附件九十七、軟體更新及軟體更新管理系統

1. 實施時間及適用範圍：
   1.1 中華民國一百十七年一月一日起，新型式之M、N及O類車輛及中華民國一百十九年一月一日起，各型式之M、N及O類車輛允許執行軟體更新者，應符合本項規定。
   1.2 除大客車及幼童專用車以外之車輛，申請少量車型安全審驗者，得免符合本項「軟體更新及軟體更新管理系統」規定。
   1.3 申請逐車少量車型安全審驗者，得免符合本項「軟體更新及軟體更新管理系統」規定。
   1.4 檢測機構得依本項基準調和之聯合國車輛安全法規(UN Regulations)，UN R15600系列及其後續相關修正規範進行測試。
2. 名詞釋義：
   2.1 RX軟體識別號碼(RX Software Identification Number, RXSWIN)：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。
   2.2 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)，包括配置參數之改變。
   2.3 執行(Execution)：係指安裝和啟動已下載更新之過程。
   2.4 軟體更新管理系統(Software Update Management System, SUMS)：係指定義組織的過程和程序之系統方法，以符合提交軟體更新之要求。
   2.5 車輛使用者(Vehicle user)：係指操作或駕駛車輛的人、車主、車隊管理者所授權的代表或僱員，車輛製造商所授權的代表或僱員，或經授權的技術人員。
   2.6 安全狀態(Safe state)：係指一個項目發生故障時的一種操作模式，該模式沒有不合理的風險等級。
   2.7 軟體(Software)：係指電子控制系統中由數位數據和指令組成之一部分。
   2.8 空中（無線）更新(Over-the-Air (OTA) update)：係指以無線方式而非使用電纜或其他本地連接進行數據傳輸之任何方法。
   2.9 系統(System)：係指實現一種功能的零組件及/或子系統之集合。
   2.10 完整性驗證數據(Integrity validation data)：係指數位數據的表示，可以對其進行比較以檢測數據中的錯誤或更改。這可能包括檢查總和(Checksum)和雜湊值(Hash value)。
3. 軟體更新及軟體更新管理系統之適用型式及其範圍認定原則：
   3.1 車輛廠牌相同。
   3.2 設計之軟體更新過程相同。
4. 軟體更新管理系統符合性證明文件
   4.1 申請者應檢附下列文件一式三份及具體內容向審驗機構申請軟體更新管理系統符合性證明文件，再由審驗機構對申請者進行評估後，核發軟體更新管理系統符合性證明文件：
      4.1.1 描述軟體更新管理系統之文件。
      4.1.2 軟體更新管理系統符合性聲明書。
   4.2 在評估過程中，申請者應提出符合性聲明書，並向審驗機構或其檢測機構進行展示，以證明符合所規定的所有軟體更新要求之必要程序。
   4.3 當評估完成，並接獲申請者所提符合性聲明書後，應核發軟體更新管理系統(SUMS)符合性證明文件（以下簡稱SUMS符合性證明文件）。

4.4 除撤銷外，SUMS符合性證明文件自核發之日起，最多保持三年有效期。

4.5 審驗機構於核發軟體更新管理系統符合性證明文件後，得隨時驗證軟體更新管理系統(SUMS)是否持續符合規定。若經查未符合規定，則可撤銷軟體更新管理系統的符合性證明文件。

4.6 申請者應向審驗機構或其檢測機構通知有關任何影響軟體更新管理系統符合性證明文件之變化情形，並經與申請者協調確認後，應由審驗機構或其檢測機構決定是否有重新進行檢查之必要性。

4.7 在軟體更新管理系統符合性證明文件有效期屆滿前，申請者應向審驗機構申請新符合性證明文件或延伸現有SUMS符合性證明文件，經審驗機構正向評估(positive assessment)同意後，核發新的軟體更新管理系統符合性證明文件或展延其有效期三年。如已向審驗機構或其檢測機構申請變更時，則應重新評估後，核發新的符合性證明文件。

