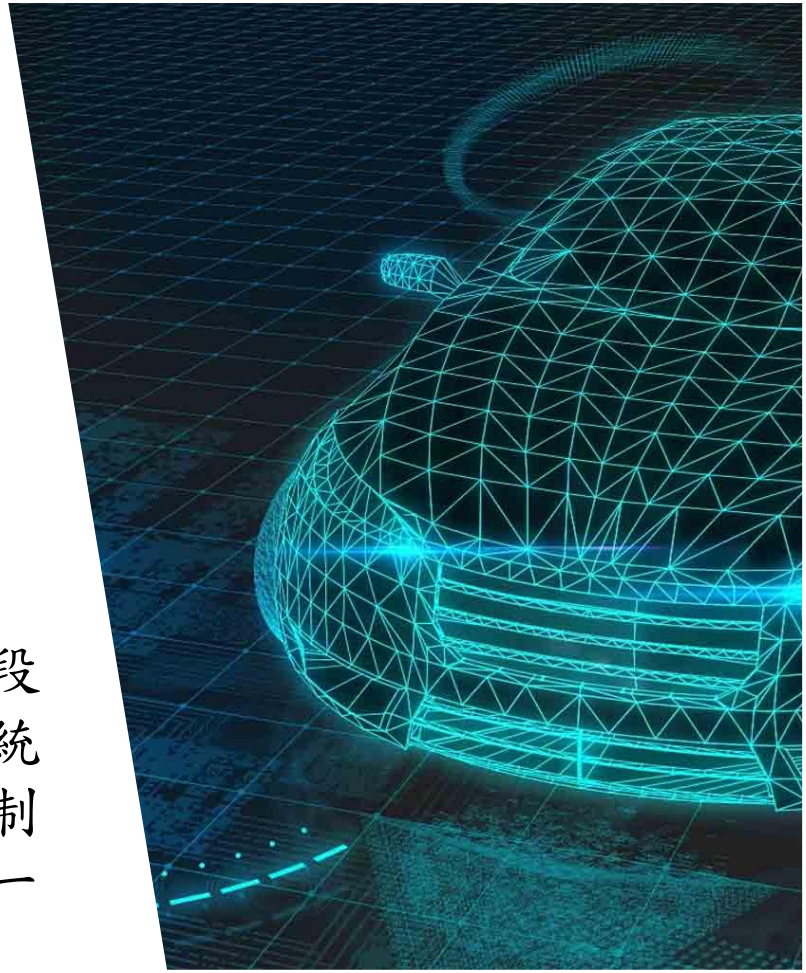
財團法人車輛安全審驗中心
Vehicle Safety Certification Center

檢測基準九十六-網路安全及網路安全管理系統法規概要說明

檢測基準九十六-網路安全及網路安全管理系統

- 因應車輛智慧化發展趨勢，UNECE自2016年起展開相關法規研議作業，並於2021年正式發布UN R155法規。
- 交通部調和導入UN R155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」，作為我國車輛型式安全審驗之管理依據。
- 本項法規要求車廠自車輛的設計階段開始至報廢回收為止，透過管理系統建立網路安全層面之對應設計或機制，以確保車輛於整個生命週期具備一定之網路安全性



檢測基準九十六-法規章節概要說明

1.實施時間及適用範圍	新型式自117年1月1日起、各型式自119年1月1日起實施，適用於M、N及具備至少一個電子控制單元的O類車輛
2.名詞釋義	介紹相關名詞定義
3.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及外部介面基本要素相同
4.網路安全管理系統符合性證明文件	介紹網路安全管理系統符合性證明文件申請並說明相關規定
5.規格 (5.1 一般規格) (5.2 網路安全管理系統要求) (5.3 對車輛型式的要求) (5.4 報告規定)	說明網路安全管理系統的規格與要求，其核心目的在於確保車輛在生命週期內皆具備防護網路攻擊的能力，並具備持續監控網路安全管理系統有效性機制
6.威脅列表及相應緩解措施	介紹威脅列表及相應緩解措施並說明相關規定

