財團法人車輛安全審驗中心
Vehicle Safety Certification Center

車安通訊季刊

遵循法令 公正專業 優質服務

第 114-04 期

＞＞專題報導

□淺談國內外車輛網路安全及軟體更新法規概況

車安中心 劉世澤

一、前言

近年來，隨者科技的快速發展，現代車輛的核心組成架構已產生根本性的轉變。車輛不再如過往般單純依賴內燃機與機械部件，而是以更為精密的電子控制單元 (ECU) 網路、大量的感測器，以及豐富的對外通訊與連結所構成。這種轉變將車輛從純粹的機械體，升級為高度智慧化的移動平台。舉例來說，車輛基本都具備更實用的服務如即時導航、車載資訊娛樂系統，更便捷的控制如車輛遠端控制功能、軟體更新(OTA)、或是能夠實現智慧交通與安全協作的車輛網通訊(V2X)功能，以及電動化和更高階的智慧駕駛系統。

然而，隨著車輛電動化和智慧化進程的加速，全球汽車產業正同時面臨前所未有的網路安全挑戰。這場智慧化革命雖帶來了極大的便利與功能提升，卻也將車輛暴露於全新的數位風險之中。這些風險的影響範圍極廣，不僅威脅到數據隱私，更可能直接危及駕駛與乘客的生命安全。為應對這一嚴峻的局面，聯合國歐洲經濟委員會（UNECE）的世界車輛法規協調論壇（WP.29）已採取強制性措施，並於2021年發布了兩項關鍵法規，為全球汽車產業建立了強制性的安全標準：UN R155「CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM」及UN R156「SOFTWARE UPDATE AND SOFTWARE UPDATES MANAGEMENT SYSTEM」。

我國交通部亦將此二法規調和導入，並於2024年公告發布車輛安全檢測基準「九十六、網路安全及網路安全管理系統」與「九十七、軟體更新及軟體更新管理系統」。根據規劃，新型式的 M 類及 N 類車輛將於2028年正式開始實施，而各型式的 M 類及 N 類車輛應於2030年符合這項新規定。

二、何謂車用網路安全及軟體更新

在智慧車輛時代，網路安全（Cybersecurity）與軟體更新（Software update）管理已不再是傳統資訊安全領域的單一議題，而是汽車工業的核心挑戰。車

Copyright © 2025 VSCC 版權所有

財團法人車輛安全審驗中心
Vehicle Safety Certification Center
車安通訊季刊
遵循法令 公正專業 優質服務

用網路安全與軟體更新管理指的是一套全面的技術、流程與控制措施，旨在保護車輛的電子系統、網路、軟體和資料，使其免受未經授權的存取、損害、修改或破壞，同時也要考量進行軟體更新過程中更新套件之真實性與完整性、網路穩定性等，這些保護措施涵蓋了所有可能的數位接口，例如：

無線通訊： 藍牙、Wi-Fi、4G/5G、GPS、車聯網 (V2X)。
有線連接： OBD (車載診斷系統)、CAN 匯流排、USB 連接埠。
軟體更新： 透過 OTA (Over-The-Air) 方式進行的遠端軟體更新。

回顧2015年的 Jeep Cherokee 遠端駭客攻擊，這是一場震驚全球車輛產業的事件。攻擊者揭露了連網汽車的致命弱點：他們僅透過車輛的 Uconnect 資訊娛樂系統，便能利用網路連線，突破資安防線並遠端控制車輛。最讓人可怕的是，當車輛在道路上正常行駛時，攻擊者可以隨意切斷引擎動力、讓煞車失靈，甚至操縱方向盤，使駕駛人完全喪失對車輛的控制。這起事件的影響力極大，迫使車輛製造廠 Chrysler (FCA) 史無前例地召回 140 萬車輛進行軟體更新，成為汽車史上首次因網路安全漏洞而進行的大規模召回行動。

