車輛資安、軟體更新測試技術與驗證

財團法人車輛研究測試中心 研究發展處

車輛資安、軟體更新測試技術與驗證-發展歷程

ARTC 車輛中心

2028.01 法規生效
新型式車輛正式實施安全審驗標準附件96、97

2026.07 服務開始
開始對各大車廠提供資安檢測服務

2026.06 VSCC認證通過
通過VSCC第三方合格資安實驗室

2026.03 建立實驗室
建立車輛資安實驗室

2025.12 建立檢測技術
建立車輛資安檢測技術

2025.10 檢測人員培訓
車輛資安檢測人員培訓

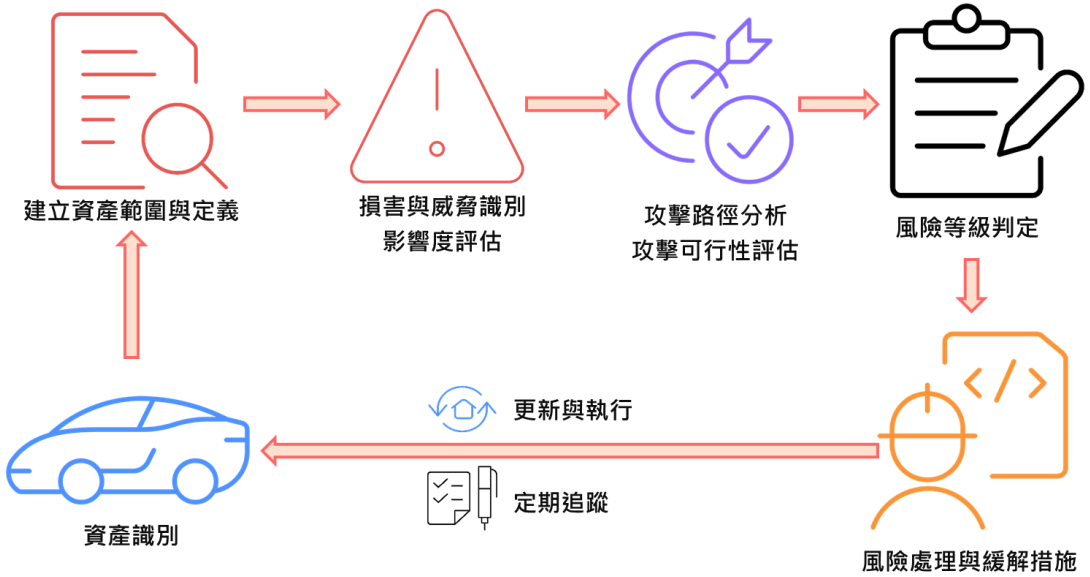
2024.10 資安法規國際合作
與TÜV SÜD攜手建立資安驗證技術

▲ARTC與TÜV SÜD簽訂合作協議

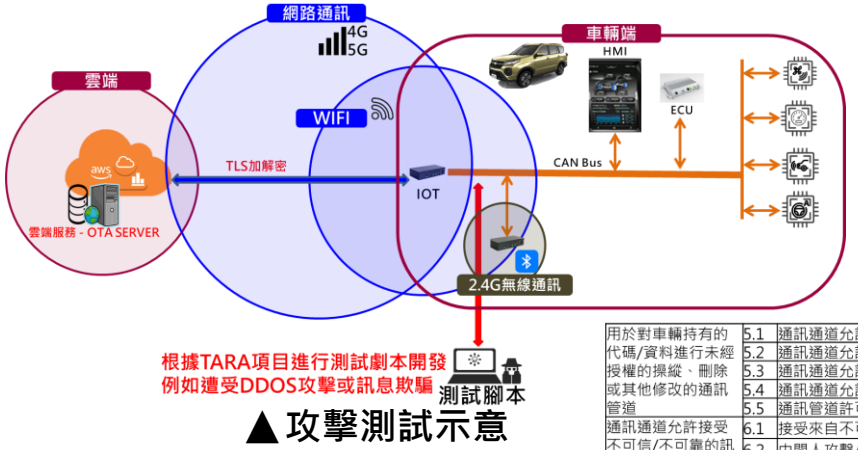

▲前往歐洲進行車輛資安法規培訓

車輛資安測試與驗證服務

- 中心可協助車輛廠商透過對產品建立**威脅與危害影響性分析(TARA)**，對於車輛資安防護可以進一步提升。並且透過TARA分析後的內容**改善並降低各項危害因子**的影響性，並協助驗證業者提出的緩解機制可以正常運行。
  - **驗證目標商品威脅與影響性分析(TARA) ：**
    - **遠端攻擊測試：**透過網際網路連線到車輛系統，進行遠端攻擊。例如，他們可以更改系統中的軟體或硬體，並接管某些車輛功能。
    - **物理接觸攻擊測試：**從車輛內或外部物理接觸到車輛系統。例如，在車輛內部，他們可以透過資料線接入ECU，或者在車輛外部，他們可以利用物理瑕疵來入侵車輛系統。
