附件九十六、網路安全及網路安全管理系統

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及N類車輛及中華民國一百十九年一月一日起，各型式M及N類車輛，應符合本項規定。
   1.2 中華民國一百十七年一月一日起，新型式O類車輛及中華民國一百十九年一月一日起，各型式O類車輛若具備至少一個電子控制單元者，應符合本項規定。
   1.3 本規定不影響其他依法授權可對車輛的資料、功能和資源進行存取及此類存取的條件，亦不排除個人資料保護相關法令之適用。
   1.4 本規定不影響其他依法管理替換零件和組件的開發和安裝/系統集成，物理和數位，與網路安全有關部分。
   1.5 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「網路安全及網路安全管理系統」規定。
   1.6 申請逐車少量車型安全審驗者，得免符合本項「網路安全及網路安全管理系統」規定。
   1.7 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 R155 00系列及其後續相關修正規範進行測試。
2. 名詞釋義
   2.1 網路安全(Cyber security) ：係指保護道路使用車輛及其功能免受電氣或電子零組件網路威脅的條件。
   2.2 網路安全管理系統 (Cyber Security Management System ，CSMS)：係指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。
   2.3 系統(System)：係指實現一種功能的零組件及/或子系統之集合。
   2.4 開發階段(Development phase)：係指車型於型式審驗之前的期間。
   2.5 生產階段(Production phase)：係指車型的生產期間。
   2.6 生產後階段(Post-production phase)：係指該車型下所有車輛於車型停產後至車輛報廢之期間。
   2.7 緩解(Mitigation)：係指降低風險之措施。
   2.8 風險(Risk)：係指特定威脅利用車輛漏洞從而對組織或個人造成傷害的可能性。
   2.9 風險評估(Risk Assessment)：係指發現、識別和描述風險（風險識別），理解風險的性質並確定風險等級（風險分析），以及將風險分析的結果與風險標準進行比較，以確定風險和/或其程度是否可接受或可容忍之總體過程（風險評估）。
   2.10 風險管理(Risk Management)：係指指導和管制組織有關風險的協調活動。
   2.11 威脅(Threat)：係指可能對系統、組織或個人造成損害的意外事件的潛在原因。
   2.12 漏洞(Vulnerability)：係指資產或緩解措施的弱點，可以被一個或多個威脅利用。
3. 網路安全及網路安全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 與網路安全相關的電子電氣架構和外部介面的基本要素相同。
4. 網路安全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網路安全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並核發CSMS符合性證明文件：

4.1.1 描述網路安全管理系統之文件。

4.1.2 宣告聲明書。

4.2 在評估過程中，申請者應提出宣告聲明書，以證明符合本法規所有網路安全要求之必要程序。

4.3 當評估完成並接獲申請者所提交之宣告聲明書後，應核發CSMS 符合性證明文件。

4.4 審驗機構或檢測機構應使用本法規所規定之格式核發CSMS符合性證明文件。

4.5 CSMS符合性證明文件除撤銷外，自核發日起最長有效期為三年。

4.6 審驗機構於核發CSMS符合性證明文件後，得隨時驗證其是否持續符合規定。如經查未符合規定，則應撤銷CSMS符合性證明文件。

4.7 申請者應向審驗機構或檢測機構通知有關任何影響CSMS符合性證明文件之變化情形，並經與申請者協商確認後，應由審驗機構或檢測機構決定是否有重新進行檢查之必要性。

4.8 在CSMS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證或延伸現有CSMS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CSMS符合性證明文件或延長其證明有效期三年。審驗機構應驗證CSMS是否持續符合本法規的要求。若已向審驗機構或檢測機構申請變更時，則應正向重新評估後，核發新的符合性證明文件。