檢測基準九十六-名詞釋義

網路安全(Cyber security)	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
網路安全管理系統 (Cyber Security Management System，CSMS)	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
緩解(Mitigation)	降低風險之措施 範例說明：車輛應驗證其收到的資訊的真實性和完整性
風險(Risk)	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 範例說明：通訊頻道允許接受不可信/不可靠的資訊
威脅(Threat)	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 範例說明：感染病毒的USB連接到車輛
漏洞(Vulnerability)	指資產或緩解措施的弱點，可以被一個或多個威脅利用 範例說明：員工濫用特權（內部攻擊）

檢測基準九十六-CSMS及VTA

➢ 核心架構包含**網路安全管理系統要求(CSMS)**及**車輛型式要求(VTA)**：

網路安全管理系統(CSMS)之要求

4.CSMS符合性證明文件

- 描述網路安全管理系統之文件
- 宣告聲明書
- CSMS符合性證明文件最長有效期為三年
- 若CSMS符合性證明文件有任何變化，申請者應向審驗/檢測機構確認是否有必要重新進行檢查

5.2網路安全管理系統要求

- 涵蓋車輛全生命週期
- 使用的流程可確保充分考慮安全性((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

5.4報告規定

- 至少每年一次向審驗機構回報監測活動的結果，應向審驗/檢測機構報告並確認其實施緩解措施仍然有效
- 審驗機構核實相關資訊，或糾正申請者無效資訊
- 如報告或回覆內容不充分。審驗機構得依規定撤銷CSMS符合性證明文件

車輛型式(VTA)之要求

5.3對車輛型式的要求

- 具備有效之CSMS符合性證明文件
- 對認可車輛型式，識別和管理與供應商相關風險
- 對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
- 應實施適當的緩解措施以保護車輛型式
- 採取適當且相稱的措施，以確保用於售後市場軟體、服務、應用程式或資料儲存和執行。
- 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
- 密碼模組應符合共識標準

6.威脅列表及相應緩解措施

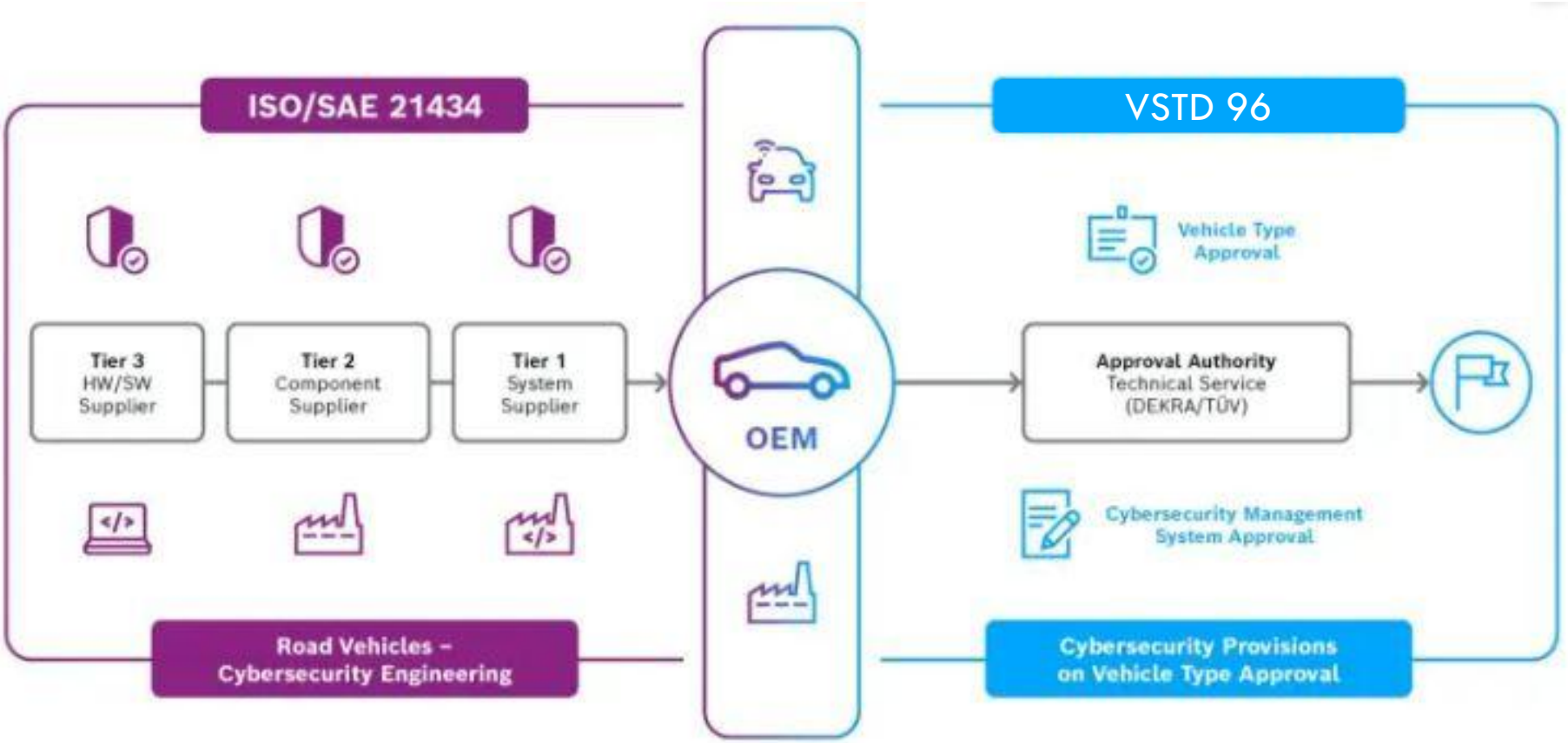
- 威脅、漏洞和攻擊方法、對威脅的緩解措施及車輛區域外部對威脅的緩解措施，應考慮風險評估和緩解措施
- 高等級漏洞及其相應範例指標...，應連接相應的緩解措施
- 威脅分析應考慮可能的攻擊影響

