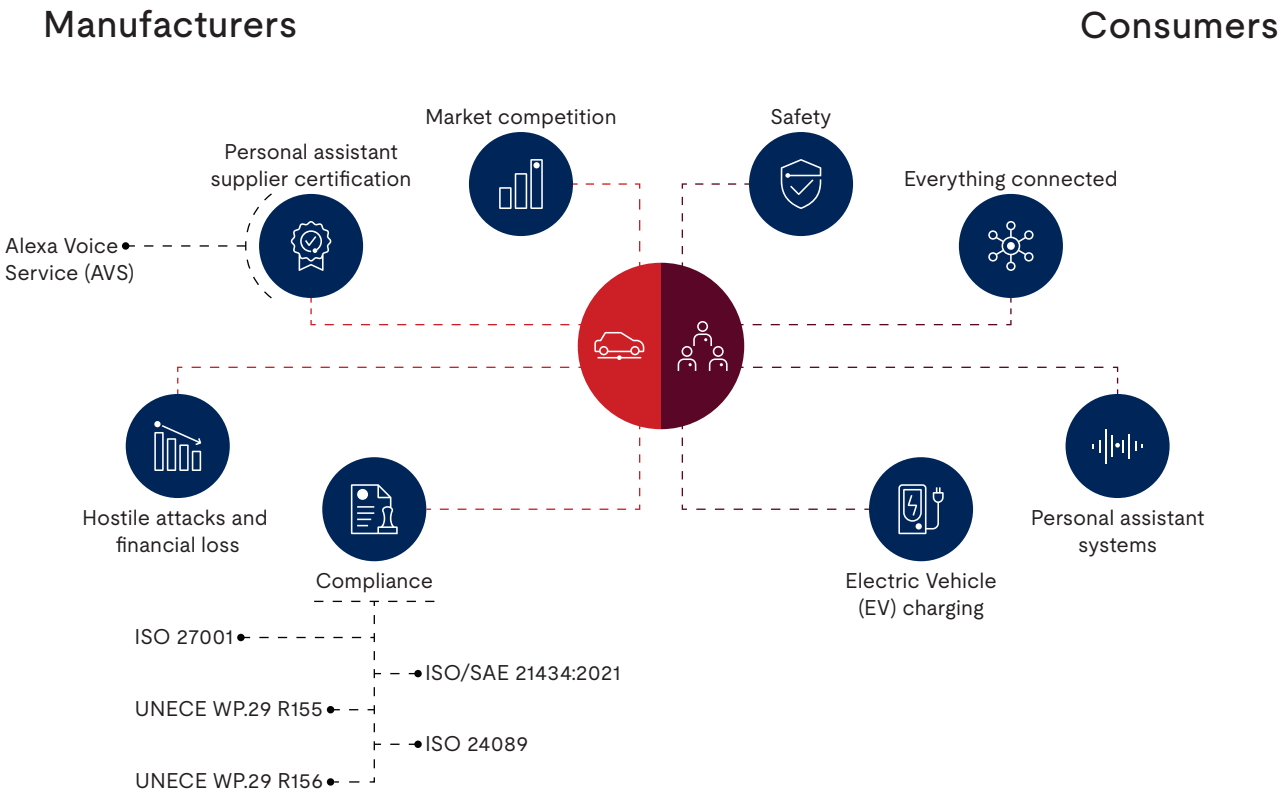
汽車網路安全

汽車技術的進步導致網路安全風險升高

從資訊娛樂系統和操作感應器到行動應用程式整合乃至駕駛自動化，汽車技術日新月異持續迅速進步。現代車輛內建有最多 150 個電子控制單元和 1 億行的程式碼。許多觀察家預估 2030 年汽車將內建大約 3 億行軟體程式碼。而相比之下，廣為大眾使用的個人電腦軟體僅接近 4,000 萬行。雖然每一行程式碼和每一個連接點都增強了功能和可用性，但也帶來漏洞和網路攻擊的風險。

