道路車輛網路安全工程產業指引
第 3 部：威脅分析及風險評鑑

Industrial guideline for road vehicles cybersecurity engineering
Part 3: threat analysis and risk assessment

(TTVMA IG-003:2026)

台灣區車輛工業同業公會

2026 年 9 月 制定公告

目錄

前言

車輛工業同業公會為協助車輛產業及早因應國際網路安全要求及強化資訊安全能力，結合工研院機械所，邀集產官學研專家組成技術暨審查委員會，經由經濟部標準檢驗局指導，訂定本產業指引並公告之。

本指引參照 CNS 21434 訂定之第 15 節，內容為針對產品之網路安全威脅分析及風險評鑑，提供實踐指引，供國內車輛產業廠商參考使用，協助業者加速建構相關能量。

1. 適用範圍

本指引之適用範圍等同於 CNS 21434 的適用範圍，惟本指引僅針對 CNS 21434 第 15 節之相關要求、建議及許可事項，提供實踐指引。

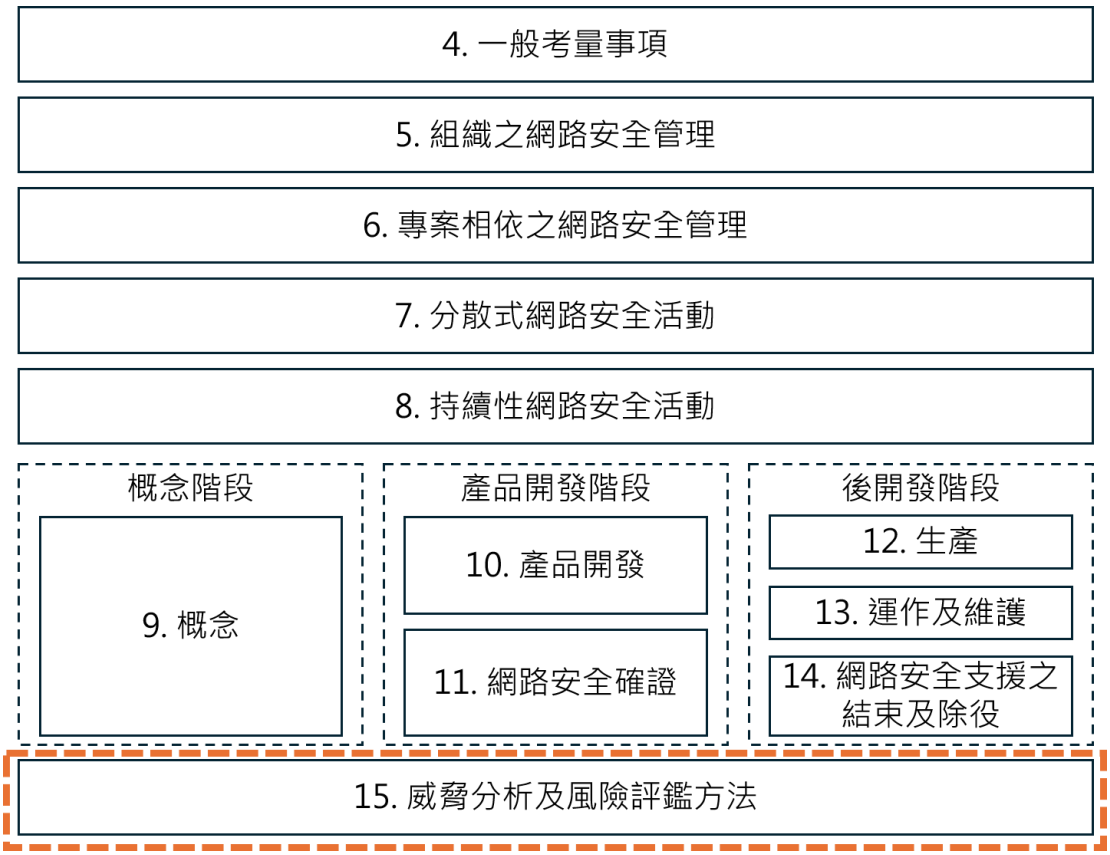

圖 1　CNS 21434 架構概觀

2. 引用標準

本指引所引用之標準如下所列：

ISO/SAE 21434:2021 Road vehicles - Cybersecurity engineering

CNS 21434:2025 道路車輛 - 網路安全工程

3. 用語、定義及縮寫

3.1 用語及定義

下列用語及定義適用於本指引，其主要參照 CNS 21434 及車輛產業習慣。

3.1.1 架構設計(architectural design)

允許識別組件(3.1.7)、其邊界、介面及互動之表示。

3.1.2 資產(asset)

具有價值或貢獻價值之物件。

備考：資產具有 1 或多個網路安全性質(3.1.20)，若其遭破解可能會導致 1 或多種損害情境(3.1.22)。

3.1.3 攻擊可行性(attack feasibility)

攻擊路徑(3.1.4)屬性，描述成功履行相應行動集之難易程度。

3.1.4 攻擊路徑(attack path)

攻擊。

為實現威脅情境(3.1.33)而履行之一系列蓄意行動。

3.1.5 攻擊者(attacker)

履行攻擊路徑(3.1.4)的個人、團體或組織。

3.1.6 稽核(audit)

過程之檢查以判定過程目標實現之程度。

3.1.7 組件(component)

邏輯及技術上可分離之部件。

3.1.8 顧客(customer)

接受服務或產品之個人或組織。

3.1.9 網路安全(cybersecurity)

道路車輛網路安全。

資產(3.1.2)得到充分保護，避免遭受道路車輛、其功能及其電機或電子組件(3.1.7)之項目(3.1.25)的威脅情境(3.1.33)。

備考：在本指引中，為求簡潔，使用〝網路安全〞用語，而非〝道路車輛網路安全〞。

3.1.10 網路安全評鑑(cybersecurity assessment)

網路安全(3.1.9)之判斷。

3.1.11 網路安全案例(cybersecurity case)

具有證據支援之結構化論點，以示風險(3.1.29)的存在並非不合理。

3.1.12 網路安全聲明(cybersecurity claim)

風險(3.1.29)之相關聲明。

備考：網路安全聲明可包含保留或分擔風險之調整。

3.1.13 網路安全概念(cybersecurity concept)

項目(3.1.25)之網路安全要求事項、運作環境(3.1.26)要求事項，以及網路安全控制措施(3.1.14)的相關資訊。

3.1.14 網路安全控制(cybersecurity control)

修正風險(3.1.29)之措施。

3.1.15 網路安全事件(cybersecurity event)

項目(3.1.25)或組件(3.1.7)相關之網路安全資訊(3.1.18)。

3.1.16 網路安全目標(cybersecurity goal)

與 1 或多種威脅情境(3.1.33)相關之概念級網路安全要求事項。

3.1.17 網路安全事故(cybersecurity incident)

可能涉及利用脆弱性(3.1.38)之現場情況。

3.1.18 網路安全資訊(cybersecurity information)

尚未判定相關性之網路安全(3.1.9)資訊。

3.1.19 網路安全介面協議(cybersecurity interface agreement)

顧客(3.1.8)與供應者間關於分散式網路安全活動(3.1.23)之協議。

3.1.20 網路安全性質(cybersecurity property)

可能值得保護之屬性。

備考：屬性包含機密性、完整性及/或可用性。

3.1.21 網路安全規格(cybersecurity specification)

網路安全要求事項及相對應之架構設計(3.1.1)。

3.1.22 損害情境(damage scenario)

涉及車輛或車輛功能並影響道路使用者(3.1.31)之不良後果。

3.1.23 分散式網路安全活動(distributed cybersecurity activities)