4.9 對於CSMS相關之車型，若製造商符合CSMS之符合性證明文件期滿或撤銷則應辦理變更認證，其包含無法符合審驗者得撤銷其符合性證明文件。

5. 規格

5.1 一般規格

5.1.1 本法規的要求不應限制其他車輛安全檢測基準項目的規定或要求。

5.2 網路安全管理系統要求

5.2.1 審驗機構或檢測機構應驗證並評估申請者是否具有網路安全管理系統，並應驗證其符合本項法規。

5.2.2 網路安全管理系統應包括：

5.2.2.1 申請者應向審驗機構或檢測機構證明網路安全管理系統適用於以下階段：

(a) 開發階段；

(b) 生產階段；

(c) 生產後階段。

5.2.2.2 申請者應證明其網路安全管理系統中使用的流程可確保充分考慮安全性，包括附件中所列的風險和緩解措施。應包括：

(a) 申請者組織內用於管理網路安全的流程；

(b)用於識別車輛型式風險的過程。在相關過程中，應考慮條文6規定所列出之相關威脅；

(c)用於評估、分類和處理已識別風險的程序；

(d)驗證所識別的風險是否得到適當管理的流程；

(e)用於測試車輛型式網路安全的程序；

(f)用於確保風險評估與時俱進的程序；

(g)用於監控、檢測和反應網路攻擊、網路威脅和車輛型式漏洞的過程，以及用於評估所實施的網路安全措施是否仍然有效的過程，以確保新的網路威脅和漏洞可被識別。

(h)用於提供相關資料以支持對未遂或成功的網路攻擊進行分析的流程。

5.2.2.3 申請者應證明其網路安全管理系統中使用的流程將確保，依條文5.2.2.2(c)、 5.2.2.2(g)規定中提到的分類，需要申請者反應之網路威脅和漏洞，應於合理之時間範圍內獲得緩解。

5.2.2.4 申請者應證明其網路安全管理系統中使用的流程將確保依條文5.2.2.2(g) 規定所述的監控應持續進行。

(a)將首次登記領牌後之車輛納入監測；

(b)包括從車輛資料和車輛紀錄（如保養維修紀錄）中分析和檢測網路威脅、漏洞和網路攻擊的能力。此功能應遵守條文1.3規定及車主或駕駛的隱私權，尤其須經其同意。（本法規不影響其他法規、區域或國家立法關於授權存取車輛、其資料、功能和資源以及相關存取條件，其亦不排除國家或地區有關個人資料保護相關法令之適用。）

5.2.2.5 申請者應依條文5.2.2.2規定的要求證明其網路安全管理系統將如何管理與簽約供應商、服務提供商或製造商的子組織可能存在的依賴關係。

5.3 對車輛型式的要求

5.3.1 申請者應持有與審驗相關車輛型式之網路安全管理系統有效符合性證明文件。

5.3.2 申請者應對所認可的車輛型式，識別和管理與供應商相關的風險。

5.3.3 申請者應識別車輛型式的關鍵要素，並對該車輛型式進行詳盡的風險評估，並應適當處理/管理已識別的風險。風險評估應考慮車輛型式的各個要素及其互動。風險評估應進一步考慮與任何外部系統的互動。在評估風險時，申請者應考慮依條文6.5規定之所有威脅相關的風險以及任何其他相關風險。

5.3.4 申請者應保護車輛型式免申請者風險評估中確定風險。應實施適當的緩解措施以保護車輛型式。實施的緩解措施應包括依條文6.6、6.7規定與識別的風險相關的所有緩解措施。惟若依條文6.6或條文6.7部分規定提到的緩解措施與識別的風險不相關或不充分，則申請者應確保實施另一種適當的緩解措施。