4.8 若申請者所取得之軟體更新管理系統符合性證明文件因逾期而失其效力時，不影響先前據此所取得之車輛型式安全審驗合格證明之有效性。

5. 通則

5.1 對申請者之軟體更新管理系統要求

5.1.1 初步評估之驗證程序

5.1.1.1 將與本項法規有關的資訊，於申請者處記錄及安全地保存，並可提供予審驗機構或其檢測機構之程序。

5.1.1.2 可唯一識別所有初始和更新軟體版本資訊的程序，包括完整性驗證數據，以及型式認證系統相關之硬體零組件。

5.1.1.3 對於具有RXSWIN的車輛型式，可藉以存取和更新有關該車輛型式於軟體更新前後 RXSWIN資訊的程序。這應包括更新每個RXSWIN的軟體版本及其所有相關軟體的完整性驗證數據能力。

5.1.1.4 對於具有RXSWIN的車輛型式，申請者可藉以驗證型式認證系統零組件所存在之軟體版本與相關RXSWIN所定義版本一致的程序。

5.1.1.5 可藉以確定更新的系統與其他系統任何相互依賴關係的程序。

5.1.1.6 申請者能夠識別目標車輛進行軟體更新的程序；

5.1.1.7 在軟體更新發布前確認其與目標車輛配置相容性的程序，應包括在發布前評估目標車輛最後已知的軟體/硬體配置與更新之相容性。

5.1.1.8 評估、識別和記錄軟體更新是否會影響任何型式認證系統的程序，並應考慮更新是否會影響或改變用於定義更新可能影響的系統任何參數，或是否會改變用於對這些系統進行型式認證的任何參數（如相關法律所定義）。

5.1.1.9 評估、識別和記錄軟體更新是否會增加、改變或啟用車輛型式認證時，不存在或未啟用的任何功能，或改變或禁用法律規定的任何其他參數或功能之程序。該評估應考慮包括如下：

(a) 將需要修改的條目資訊；

(b) 測試結果不再涵蓋改裝後的車輛；

(c) 車輛功能的任何修改將影響車輛型式認證。

5.1.1.10 評估、識別和記錄軟體更新是否會影響車輛安全和持續運行所需的任何其他系統，或者更新是否會增加或改變車輛與註冊時相比的功能之程序；

5.1.1.11 車輛使用者能夠被通知更新資訊的程序；

5.1.1.12 申請者應能依據條文5.1.2.3和5.1.2.4規定之資訊提供予審驗機構或檢測機構的程序。

5.1.2 申請者應記錄並儲存適用於提供車型每次更新的資訊如下：

5.1.2.1 描述申請者用於軟體更新流程的文件，以及用於展演其符合的任何相關標準；

5.1.2.2 描述更新前後任何相關型式認證系統配置的文件，包括型式認證系統的硬體和軟體（包括軟體版本），以及任何相關車輛或系統參數的唯一標識。

5.1.2.3 對於每個RXSWIN，應當有一個可核對的記錄器(auditable register)，描述更新前後與該車型RXSWIN相關的所有軟體。這應包括每個RXSWIN所有相關軟體的軟體版本及其完整性驗證數據資訊。

