



第 112-03 期

>> 專題報導

□ 聯合國 UNECE 車輛網路安全及軟體更新法規介紹

車安中心 鄭碩群

一、前言

車輛自從邁入電子化的時代後，為了控制車輛的各項性能，透過導入各項感測設備後，人們可進一步了解車輛的運作情形，並對其進行控制，以達成能源的有效利用，更可介入車輛控制以避免或減輕於行駛過程中可能產生的風險或事故。

隨著新科技的應用也帶來不少新的挑戰，在自駕車輛及聯網車輛的持續發展下，車輛與網路連線並進行控制或進行更新不再是科幻電影才會有的情節，而是各個先進國家為了達成零傷亡願景或減少環境汙染，爭相進行發展的重點交通科技，在發展的過程中，為了確保車輛於特定層面上的各項性能，聯合國歐洲經濟委員會(UNECE)近年來針對自駕車輛及聯網車輛訂定一系列的新法規，包含網路安全(Cyber Security)、軟體更新(Software Update)、自動車道維持系統(Automated Lane Keeping Systems)，以及事件數據紀錄器(Event Data Recorder)等新車輛法規，並由各先進國家有規劃的導入法規，以推動自駕或聯網技術的發展，本篇文章將摘要介紹聯合國所訂定之UN R155 網路安全及UN R156 軟體更新法規內容。

二、法規概要

我國現行導入實施的車輛安全法規多數來自聯合國歐洲經濟委員會(UNECE)的世界車輛法規調和論壇(WP.29)所討論之車輛法規，該論壇下有許多工作組針對車輛所涉各個層面，訂定統一技術標準之法規，如汙染及能源(GRPE)、噪音及輪胎(GRBP)、燈光及訊號(GRE)、一般安全(GRSG)、被動安全(GBPE)及自動/自駕/聯網車輛(GRVA)等六個面向。

本篇文章介紹的網路安全及軟體更新之車輛法規，則是由自動/自駕/聯網車輛工作組(GRVA)旗下之網路安全/無線軟體更新特別工作組(Task



Force on CS/OTA)進行研議，經過特別工作組自2018年起的多次會議討論，於2020年6月第181次之世界車輛法規調和論壇正式投票通過，且於2021年1月22日生效，後續於2021年3月4日由聯合國歐洲經濟委員會正式公告UN R155網路安全及網路安全管理系統、UN R156軟體更新及軟體更新管理系統等兩項法規，全球包含歐盟、日本、韓國、英國及澳大利亞等國家皆導入實施，其中歐盟及日本已強制實施相關法規，有關實施情形、適用對象及實施時間摘要說明如下：

(1) 歐盟：

A.網路安全：透過(EU) 2019/2144指令^[1]要求M、N類之新型式車輛自2022年7月6日、各型式車輛自2024年7月7日起，應具備防護網路攻擊的能力，並於(EU) 2022/1398^[2]指令進行補充，於車輛符合UN R155 00 Series之狀況下即滿足前述要求。

B.軟體更新：透過(EU) 2022/2236^[4]指令對(EU) 2018/858^[3]進行補充，要求允許執行軟體更新的M、N、O類之新型式車輛自2024年7月7日起、各型式車輛自2026年7月7日起，應依照指令中Annex IV之要求，透過符合UN R156 00 Series滿足相關要求。

(2) 日本：於2020年12月25日公告^[5]，具備自動運行裝置(可代替駕駛人於行駛過程中認知、預判、決定及操作之相關裝置，相似於SAE自駕等級分類LEVEL3以上之相關裝置或功能^[6])之車輛應符合網路安全及軟體更新之相關要求，並依照是否具備無線軟體更新功能分階段實施

A.具備無線軟體更新功能者：新型式為2022年7月1日起；各型式為2024年7月1日起應符合相關要求。

B.未具備無線軟體更新功能者：新型式為2024年1月1日起；各型式為2026年5月1日起應符合相關要求。

另未具備自動運行裝置之車輛亦可適用，但未被強制要求符合相關規定。

三、網路安全

有關網路安全法規，本次將基於UNECE於2021年3月4日所發布之00



財團法人車輛安全審驗中心

遵循法令 公正專業 優質服務

車安通訊季刊



Series檔案^[7]進行說明，其法規項目為「網路安全及網路安全管理系統相關之車輛認證一致性規定(Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system)」，本項規定適用於M類客車及N類貨車、安裝至少一個電子控制單元(Electronic Control Unit ; ECU)的O類拖車，以及配備UNECE所描述等級3自動駕駛功能的L6及L7類車輛。