5.3.5 申請者應採取適當且相稱的措施，以確保車輛型式（如提供）的專用環境用於售後市場軟體、服務、應用程式或資料儲存和執行。

5.3.6 申請者應在型式審驗之前進行適當和充分的測試，以驗證所實施的安全措施的有效性。

5.3.7 申請者應實施以下措施：

(a)檢測並防止針對該型式車輛的網路攻擊；

(b)支援申請者在檢測與車輛型式相關的威脅、漏洞和網路攻擊方面的監控能力；

(c)提供資料取證能力，以分析未遂或成功的網路攻擊。

5.3.8 用於本法規目的的密碼模組應符合共識標準。如果使用的密碼模組不符合共識標準，則申請者應證明其使用的合理性。

5.4 報告規定

5.4.1 申請者應至少每年一次或更頻繁地（若有相關狀況）向審驗機構或檢測機構報告其監測活動的結果，如4.2.2.2.(g)所定義，這應包括關於新的網路攻擊資

訊。申請者還應向審驗機構或檢測機構報告並確認為其車輛型式實施的網路安全緩解措施仍然有效，並且已採取任何其他措施。

5.4.2 審驗機構或檢測機構應核實所提供的資訊，並在必要時要求申請者糾正任何檢測無效資訊。

如報告或回覆內容不充分，審驗機構得依4.6之規定撤銷CSMS符合性證明文件。

6. 威脅列表及相應緩解措施

6.1 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。

6.2 A部分、B 部分和C部分應考慮用於申請者實施的風險評估和緩解措施。

6.3 高等級漏洞及其相應範例指標已編入A部分。相同指標部分也於B和C部分表中被使用以連接每個攻擊/漏洞列表相應的緩解措施。

6.4 威脅分析也應考慮可能的攻擊影響。相關部分可能有助於確定風險的嚴重性和識別額外的風險。可能攻擊影響包括：

(a) 車輛的安全運作受影響；
(b) 車輛功能停止工作；
(c) 軟體修改，性能改變；
(d) 軟體改變但沒有影響操作；
(e) 資料完整性被破壞；
(f) 違反資料機密性；
(g) 無法取得資料；
(h) 其他，包括犯罪。

6.5 A部分：威脅、漏洞和攻擊相關方法

6.5.1 威脅之高等級描述和相關漏洞或攻擊方法，如表一。

表一： 威脅之高等級描述和相關漏洞或攻擊方法

漏洞/威脅的高等級和次等級描述			漏洞或攻擊方法範例	
4.3.1 現場車輛相關後端伺服器的威脅	1	用作攻擊車輛或擷取資料的手段的後端伺服器	1.1	員工濫用特權（內部攻擊）
			1.2	未經授權對伺服器進行網路存取（例如通過後門、未修補的系統軟體漏洞、SQL攻擊或其他方式啟用）
			1.3	對伺服器的未經授權的物理存取（例如通過USB 隨身碟或其他連接到伺服器的媒體進行）
	2	後端伺服器服務中斷，影響車輛運作	2.1	對後端伺服器的攻擊使其停止運作，例如阻止後端伺服器與車輛互動與提供車輛運作所需之服務
	3		3.1	員工濫用特權（內部攻擊）

漏洞/威脅的高等級和次等級描述			漏洞或攻擊方法範例	
		後端伺服器上保存的車輛相關資料遺失或受損（“資料洩露”）	3.2	雲端中資訊遺失 資料由第三方雲端服務提供商儲存時，敏感資料可能因攻擊或事故而遺失
			3.3	對伺服器的未經授權的聯網存取 (例如通過後門、未修補的系統軟體漏洞、SQL 攻擊或其他方式啟用)
			3.4	對伺服器的未經授權的物理存取（例如通過 USB 隨身碟或其他連接到伺服器的媒體進行）
			3.5	意外共享資料導致的資料外洩（行政管理疏失）
4.3.2 對車輛通訊頻道的威脅	4	車輛接收到的資訊或資料的欺騙	4.1	資訊欺騙通過模擬（例如，列隊期間的 802.11p V2X、GNSS 資訊等）
			4.2	女巫攻擊（為欺騙其他車輛，如道路中有很多車輛一般）
	5	用於對車輛持有的代碼/資料進行未經授權的操作、刪除或其他修改的通訊頻道	5.1	通訊頻道允許程式碼注入，例如已受到篡改之軟體二進制文件可能被注入到通訊流中
			5.2	通訊頻頻道允許操縱車輛持有資料/代碼
			5.3	通訊頻道允許覆蓋車輛持有資料/代碼
			5.4	通訊頻道允許刪除車輛持有資料/代碼
			5.5	通訊頻道允許將資料/代碼引入車輛（寫入資料代碼）
	6	通訊頻道允許接受不可信/不可靠的資訊或容易受到會話劫持/重播攻擊	6.1	從不可靠或不受信任的來源接受資訊
			6.2	中間人攻擊/會話劫持
			6.3	重播攻擊，例如對通訊匝道的攻擊以允許攻擊者執行ECU 軟體或匝道韌體降級
	7	資訊很容易被揭露 例如，通過竊聽通訊或允許未經授權存取敏感文件或文件夾	7.1	資訊截取 / 干擾輻射 / 監控通訊
			7.2	未經授權存取文件或資料
	8		8.1	發送大量垃圾資料進入車輛資訊系統，使其無法正常提供服務