5.1.2.4 列出更新的目標車輛，並確認這些車輛最後已知配置與更新相容性的文件。

5.1.2.5 描述該車型的所有軟體更新文件：

(a) 更新的目的

(b) 更新可能影響之車輛系統或功能

(c) 已通過型式認證之軟體更新（依實際狀況）

(d) 軟體更新是否影響到型式認證系統任何相關要求（依實際狀況）

(e) 軟體更新是否影響到任何系統型式認證參數

(f) 是否已取得審驗機構對更新之認可

(g) 執行更新方式及執行條件

(h) 確認可安全且可靠的執行軟體更新

(i) 確認軟體更新已完成並通過認證和確認程序

5.1.3 安全性—申請者應展演下列程序：

5.1.3.1 確保軟體更新受到保護之程序，其可於更新過程開始之前合理的防止竄改；

5.1.3.2 對所使用的更新程序進行保護，以合理地防止其被破壞，包括開發更新交付系統；

5.1.3.3 用於驗證和確認車輛使用的軟體功能和代碼的程序是適當的。

5.1.4 對軟體無線（空中）更新的額外要求

5.1.4.1 申請者應展演將使用之流程和程序，以評估若在駕駛過程中進行無線（空中）更新，不會影響安全。

5.1.4.2 申請者應展演所使用的流程和程序，以確保當無線（空中）更新需要一個特定熟練或複雜的動作時（例如在編譯後重新校準一個傳感器，以完成更新過程），只有當一個熟練地做該動作的人在場或控制該流程時才能進行更新。

5.2 對車輛型式的要求

5.2.1 對軟體更新的要求

5.2.1.1 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。

5.2.1.2 在車輛型式使用RXSWIN時：

5.2.1.2.1 每個RXSWIN應是唯一可識別的。當申請者修改型式認證相關軟體時，如果導致型式認證延伸或新的型式認證，應更新RXSWIN。

5.2.1.2.2 每個RXSWIN應通過使用電子通訊界面，至少通過標準介面（OBD埠），以標準化的方式易於讀取。

如果車輛未擁有RXSWIN，申請者應向審驗機構聲明車輛或單個ECU的軟體版本，並與相關型式認證連結。每次更新所聲明的軟體版本時，應更新該聲明。在這種情況下，軟體版本應通過使用電子通訊界面，至少通過標準介面（OBD埠），以標準化的方式易於讀取。

5.2.1.2.3 申請者應保護車輛上的RXSWIN和/或軟體版本，以防止未經授權修改。在進行型式認證時，應以保密方式提供申請者作為防止未經授權修改RXSWIN和/或軟體版本所採取的措施。

5.2.2 對軟體無線（空中）更新的額外要求

5.2.2.1 車輛應具備以下有關軟體更新的功能：

5.2.2.1.1 申請者應確保在更新失敗或中斷的情況下，車輛能夠將系統恢復到以前的版本，或者在更新失敗或中斷後，車輛能夠置於安全狀態。

5.2.2.1.2 申請者應確保車輛只在有足夠的電力完成更新過程時才能執行軟體更新（包括可能恢復到以前的版本或將車輛置於安全狀態所需的電力）。

5.2.2.1.3 當執行更新可能影響車輛的安全時，申請者應展演如何安全地執行更新。此應通過技術手段實現，以確保車輛處於可以安全執行更新的狀態。

5.2.2.2 申請者應證明，在執行更新之前，車輛使用者能夠被告知有關更新的情況。所提供的資訊應包括：

(a)更新的目的。這可能包括更新的關鍵性，以及更新是否是為了召回、安全和/或防護性(security)目的。

(b)對車輛功能更新所實施的任何改變；

(c)完成更新執行的預期時間；

(d)在執行更新期間可能無法使用的任何車輛功能；

(e)任何可能幫助車輛使用者安全執行更新的指示；

在內容相似的更新群體情況下，一個資訊可以覆蓋一個群組。

5.2.2.3 在駕駛時執行更新可能不安全的情況下，申請者應證明：

(a)確保在執行更新的過程中不能駕駛車輛；

(b)確保駕駛者不能使用車輛的任何功能，以免影響車輛的安全或更新的成功執行。

5.2.2.4 在執行更新後，申請者應證明如何執行以下內容：

(a)告知車輛使用者更新成功（或失敗）；

(b)通知車輛使用者所實施的改變以及對使用手冊的任何相關更新（如果適用）。

5.2.2.5 車輛應確保在執行軟體更新前必須滿足所需的先決條件。