故前述所提之任何這些環節的安全漏洞都可能被利用。因此，其核心目標不僅是維護使用者隱私，更關鍵在於確保車輛各項功能的正常運作，從而直接保障駕駛與乘客的生命安全。

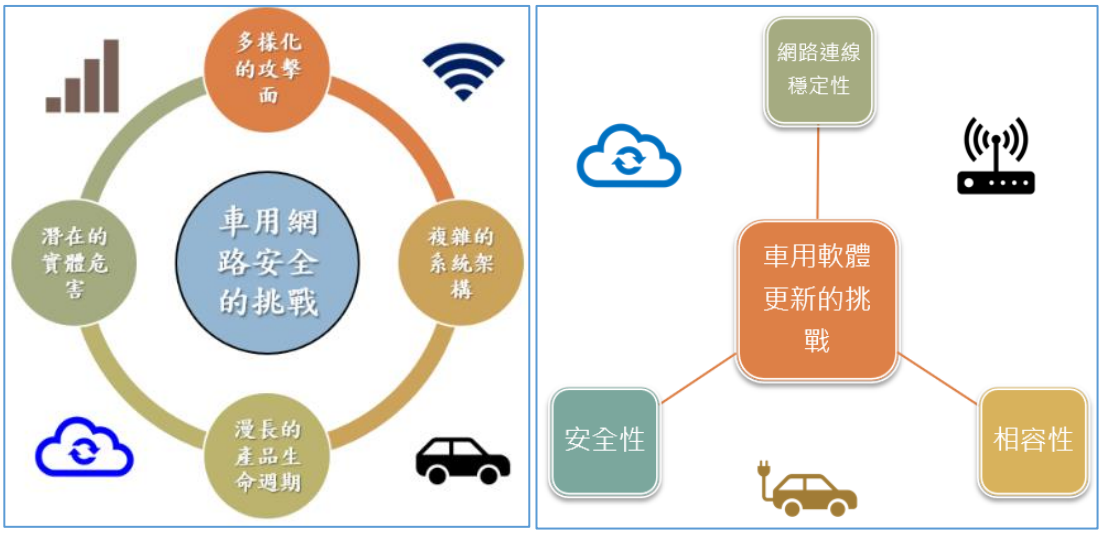

圖 1. 車輛網路安全及軟體更新之挑戰

財團法人車輛安全審驗中心 地址：505029 彰化縣鹿港鎮鹿工北二路 2 號
電話：04-781-2180 傳真：04-781-2181 E-mail：service@vscc.org.tw
Copyright © 2025 VSCC 版權所有

三、國際標準及法規概況

為應對智慧車輛帶來的全新挑戰，聯合國歐洲經濟委員會（UNECE）的強制性要求已在全球範圍內生效：

新型式車輛： 自 2022 年 7 月起，新型式車輛須符合 UN R155(網路安全)及UN R156 (軟體更新) 相關規定。

各型式車輛： 自 2024 年 7 月起，則對所有車型強制實施。

這兩項法規的核心精神在於建立以風險為基礎的系統化方法，並考量車輛產品的全生命週期。由於一輛汽車的生命週期長達十數年，從設計、生產、銷售到最終報廢，其網路安全防護必須是持續性的，需要在整個生命週期中不間斷地進行監控、維護與更新。

然而，UN R155/R156 規定雖然強制要求車輛製造廠必須建立並維護一套完整的網路安全管理系統 (CSMS) 及軟體更新管理系統 (SUMS)，但它們並未詳細說明達成這些目標的具體步驟。因此，國際標準化組織（ISO）發布了兩套關鍵的技術標準，作為法規與工程實踐之間的橋樑：

ISO/SAE 21434:《道路車輛 — 網路安全工程》，於 2021 年 8 月發布。

ISO 24089：《道路車輛 — 軟體更新工程》，於 2023 年 2 月發布。

這兩套 ISO 標準為車輛製造廠提供了具體且可操作的系統化方法與工程流程。它們指導車輛製造廠如何在車輛產品的整個生命週期中，建構、實施並維護法規所要求的管理系統，確保軟體更新過程的安全性、可靠性與合規性。簡單來說，ISO 標準提供了詳細的藍圖，讓車輛製造廠能夠依循公認的、系統化的框架，來滿足網路安全與軟體更新法規的強制性要求。