責任由顧客(3.1.8)與供應者間分配項目(3.1.25)或組件(3.1.7)之網路安全活動。

3.1.24 衝擊(impact)

估計損害情境(3.1.22)造成之損害或實際傷害之強度。

3.1.25 項目(item)

於車輛級實作功能之組件(3.1.7)或組件集。

備考：若系統於車輛級之實作功能，則其可為項目，此外為組件。

3.1.26 運作環境(operational environment)

考量運作使用中之互動的全景。

備考：項目(3.1.25)或組件(3.1.7)之運作使用，可包含於車輛功能中、生產中及/或服務及修復中之使用。

3.1.27 全景外(out-of-context)

非於特定項目(3.1.25)之全景下開發。

例：將具有假設性網路安全要求事項之處理單元整合至不同項目中。

3.1.28 滲透測試(penetration testing)

網路安全測試，藉由模擬真實世界攻擊，以識別遭破解之網路安全目標(3.1.16)之方法。

3.1.29 風險(risk)

網路安全風險。

對道路車輛網路安全(3.1.9)之不確定性影響，以攻擊可行性(3.1.3)及衝擊(3.1.24)表示。

3.1.30 風險管理(risk management)

指導及管制組織有關風險(3.1.29)的協調活動。

3.1.31 道路使用者(road user)

使用道路的人。

例：乘客、行人、騎自行車的人、駕駛者或車主。

3.1.32 裁適(tailor)

省略或以與 ISO/SAE 21434 中不同描述之方式履行活動。

3.1.33 威脅情境(threat scenario)

為實現損害情境(3.1.22)，破解 1 或多項資產(3.1.2)的網路安全性質(3.1.20)的潛在原因。

3.1.34 分類(triage)

分析以判定網路安全資訊(3.1.18)與項目(3.1.25)或組件(3.1.7)之相關性。

3.1.35 觸發(trigger)

分類(3.1.34)之準則。

3.1.36 確證(validation)

經提供客觀證據，以確認項目(3.1.25)之網路安全目標(3.1.16)係適切且已達成。

3.1.37 查證(verification)

經提供客觀證據，以確認已滿足特定要求事項。

3.1.38 脆弱性(vulnerability)

可被利用作為攻擊路徑(3.1.4)一部分之弱點(3.1.40)。

3.1.39 脆弱性分析(vulnerability analysis)

系統化識別及脆弱性(3.1.38)評估。

3.1.40 弱點(weakness)

能導致非期望行為之缺陷或特性。

例 1：缺少要求事項或規格。

例 2：架構或設計缺點，包含安全協定之不正確設計。

例 3：實作弱點，包含硬體和軟體缺陷、安全協定之不正確實作。

例 4：運作過程或程式中之瑕疵，包含誤用及使用者培訓不足。

例 5：使用過時或已廢止之功能，包含密碼學上之演算法。

3.2 縮寫

CAL	網路安全保證等級(cybersecurity assurance level)
CVSS	通用脆弱性評分系統(common vulnerability scoring system)
E/E	電機和電子(electrical and electronic)
ECU	電子控制單元(electronic control unit)
OBD	車載診斷(on-board diagnostic)
OEM	原始設備製造商(original equipment manufacturer)
PM	許可事項(permission)
RC	建議事項(recommendation)
RQ	要求事項(requirement)

RASIC	負責、當責、支援、知情及已諮詢(responsible, accountable, supporting, informed, consulted)
TARA	威脅分析及風險評鑑(threat analysis and risk assessment)
WP	工作產出(work product)

4. 一般考量事項

參照 CNS 21434 第 4 節，以了解該標準的涵蓋範圍及相關限制。

5. CNS 21434 第 15 節之實踐指引

第 15 節 威脅分析及風險評鑑

15.1 一般

本節描述判定道路使用者受威脅情境衝擊程度之方法。此等方法及其工作產出統稱為威脅分析及風險評鑑(TARA)，並從受影響的道路使用者觀察點履行。本節中定義的方法是通用模組，可從項目或組件生命週期之任何點系統化調用：

- 資產識別(參照 CNS 21434 之第 15.3 節)。
- 威脅情境識別(參照 CNS 21434 之第 15.4 節)。
- 衝擊評級(參照 CNS 21434 之第 15.5 節)。
- 攻擊路徑分析(參照 CNS 21434 之第 15.6 節)。
- 攻擊可行性評級(參照 CNS 21434 之第 15.7 節)。
- 風險值判定(參照 CNS 21434 之第 15.8 節)。
- 風險處理決定(參照 CNS 21434 之第 15.9 節)。

因此為通用模組，故本節中定義的工作產出將記錄為其他節中產生工作產出的一部分。

參照 CNS 21434 之附錄 H，藉由實際示例，而對此等方法進行說明。

組織特定衡量尺度可適用於衝擊評級、攻擊可行性評級及風險值確定，並對映至本標準中定義之對應尺度。

15.2 目的

本節之目的為：

(a) 識別資產、其網路安全性質及其損害情境。

(b)識別威脅情境。

(c) 判定損害情境之衝擊評級。

(d)識別實現威脅情境之攻擊路徑。

(e)判定攻擊路徑可利用性之程度。

(f) 判定威脅情境之風險值。

(g)針對威脅情境選擇適當之風險處理選項。

15.3 資產識別

15.3.1 輸入

15.3.1.1 先決條件

應提供以下資訊：

- 項目定義 CNS 21434 之[WP-09-01]。

15.3.1.2 進一步的支援資訊

可考量以下資訊：

- 網路安全規格 CNS 21434 之[WP-10-01]。

15.3.2 要求事項及建議事項

[RQ-15-01]應識別損害情境。

備考 1：損害情境可包含：

- 此項目之功能與不良後果間的關係。
- 對道路使用者造成傷害之描述。
- 相關資產。

[RQ-15-02]應識別具網路安全性質且其遭破解會導致損害情境之資產。

備考 2：資產識別可基於：

- 分析項目定義。
- 履行衝擊評級。
- 從威脅情境中導出之資產。
- 使用預定義之型錄。

例 1：若資產是儲存於資訊包容系統中的個資(顧客個人偏好)，則其網路安全性質為機密性。損害情境為未經顧客同意而洩露個資導致損失機密性。

例 2：若資產為煞車功能之資料通訊，則其網路安全性質為完整性。損害情境為車輛高速行駛時意外緊急煞車而被後車碰撞(追撞)。

- RQ-15-01、RQ-15-02 說明
  1. 資產係指具有價值，或對價值產生貢獻之物件。
  2. 資產識別為風險分析之起點，組織應依據項目定義中所界定之架構、系統邊界、假設條件與功能說明，識別項目所涉及之資產。
  3. 標準中建議之四種資產識別方法

(1) 分析項目定義：透過待分析之車輛、系統或項目功能說明與設計文件，識別關鍵資產。例如：遠端控制功能中的「控制指令」。

(2) 執行影響識別評級：透過評估功能失效對道路使用者、環境或財產之影響，反向推導出關鍵資產。例如：儲存之個人隱私資料。

(3) 由威脅情境推導資產：於威脅情境分析過程中，識別攻擊者可能針對之目標資產。例如：OTA 升級系統中的「OTA 升級封包」。

(4) 使用預先定義之資產型錄：利用產業標準或組織內部資產清冊進行快速識別。目前實務上最常見方法為使用預先定義之資產庫，惟組織應於實務運作過程中持續更新與維護該資產庫。