漏洞/威脅的高等級和次等級描述			漏洞或攻擊方法範例	
		通過通訊頻道進行拒絕服務攻擊以破壞車輛功能	8.2	黑洞攻擊，以中斷車輛之間的通訊，攻擊者能夠阻止車輛之間的資訊
	9	非特權使用者能夠獲得對車輛系統的特權存取	9.1	非特權使用者能夠獲得特權存取，例如 root 存取
	10	嵌入通訊媒體的病毒能夠感染車輛系統	10.1	病毒嵌入通訊媒體感染車輛系統
	11	車輛接收的資訊（例如 X2V 或診斷資訊）或在車輛內部傳輸的資訊包含惡意內容	11.1	惡意內部（例如 CAN）資訊
			11.2	惡意V2X 資訊，例如基礎設施到車輛或車輛-車輛資訊（例如 CAM、DENM）
			11.3	惡意診斷資訊
			11.4	惡意專有資訊（例如，通常從 OEM 或零組件/系統/功能供應商發送的資訊）
4.3.3. 對車輛更新程序的威脅	12	濫用或破壞更新程序	12.1	無線軟體更新程序受到破解 包括製作系統更新程式或韌體
			12.2	區域/物理軟體更新程式受到破解 包括製作系統更新程式或韌體
			12.3	雖更新程序完整，惟軟體在更新過程之前被操縱（因此已屬遭受破壞）
			12.4	允許無效更新之軟體提供商的密碼鍵受到破解
	13	可以拒絕合法更新	13.1	針對更新伺服器或網路的拒絕服務攻擊，以防止推出關鍵軟體更新和/或解鎖客戶特定功能
4.3.4 因人為意外行為促成網路攻擊而對車輛造成的威脅	15	合法行為者能夠採取行動，在不知不覺中促進網路攻擊	15.1	無辜受害者（例如所有者、操作員或維護工程師）被誘騙採取措施無意中載入惡意軟體或啟用攻擊
			15.2	未遵循定義的安全程序
4.3.5 對車輛	16	操縱車輛功能的連接性使網路攻	16.1	對設計用於遠程操作系統的功能進行操縱，例如遙控鑰匙、防盜器和充電樁

漏洞/威脅的高等級和次等級描述			漏洞或攻擊方法範例	
外部連接和連接的威脅		擊變為可行，可能包括遠程資訊服務；允許遠程操作的系統；和使用短距離無線通訊的系統	16.2	操縱車輛遠程資訊服務（例如操縱敏感貨物的溫度測量，遠程解鎖貨門）
			16.3	干擾短距離無線系統或感測器
	17	託管的第三方軟體，例如娛樂應用程式，用作攻擊車輛系統的手段	17.1	軟體安全性較差或損壞的應用程式，作為攻擊車輛系統的方法
	18	連接到外部連接埠的設備，例如USB 端口、OBD 端口，用作攻擊車輛系統的手段	18.1	如作為攻擊點的 USB 或其他連接埠之外部連接埠，例如通過程式碼注入
			18.2	感染病毒的媒體連接到車輛系統
			18.3	用於促成攻擊之診斷存取（例如 OBD 連接埠中的伺服器鑰(dongles)），例如操縱車輛參數（直接或間接）
4.3.6 對車輛資料/代碼的威脅	19	擷取車輛資料/代碼	19.1	從車輛系統中擷取版權或專有軟體（產品盜版）
			19.2	未經授權存取車主的個人身份、支付帳戶資訊、通訊錄資訊、位置資訊、車輛電子身份證等隱私資訊
			19.3	擷取密碼鍵
	20	操縱車輛資料/代碼	20.1	非法/未經授權更改車輛電子 ID
			20.2	身份欺詐 例如，若使用者在與收費系統或申請者之後端伺服器通訊時想顯示另一個身份
			20.3	規避監控系統的行動（例如駭入/篡改/阻擋資訊，例如 ODR 追蹤器資料或運作次數）
			20.4	篡改車輛行駛資料（如里程、行駛速度、行駛方向等）的資料篡改
			20.5	未經授權更改系統診斷資料
	21	刪除資料/代碼	21.1	未經授權刪除/操縱系統事件日誌
	22	惡意軟體介紹	22.2	引入惡意軟體或惡意軟體活動