    - **產品漏洞掃描：**基於動態應用程式安全測試方法進行，通常由漏洞掃描工具格式化輸入，以測試目標軟體是否存在已知的常見安全漏洞。除了檢測已知的漏洞外，還可以通過使用已知攻擊模式進行漏洞掃描來檢測目標軟體中的未知漏洞。例如，攻擊者可能利用硬體漏洞，繞過車輛的安全措施。



▲威脅與危害影響性分析(TARA)流程



▲攻擊測試示意

用於對車輛持有的代碼/資料進行未經授權的操縱、刪除或其他修改的通訊管道	5.1	通訊通道允許程式碼注入，例如，被篡改的軟體二進位檔案可能會被注入到通訊流中。
	5.2	通訊通道允許操縱車輛 持有資料/代碼
	5.3	通訊通道允許覆蓋車輛 保存的資料/代碼
	5.4	通訊通道允許擦除車輛 持有的資料/代碼
	5.5	通訊管道許可向車輛發送資料/代碼（寫入資料代碼）
通訊通道允許接受不可信/不可靠的訊息，或容易受到會話劫持/重播攻擊	6.1	接受來自不可靠或不可信來源的訊息
	6.2	中間人攻擊/會話劫持
	6.3	重播攻擊，例如針對通訊網關的攻擊允許攻擊者降級ECU的軟體或網關的韌體。
資訊可以輕易公開。例如，透過竊聽通訊或允許未經授權存取敏感檔案或資料夾	7.1	攔截訊息/幹擾輻射/監控通信
	7.2	未經授權存取文件或數據
對系統的物理操縱可能會導致攻擊	32.1	操縱電子硬件，例如將未經授權的電子硬體添加到車輛中以實現“中間人”攻擊
	32.1	電子硬體取代經授權的電子硬體（例如感測器）
	32.1	操縱感測器收集的資訊（例如，使用磁鐵篡改連接到變速箱的霍爾效應感測器）