4. 常見資產分類範例

(1) 身分與組態資訊：例如汽車 VIN 碼(Vehicle Identification Number，車輛識別號碼)、軟硬體版本資訊、重要設定參數等。

(2) 韌體與應用程式：包含控制器可執行程式、韌體、第三方應用程式及相關金鑰。

(3) 資料：車輛系統運行過程中蒐集、產生或記錄之資訊，例如使用者資料、系統日誌。

(4) 通訊資訊：透過車載網路或外部通訊介面傳輸之資料，例如控制指令與狀態資訊。

5. 資產定義說明「應保護何種項目」，但資產本身屬於廣泛概念，需進一步轉換為具體且可衡量之保護目標，即網路安全性質。

6. 網路安全性質係指資產所具備且需受保護之特性，一旦該特性遭破壞，將導致資產受損，並可能引發損害情境。

7. 三大基本網路安全性質

(1) 機密性：確保資訊不被未授權之實體存取或揭露。例如：資訊娛樂系統中儲存之個人資料。

(2) 完整性：確保資訊或系統狀態不被未授權篡改或破壞。例如：煞車系統控制指令之完整性。

(3) 可用性：確保系統或服務於需要時可被授權實體正常存取與使用。例如：煞車控制指令於行駛期間可正常運作。

8. 網路安全性質之適用性說明：並非所有資產皆需保護所有網路安全性質。例如：整車 VIN 碼或部分軟硬體版本資訊屬公開資訊，通常無需保護其機密性。除基本三大屬性外，亦可視情況考量擴充屬性，例如：不可否認性、真實性、授權。

9. 損害情境係指當資產之網路安全性質遭破壞後，對車輛或其功能造成不良影響，進而影響道路使用者之情境。損害情境為連結「網路攻擊」與「實際危害」之核心橋樑。

10. 損害情境範例：

(1) 範例一

資產：資訊娛樂系統中儲存之個人資料

網路安全性質：機密性

損害情境：資料遭未授權存取與外洩，導致使用者隱私權受侵害。

(2) 範例二

資產：煞車系統控制指令

網路安全性質：完整性

損害情境：控制指令遭篡改，車輛於中速行駛時發生非預期煞車，造成追撞事故。

(3) 範例三

資產：煞車系統控制指令

網路安全性質：可用性

損害情境：控制指令失效，車輛於中速行駛時無法正常煞車，導致重大交通事故。

- RQ-15-01、RQ-15-02 實踐方式

1. 以頭燈系統項目為例，說明如何：

(1) 識別資產。

(2) 定義資產之網路安全性質及建立對應之損害情境。

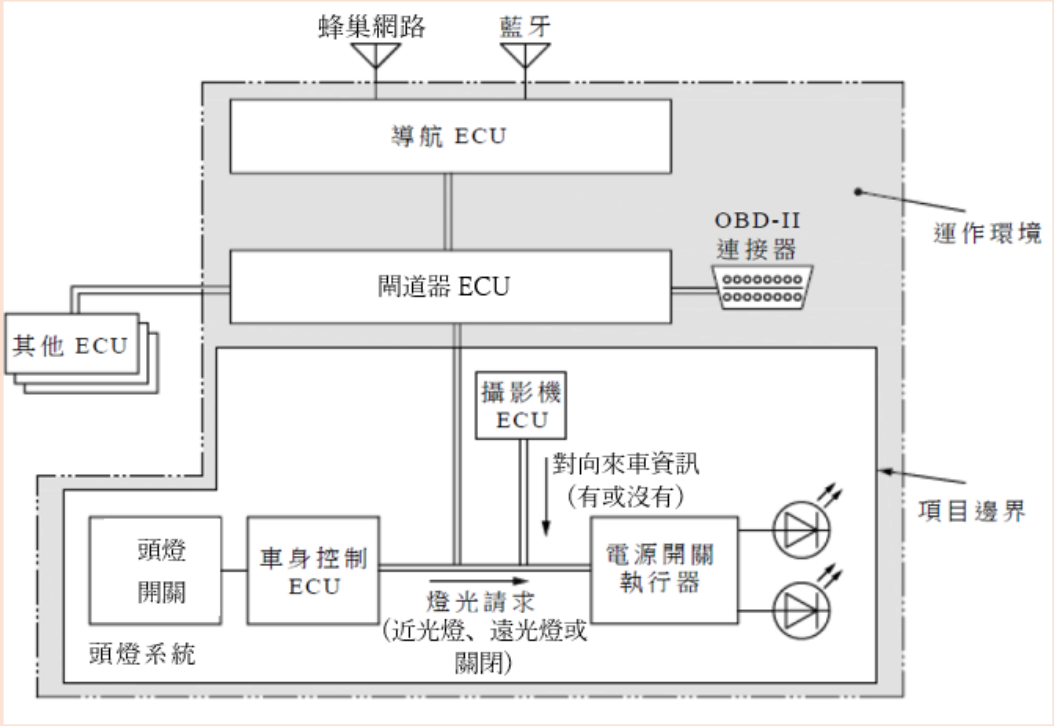

圖 1　CNS 21434 附錄 H.2 頭燈系統項目範例

2. 資產識別(使用預定義之型錄/資產清冊)

透過預定義之型錄/資產清冊進行識別，本案例中可識別之資產包括：燈光控制指令、對向來車存在與否之訊號、車身控制 ECU 之韌體、攝影機 ECU 之韌體。

3. 損害情境識別

(1) 範例一

資產：燈光控制指令

網路安全性質：完整性

損害情境：當燈光控制指令之完整性遭破壞時，車輛於夜間中速行駛期間，燈光可能遭非預期關閉，導致與狹窄靜止物體（如樹木）發生前方碰撞，造成駕駛或乘客受傷及車輛損壞。

(2) 範例二

資產：燈光控制指令

網路安全性質：可用性

損害情境：當燈光控制指令之可用性遭破壞時，燈光功能無法正常運作，導致車輛於夜間無法安全行駛。

(3) 範例三

資產：對向車存在與否之訊號

網路安全性質：完整性

損害情境：當對向車存在訊號之完整性遭破壞時，車輛於夜間中速行駛時未能正確切換至近光燈，導致對向車駕駛眩光，進而造成對向車失控或事故。

(4) 範例四

資產：對向車存在與否之訊號

網路安全性質：可用性

損害情境：當對向車存在訊號之可用性遭破壞時，自動遠光燈功能失效，頭燈長期維持近光燈狀態，降低夜間可視距離，增加事故風險。

(5) 範例五

資產：車身控制 ECU 韌體

網路安全性質：完整性

損害情境：當車身控制 ECU 韌體之完整性遭破壞時，頭燈功能可能失效，車輛於夜間行駛時發生碰撞事故，造成傷害與財產損失。

表 1　損害情境識別範例

功能項	資產	機密性	完整性	可用性	損害情境
頭燈	燈光控制指令	-	X	-	夜間行駛時燈光遭非預期關閉，導致前方碰撞事故
頭燈	燈光控制指令	-	-	X	夜間燈光功能不可

					用，無法安全行駛
頭燈	對向車存在訊號	-	X	-	未切換近光燈造成對向駕駛眩光
頭燈	對向車存在訊號	-	-	X	自動遠光失效，降低夜間視野
頭燈	車身控制 ECU 韌體	-	X	-	頭燈功能失效導致碰撞

- RQ-15-01、RQ-15-02 產出文件
  - 損害情境(對應 CNS 21434 之 WP-15-01)、具有網路安全性質之資產(對應 CNS 21434 之 WP-15-02)。
    - ➔一、二階文件(手冊/程序書)：網路安全管理手冊、網路安全風險管理程序書。
    - ➔ 三階文件(作業指導書)：TARA 指引(須內含資產類別定義、網路安全性質對應原則與權重計算公式)。
    - ➔四階文件(範本/表單)：損害情境識別表。