漏洞/威脅的高等級和次等級描述			漏洞或攻擊方法範例	
	23	引入新軟體或覆蓋現有軟體	23.1	偽造車輛控制系統或資訊系統之軟體
	24	系統或操作中斷	24.1	拒絕服務 例如這可能會在內部網路上通過淹沒CAN 匯流排(by flooding a CAN bus)觸發，或通過高頻率資訊傳遞在 ECU 上引發故障
	25	操縱車輛參數	25.1	非法存取、篡改車輛關鍵功能的配置參數，如煞車資料、安全氣囊展開門檻值等
			25.2	未經授權之偽造充電參數存取，如充電電壓、充電功率、電池溫度等
4.3.7 如果沒有得到充分保護或加固，可能會被利用的潛在漏洞	26	加密技術可能受到損害或應用不足	26.1	短加密密碼鍵和長有效期的結合使攻擊者能夠破解加密
			26.2	未充分使用加密演算法來保護敏感系統
			26.3	使用已經或即將被棄用的加密演算法
	27	零件或供應品可能會受到破壞，從而使車輛受到攻擊	27.1	透過用於實現攻擊或未能滿足阻止攻擊的設計標準之硬體或軟體
	28	軟體或硬體開發允許存在漏洞	28.1	軟體錯誤 軟體錯誤的存在可能是潛在可利用漏洞的基礎 如果軟體尚未經過測試以驗證不存在已知的錯誤代碼/錯誤並降低存在未知錯誤代碼/錯誤的風險，則尤其如此
			28.2	使用源自於開發之餘項（例如除錯連接埠、JTAG 連接埠、微處理器、開發認證、開發人員密碼等）以允許存取 ECU 或允許攻擊者獲得更高的權限
	29	網路設計引入漏洞	29.1	多餘的網路連接埠保持開啟狀態，並提供對網路系統的存取
			29.2	規避網路分離以獲得控制權 具體範例為使用未受保護的通訊匝道或接入點（例如卡車與拖車之通訊匝道）來繞過保護並獲得對其他網路分段的存取權限以執行惡意行為，例如發送任意 CAN匯流排資訊

漏洞/威脅的高等級和次等級描述			漏洞或攻擊方法範例	
	31	可能會發生意外的資料傳輸	31.1	資訊洩露 當汽車更換使用者時，個人資料可能會洩露（例如被出售或新租用者用作租用車輛）
	32	系統的物理操作可以實現攻擊	32.1	電子硬體操作，例如在車輛中增加未經授權的電子硬體以啟用“中間人”攻擊 更換授權的電子硬體（例如感測器）帶有未經授權的電子硬體 操縱由感測器收集的資訊（例如使用磁鐵篡改連接到齒輪箱的霍爾感測器(Hall effect sensor)）

6.6 B部分：緩解對車輛的威脅

6.6.1「車輛通訊頻道」相關的威脅緩解措施，如表二。

表二：「車輛通訊頻道」相關的威脅緩解措施

參考表一	對“車輛通訊頻道”的威脅	參考	緩解
4.1	通過冒充來欺騙資訊（例如，列隊期間的802.11p V2X、GNSS資訊等）	M10	車輛應驗證其收到的資訊的真實性和完整性
4.2	女巫(Sybil)攻擊（為了欺騙其他車輛，如道路中有很多車輛一般）	M11	應實施安全控制以儲存加密密碼鍵（例如使用硬體安全模塊）
5.1	通訊頻道允許注入程式碼到車輛持有的資料/代碼中，例如篡改的軟體二進制文件可能被注入到通訊流中	M10 M6	車輛應驗證其收到的資訊的真實性和完整性 系統應通過設計實現安全性以最小化風險
5.2	通訊頻道允許操縱車輛持有的資料/代碼	M7	應採用存取控制技術和設計來保護系統資料/代碼
5.3	通訊頻道允許覆蓋車輛持有的資料/代碼		
5.4 21.1	通訊頻道允許刪除車輛持有的資料/代碼		
5.5	通訊頻道允許將資料/代碼引入車輛系統(寫入資料代碼)		
6.1	從不可靠或不受信任的來源接受資訊	M10	車輛應驗證其收到的資訊的真實性和完整性
6.2	中間人攻擊/會話劫持	M10	

