



■作者：TIMO VAN ROERMUND/ 恩智浦半導體汽車電子事業部安全架構師

在駭客橫肆的世界中 聯網汽車要如何保障安全？

如果駭客駭入收音機，有可能傳送指令訊息給剎車或是轉向系統嗎？如果有可能，我們又該如何妥善防範？上述情境是兩名白帽駭客想迫切得知的問題。在一次知名的駭客行動中，由一名 **Wired** 雜誌記者駕駛一部吉普車 (Jeep)，而兩名駭客成功遠距離終止了吉普車的引擎傳動。在那當下，車輛駭客攻擊就此成為真正的威脅。

自此之後，汽車產業歷經諸多改變，車輛安全性自然成為汽車製造商的首要考量。目前許多新款車輛搭載電子控制器、具有運算能力、能運行程式碼，還能透過無線網路與外界連結，因此攻擊面無疑相當廣大。若媒體對外公布一起駭客攻擊事件，其影響將重重傷害汽車製造商的品牌商譽。

若無完善安全性，道路安全將蕩然無存

如同在吉普車駭客攻擊所看到的，一旦駭客取得收音機的控制權限，就能輕易透過車內網路控制車輛方向和煞車系統。事實上，車輛中的安全閘道能作為防火牆，進而監控進出車輛訊息，也能將至關安全性的系統與其他應用程式隔離（例如資訊娛樂系統），但該吉普車的車內網路並未搭載安全閘道。

車內網路必須受到妥善保護，抵禦意圖操縱並竊取資料的入侵者攻擊。這表示必須重新規劃車載網路架構，以區分、隔離車載網路中不同的領域系統。

此外，必須採用高強度的加密和驗證技術，確保車輛僅與已知且信任的實體進行安全通訊，並進而保護車載網路內部的代碼和資料。

汽車製造商還需要施行哪些安全性預防措施？車用處理器能提供什麼樣的硬體安全性？上述問題和疑慮是我們最常在業界耳聞的議題。

恩智浦最早於 2015 年在車用處理器實施硬體安全性

車用處理器會產生、處理、交換並儲存龐大的敏感資料，無疑會成為駭客攻擊的目標，因此車用處理器必須具備高度安全性。

從 2015 年開始，恩智浦就專注於處理器層級的安全性，並推出車用專屬硬體安全模組 (HSM)，能針對車用應用程式提供內建於晶片的安全性功能，防止軟體遭惡意操縱，並支援安全性軟體更新和資料保護等功能。恩智浦更早在 2010 年，就已推出符合並相容於安全硬體延伸 (SHE) 的車用 MCU 產品。

重新思考汽車架構，締造車內安全與道路安全的新可能

領域式架構方法，將擁有相同安全性考量的應用程式劃分為群組。領域式架構幫助車輛製造商簡化複雜性，並針對車輛內對安全性和升級能力的不同考量進行區分。



車輛製造商降低車輛的軟體複雜度)。

現今對安全性閘道和駕駛輔助系統等強大電子控制單元的安全性需求不斷提高，S32 內建的硬體安全引擎為密碼編譯演算法提升執行實作的嚴密性，更運用了金融、銀行及政府身分識別領域的技術和專業知識，以滿足安全需求。

為車輛平台帶來安全性的通用方法

時至今日，每一款由恩智浦製造的新款車用處理器和控制器，皆包含專屬的硬體安全性模組：在 S32 平台稱為硬體安全引擎 (HSE)，而在 i.MX 8 則稱為安全控制器 (SECO)。兩款模組 (或稱為引擎) 完全符合「EVITA Full」規格的功能性目標，並能獨立管理安全性功能，絲毫不會影響處理器或控制器本身的效能 / 功能。安全開機程序和即時完整性檢查架構，能驗證軟體是否具備真確性、受信任並且未經改動。這些模組也提高修正作業時的靈活性，讓車輛製造商能修正安全性漏洞，還具備安全的線上更新功能，車輛上路後製造商仍能輕鬆更新軟體，無須進行耗費高額成本的召回程序。

此外還具備生命週期管理機制，能針對若干控制器和處理器功能進行鎖定控制。例如，除錯和序列下載是車輛開發和製造期間相當關鍵的功能，然而若駭客可以在量產車上取得這些功能，將會帶來難以想像的危害。最後，這些模組亦搭載內建的硬體防護功能，能防止對處理器電壓、溫度和功率的竄改以及透過硬體執行的資源隔離攻擊。

S32 車用平台的設計，能因應未來軟體、連線功能和安全性的成長發展

恩智浦新款 S32 車用平台，適用於搭載豐富車內體驗及自動化駕駛功能，能快速研發上市的車輛，並提供更多軟體及功能，為車輛的未來帶來無限可能。(註：深入瞭解 S32 的共通架構如何協助

i.MX 8/8X 應用程式處理器，提高駕駛資訊系統的安全性基準

應用程式處理器原本最早的形式是車載資通訊系統，而經過多年發展，今日的駕駛資訊系統包含抬頭顯示器、數位儀表板、導航、媒體播放器、語音和資料通訊，並執行多種複雜的軟體堆疊，無疑需要最高的安全性。恩智浦採用分層次防禦機制，全面保護整個處理單元，從硬體、軟體到通訊連結皆囊括在內。

i.MX 8 的安全控制器 (SECO) 是系統的信任根 (RoT)，其功能不侷限在金鑰管理，也用於驗證、監控和鎖住系統的控制器韌體，同時也是電源啟動和執行時間等多種並行作業系統的 RoT。i.MX 8 的硬體式竄改偵測和防護功能，以及處理器內建硬體防火牆網域則能輔助 SECO，維持服務的資料與記憶體完整性，進而提高駕駛資訊系統的安全性基準。

必須保障安全性，讓駕駛能信任自己的汽車

絕不能讓駭客取得車輛的控制能力，或窺探駕駛及金融資訊等資料的隱私。車輛製造商務必使用安全性解決方案，防止電子系統遭受潛在的網路攻擊。

註：深入瞭解 S32 的共通架構如何協助車輛製造商降低車輛的軟體複雜度 <https://blog.nxp.com/automotive/cars-are-made-of-code> CTA