15.4 威脅情境識別

15.4.1 輸入

15.4.1.1 先決條件

應提供以下資訊：

- 項目定義 CNS 21434 之[WP-09-01]。

15.4.1.2 進一步的支援資訊

可考量以下資訊：

- 網路安全規格 CNS 21434 之[WP-10-01]。
- 損害情境 CNS 21434 之[WP-15-01]。
- 具有網路安全性質之資產 CNS 21434 之[WP-15-02]。

15.4.2 要求事項及建議事項

[RQ-15-03]應識別威脅情境，包含：

- 目標資產。
- 資產的網路安全性質遭破解。
- 網路安全性質遭破解的原因。

備考 1：進一步資訊可包含於威脅情境中或與威脅情境相關聯，例：損害情境，以及資產、攻擊者、方法、工具及攻擊面間的技術相互依賴性。

備考 2：威脅情境識別的方法可使用小組討論及/或系統方法，例：

- 因合理可預見的誤用及/或濫用而導致惡意使用案例之釐清。
- 基於 EVITA、TVRA、PASTA、STRIDE(欺騙、篡改、否認、資訊洩露、阻絕服務、特權提升)等框架之威脅模組方法。

備考 3：一個損害情境可對應多個威脅情境，一個威脅情境亦可導致多個損害情境。

例：欺騙煞車 ECU 之 CAN 訊息將導致 CAN 訊息之完整性喪失，進而導致煞車功能之完整性喪失。

- RQ-15-03 說明

1. 威脅情境係指一個或多個資產之網路安全性質遭破壞的潛在原因，用以實現特定之損害情境。
   (1) 損害情境描述「最終會發生什麼危害」
   (2) 威脅情境描述「攻擊如何發生」
   因此，在完成損害情境識別後，組織應進行威脅建模，以識別可能導致損害情境發生之威脅情境。損害情境的實現，往往需透過一個或多個威脅情境之實施才會發生。
2. 為使威脅分析具體且貼近實際攻擊情境，威脅情境可關聯下列資訊：
   (1) 對應之損害情境：每一威脅情境應明確說明其所導致之損害情境。
   (2) 資產之技術依賴關係：技術依賴性係指系統中不同組件(如 ECU、資料、功能模組)間之交互與依賴邏輯。

(3) 在威脅情境中納入技術依賴關係，有助於識別攻擊的連鎖反應(Cascading Effect)，即單一資產遭破壞後，如何透過依賴鏈影響其他資產與功能，例如攝影機 ECU 韌體遭篡改，影響物件偵測結果導致遠光燈控制判斷錯誤。

(4) 攻擊者類型：外部駭客、內部人員、維修人員、惡意第三方等。

(5) 攻擊方法：中間人攻擊、惡意韌體植入、社交工程、訊號干擾、已知漏洞利用。

(6) 攻擊工具：漏洞利用腳本、無線訊號干擾器、偽造封包工具

(7) 攻擊面：實體介面、無線介面、OTA 更新介面、診斷介面。

3. 威脅情境識別對實務經驗與攻擊案例資料庫之完整性要求較高。標準建議以下兩種方法：

(1) 方法一：從合理可預見之誤用/濫用情境出發所謂「誤用/濫用情境」，係指非正常使用行為、攻擊者故意之惡意行為或利用系統設計/實作缺陷進行之濫用。舉例，透過無線介面注入惡意控制指令、利用已知漏洞進行未授權存取等。這些情境應為「合理可預見」，是攻擊者具備實施能力，而非極端或不可能發生之假設。

(2) 方法二：使用成熟的威脅建模方法，例如使用微軟提出的威脅分析模型技術 STRIDE，包含六類威脅：

A. 欺騙(Spoofing)：冒充合法實體身分，使系統誤認為合法來源。如偽造合法 ECU ID 進行控制操作。

B. 篡改(Tampering)：未經授權修改資料、程式碼或系統狀態。如攔截並修改控制封包。

C. 否認(Repudiation)：攻擊者否認其執行過某項操作。如未保留日誌導致無法追蹤攻擊來源。

D. 資訊洩漏(Information Disclosure)：未經授權存取敏感資訊。如攔截未加密之個人資料。

E. 阻絕服務(Denial of Service)：使合法使用者無法正常存取系統或服務。如發動 DoS 攻擊使煞車控制系統無法回應。

F. 特權提升(Elevation of Privilege)：取得超出原有權限之存取能力。如攻擊者透過漏洞取得管理者權限。

- RQ-15-03 實踐方式

表 2　威脅情境識別範例

損害情境	威脅分析	
	威脅類型	威脅情境
燈光控制指令的完整性被破壞，車輛在夜間中速行駛時，燈光被非預期地關閉，導致與狹窄靜止物體(如樹木)發生前部碰撞，造成人身傷害和車輛損害。	欺騙	攻擊者偽造「頭燈請求」訊號，破壞該訊號資料通訊的完整性，導致頭燈非預期地關閉。
	篡改	攻擊者篡改車身控制 ECU 發送的「頭燈請求」訊號，破壞該訊號資料通訊的完整性，導致頭燈非預期地關閉。
	…	…
對向車存在與否的訊號的可用性被破壞，自動遠光燈功能失效，頭燈始終保持近光燈狀態。降低夜間視野，增加事故風險。	阻絕服務	攻擊者對 CAN 匯流排發送阻絕服務攻擊，導致車身控制器無法獲取對向車輛訊號，無法觸發遠光燈切換。
	…	…
…	…	…

- RQ-15-03 產出文件
  - ■ 威脅情境(對應 CNS 21434 之 WP-15-03)。
    - ➔一、二階文件(手冊/程序書)：網路安全管理手冊、網路安全風險管理程序書。
    - ➔ 三階文件(作業指導書)： TARA 指引。
    - ➔ 四階文件(範本/表單)：威脅情境識別表。

15.5 衝擊評級

15.5.1 輸入

15.5.1.1 先決條件

應提供以下資訊：

- 損害情境 CNS 21434 之[WP-15-01]。

15.5.1.2 進一步的支援資訊

可考量以下資訊：

- 項目定義 CNS 21434 之[WP-09-01]。
- 具有網路安全性質之資產 CNS 21434 之[WP-15-02]。

15.5.2 要求事項及建議事項

[RQ-15-04]應分別依人身設備安全、財務、運作及隱私(S、F、O、P)之衝擊類別對道路使用者造成的潛在不良後果以評鑑損害情境。

備考 1：本標準不提供不同衝擊類別間的關係(例：權重)。

備考 2：可考量新增衝擊類別。

備考 3：若考量新增衝擊類別，則可依 CNS 21434 第 7 節於供應鏈中共享該等類別的理由闡述及解釋。

[RQ-15-05]對於每個衝擊類別，損害情境的衝擊評級應判定為以下之一：

- 嚴重。
- 主要。
- 中等。
- 可忽略。

備考 4：可依 CNS 21434 之附錄 F 中提供的表格對財務、運作及隱私相關衝擊進行評級。

[RQ-15-06]人身設備安全相關衝擊評級應導自 ISO 26262-3:2018 之 6.4.3。

備考 5：CNS 21434 之附錄 F 中的表 F.1 可用於將人身設備安全衝擊準則對映至衝擊評級。

備考 6：功能安全評估可再利用於此用途。

[PM-15-07]若損害情境產生衝擊評級，且可提出另一個衝擊類別的每個衝擊被視為不重要的論點，則可省略對其他衝擊類別之進一步分析。

例：若損害情境的安全衝擊被評級為〝嚴重〞，因此不進一步分析此損害情境的財務衝擊。

- RQ-15-04、RQ-15-05、RQ-15-06、PM-15-07 說明

1. 組織應針對已識別之損害情境進行定性化評估，且評估範圍須涵蓋四類影響面向，分別為：安全、財務、運作及隱私影響。對於每一影響類別，應進一步判定其影響等級，例如「嚴重」、「主要」、「中等」或「可忽略」等級。各等級之定義與判定標準可參考 CNS 21434 附錄 F 所提供之說明，並結合組織自身產品特性與使用情境進行具體化定義。
2. CNS 21434 本身並未明確規定上述四項影響類別之權重配置方式，因此組織可依產品特性、產業風險屬性及企業風險承受能力，自行訂定各影響類別之權重比例。另一種實務作法，係直接採用四項影響中評級最高者作為該損害情境之整體彙總影響等級，以確保風險評估結果偏向保守且符合安全優先原則。