參考表一	對“車輛通訊頻道”的威脅	參考	緩解
6.3	重播攻擊，例如對通訊匝道的攻擊允許攻擊者降級 ECU 的軟體或匝道的韌體		車輛應驗證其收到的資訊的真實性和完整性
7.1	資訊攔截/干擾輻射/監控通訊	M12	傳輸到車輛或從車輛傳出的機密資料應受到保護
7.2	未經授權存取文件或資料	M8	通過系統設計和存取控制，未經授權的人員應該不可能存取個人或系統關鍵資料 安全控制範例可以在OWASP中找到
8.1	向車輛資訊系統發送大量垃圾資料，使其無法正常提供服務	M13	應採用檢測和從拒絕服務攻擊中恢復的措施
8.2	黑洞攻擊，通過阻止向其他車輛傳輸資訊來中斷車輛之間的通訊	M13	應採用檢測和從拒絕服務攻擊中恢復的措施
9.1	非特權使用者能夠獲得特權存取，例如 root 存取	M9	應採取措施防止和檢測未經授權的存取
10.1	嵌入通訊媒體的病毒感染車輛系統	M14	應考慮保護系統免受嵌入式病毒/惡意軟體侵害的措施
11.1	惡意內部（例如 CAN）資訊	M15	應考慮檢測惡意內部資訊或活動的措施
11.2	惡意 V2X 資訊，例如基礎設施到車輛或車輛-車輛資訊（例如 CAM、DENM）	M10	車輛應驗證其收到的資訊的真實性和完整性
11.3	惡意診斷資訊		
11.4	惡意專有資訊（例如通常從 OEM 或零組件/系統/功能供應商發送的資訊）		

6.6.2「更新過程」相關的威脅緩解措施，如表三。

表三：「更新過程」相關的威脅緩解措施

參考表一	對“更新過程”的威脅	參考	緩解
12.1	無線軟體更新程序受到破壞 這包括製作系統更新程式或韌體	M16	應採用安全的軟體更新程序

參考表一	對“更新過程”的威脅	參考	緩解
12.2	區域/物理軟體更新程序受到破壞 這包括製作系統更新程序或韌體		
12.3	雖更新過程完整，惟軟體在更新過程之前被操縱（因此屬遭受破壞）		
12.4	允許無效更新的軟體提供商的密碼鍵受到破壞	M11	應實施安全控制以儲存加密密碼鍵
13.1	針對更新伺服器或網路的拒絕服務攻擊，以防止推出關鍵軟體更新和/或解鎖客戶特定功能	M3	應於後端系統採用安全控制 在後端伺服器對提供服務至關重要的地方，有系統中斷時的恢復措施 可以在OWASP中找到安全控制範例

6.6.3「促進網路攻擊的非故意人為行為」相關威脅的緩解措施，如表四。

表四：「促進網路攻擊的非故意人為行為」相關威脅的緩解措施

參考表一	與“意外的人類行為”相關的威脅	參考	緩解
15.1	無辜的受害者（例如所有者、操作員或維護工程師）被誘騙採取措施無意中載入惡意軟體或發動攻擊	M18	應根據最小存取權限原則，實施定義和控制使用者角色和存取權限的措施
15.2	未遵循定義的安全程序	M19	組織應確保定義並遵循安全程序，包括與安全功能管理相關的操作和存取的日誌記錄

6.6.4「外部連接性和連接」相關威脅的緩解措施，如表五。

表五：「外部連接性和連接」相關威脅的緩解措施

參考表一	對“外部連接和連接”的威脅	參考	緩解
16.1	對設計用於遠程操作車輛系統的功能進行操縱，例如遙控鑰匙、防盜器和充電樁	M20	應於具備遠程存取權限的系統採用安全控制
16.2	操縱車輛遠程資訊服務（例如操縱敏感貨物的溫度測量，遠程解鎖貨門）		
16.3	干擾短距離無線系統或感測器		

參考表一	對“外部連接和連接”的威脅	參考	緩解
17.1	損壞的應用程序，或那些軟體安全性較差的，用作攻擊車輛系統的方法	M21	軟體應經過安全評估、認證和完整性保護 應採用安全控制措施，以最大限度地降低旨在或可預見的車輛上託管的第三方軟體的風險
18.1	作為攻擊點的 USB 或其他連接埠之外部連接埠，例如通過注入程式碼	M22	安全控制應採用於外部連接埠
18.2	感染病毒的媒體連接到車輛		
18.3	用於促進攻擊的診斷存取（例如 OBD 連接埠中的伺服器鑰(dongles)），例如操縱車輛參數（直接或間接）	M22	安全控制應採用於外部連接埠