接下來，本篇專題將以車輛安全檢測基準「九十六、網路安全及網路安全管理系統」及「九十七、軟體更新及軟體更新管理系統」深入探討這兩項與過往不同的法規。

Copyright © 2025 VSCC 版權所有

UN R155	ISO/SAE 21434
▫ 性質：全球首個針對車輛網路安全所制定的強制性法規。 ▫ 核心要求：要求汽車製造商建立並維護一套健全的網路安全管理系統 (CSMS)，並涵蓋車輛從概念設計、開發、生產、售後維護到報廢的整個生命週期，系統化地識別、評估和處理網路安全風險。	▫ 主要目的：幫助車輛製造商及其供應鏈（如 Tier 1 和 Tier 2 供應商）系統化將網路安全考量融入到產品開發和管理流程中。 ▫ 核心內容：提供了詳細的網路安全工程方法，涵蓋車輛產品和其組件的整個生命週期，並定義如何進行網路安全管理、威脅分析與風險評估 (TARA)、網路安全規格定義、安全軟體開發、測試驗證、事件響應和軟體更新管理等活動。

圖 2. UN R155 與 ISO/SAE 21434 差異

UN R156	ISO 24089
▫ 性質：強制性的國際法規。所有配備軟體更新功能的車輛。 ▫ 核心要求：主要目標是確保車輛的軟體更新過程是安全、受控且可追溯的。它要求汽車製造商建立並維護一套健全的軟體更新管理系統 (SUMS)。	▫ 主要目的：旨在幫助車輛製造商及其供應鏈（包括 Tier 1 和 Tier 2 供應商）系統化地實施和管理軟體更新活動，確保這些更新的安全性、可靠性和合規性 ▫ 核心內容：為汽車產業提供了一套詳細的軟體更新工程方法，涵蓋了從軟體更新概念、開發、生產、部署到運營和維護的整個生命週期。

圖 3. UN R156 與 ISO 24089 差異

四、檢測基準「九十六、網路安全及網路安全管理系統」概要說明

我國交通部因應國際趨勢，並已調和導入UN R155與R156，並訂有車輛安全檢測基準「九十六、網路安全及網路安全管理系統」及「九十七、軟體更新及軟體更新管理系統」。根據規劃，新型式的 M 類及 N 類車輛將於2028年正式開始實施，而各型式的 M 類及 N 類車輛應於2030年符合這項新規定。

其中「九十六、網路安全及網路安全管理系統」旨在建立一種以風險為基礎的系統方法，並定義組織化的流程、職責和治理，以處理與車輛網路威脅相關的風險及保護免受網路攻擊，其效力貫穿車輛從概念設計到最終報廢的整個生命週期。此法規的核心要求分為兩部分，一是強制車輛製造商必須

Copyright © 2025 VSCC 版權所有

建立並維護一套健全的「網路安全管理系統」(Cyber Security Management System, CSMS),二是「對車輛型式的要求」(Requirements for the Vehicle Type),申請者可實施適當的緩解措施以保護車輛型式威脅列表及相應緩解措施,其威脅列表及相應緩解措施於本項基準表一所列之威脅之高等級描述和相關漏洞或攻擊方法說明。其中法規條文第5.2節「網路安全管理系統」部分5項要求,第5.3節「對車輛型式的要求」部分8項要求及第5.4節「報告規定」2項要求,摘要如下:

5.2 網路安全管理要求	5.3 對車輛型式的要求	5.4 報告規定
◆ 涵蓋車輛全生命週期 ◆ 使用的流程可確保充分考慮和管理網路安全性((a)~(h)),包括第6章(表一)所列的風險和緩解措施 ◆ 網路威脅和漏洞,應於合理之時間範圍內獲得緩解 ◆ 確保所訂流程之監控偵測持續進行 ◆ 供應商網路安全風險管理	◆ 具備有效CSMS符合性證書 ◆ 識別管理與供應商相關風險 ◆ 詳盡風險識別及評估 ◆ 確定風險之適當緩解措施 ◆ 採取適當且相稱的措施 ◆ 充分測試及驗證安全有效性 ◆ 檢測、監控及分析威脅、網路攻擊 ◆ 加密模組採共識標準	◆ 回報監測活動的結果,確認實施結果有效 ◆ 核實相關資訊,或糾正無效資訊

圖 4. 「網路安全管理系統」、「對車輛型式的要求」及「報告規定」條文摘要

其中有關第5.4節「報告規定」,車輛製造廠在取得 CSMS(網路安全管理系統)符合性證明文件後,其維護之責任並非終止,而是進入一個持續監控與報告的循環。車輛製造廠有義務至少每年一次(或更頻繁地)向審驗機構或檢測機構提交其監測結果,內容必須包括最新的網路攻擊資訊以及對已認證車型的緩解措施有效性確認。審驗機構將嚴格核實這些報告,以確保製造廠的安全系統持續有效運作。