- RQ-15-04、RQ-15-05、RQ-15-06、PM-15-07 實踐方式

表 3　損害情境的影響分析

損害情境	影響分析							
	安全		財務		運作		隱私	
	等級	備註	等級	備註	等級	備註	等級	備註
燈光控制指令的完整性被破壞，車輛在夜間中速行駛時，燈光被非預期地關閉，導致與狹窄靜止物體(如樹木)發生前部	嚴重	威脅生命的傷害	主要	大量財務損失	主要	車輛重要功能受損	可忽略	不涉及

碰撞，造成人身傷害和車輛損害。								
對向車存在與否的訊號的可用性被破壞，自動遠光燈功能失效，頭燈始終保持近光燈狀態。降低夜間視野，增加事故風險。	中等	輕度和中度傷害	中等	少量財務損失	中等	功能的部分退化	可忽略	不涉及
…	…	…	…	…	…	…	…	…

- RQ-15-04、RQ-15-05、RQ-15-06、PM-15-07 產出文件
  - 具相關衝擊類別之衝擊評級(對應 CNS 21434 之 WP-15-04)。
    - ➔一、二階文件(手冊/程序書)： 網路安全管理手冊、網路安全風險管理程序書。
    - ➔三階文件(作業指導書)：衝擊評級判定作業指導書(須內含 S、F、O、P 四大類別之判定基準與最高等級彙總規則)。
    - ➔四階文件(範本/表單)：損害情境衝擊評級表(可與 RQ-15-01、RQ-15-02 產出之四階文件損害情境識別表合併為同一表格)。

15.6 攻擊路徑分析

15.6.1 輸入

15.6.1.1 先決條件

應提供以下資訊：

- 項目定義 CNS 21434 之[WP-09-01]或網路安全規格 CNS 21434 之[WP-10-01]。

備考：若對項目履行攻擊路徑分析，則應使用項目定義。若對組件履行攻擊路徑分析，則應使用網路安全規格。

- 威脅情境 CNS 21434 之[WP-15-03]。

15.6.1.2 進一步的支援資訊

可考量以下資訊：

- 網路安全事故之弱點 CNS 21434 之[WP-08-04]。
- 產品開發期間發現之弱點[WP-10-05]。
- 架構設計；
- 先前已識別之攻擊路徑[WP-15-05](若有)。
- 脆弱性分析[WP-08-05]。

15.6.2 要求事項及建議事項

[RQ-15-08]應分析威脅情境以識別攻擊路徑。

備考 1：攻擊路徑分析可基於：

- 自上而下的方法，藉由分析威脅情境可能實現的不同方式來推攻擊路徑，例：攻擊樹、攻擊圖。
- 自下而上的方法，從已識別的脆弱性構建攻擊路徑。

備考 2：若部分攻擊路徑無導致威脅情境的實現，則可停止對此部分攻擊路徑之分析。

[RQ-15-09]攻擊路徑應與攻擊路徑可實現之威脅情境相關聯。

備考 3：於產品開發早期階段，因無法得知具體實作細節是否可識別特定脆弱性，攻擊路徑通常是不完整或不精確。於產品開發過程中，攻擊路徑可隨著更多可用資訊而更新，例：經過脆弱性分析後。

例：

- 威脅情境：欺騙煞車 ECU 之 CAN 訊息將導致 CAN 訊息喪失完整性，導致煞車功能完整性喪失。
- 實現上述威脅情境之攻擊路徑：
  i. 藉由蜂巢介面，ECU 之遙測訊號遭破解。
  ii. 藉由 ECU 遙測訊號之 CAN 通訊，ECU 閘道器遭破解。
  iii. ECU 閘道器傳送惡意煞車請求訊號(無須快速減速)。

- RQ-15-08、RQ-15-09 說明

1. 攻擊路徑係指攻擊者為實現某一威脅情境所採取的一連串蓄意行動步驟。換句話說：

(1) 威脅情境說明「攻擊如何發生」。

(2) 攻擊路徑說明「攻擊如何一步一步實現」。

因此，攻擊路徑可視為威脅情境的具體執行流程。組織應從已識別之威脅情境出發，系統化找出攻擊者可能利用之攻擊路徑。此分析通常高度依賴：實務攻擊經驗、已知漏洞資料庫(如 CVE (Common Vulnerabilities and Exposures，常見漏洞與暴露))、政府或產業公開攻擊案例、過往專案經驗。

2. 攻擊路徑分析方法。
   (1) 自上而下法：從攻擊目標(例如破壞完整性)出發，逐步拆解攻擊如何發生。常以攻擊樹方式進行。
   (2) 自下而上法：從已知脆弱性或攻擊面出發，分析其可能導致的威脅情境。如已知除錯介面未關閉、已知通訊未加密、已知第三方組件存在漏洞。
3. 在建立攻擊樹時應注意：
   (1) 相同威脅情境可能對應多條攻擊路徑。
   (2) 系統架構越複雜，可拆解之攻擊路徑越多。
   (3) 必須納入已知漏洞與歷史資料，應參考 CVE 資料庫、NVD、CERT 公告、政府安全通報、過往專案的攻擊模型(若適用)，可沿用既有攻擊路徑模型。
   (4) 每個攻擊動作宜對應一個可識別的脆弱性(或盡可能對應)，如通訊界面未加密、已知介面(除錯用介面如 JTAG)未關閉。
   (5) 若某分支路徑無法合理導致威脅情境成立，則可終止該分支分析，避免無限展開。
   (6) 若收集資訊不足，無法滿足攻擊路徑分析時，如架構不明確、組件功能未定義、介面細節缺失等，應該待後續資訊明確後，再更新攻擊路徑。
4. 攻擊樹是一種結構化、圖形化的威脅分析方法，自上而下拆解攻擊目標，列舉所有可能攻擊路徑。

