通過網路韌性法案（Cyber Resilience Act，CRA），要求 2027 年前軟體供應商須提供 SBOM，涵蓋車載軟體、車聯網技術，若未符規定，將面臨至少 1,500 萬歐元的罰款。

各國高度重視車輛資安政策把關供應鏈來源

除資訊安全標準外，各國推出資安政策，在供應鏈上對涉及敏感數據和技術的外國供應商採更嚴格的管制。美國商務部於 2024 年提出政策，計劃在 2027 年禁用來自中國大陸車聯網軟體零組件，到 2030 年則禁用硬體零組件，主要車廠如福特與通用調整供應鏈，逐步淘汰中國製零組件。

歐盟對車聯網資安的關注，針對中國大陸的車輛軟體安全風險進行調查，2024 年 9 月歐盟宣布計劃在未來幾周推出「資訊與通訊技術供應鏈工具箱」以管理風險；韓國政府反映對美國政策的憂慮，希望美方設立寬限期減少對韓國車企的衝擊；中國大陸對此持反對態度。

台灣持續推動導入 UN R155、UN R156 政策及驗證能量

因應聯合國 UN R155、UN R156 規定，我國交通部計畫從 2028 年起分階段實施；2024 年 10 月車輛中心與德國 TÜV SÜD 簽署合作備忘錄，設立台灣首座符合 UN R155、R156 標準的驗證機構，協助業者獲取資安防護、軟體更新等領域的測試技術認證，拓展國際市場。

圖 1. UNECE R155、R156 規範內容

資料來源：車輛中心

台灣以 ICT 能量持續拓展車用資安

台灣廠商積極投入車聯網資安，2021 年 MIH 電動車開放平台 EVKit 推動「設計安全」概念，建議在零組件設計階段進行威脅分析和風險評估（TARA），並透過 Zero Trust 加強用戶身份驗證；今年 VicOne 將 SBOM 整合到 XZETA 平台，應用漏洞衝擊評分技術（VVIR）自動偵測異常並即時排除，並獲 ISO/SAE 21434 認證，此外，VicOne 與公信電子、微軟、緯創等策略夥伴合作，確保台灣供應鏈符合國際車廠資安要求；台達電、聯發科等 ICT 廠商成立科絡達發展加密技術，僅當公鑰和私鑰配對時允許更新，確保資料傳輸安全，並計劃拓展日本市場，推動當地電動化與數位轉型。

台灣企業致力發展符合國際車輛網路安全及軟體更新管理標準的資安技術，以此為核心推動供應鏈升級與優化，未來持續與國際夥伴合作，提升國際資安藍海的競爭力。