若製造廠提交的報告或回覆被認定不充分,審驗機構將有權撤銷其 CSMS 符合性證明文件。這明確說明,國際法規要求車輛網路安全必須是一種持續性、全生命週期的管理狀態,而非一次性的認證。

Copyright © 2025 VSCC 版權所有

另條文第6章「威脅列表及相應緩解措施」包含：
本節由三部分所組成。A部分描述威脅、漏洞和攻擊方法的基線。B部分描述適用於車輛型式對威脅的緩解措施。C部分描述用於車輛區域外部對威脅的緩解措施，如在IT後端。

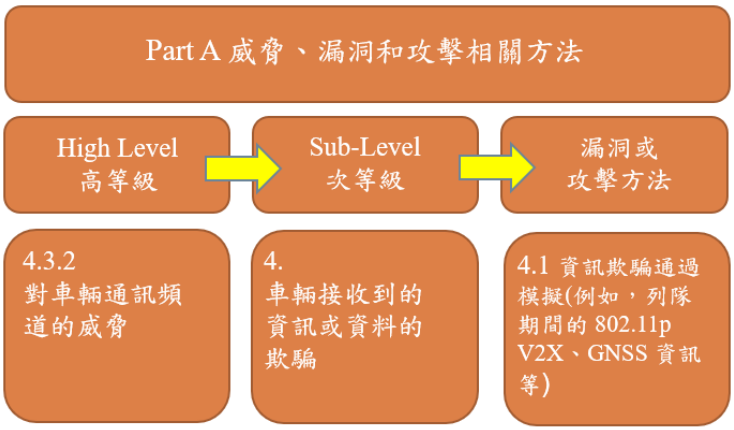

圖 5. A 部分描述威脅、漏洞和攻擊方法範例說明

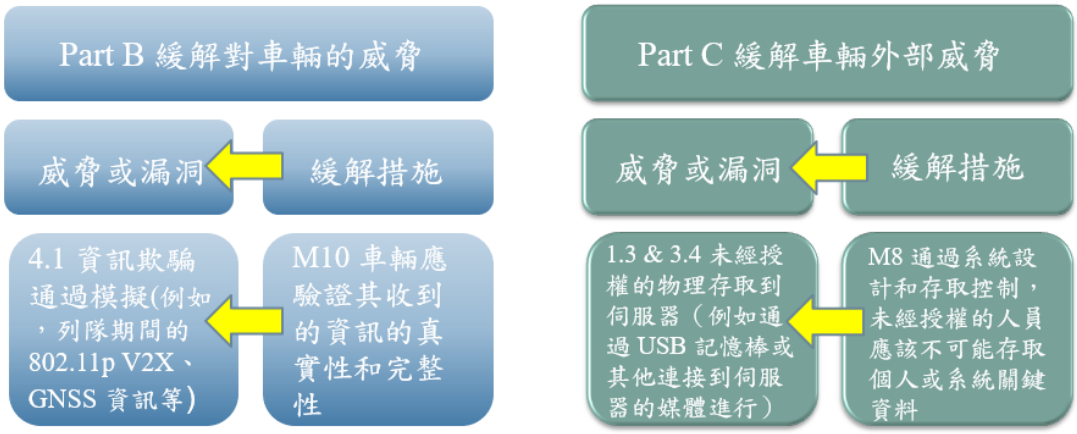

圖 6. B 部分描述適用於車輛型式對威脅的緩解措施及 C 部分描述用於車輛區域外部對威脅的緩解措施範例說明

如前述章節所提，ISO/SAE 21434《道路車輛 — 網路安全工程》是達成「網路安全及網路安全管理系統」法規要求之重要參考及指引。其中對網路安全的具體方法進行了詳細闡述。其核心環節之一，即威脅分析與風險評估（Threat Analysis and Risk Assessment, TARA），為管理車輛網路安全風險提