在本項法規的定義中，「網路安全」指的是道路車輛及其功能就攻擊對象為電子或電氣組件的網路威脅受到保護的情形，並透過建立網路安全管理系統(Cyber Security Management System ; CSMS)，以及在車輛上實施相對應的措施，以達到前述所指的網路安全狀況，另外值得注意的是，這邊所提到的系統並非一個功能或是裝置，而是管理系統，即一個用於對應相關要求的管理制度的集合。

另外，在認證的角度上，本項法規認證係以製造廠指定之車輛型式，以及網路安全相關電子/電氣架構或外部介面的必要特點等兩項進行判斷，舉例說明：假設車輛採用某一種晶片及程式對車輛遭遇的外部網路攻擊評估，如果同一廠牌的不同車系上沒有採用同一應對模式執行網路安全管理，則沒辦法視為是同一種車輛型式，反之，若採用同一模式應對模式，雖然車輛因為設計造成外型可能不同，但視為是同一種車輛型式。

本項法規的認證是由認證機構在確認製造廠申請之車輛型式滿足本項法規的要求後進行核發，其中認證機構或檢測機構將透過文件檢查以及試驗等方式進行確認，確保製造廠已針對車輛可能遭遇之任何威脅進行評估並對應，在本項法規的測試與過往法規的執行方式較為不同，是由認證機構或檢測機構與車輛製造廠合作，透過取樣方式執行並就所紀錄之網路安全措施進行確認，取樣必須聚焦但不限於經評估的高風險。

在網路安全管理系統上，製造廠必須針對車輛型式建立並維持網路安全管理系統，目的是透過本項系統建立橫跨開發、生產及後生產階段之管理系統，用於管理車輛可能遭遇的風險及其對應減輕措施，以及管理如供應商、服務提供者或製造廠的次等組織等相關單位，並於車輛投入使用後持續進行監控、分析並偵測網路威脅、弱點及網路攻擊，其中針對用於已



財團法人車輛安全審驗中心 住址：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@vsc.org.tw

Copyright © 2023 VSCC 版權所有



識別風險的評估、分類及處置的程序、監測車輛型式上網路威脅及弱點的程序(以偵測並對應網路攻擊)，以及鑒於已識別的新網路威脅及弱點，評估現行網路安全措施是否仍有效的程序等三項，CSMS必須就需要車輛製造廠進行回應的相關網路威脅及弱點在合理的時間內進行減輕措施。

在車輛上，製造廠必須針對該車輛型式取得有效的CSMS符合證明，並就風險進行識別、管理、處置、評估、驗證，以及執行相關對應措施，為了證明車輛符合相關規定，應依照規定於必要時須向檢測機構進行說明或示範，其中於各層面需要注意之細節，如下所述：

- (1) 在風險識別上，必須降至供應商等級，了解可能與供應商相關的風險，另外，識別網路安全的關鍵相關元素上，必須考量法規中附件五的威脅及對應減輕措施列表所列出之資訊。
- (2) 用以儲存及執行後市場軟體、服務、應用程式或數據的特定環境必須要有合適的對應措施。
- (3) 製造廠於申請認證前必須執行測試以驗證所實施安全措施的有效性。
- (4) 製造廠實施措施的目的包含偵測並避免網路攻擊、輔助偵測威脅、弱點及網路攻擊的監測能力，以及提供數據分析能力以分析未遂或成功的網路攻擊等三項。
- (5) 使用於對應法規要求的加解密模組必須符合共識標準 (consensus standards；註：由相關利益團體參與，用於設定產品開發及生產的一致性標準)，若使用非符合共識標準的模組，則製造廠必須說明其使用上的正當性。