註1：ISO/SAE 21434為參考標準

註2：詳細內容請參閱車輛安全檢測基準相關條文

補充說明-ISO/SAE 21434概要(1/3)

- ISO/SAE 21434與車輛安全檢測基準兩者間之關係



補充說明-ISO/SAE 21434概要(2/3)

7.2

7.2.2. The Cyber Security Management System shall cover the following aspects:

7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases:

(a) Development phase;

(b) Production phase;

(c) Post-production phase.

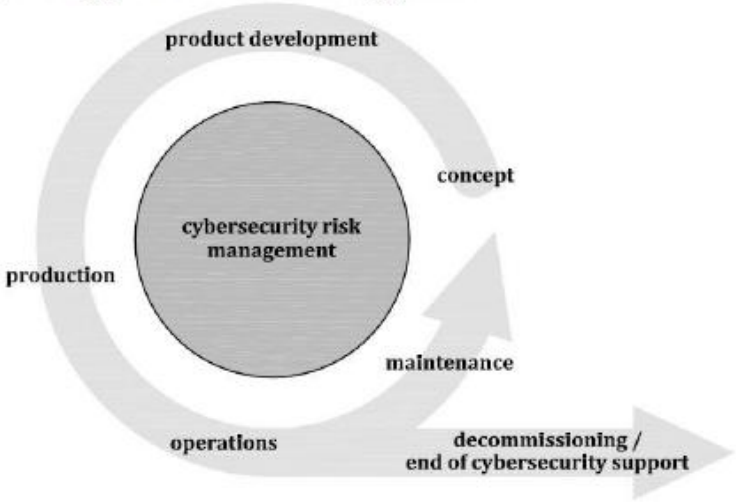


Figure 2 — Overall cybersecurity risk management

摘錄 ISO/SAE 21434

檢測基準九十六-章節5.2.2

- 基於**風險之系統化管理**
- **全生命週期**考量
- 供應鏈管理
- 測試與驗證、**持續監控**
- 事故響應與數據取證

補充說明-ISO/SAE 21434概要(3/3)