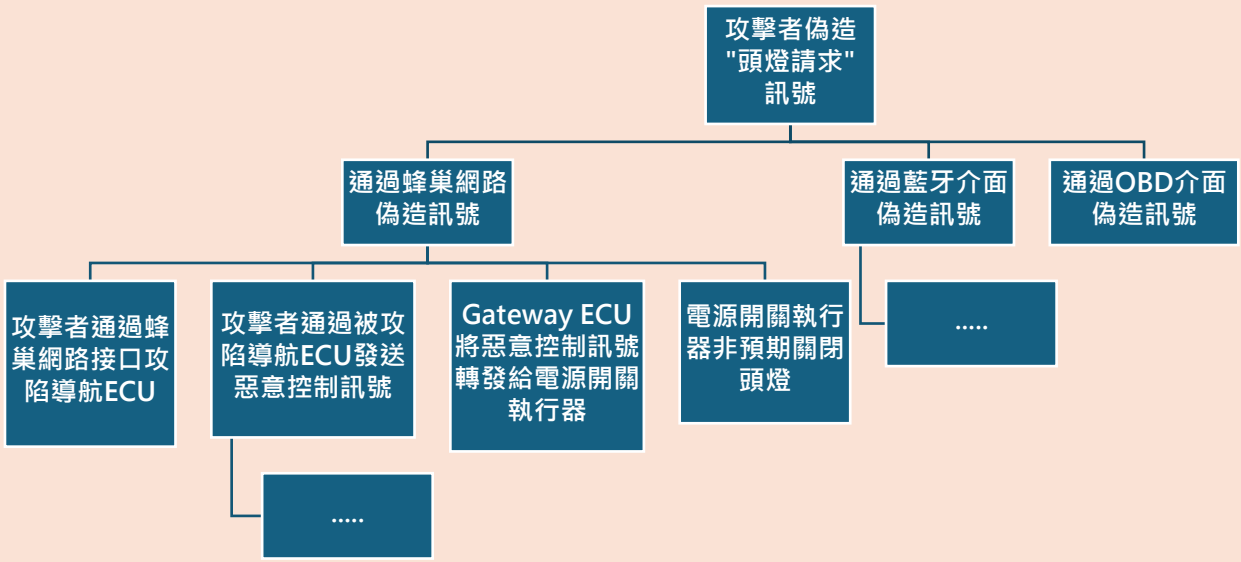

圖 2　攻擊樹方法範例

- RQ-15-08、RQ-15-09 實踐方式

表 4　攻擊路徑分析範例

威脅情境	攻擊路徑分析	
	編號	攻擊路徑
攻擊者偽造「頭燈請求」訊號，破壞資料通訊完整性，導致頭燈非預期關閉。	1	1) 攻擊者透過蜂巢網路介面攻陷導航 ECU。 2) 攻擊者利用已攻陷之導航 ECU 發送惡意控制訊號。 3) 閘道器 ECU 將惡意控制訊號轉發至電源開關執行器。 4) 電源開關執行器執行關閉頭燈之動作。
	2	1) 攻擊者透過藍牙介面攻陷導航 ECU。 2) 攻擊者透過被攻陷之 ECU 發送惡意控制訊號。 3) 閘道器 ECU 將訊號轉發至電源開關執行器。 4) 電源開關執行器關閉頭燈。
	3	1) 攻擊者取得 OBD (On-Board Diagnostics，車載診斷系統)介面之實體存取權限。 2) 攻擊者透過 OBD 發送帶有惡意控制命令之封包。 3) 閘道器 ECU 將封包轉發至電源開關執行器。 4) 電源開關執行器非預期關閉頭燈。
攻擊者對 CAN 總線發動阻絕服務攻擊，使車身控制器無法取得對向	1	1) 攻擊者透過蜂巢介面攻陷導航 ECU。 2) 攻擊者透過被攻陷 ECU 發送大量惡意封包。 3) 惡意封包透過閘道器進入 CAN 總線。 4) 攻擊者使用大量高優先級封包癱瘓 CAN 通訊。

車訊號，導致遠光燈切換失效。	2	1) 攻擊者於車輛解鎖時接入支援藍牙之 OBD 轉接器。 2) 攻擊者透過藍牙攻陷駕駛者智慧型手機。 3) 攻擊者利用手機與 OBD 裝置向閘道器 ECU 發送訊息。 4) 惡意訊息進入車載網路。 5) 攻擊者以高頻率封包造成 CAN 阻絕服務。
…	…	…

- RQ-15-08、RQ-15-09 產出文件
  - ■ 攻擊路徑(對應 CNS 21434 之 WP-15-05)。
    - ➔一、二階文件(手冊/程序書)：無。
    - ➔ 三階文件(作業指導書)：攻擊路徑評估指導書。
    - ➔四階文件(範本/表單)：攻擊路徑分析表。

15.7 攻擊可行性評級

15.7.1 輸入

15.7.1.1 先決條件

應提供以下資訊：

- 攻擊路徑 CNS 21434 之[WP-15-05]。

15.7.1.2 進一步的支援資訊

可考量以下資訊：

- 架構設計;
- 脆弱性分析 CNS 21434 之[WP-08-05]。

15.7.2 要求事項及建議事項

[RQ-15-10]針對每條攻擊路徑，應依下表中的描述判定攻擊可行性評級。

表 5：攻擊可行性評級及說明

攻擊可行性評級	說明
高	利用較低努力完成攻擊路徑。
中	利用中等努力完成攻擊路徑。
低	利用較高努力完成攻擊路徑。
非常低	利用非常高努力完成攻擊路徑。

[RC-15-11]攻擊可行性評級方法應基於以下方法之一定義：

(a) 基於攻擊潛在性之方法。

(b) 基於 CVSS 之方法。

(c) 基於攻擊向量之方法。

備考 1：方法的選擇取決於生命週期的階段及可用資訊。

- RQ-15-10、RC-15-11 說明
  1. 組織必須針對每一條已識別之攻擊路徑，判定其「攻擊可行性等級」。這個等級是後續風險等級計算的關鍵輸入參數，將直接影響風險高低判定，以及安全防護措施的優先順序。
  2. 標準本身並未強制規定必須採用特定評估方法，而是允許組織依據專案階段與資訊成熟度彈性選擇合適模型。例如，在專案早期階段，系統架構與技術細節尚未完全明確時，可採用以攻擊向量為基礎的簡化評估方式；隨著專案推進，設計逐步明確、訊息更加完整時，則可轉換為基於攻擊潛在性或 CVSS 的方法。
- RQ-15-10、RC-15-11 實踐方法

  併同[RC-15-12]、[RC-15-13]、[RC-15-14]進行闡述。
- RQ-15-10、RC-15-11 產出文件

  併同[RC-15-12]、[RC-15-13]、[RC-15-14]進行闡述。

[RC-15-12]若使用基於攻擊潛在性的方法，則宜依核心因素判定攻擊可行性評級，包含：

(a) 經過時間。

(b) 專業知識。

(c) 對項目或組件的知識。

(d) 機會窗口。

(e) 設備。

備考 2：核心攻擊潛在性因素可從 ISO/IEC 18045 推導出。

備考 3：CNS 21434 之附錄 G.2 提供基於潛在性攻擊，判定攻擊可行性之指導綱要。

[RC-15-13]若使用基於 CVSS 的方法，則宜依基本衡量尺度群的可利用性衡量尺度以判定攻擊可行性評級，包含：

(a) 攻擊向量。

(b) 攻擊複雜度。

(c) 所需權限。

(d) 用戶互動。

備考 4：CNS 21434 附錄 G.3 提供基於 CVSS 方法判定攻擊可行性之指導綱要。

[RC-15-14]若使用基於攻擊向量的方法，則應依評估攻擊路徑的主要攻擊向量(參照 CVSS 之 2.1.1)來判定攻擊可行性評級。

備考 5：CNS 21434 附錄 G.4 提供基於攻擊向量方法判定攻擊可行性之指導綱要。

備考 6：於早期開發階段(例：概念階段)，當沒有足夠資訊識別特定攻擊路徑時，基於攻擊向量方法可能僅適合估計攻擊的可行性。

- RC-15-12、RC-15-13、RC-15-14 說明

  1. 組織需依據 CNS 21434 附錄 G.2、G.3 與 G.4 所提供的方法，對每一條攻擊路徑進行攻擊可行性評級。其中 CNS 21434 附錄 G 提供了詳細的三種判定攻擊可行性評級的準則，組織可依專案成熟度與技術資訊完整度選擇適用方法。以下基於攻擊潛在性之方法為例進行說明。