▲測試目的示意

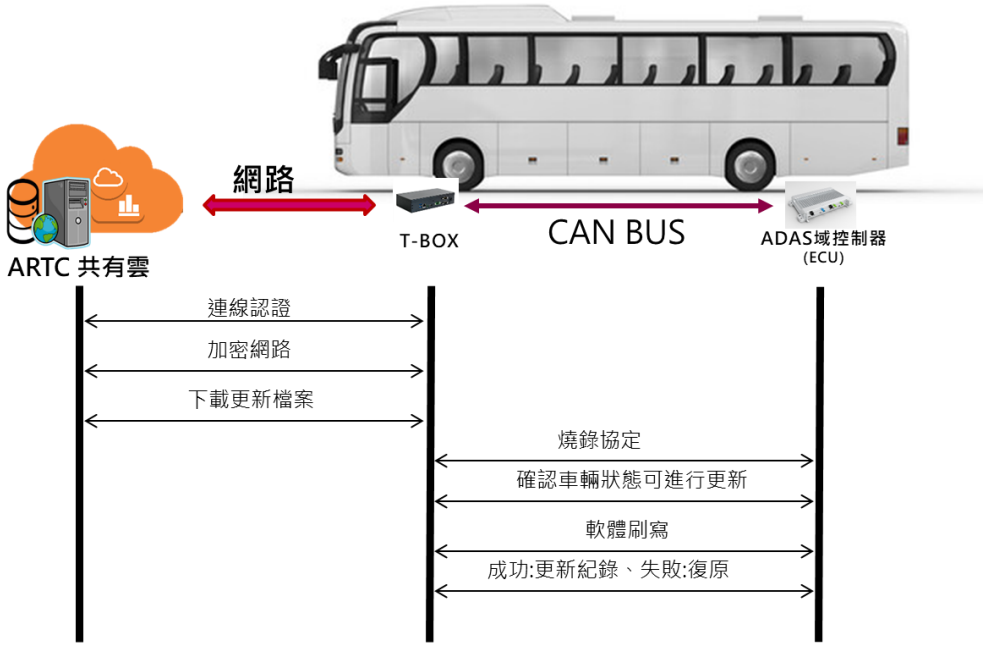
OTA車輛軟體更新測試與驗證-技術規格

特色：

資安防護之OTA車輛軟體更新技術，其包含雲端更新伺服器的建立，以及檔案傳輸過程中對資料的保護及驗證，將資料傳輸至車載硬體上後，透過檢測車輛的安全性與軟體更新的需求進行ECU的刷寫。

驗證技術：

- **符合國際標準UNR 156 (ISO 24089)規範**
  - 更新紀錄
  - 使用者告知
  - 車輛安全
  - 更新失敗100%復原
- **符合車輛安全檢測基準97**
- **符合國際標準AES資料加密技術**
  - 保護檔案完整性100%
- **符合國際標準資料驗證SHA技術**
  - 保護檔案正確性100%
- **符合ISO 14229-1 UDS通訊協議**
  - 權限驗證防止非法燒錄