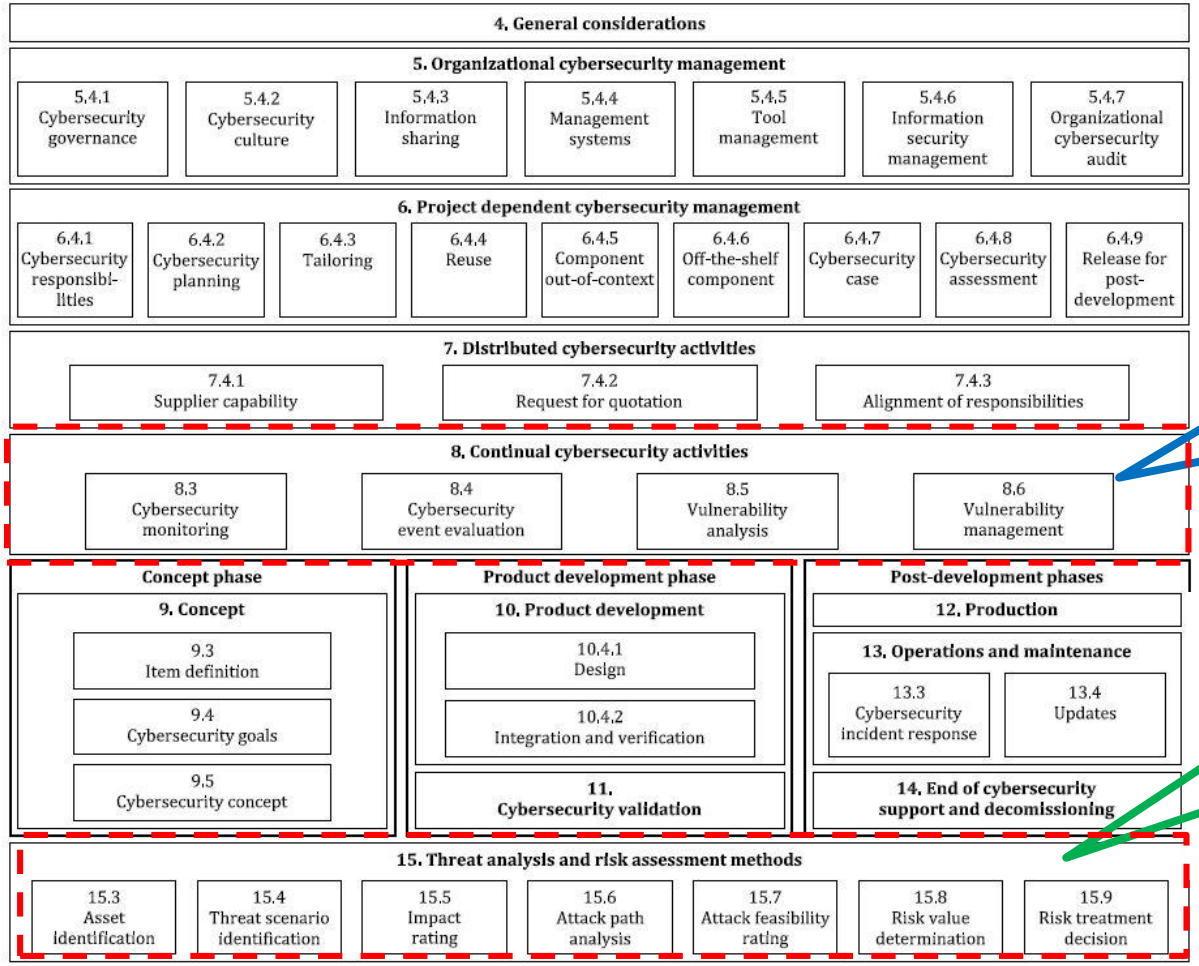


Figure 1 — Overview of this document

VSTD 96 ⇔ ISO/SAE 21434
範例說明：

檢測基準96條文5.2.2.2 (g)、5.2.2.4，可參考第8章 Cotinual cybersecurity activities (持續的網路安全活動)