6.6.5「攻擊潛在目標或動機」之相關的威脅緩解措施，如表六。

表六：「攻擊潛在目標或動機」之相關的威脅緩解措施

參考表一	對“攻擊的潛在目標或動機”的威脅	參考	緩解
19.1	從車輛系統中擷取版權或專有軟體（產品盜版/遭竊軟體）	M7	應採用存取控制技術和設計來保護系統資料/代碼 可以在OWASP中找到安全控制範例
19.2	未經授權存取車主的個人身份、支付帳戶資訊、通訊錄資訊、位置資訊、車輛電子身份證等隱私資訊	M8	通過系統設計和存取控制，未經授權的人員不應存取個人或系統關鍵資料 可以在OWASP中找到安全控制範例
19.3	擷取密碼鍵	M11	應實施安全控制以儲存加密密碼鍵，例如安全模塊
20.1	非法/未經授權更改車輛電子 ID	M7	應採用存取控制技術和設計來保護系統資料/代碼 可以在OWASP中找到安全控制範例
20.2	身份欺詐 例如，如果使用者在與收費系統通訊時想顯示另一個身份，製造商後端		

參考表一	對“攻擊的潛在目標或動機”的威脅	參考	緩解
20.3	規避監控系統的行動（例如黑客/篡改/阻止資訊，例如 ODR 跟踪器資料或運作次數）	M7	應採用存取控制技術和設計來保護系統資料/代碼 可以在OWASP中找到安全控制範例 通過關聯來自不同資訊源的資料，可以緩解對感測器或傳輸資料的資料操縱攻擊
20.4	篡改車輛行駛資料（如里程、行駛速度、行駛方向等）的資料篡改		
20.5	未經授權更改系統診斷資料		
21.1	未經授權刪除/操縱系統事件日誌	M7	應採用存取控制技術和設計來保護系統資料/代碼 可以在OWASP中找到安全控制範例
22.2	引入惡意軟體或惡意軟體活動	M7	應採用存取控制技術和設計來保護系統資料/代碼 可以在OWASP中找到安全控制範例
23.1	偽造車輛控制系統或資訊系統軟體		
24.1	拒絕服務，例如，這可能會在內部網路上通過淹沒CAN匯流排觸發，或通過高頻率資訊傳遞在 ECU 上引發故障	M13	應採用檢測和從拒絕服務攻擊中恢復的措施
25.1	未經授權篡改車輛關鍵功能的配置參數，如煞車資料、安全氣囊展開門檻值等	M7	應採用存取控制技術和設計來保護系統資料/代碼 可以在OWASP中找到安全控制範例
25.2	未經授權篡改充電參數，如充電電壓、充電功率、電池溫度等		

6.6.6 「可被利用的未充分保護或強化的潛在漏洞」相關威脅的緩解措施，如表七。

表七：「可被利用的未充分保護或強化的潛在漏洞」相關威脅的緩解措施

參考表一	對“如果沒有得到充分保護或加固就可能被利用的潛在漏洞”的威脅	參考	緩解
26.1	短加密密碼鍵和長有效期的結合使攻擊者能夠破解加密	M23	應遵循軟體和硬體開發的網路安全最佳實踐
26.2	未充分使用加密演算法來保護敏感系統		
26.3	使用不推薦使用的加密演算法		
27.1	硬體或軟體，旨在實現攻擊 或未能滿足阻止攻擊的設計標準	M23	應遵循軟體和硬體開發的網路安全最佳實踐
28.1	軟體錯誤的存在可能是潛在可利用漏洞的基礎 如果軟體尚未經過測試以驗證不存在已知的錯誤代碼/錯誤並降低存在未知錯誤代碼/錯誤的風險，則尤其如此	M23	應遵循軟體和硬體開發的網路安全最佳實踐 具有足夠覆蓋範圍的網路安全測試
28.2	使用源自於開發之餘項（例如除錯連接埠、JTAG 連接埠、微處理器、開發認證、開發人員密碼等）以允許攻擊者存取 ECU 或獲得更高的權限		
29.1	多餘的網路連接埠保持開啟狀態，提供對網路系統的存取		
29.2	規避網路分離以獲得控制權 具體範例是使用未受保護的通訊匝道或接入點（例如卡車與拖車之通訊匝道）來繞過保護並獲得對其他網路分段的存取權限以執行惡意行為，例如發送任意 CAN 匯流排資訊	M23	應遵循軟體和硬體開發的網路安全最佳實踐 應遵循系統設計和系統集成的網路安全最佳實踐