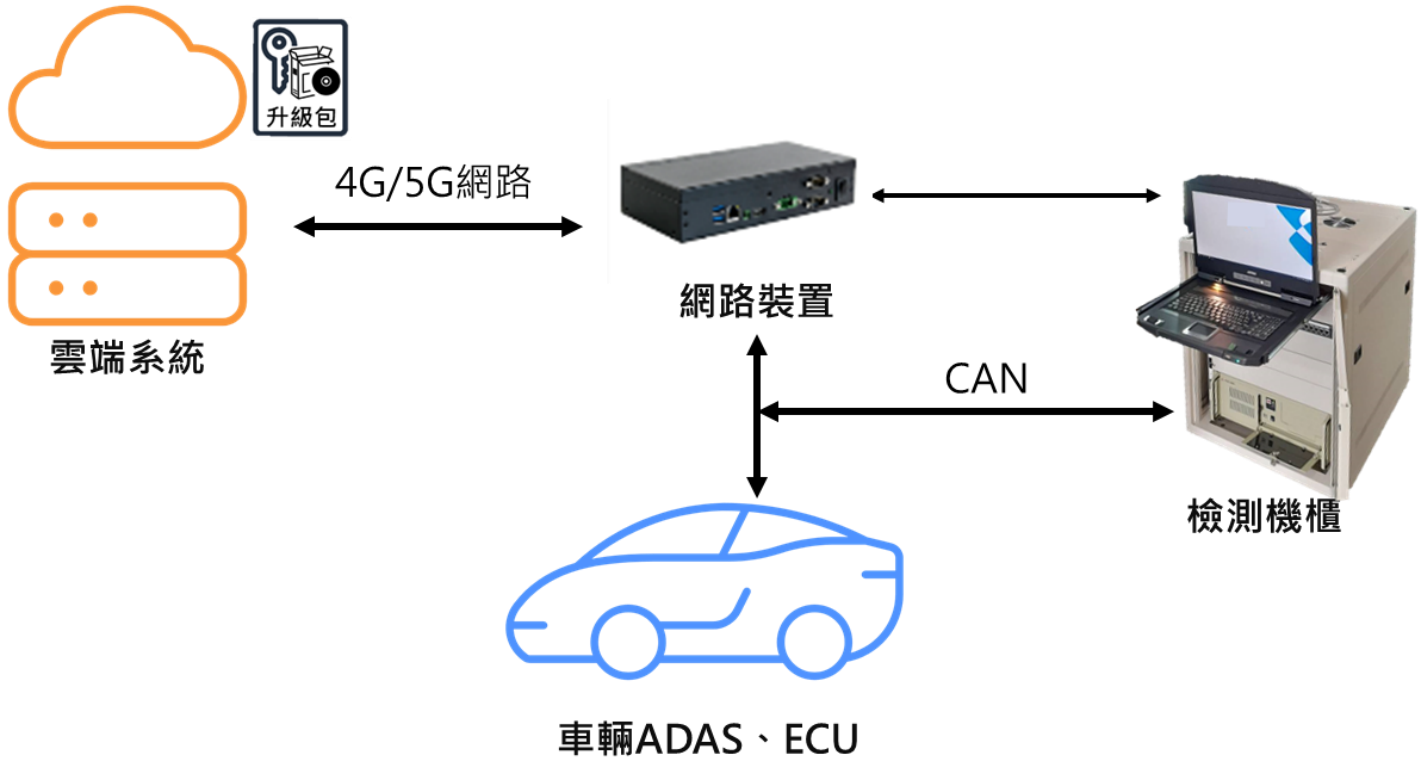
▲ 資安防護之OTA車輛軟體更新系統架構

▲ 更新軟體上傳與通知

OTA車輛軟體更新測試與驗證-檢測服務

- 中心可協助車輛廠商建立**車輛遠端更新技術之能量**，並且可以協助廠商通過法規標準之相關系統驗證，**節省後續實車檢測時間與成本**。
  - **ISO24089軟體更新檢測：**使用ISO 24089特製之檢測系統，**模擬檢測車輛進行遠端軟體更新過程中的11種法規訂定的檢測環境**。

R156檢測項目		
1	主要要求	更新檔案真實性與完整性
2		RXSWIN更新/軟體版本更新
3		RXSWIN讀取/軟體版本讀取
4		RXSWIN讀取/軟體版本防竄改
5	遠端更新要求	更新失敗處理
6		電量保障
7		更新影響車輛安全
8		用戶告知
9		更新影響駕駛安全
10		更新結果告知
11		更新條件



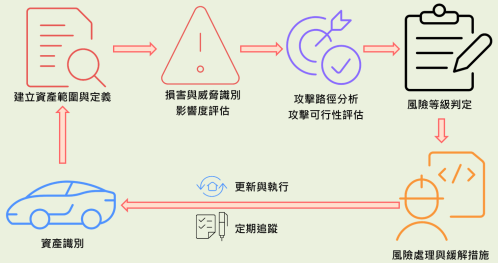
車輛資安、軟體更新測試技術與驗證-產業合作模式

- 透過車輛資安檢測之能量， ARTC協助廠商導入符合UN R155與UN R156法規的車輛資安技術與軟體更新管理系統，提升產業競爭力接軌國際。
- ARTC協助廠商整車驗證-車輛資安與OTA車輛軟體更新之驗證技術。