Copyright © 2025 VSCC 版權所有

供了系統化的方法。TARA 的主要目的在於系統性地分析潛在的網路安全威脅，並量化評估其風險等級，從而作為決定網路安全處理措施的依據。

具體流程步驟如下：

(一) 資產識別 (Asset Identification)：確定需受保護的關鍵資產，例如車輛功能、核心電子控制單元（ECU）及相關敏感數據。

(二) 威脅情境識別 (Threat Scenario Identification)：針對已識別的資產，設想潛在的威脅情境，例如未經授權的存取或資料竄改。

(三) 衝擊評級 (Impact Rating)：評估一旦威脅發生，可能對安全（Safety）、隱私（Privacy）、營運（Operation）或財務（Financial）等方面造成的嚴重衝擊程度。

(四) 攻擊路徑分析 (Attack Path Analysis)：詳細分析潛在攻擊者可能採用的入侵或利用漏洞路徑。

(五) 攻擊可行性評級 (Attack Feasibility Rating)：評估實現該攻擊路徑所需的時間、專業知識、資源與工具等，以判斷其攻擊難度與可行性。

(六) 風險值確定 (Risk Value Determination)：綜合評估衝擊程度與攻擊可行性，確立每個威脅情境的風險值。

(七) 風險處理決策 (Risk Treatment Decision)：根據風險值，決定應採取的風險處理策略，包括降低（Mitigate）、規避（Avoid）、轉移（Transfer）或接受（Accept）風險。

這個系統化的分析流程（指 TARA）構成了網路安全管理系統（CSMS）的核心基石，確保風險管理並非隨意的行為，而是一套系統化、基於證據的規範。它必須貫穿車輛的整個生命週期，涵蓋從概念設計、產品開發、量產製造，到後期的運營維護乃至最終的報廢階段，故車輛製造商能夠確保車輛產品在整個生命週期內得到全面且有效的網路安全保護。

五、檢測基準「九十七、軟體更新及軟體更新管理系統」概要說明

「九十七、軟體更新及軟體更新管理系統」之其一核心目標是要求車輛製造廠（OEM）建立並維護一套標準化、安全的「軟體更新管理系統」（Software Update Management System, SUMS），以應對日益普及的 OTA（Over-The-Air，

Copyright © 2025 VSCC 版權所有

無線/空中更新）技術所帶來的安全與法規挑戰。軟體更新管理系統（SUMS）係指一套系統性的方法，用於定義組織的過程和程序，以確保軟體更新的提交滿足法規要求並確保所有軟體更新過程都是安全、受控且可追溯的；而軟體更新（Software Update）係指用於將軟體升級到新版本的套裝軟體（Package），亦包括配置參數的變更。法規另一部分則是「對車輛型式的要求」（Requirements for the Vehicle Type），旨在要求車輛軟體更新過程中，應保護軟體更新的真實性和完整性，以合理地防止其被破壞，並合理地防止無效更新。本項法規第5.1節「軟體更新管理系統」部分計9個程序流程、5項記錄、4個安全保障、軟體無線（空中）更新，第5.2節對「對車輛的型式」部分具3項要求，內容摘要如下：