6.6.7「車輛資料遺失/資料洩露」相關威脅的緩解措施，如表八。

表八：「車輛資料遺失/資料洩露」相關威脅的緩解措施

參考表一	“車輛資料遺失/資料洩露”的威脅	參考	緩解
31.1	資訊洩露 當汽車更換使用者時，個人資料可能會被洩露(例如被出售或新租用者用作租用車輛)	M24	應遵循保護資料完整性和機密性的最佳做法來儲存個人資料

6.6.8「對系統進行物理操作以進行攻擊」相關威脅的緩解措施，如表九。

表九：「對系統進行物理操作以進行攻擊」相關的威脅的緩解措施

參考表一	“對系統進行物理操作以進行攻擊”的威脅	參考	緩解
32.1	操縱OEM硬體，例如將未經授權的硬體添加到車輛以實現“中間人”攻擊	M9	應採取措施防止和檢測未經授權的存取

6.7 C部分：緩解車輛外部威脅

6.7.1「後端伺服器」相關威脅的緩解措施，如表十。

表十：「後端伺服器」相關威脅的緩解措施

參考表一	對“後端伺服器”的威脅	參考	緩解
1.1 & 3.1	員工濫用特權（內部攻擊）	M1	安全控制應用於後端系統，以盡量減少內部攻擊的風險
1.2 & 3.3	未經授權的聯網存取 到伺服器（例如透過後門、未修補的系統軟體漏洞、SQL 攻擊或其他方式啟用）	M2	安全控制應用於後端系統，以最大限度地減少未經授權的存取 可以在OWASP中找到安全控制範例
1.3 & 3.4	未經授權的物理存取 到伺服器（例如通過 USB 記憶棒或其他連接到伺服器的媒體進行）	M8	通過系統設計和存取控制，未經授權的人員應該不可能存取個人或系統關鍵資料
2.1	對後端伺服器的攻擊使其停止運作，例如它阻止它與車輛交互並提供它們所依賴的服務	M3	安全控制應用於後端系統 在後端伺服器對提供服務至關重要的地方，有系統中斷時的恢復措施 可以在OWASP中找到安全控制範例

參考表一	對“後端伺服器”的威脅	參考	緩解
3.2	雲端中資訊遺失. 資料由第三方雲端服務提供商儲存時，敏感資料可能因攻擊或事故而遺失	M4	應用安全控制來最小化與雲端計算相關的風險 可以在OWASP和NCSC雲端計算指南中找到安全控制範例
3.5	資訊外洩 透過意外共享資料（例如管理錯誤，將資料儲存在車庫的伺服器中）	M5	安全控制應用於後端系統以防止資料洩露 可以在OWASP中找到安全控制範例

6.7.2 對「非預期的人為行為」相關威脅的緩解措施，如表十一。

表十一：對「非預期的人為行為」相關威脅的緩解措施

參考表一	與“意外的人類行為”相關的威脅	參考	緩解
15.1	無辜的受害者（例如所有者、操作員或維護工程師）被誘騙採取措施無意中載入惡意軟體或發動攻擊	M18	應根據最小存取權限原則，實施定義和控制使用者角色和存取權限的措施
15.2	未遵循定義的安全程序	M19	組織應確保定義並遵循安全程序，包括與安全功能管理相關的操作和存取的日誌記錄

6.7.3「物理資料遺失」相關威脅的緩解措施，如表十二。

表十二：「物理資料遺失」相關威脅的緩解措施

參考表一	“資料物理遺失”的威脅	參考	緩解
30.1	損害由第三方造成 在交通事故或盜竊的情況下，敏感資料可能會因物理損壞而遺失或受損	M24	應遵循保護資料完整性和機密性的最佳做法來儲存個人資料 可以在ISO/SC27/WG5中找到安全控制範例
30.2	DRM（數位版權管理）衝突造成的損失 由於DRM問題，使用者資料可能會被刪除		

參考表一	“資料物理遺失”的威脅	參考	緩解
30.3	由於 IT 零組件磨損，敏感資料（完整性）可能會遺失，從而導致潛在的級聯問題（例如，在密碼鍵更改的情況下）		