另本項法規於附件五對威脅及其對應減輕措施進行條列，其主要分為三大部分：威脅相關的弱點或攻擊方式、對車輛本身的威脅減輕措施，以及車輛外部(非車輛本身)的威脅減輕措施，就基本的弱點、威脅及減輕措施進行釐清。

四、軟體更新

於軟體更新部分，則是基於UNECE於2021年3月4日所發布之00 Series 檔案^[8]進行說明，其法規項目為「軟體更新及軟體更新管理系統相關之車



輛認證一致性規定(Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system)」，本項規定適用於允許進行軟體更新的M、N、O、R、S、T類車輛，其中M、N、O類分別為客車、貨車及拖車，R、S、T則屬於農業用的相關車輛。

而在本項法規的定義中，「軟體更新」指的是用於將軟體升級至新版本，且包含設定參數變更的套件(Package)，並透過建立軟體更新管理系統(Software Update Management System；SUMS)，以符合標準的程序於車輛上實施軟體更新。

在認證的角度上，本項法規認證係以製造廠指定之車輛型式，以及軟體更新程序相關車輛設計的必要特點等兩項進行判斷。另外，與網路安全法規的情況類似，本項規定中同樣針對軟體更新管理系統以及車輛分別進行要求，在軟體更新管理系統中，於首次評估必須針對特定程序進行驗證、製造廠必須進行紀錄或儲存的相關資訊、針對安全性進行說明或示範，以及針對無線軟體更新(Software Update Over-The-Air)的額外要求等四大項目。

其中對於首次評估當中需驗證的程序，包含用於紀錄、辨識、驗證、釐清及各項軟體更新相關資料及更新情形，且製造廠對指定之車輛型式執行軟體更新時，必須對特定資訊進行紀錄及儲存，用以確保及追蹤車輛於軟體更新前後的狀況，於安全性部分，製造廠必須確保軟體更新過程受到保護以避免更新程序開始前受到影響及危害，並能驗證及確認車輛的軟體功能性及所使用的軟體程式碼是否合適，額外於無線軟體更新部分則必須說明並示範其安全性，以及於需要特定技能或複雜行動下狀況，如何完成更新作業，另有關前述程序及資訊摘要分別如表一及表二所示：

表一、軟體更新管理系統進行首次評估當中需驗證的程序

項次	程序
1	製造廠對法規相關資訊紀錄並安全儲存，且可於驗證機構或檢測機構要求時，開放資料供相關單位確認的程序



財團法人車輛安全審驗中心

遵循法令 公正專業 優質服務

車安通訊季刊



項次	程序
2	用於識別所有初始/已更新的軟體版本(包含完整性驗證數據)及經過型式認證的相關硬體組件資訊的程序
3	若車輛具備軟體識別代碼(RXSWIN，由製造廠定義用於代表型式認證相關軟體更新的特定識別碼(Identifier)，於更新前後可存取及更新軟體識別代碼的程序，以及製造廠用於驗證經型式認證系統是否與現行軟體版本相同的程序
4	用於辨識更新系統與其他系統相依關係的程序
5	可使製造廠辨識目標車輛的程序
6	用於確認目標車輛設定與軟體更新相容性的程序
7	用於評估、識別及紀錄軟體更新是否會影響經型式認證系統的程序
8	用於評估、識別及紀錄軟體更新是否會增加、變更或啟用任何於車輛執行型式認證時未呈現或啟用的功能，或變更、解除任何其他法規所定義的參數或功能的程序
9	若軟體更新將影響任何其他車輛的安全及持續運作所需系統，或更新將增加或變更註冊時的功能性時，用於評估、識別及紀錄前述情形的程序
10	用於通知車輛使用者更新事宜的程序
11	製造廠可依照相關規定向權責單位及檢測機構開放資料的程序

表二、軟體更新管理系統必須紀錄及儲存的相關資料

項次	資料
1	用於說明或示範軟體更新程序符合性的說明資料
2	描述更新前後任何相關經型式驗證系統的設定資料
3	對於每個軟體識別代碼
4	條列更新目標車輛，以及前述車輛最後已知系統設定的相容性確認資料。
5	更新目的、受影響系統及功能、哪些對象已經過型式認證(如有)、軟體更新是否影響經型式驗證系統符合要求、是否影響型式認證參數、更新是否由認證單位要求、更新如何執行及其可執行的狀況、更新將以安全且穩固方式執行的確認、更新已通過驗證及確認程序