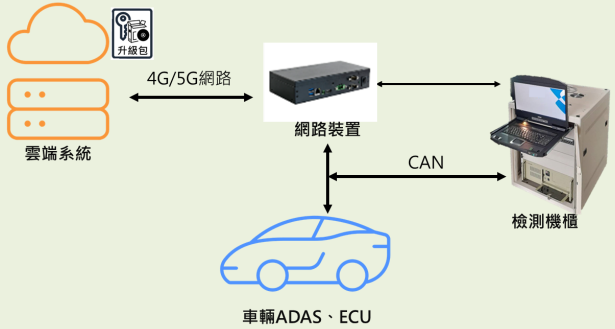
研究單位

OTA車輛軟體更新技術

車輛資安技術

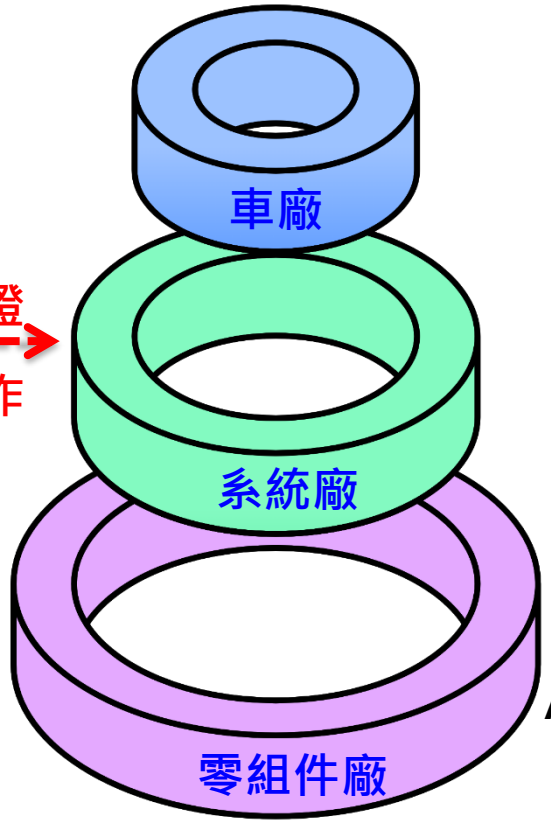


UNR156(ISO 24089)檢測



技術驗證

業界合作



ADAS、ECU

車輛資安、軟體更新測試技術與驗證-可授權專利

車輛聯網

➢ 主要布局資安防護與軟體更新、車外通訊、車內通訊&車網管理等技術專利，相關可授權專利清單如下：

技術分類	專利名稱(國別)	
資安防護與軟體更新OTA	• 可防止資訊未授權修改之更新系統及其方法(TW/US/JP) (審查中)	
車外通訊	• 行車安全輔助網絡管理系統及其方法(TW/CN/US) • 車用複合式通訊系統與方法(TW/CN/US)	• 基於資訊融合的路口警示系統與方法(TW/US) • 路口動態圖資更新共享系統及方法(TW/CN/US) • 自動駕駛車輛通訊安全系統及方法(TW/CN/US)
車內通訊& 車網管理	• 電動車運行資料彙集系統(TW) • 雙頻微型化天線及其設計方法(TW/CN) • 行動裝置金鑰製作方法(CN) • 車用生物特徵辨識使用權限管理系統及其方法(TW) • 電動車遞迴式車輛路徑規劃方法(TW/CN)	• 整合式車輛晶片卡的互動監控系統(TW/CN) • 車載網路資料取樣轉換方法及系統(TW/US) • 自駕車遠端監控系統及其方法(TW/CN/US) • 自動駕駛協控系統與控制方法(TW/CN/US) • 車用分散式網路管理系統及方法(TW/CN/US)

註：歷年可授權專利項目，詳細請參閱本中心官網。

合作方式與聯絡資訊

可授權專利

可移轉技術

業界合作(先期參與)

ARTC網站
報紙媒體
成果發表
工會新訊

技術精進
商品加值
縮短研發
搭配計畫

技術移轉
技術服務
業界合作
專利授權

可移轉技術：鄭先生，04-7811222分機2367，steven0829@artc.org.tw
蔡小姐，04-7811222分機5105，Lijun7329@artc.org.tw
可授權專利：陳小姐，04-7811222分機2345，chloe@artc.org.tw

更詳細資訊請參考車輛中心官網
https://www.artc.org.tw/