     (1) 經過時間：此參數包含識別漏洞、開發利用方式以及成功執行攻擊所需的時間。耗時越短，表示攻擊門檻越低，可行性越高。例如：一天內可完成的評為 0 分，一週內為 1 分，一個月內為 4 分，六個月內為 17 分。

表 6　經過時間評估

經過時間	數值
≤ 1 天	0
≤ 1 週	1
≤ 1 個月	4
≤ 6 個月	17

(2) 專業知識：此項衡量攻擊者所需具備的技術能力層級。外行(僅依公開步驟操作)為 0 分；熟悉產品安全行為的精通技術人員為 3 分；具備底層架構與安全原理知識的專家為 6 分；若攻擊需跨多領域專家合作，則為 8 分。

表 7　專業知識評估

專業經驗	描述	數值
外行	與專家或精通的攻擊者相比，不了解情況，沒有特別的專長。 例：普通人使用公開的攻擊步驟描述進行攻擊。	0
精通	知識淵博，即熟悉產品或系統類型的安全行為。 例：有經驗的車主、普通技術人員知道簡單和流行的攻擊方法，如里程表的調整、安裝假冒的組件。	3
專家	熟悉底層演算法、通訊協定、硬體、架構、安全行為、採用的安全原則和概念、定義新攻擊的技術和工具、密碼學、產品類型的經典攻擊、產品或系統類型中實作的攻擊方法等。 例：有經驗的技術員或工程師。	6
多領域專家	攻擊的不同步驟需要專家級別的不同領域專業知識。 例：多個經驗豐富的工程師，他們在不同的領域都有專長，而且在攻擊的不同步驟中都需要專家級別。	8

(3) 對項目或組件的知識(所需資訊)：此參數指攻擊者對項目或組件了解的程度，或攻擊者取得相關系統資訊的難易程度。若僅需公開資訊(如官網文件、論壇資料)，為 0 分；若需內部限制性文件為 3 分；若需機密資訊(如原始碼、防盜設計細節)為 7 分；若需嚴格保密資訊(僅極少數人知悉)則為 11 分。

表 8　所需資訊評估

資訊等級	描述	數值
公開資訊	有關該項目或組件的公開資訊(如從網際網路上獲得的資訊)。 例：在產品首頁或網路論壇上發布的資訊和文件。	0
限制性資訊	有關項目或組件的限制性資訊。 例：在開發者組織內部控制的知識，並根據保密協議與其他組織共享(如製造商和供應商之間共享的內部文件、要求和設計規格)。	3
機密資訊	關於項目或組件的機密資訊。 例，在開發者組織內的不同團隊之間共享的知識，只有指定團隊的成員才能存取這些資訊(如與防盜器有關的資訊、軟體原始碼)。	7
嚴格保密資訊	關於項目或組件的嚴格保密資訊。 例：只有少數人知道的知識，在嚴格的「須知(Need-to-know)」基礎上，對其存取進行非常嚴格的控制，並由個人承擔。 例：由製造商和/或供應商內部記錄的客戶特定的校準或記憶體對應圖。	11

(4) 機會窗口：此項參數衡量攻擊實施所需的存取條件與時間限制。它結合了存取類型(如邏輯和實體)和存取時間(如無限和有限)。根據攻擊的類型，這可能包括發現可能的目標、進入目標、利用目標的運作、對目標進行攻擊的時間、保持不被發現、規避偵測和網路安全控制措施等。若可透過公開網路遠端存取，且無時間限制，為 0 分；若需有限遠端條件(如藍牙配對時間)，為 1 分；若需有限實體存取(如未上鎖車輛的 OBD 介面)，為 4 分；若幾乎難以實現(如需拆解晶片或暴力破解)，則為 10 分。

表 9　機會窗口評估

機會窗口	描述	數值
無限的	透過公開/不信任的網路，沒有任何時間限制的高可用性(即資產總是可以存取)。沒有實體存在或時間限制的遠端存取，以及對項目或組件的無限制實體存取。 例：遠端攻擊，如車輛到任何事物(V2X)或手機介面，沒有任何先決條件；車主無限制的實體存取，進行晶片調整。	0
容易	高可用性和有限的存取時間。遠端存取，無需親自到項目或組件處。 例：藍牙的配對時間、遠端軟體更新、需要車輛靜止的遠端攻擊。	1
中等	項目或組件的低可用性。有限的實體和/或邏輯存取。在不使用任何特殊工具的情況下對車輛內部或外部進行實體存取。 例：攻擊者進入一輛未上鎖的汽車，並獲得了暴露的實體介面，例如透過車載診斷連接埠(OBD)的實體存取。	4
困難	該項目或組件的可用性非常低。對該項目或組件的存取程度不實際，無法實施攻擊。 例：解除積體電路的封裝以提取資訊、用暴力破解密碼金鑰，且其速度必須比金鑰輪換的速度快。	10

(5) 設備：此項參數評估攻擊者可用來發現脆弱性和/或執行攻擊所需工具的取得難度。若僅需標準工具(筆電、CAN 轉接器、簡易腳本)為 0 分；若需專用設備(硬體除錯工具、HIL 測試台)為 4 分；若需高度客製或受管制設備為 7 分；若攻擊不同階段需多種客製設備則為 9 分。

表 10　設備參數評估

設備分類	描述	數值
標準	設備對攻擊者來說是現成的。這種設備可以是產品本身的一部分(如作業系統中的除錯器)，或者可以很容易地得到(如網路資源、通訊協定分析器或簡單的攻擊腳本)。 例：筆記型電腦、CAN 轉接器、車載診斷器、普通工具如螺絲起子、電烙鐵、鉗子。	0
專用	設備對攻擊者來說不是現成的，但可以輕易獲得。這可以包括購買適量的設備(例如電力分析工具，使用數百台連接在網際網路上的個人電腦就屬於這個類別)，或開發更廣泛的攻擊腳本或程式。如果一個攻擊的不同步驟需要由專門設備組成的明顯不同的測試台，這將被評為客製化。 例：專門的硬體除錯設備、車載通訊設備如硬體在迴路(HIL)測試台、高階示波器、訊號產生器、特殊化學品。	4
客製化	設備是專門生產的(如非常複雜的軟體)，不容易向公眾提供(如黑市)，或者設備非常專業，其分配受到控制，甚至有可能受到限制。或者，該設備非常昂貴。 例：製造商限制的工具、電子顯微鏡。	7
多種客製化	引入這個概念是為了考慮到在攻擊的不同步驟中，需要不同類型的客製化設備的情況。	9

2. 完成上述五項參數評分後，將分數加總，即為攻擊潛在性總分。再依攻擊潛在性對照表轉換為攻擊可行性等級：總分 0–13 為「高」，14–19 為「中」，20–24 為「低」，25 以上為「很低」。

表 11　攻擊潛在性映射表

攻擊可行性評級	攻擊潛在性總分
高	0-13
中	14-19
低	20-24
非常低	≥25

- RQ-15-10 至 RC-15-14 實踐方式

  組織可依據專案的資訊成熟度，選擇合適的評估方法。以下提供基於「攻擊向量」與「攻擊潛在性」兩種不同評估方法的實作範例，工程師需依據所選方法評估每條攻擊路徑，並記錄其結果。