互連的產品和系統中的軟體漏洞和生態系統中的薄弱環節是攻擊者的目標。汽車產業的網路攻擊會升高公共安全的風險，因此互連產品和系統的網絡安全，對於安全採用現代汽車技術至關重要。

汽車網路安全的趨勢和挑戰



與 UL Solutions 合作

您在汽車產品開發生命週期的網路安全旅程

01 Advisory

- Understanding the automotive cybersecurity landscape

02 Training

- Understanding regulatory and standard requirements

03 Gap analysis

- Identifying cybersecurity risks and gaps
- Mitigating risks and gaps by strengthening cybersecurity posture

04 Certification

- Achieving regulatory approval and market access
- AVS

05 Lifecycle management

- Maintaining secure operations during the entire life cycle

Time to market

Benchmarking

Brand protection

Risk and cost control

汽車網路安全解決方案

- 指導和協助原始設備製造商 (OEM) 以及汽車零組件和系統製造商
- 克服產業的高度複雜性並開發汽車網路安全標準和最佳實務框架
- 幫助您識別和管理軟體漏洞和網路風險

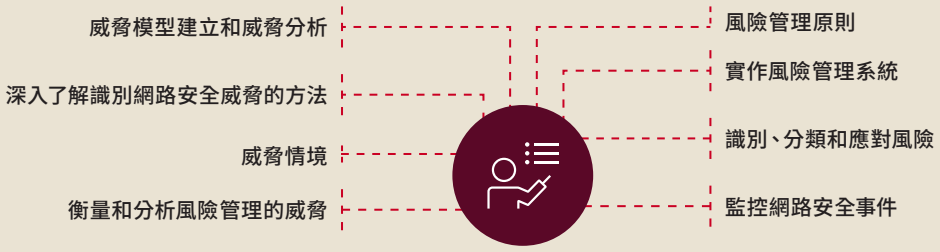
我需要了解和實作汽車網路安全標準和最佳實務。

汽車網路安全服務——分析風險、緩解威脅、維持合規性並培訓您的團隊，解決現代汽車創新技術中存在的網路安全問題。

汽車網路安全服務
UNECE WP.29 | ISO/SAE 21434

我需要增加我的汽車網路安全知識。

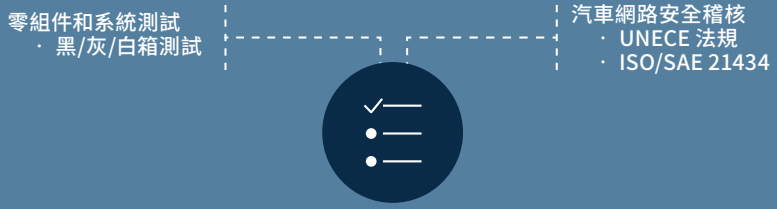
汽車網路安全培訓——應用網路安全原則、流程、必要的標準和要求，以降低汽車產品和系統的網路威脅風險。



汽車網路安全培訓
ISO/SAE 21434 | UL 認證汽車網路安全專業人員或 UL-CCSP

我們的網路安全成熟度？如何邁向成功？

汽車網路安全稽核和測試——發現產品和軟體濫用風險並驗證安全措施是否符合產業要求，包括 ISO/SAE 21434 和 WP.29。



汽車網路安全稽核和測試
ISO/SAE 21434 | UNECE WP.29

為什麼為了您的網路安全選擇 UL Solutions？

- 獨立、受信賴的第三方
- 完整的生命週期解決方案
- 硬體和軟體安全評估
- 安全開發實務評估
- 網路安全專業知識
- 產業相關知識
- 網路安全和安規
- 全球團隊和本地支援

網路安全基礎

- 全球標準和框架的專業知識
- 最佳實務的豐富知識
- 推出越來越多物聯網（IoT）安全解決方案

瀏覽 UL.com/automotive-cybersecurity，更深入了解並與我們的專家交流。

UL Solutions

UL.com/Solutions

IMS23CS705800zhTW