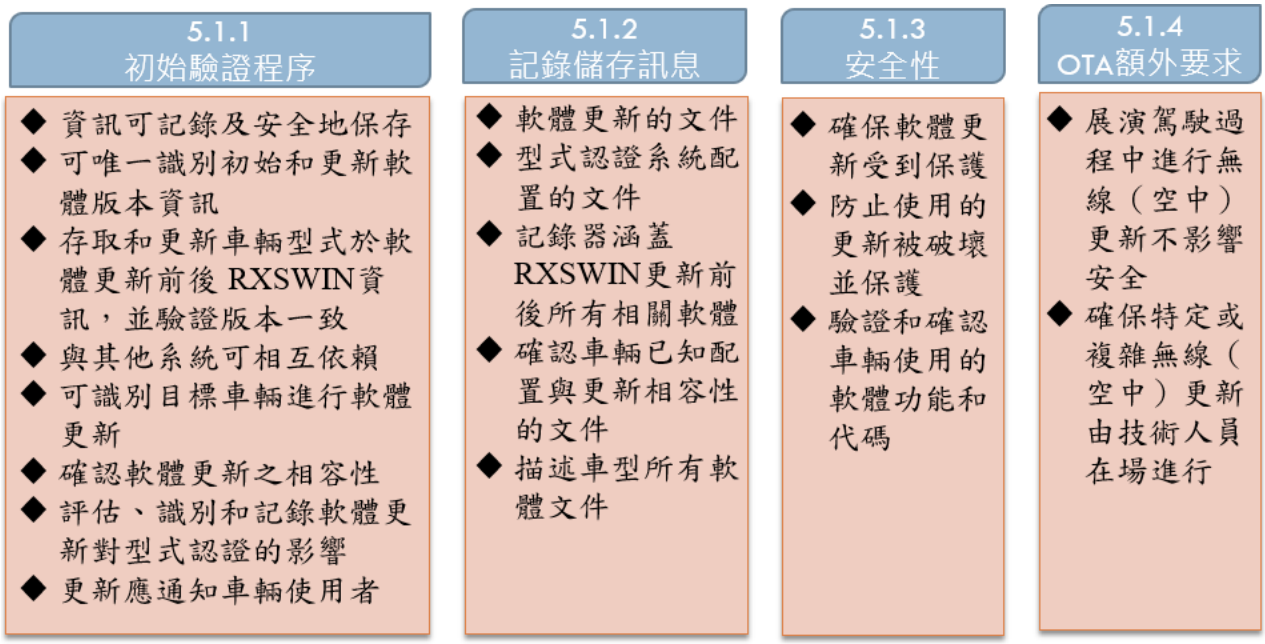

圖 7. 「軟體更新管理系統」條文摘要

Copyright © 2025 VSCC 版權所有

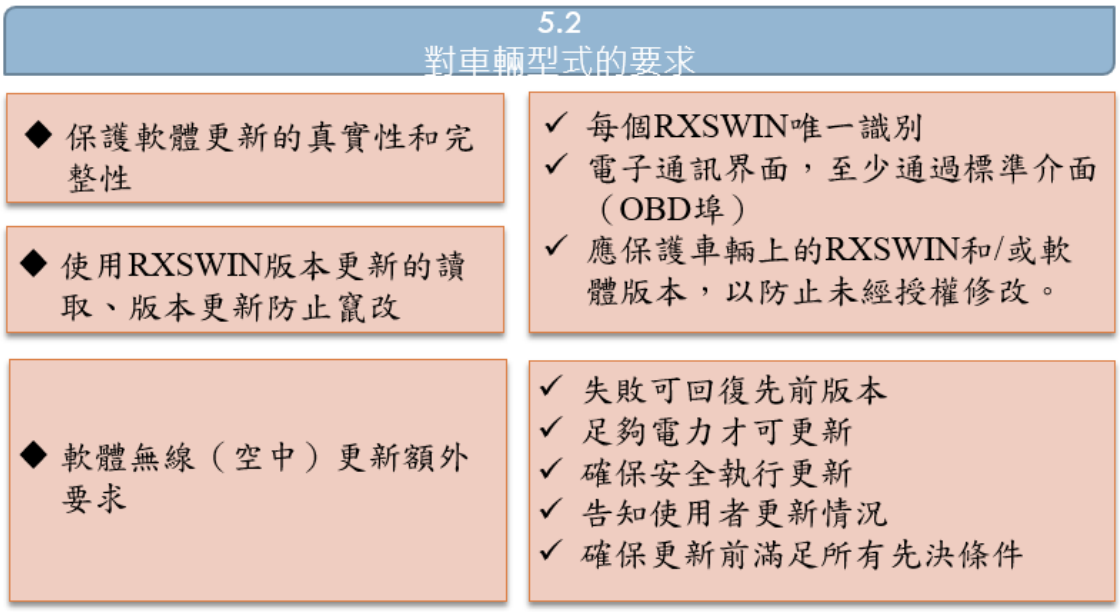

圖 8. 「對車輛型式的要求」條文摘要

在本項法規當中，RX軟體識別碼（RX Software Identification Number, RXSWIN）扮演非常重要的角色，其係指由申請者定義之專用識別碼，代表電子控制系統之型式認證相關軟體資訊。它的主要目的是提供一個唯一且可追溯的方式來識別車輛上的軟體版本。當車輛製造商對任何與法規安全相關的系統（如煞車、轉向系統的控制軟體）進行更新時，如果該更新的幅度大到需要申請型式認證的延伸或新的認證，就必須更新RXSWIN。這確保了審驗機構與車輛製造廠能夠清楚地追蹤每一次關鍵軟體的變更，並確認更新後的版本依然符合法規要求，防止未經授權的軟體修改。