財團法人車輛安全審驗中心

住址：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@vsc.org.tw

Copyright © 2023 VSCC 版權所有



於車輛型式上，必須對軟體更新的真實性及完整性進行保護，以避免其受到破壞或執行無效更新，在車輛型式使用軟體識別代碼的情況下，必須確保代碼可特別地進行識別、藉由電子通訊介面可以標準化的方式輕易讀取，以及保護該代碼避免受到非授權的修改，另法規中針對無線軟體更新具備額外要求，包含：

- (1) 車輛應具備與下述規定相關的功能：
 - A. 車輛於更新失敗或受到中斷時，可將系統回復至前一版本。
 - B. 確保車輛僅可於具備足夠能源以完成更新時執行軟體更新。
 - C. 於更新可能影響車輛安全時，製造廠必須說明或示範如何安全地執行更新。
- (2) 製造廠應說明或示範如何向車輛使用者通知更新事宜，且相關資訊必須包含：更新目的、車輛功能的改變、完成更新的預估時間、更新期間無法使用的功能，以及任何可協助車輛使用者安全地完成更新的指示。
- (3) 於行駛期間進行更新可能造成危險之情況下，製造廠必須確保使用者於更新期間不能行駛車輛，且確保使用者無法使用車輛上任何可能對影響車輛安全或影響成功更新的相關功能。
- (4) 於更新執行後，製造廠必須說明或示範如何向使用者通知車輛已更新成功(或失敗)，以及如何向使用者通知實施的改變及任何相關的使用者手冊更新(如適用時)。
- (5) 車輛於更新前必須滿足更新的前提條件。

五、結語

在確認過這兩項法規的內容後，我們可以發現網路安全及軟體更新與以往的聯合國法規有著較大的差異，其中在測試的執行方式及標準部分特別明顯，過往的聯合國車輛法規會針對車輛上特定的性能設定測試的方式，以及相關性能必須對應的標準，而在這兩份法規當中，多數要求則是以性質的方式進行描述，如何達成性質則是由車輛的製造廠進行規劃以及說明，對於未能有明確標準的要求而言，如何判斷其是否符合規定一事，



無論是對於認證機構或檢測機構，後續都將會是一個必須持續研究及討論的課題。

為滿足CSMS及SUMS，業界也持續研究並發展相關標準，據筆者了解，目前國際標準化組織(ISO)針對前面兩個管理系統，分別訂定了ISO 21434:2021 Road vehicles — Cybersecurity engineering^[9]及ISO 24089:2023 Road vehicles — Software update engineering^[10]等兩項標準。

隨著科技持續進步，車輛上如要提供特定功能或達成一定性能，並非僅能以測試等特定方式達成，過往幾年內的多項ADAS系統法規中，也有如前述以性質方式描述，並由製造廠自行證明其符合性的相關要求。

對於車輛安全層面而言，後續網路安全及軟體更新皆會占有一席之地，對於未來自駕車輛及聯網車輛的發展，也會是不可或缺的一個要素，其中隨著各品牌導入電動車輛，於軟體更新部分更是近年來我國關心的議題，軟體更新所涉及的層面更廣，並包含如車載系統、車輛安全及排汙能耗等等層面皆可能受到其影響，為使我國車輛安全妥善發展，車安中心將持續就各項車輛安全規定進行研究，並協助交通部為國人車輛安全審驗把關，提升國內車輛安全。

六、參考文獻

- [1] [\(EU\) 2019/2144 車輛安全要求規定。](#)
- [2] [\(EU\) 2022/1398 車輛安全要求補充規定。](#)
- [3] [\(EU\) 2018/858 型式認證要求。](#)
- [4] [\(EU\) 2022/2236 型式認證要求補充規定。](#)
- [5] [国土交通省報道発表資料](#)
- [6] [道路運送車両法第四十一条](#)
- [7] [UNECE - UN R155 00 Series](#)
- [8] [UNECE - UN R156 00 Series](#)
- [9] [ISO/SAE 21434:2021](#)
- [10] [ISO 24089:2023](#)