檢測基準96條文5.2.2.2 (b)可參考第15章 Threat analysis and risk assessment methods(威脅分析和風險評估方法)

檢測基準九十六-相關辦理流程

申請者

備妥相關文件後向檢測機構提出申請

檢測機構

- 評估申請者是否應建立CSMS管理系統
- 進行申請者CSMS管理系統驗證評估
- 出具CSMS評估報告予申請者

申請者

- 檢視是否須辦理資格變更登錄(申請者資格、製造廠)
- 檢視COP管制計畫書並研提變更增加項目
- 檢附CSMS評估報告申請符合性證明文件

審驗機構

- 審核申請者登錄資料
- 查核申請者製造廠管制計劃書內容(新增檢測基準96)
- 核發CSMS符合性證明文件予申請者

申請者

提供CSMS符合性證明文件予檢測機構，及

檢測機構

- 與申請者討論挑選最嚴苛代表件進行VTA車型檢測
- 出具檢測報告(登載CSMS編號)予申請者

申請者

備妥相關文件，提出審查報告申請

審驗機構

- 核對COP管制計畫書、CSMS符合性證明文件、VTA檢測報告及相關技術文件
- 核發檢測基準96審查報告予申請者

年度報告

應至少每年一次向審驗機構及檢測機構報告其監測活動的結果

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

檢測基準九十七-軟體更新及軟體更新管理系統法規概要說明

檢測基準九十七-軟體更新及軟體更新管理系統

- 因應車輛智慧化發展趨勢，UNECE自2016年起展開相關法規研議作業，並於2021年正式發布UN R156法規。
- 交通部調和導入UN R156訂有車輛安全檢測基準「九十七、軟體更新及軟體更新管理系統」，作為我國車輛型式安全審驗之管理依據。
- 本項法規要求車廠自車輛的設計階段開始至報廢回收為止，透過管理系統建立網路安全層面之對應設計或機制，以確保車輛於軟體更新時具備一定程序，且於更新過程中不會影響車輛安全性

檢測基準九十七-法規章節概要說明

1.實施時間及適用範圍	新型式自117年1月1日起、各型式自119年1月1日起實施，適用於M、N及O類車輛允許執行軟體更新者
2.名詞釋義	介紹相關名詞定義
3.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	介紹軟體更新管理系統符合性證明文件申請並說明相關規定
5.通則 (5.1 軟體更新管理系統要求) (5.2 對車輛型式的要求)	說明軟體更新管理系統以及對車輛型式的要求，其核心目的在於確保車輛在生命週期內其軟體更新過程的安全性、可追溯性與可靠性

檢測基準九十七-名詞釋義

軟體更新(Software update)	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。
軟體更新管理系統(Software Update Management System，SUMS)	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。
安全狀態(Safe state)	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。
軟體(Software)	指電子控制系統中由數位數據和指令組成之一部分。
空中(無線)更新(Over-the-Air (OTA) update)	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。
系統(System)	指實現一種功能的零組件及/或子系統之集合。

檢測基準九十七-SUMS及VTA

➢ 核心架構包含**軟體更新管理系統要求(SUMS)**及**車輛型式要求(VTA)**：

軟體更新管理系統(SUMS)之要求

4.SUMS符合性證明文件

- ◆ 描述軟體更新管理系統之文件
- ◆ 宣告聲明書
- ◆ SUMS符合性證明文件最長有效期為三年
- ◆ 若SUMS符合性證明文件有任何變化，申請者應向審驗/檢測機構確認是否有必要重新進行檢查

5.1軟體更新管理系統要求

- ◆ 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。
- ◆ 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
- ◆ 申請者能夠識別目標車輛進行軟體更新的程序
- ◆ 應記錄並儲存適用於提供車型每次更新的資訊
- ◆ 確保軟體更新受到保護之安全性
- ◆ 評估若在駕駛過程中進行無線(空中)更新，不會影響安全。