六、認證流程概念介紹

為符合本項法規，車輛製造廠必須通過多階段認證流程，以確保網路安全及軟體更新管理系統和車輛本身皆符合嚴格的法規要求。相關流程概念如下：

Copyright © 2025 VSCC 版權所有

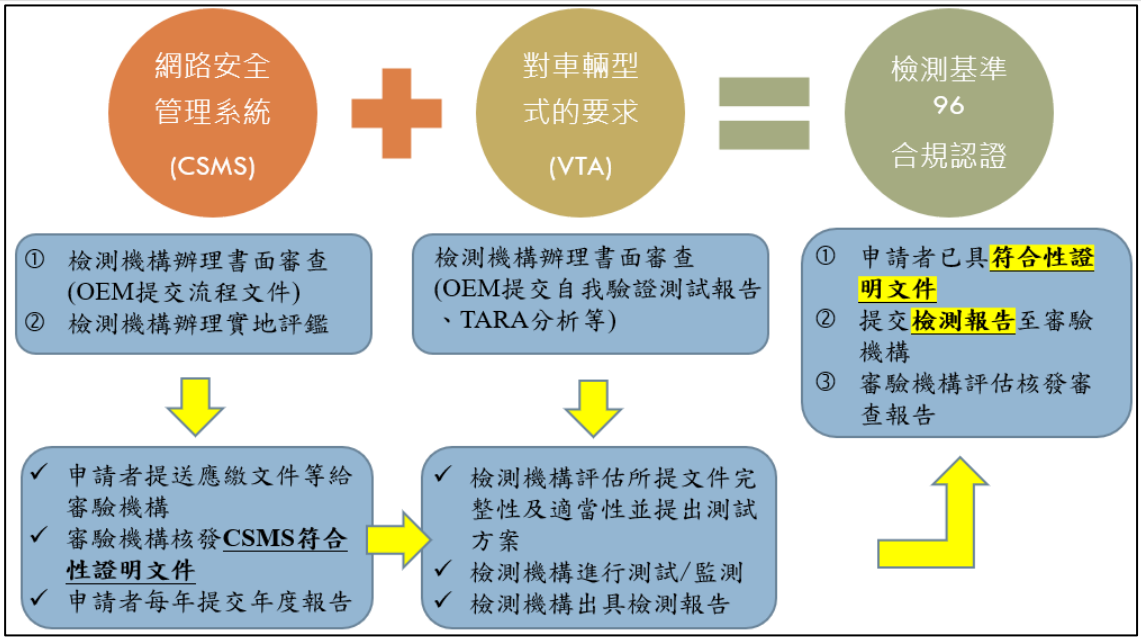

圖 9. 檢測基準 96 認證流程概念

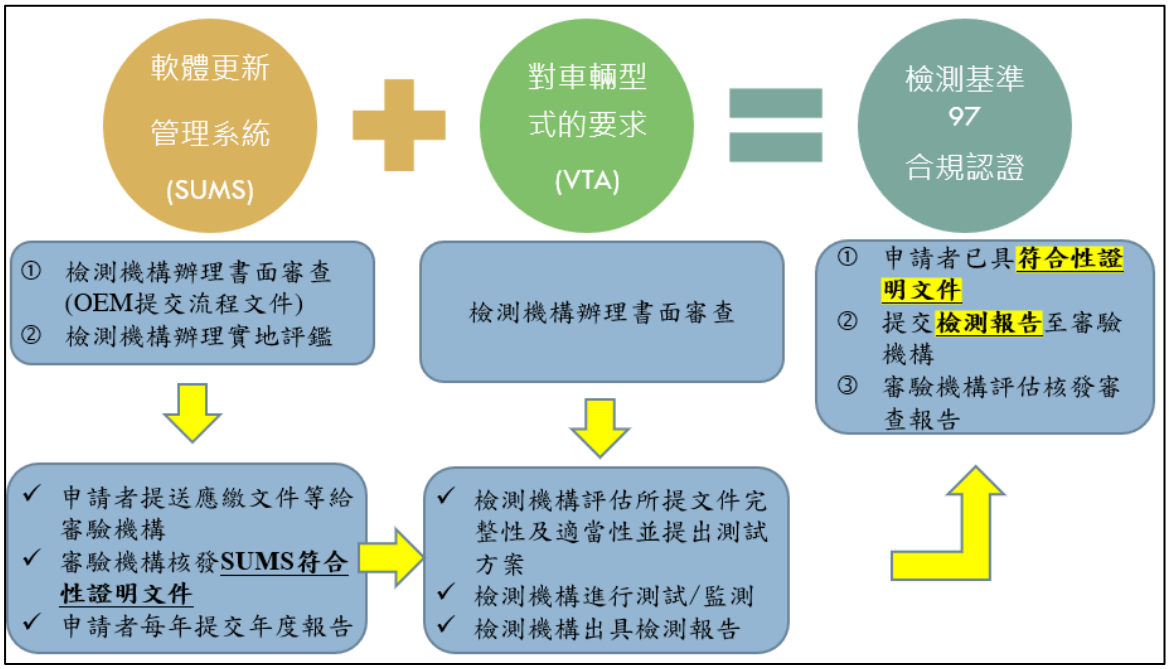

圖 10. 檢測基準 97 認證流程概念

Copyright © 2025 VSCC 版權所有

綜上所述，為符合法規要求，車輛製造廠必須通過嚴謹的兩階段認證流程。因此，這套認證流程的核心意義在於：它強制要求車輛產業必須將網路安全視為從設計、開發、測試到售後維護的全生命週期責任，確保現今普遍已具聯網功能之車輛在面對不斷演變的網路威脅時，始終維持最高標準的安全狀態。

七、結論與展望

隨著車輛產業朝向 C.A.S.E.（電動化、聯網化、智慧化等）方向迅速發展，本中心作為交通部委託的車輛型式安全審驗專業機構，必須主動應對這場車輛產業的快速變革，超前部署以精準掌握國際趨勢。值得注意的是，無論是聯合國法規UN R155/156，或是經我國順應國際趨勢調和之「九十六、網路安全及網路安全管理系統」與「九十七、軟體更新及軟體更新管理系統」，與過往著重於物理特性的檢測要求及方式截然不同，如法規要求、檢測方法和基本知識全面轉向資訊安全及軟體更新領域。因此，提升同仁對此類法規的理解與認識，亦是本篇專題介紹的核心重點。

總而言之，現代車輛已從單純的機械體，升級為高度複雜、互聯的移動智慧平台。這一項重大的轉變雖賦予了車輛無與倫比的功能與便利性，卻也同時帶來了涵蓋數據隱私乃至生命安全的嚴峻網路安全挑戰。

為應對這場車輛產業面臨的數位革命，相關強制性規範的導入，亦為全球汽車產業提供了清晰的安全框架。我國交通部積極調和並導入這兩項基準，明確規劃了 M 類及 N 類車輛在 2028 年至 2030 年的實施期程，標誌著我國車輛安全標準邁入新紀元。

面對這些法規的強制實施，車輛製造廠現在必須將網路安全視為與傳統機械安全同等重要的核心要素。這不僅是技術升級的要求，更是確保在智慧移動的新時代下，每一位駕駛與乘客安全與信任的必然承諾。

八、參考文獻

[1] 交通部車輛型式安全審驗管理辦法-附件 96 網路安全及網路安全管理系統、附件 97 軟體更新及軟體更新管理系統

[2] UN Regulation No. 155 - Cyber security and cyber security management system & UN Regulation No. 156 - Software update and software update

Copyright © 2025 VSCC 版權所有

management system

[3] Guidelines on the reporting of manufacturers to the KBA and the Technical Service under UN-R 155/156

[4] KBA-type approval procedure according to UN-R 155/156

[5] Method & Criteria for the Application of UNECE Regulation No. 155 on Cyber security

[6] Rules for technical services conducting UN-R 155 CSMS assessments for RDW, Rules for technical services conducting UN-R 155 type approval assessments for RDW

[7] ISO/SAE 21434：《道路車輛 — 網路安全工程》

[8] ISO 24089：《道路車輛 — 軟體更新工程》

Copyright © 2025 VSCC 版權所有