車輛型式(VTA)之要求

5.2對車輛型式的要求

- ◆ 具備有效之SUMS符合性證明文件
- ◆ 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。
- ◆ 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，並通過標準介面方式讀取(OBD埠)。
- ◆ 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。
- ◆ 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。
- ◆ 軟體無線(空中)更新，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。
- ◆ 車輛應確保在執行軟體更新前必須滿足所需的先決條件。

註1：ISO 24089為參考標準

註2：詳細內容請參閱車輛安全檢測基準相關條文

補充說明-ISO 24089概要

- 檢測基準97主要架構與ISO 24089總體核心架構相近，且ISO 24089部分章節與ISO/SAE 21434相關。

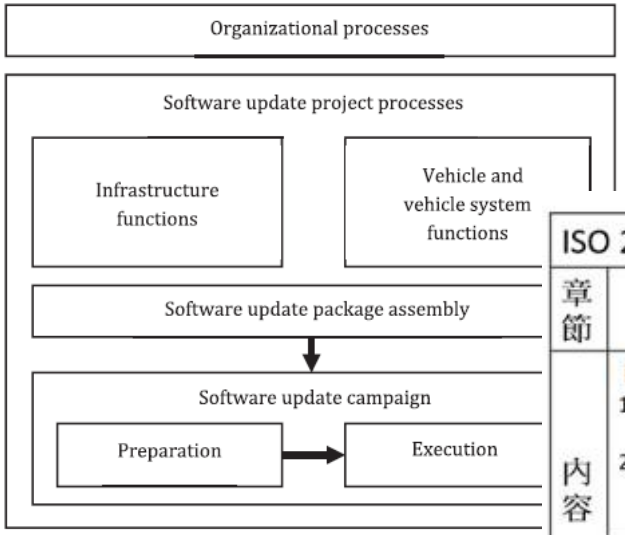


Figure 1 — Overview of this document

ISO 24089：Road vehicles — Software update engineering

章節	組織	專案	基礎設施	車輛與車輛系統
內容	軟體開發流程管理 1.需求管理、維運、品質管理...等流程 2.開發過程相關文件管理	專案管理要求 1.確認專案中各工作角色之分工 2.基礎設施和車輛系統需要完整的整合測試	SUMS的資安功能要求 1.管理基礎設施中軟體更新時所面臨的潛在網路安全風險 2.管理車輛當前配置資訊 3.向車輛使用者告知軟體升級 4.軟體升級結果管理 5.軟體升級失敗管理 6.確認軟體升級包之正確性與合法性	終端(軟體更新標的)資安功能要求 1.管理車輛、ECU、網路安全風險 2.管理車輛配置訊息 3.管理關於車輛軟體更新訊息 4.啟用軟體更新作業並驗證軟體更新包 5.管理軟體更新失敗的情況 6.確認有足夠的車內資源來應用軟體升級包
	參照 ISO 21434 的內容			

共通項目，適用於生態鍊中所有廠商

各廠商可依認證產品特性定義認證範圍

檢測基準九十七-相關辦理流程

申請者

備妥相關文件後向檢測機構提出申請

檢測機構

- 評估申請者是否應建立SUMS管理系統
- 進行申請者SUMS管理系統驗證評估
- 出具SUMS評估報告予申請者

申請者

- 檢視是否須辦理資格變更登錄(申請者資格、製造廠)
- 檢視COP管制計畫書並研提變更增加項目
- 檢附SUMS評估報告申請符合性證明文件

審驗機構

- 審核申請者登錄資料
- 查核申請者製造廠管制計劃書內容(新增檢測基準97)
- 核發SUMS符合性證明文件予申請者

審驗機構

- 核對COP管制計畫書、SUMS符合性證明文件、VTA檢測報告及相關技術文件
- 核發檢測基準97審查報告予申請者

申請者

備妥相關文件，提出審查報告申請

檢測機構

- 與申請者討論挑選最嚴苛代表件進行VTA車型檢測
- 出具檢測報告(登載SUMS編號)予申請者

申請者

提供SUMS符合性證明文件予檢測機構

報告完畢