表 12　基於攻擊向量的攻擊可行性評級

威脅情境	**攻擊路徑分析**			
	編號	**攻擊路徑**	**攻擊向量**	**攻擊可行性評級**
攻擊者偽造「頭燈請求」訊號，破壞該訊號資料通訊的完整性，導致頭燈非預期地關閉。	1	1) 攻擊者透過蜂巢網路介面攻陷導航 ECU。 2) 攻擊者透過被攻陷的導航 ECU 發送惡意控制訊號。 3) 閘道器 ECU 將惡意訊號轉發給電源開關執行器。 4) 電源開關執行器非預期地關閉頭燈。	網路	高
	2	1) 攻擊者透過藍牙介面攻陷導航 ECU。 2) 攻擊者透過偽造藍牙授權指令發送惡意控制訊號。 3) 閘道器 ECU 將惡意訊號轉發給電源開關執行器。 4) 電源開關執行器非預期地關閉頭燈。	近場	中

	3	1) 攻擊者獲得對 OBD 介面的本機存取權限。 2) 攻擊者從 OBD 介面發送惡意控制訊號。 3) 閘道器 ECU 將惡意訊號轉發給電源開關執行器。 4) 電源開關執行器非預期地關閉頭燈。	本機	低
…	…	…	…	…

表 13　基於攻擊潛在性的攻擊可行性評級

威脅情境	攻擊路徑分析		攻擊可行性評估						
	編號	攻擊路徑	花費時間	專業知識	所需資訊	機會窗口	所需設備	總分數	攻擊可行性評級
攻擊者對 CAN 匯流排發送阻絕服務攻擊，導致車身控制器無法獲取對向車輛訊	1	1) 攻擊者透過蜂巢介面利用已知漏洞入侵導航 ECU。 2) 取得 ECU 控制權。 3) 透過內部網路向 CAN 發送高優先級封包。 4) 以大量封包癱瘓總線。 5) 車身控制器無法正常接收訊號。	1	8	7	0	4	20	低
	2	1) 攻擊者在車輛駐車解鎖時，將一個支援藍牙的 OBD 轉接器連接到 OBD 介面。	1	8	7	4	4	24	低

號，無法觸發遠光燈切換。		2) 攻擊者透過藍牙介面攻陷駕駛員的智慧型手機。 3) 攻擊者透過智慧型手機和藍牙 OBD 轉接器向閘道器 ECU 發送訊息。 4) 閘道器 ECU 將惡意資訊轉發給電源開關執行器。 5) 攻擊者用大量高優先權的封包癱瘓 CAN 匯流排通訊。							
…	…	…	…	…	…	…	…	…	…

- RQ-15-10 至 RC-15-14 產出文件
  - ■ 攻擊可行性評級(對應 CNS 21434 之 WP-15-06)。
    - ➔一、二階文件(手冊/程序書)： 網路安全管理手冊、網路安全風險管理程序書。
    - ➔ 三階文件(作業指導書)：攻擊可行性評級作業指導書(須明訂依據之攻擊可行性評級的準則，如攻擊向量法、攻擊潛在性法等，及各維度之評分基準與映射表)。
    - ➔四階文件(範本/表單)： 攻擊可行性評級表(記錄針對每條攻擊路徑之攻擊可行性評級)。

15.8 風險值判定

15.8.1 輸入

15.8.1.1 先決條件

應提供以下資訊：

- 威脅情境 CNS 21434 之[WP-15-03]。
- 衝擊評級及相關衝擊類別 CNS 21434 之[WP-15-04]。
- 攻擊可行性評級 CNS 21434 之[WP-15-06]。

15.8.1.2 進一步的支援資訊

無

15.8.2 要求事項及建議事項

[RQ-15-15]針對每種威脅情境，風險值應依相關損害情境衝擊及相關攻擊路徑之攻擊可行性判定。

備考 1：若威脅情境對應多個損害情境及/或，相關損害情境對多個衝擊類別產生衝擊，則可為每個衝擊評級單獨判定個別風險值。

備考 2：若威脅情境對應多個攻擊路徑，則可適當彙總相關的攻擊可行性評級，例：威脅情境被指配至相應攻擊路徑攻擊可行性評級之最大值。

[RQ-15-16]威脅情境之風險值應為 1(含)至 5(含)之間的數值，其中 1 代表最小風險。

例：風險值判定方法：

- 風險矩陣。
- 風險公式。

- RQ-15-15、RQ-15-16 說明

1. 風險值是由兩個關鍵維度共同決定：
   (1) 第一個維度是「損害情境的影響等級」。也就是假設攻擊者成功實施攻擊後，對車輛、人員或環境所造成的後果嚴重程度。這個影響通常已在前一步驟中，針對安全、財務、運作與隱私等面向完成評估與彙總。
   (2) 第二個維度是「攻擊可行性」。也就是攻擊者成功完成該攻擊的難易程度。此部分來自攻擊路徑分析與攻擊可行性評分結果。
2. 若一個威脅情境對應多個損害情境，或某個相關損害情境在多個衝擊類別(如安全、財務、運作、隱私)中產生衝擊，實務上常見的作法是將這些衝擊類別進行彙總(通常取最高評級)，作為該損害情境最終的衝擊評級，將該損害情境在各影響類別中的結果進行彙總，以最高影響等級或既定彙總規則作為最終影響等級，

3. 若一個威脅情境對應多個攻擊路徑，可對相應攻擊路徑的攻擊可行性評級進行適當的彙總。常見作法是為該威脅情境分配所有攻擊路徑中「最高」的攻擊可行性評級。

- RQ-15-15、RQ-15-16 實踐方式

  工程師須依據彙總後的衝擊評等與攻擊可行性評級，利用風險矩陣判定最終風險值，並將結果記錄於 TARA 報告中，如下表範例：

表 14　彙總損害情境的衝擊評級

損害情境	影響分析								彙總衝擊評級
	安全		財務		運作		隱私		
	等級	備註	等級	備註	等級	備註	等級	備註	
燈光控制指令的完整性被破壞，車輛在夜間中速行駛時，燈光被非預期地關閉，導致與狹窄靜止物體(如樹木)發生前部碰撞，造成人身傷害和車輛損害。	嚴重	威脅生命的傷害	主要	大量財務損失	主要	車輛重要功能受損	可忽略	不涉及	嚴重 *(取四個影響類別中等級最高的評級)*
對向車存在與否的訊號的可用性被破壞，自動遠光燈功能失效，頭燈始終保持近光燈狀態。降低夜間視	中等	輕度和中度傷害	中等	少量財務損失	中等	功能的部分退化	可忽略	不涉及	中等 *(取四個影響類別中等級最高的評級)*

野，增加事故風險。									
…									

表 15　彙總的攻擊可行性評級(基於「攻擊向量」的評價方式)

威脅情境	攻擊路徑分析		攻擊可行性評級		彙總攻擊可行性
	編號	攻擊路徑	攻擊向量	攻擊可行性等級	
攻擊者偽造「頭燈請求」訊號，破壞該訊號資料通訊的完整性，導致頭燈非預期地關閉。	1	1) 攻擊者透過蜂巢網路介面攻陷導航 ECU。 2) 攻擊者透過被攻陷的導航 ECU 發送惡意控制訊號。 3) 閘道器 ECU 將惡意訊號轉發給電源開關執行器。 4) 電源開關執行器非預期地關閉頭燈。	網路	高	高 *(取攻擊路徑中最高的攻擊可行性評級)*
	2	1) 攻擊者透過藍牙介面攻陷導航 ECU。 2) 攻擊者透過偽造藍牙授權指令發送惡意控制訊號。 3) 閘道器 ECU 將惡意訊號轉發給電源開關執行器。 4) 電源開關執行器非預期地關閉頭燈。	近場	中	
	3	1) 攻擊者獲得對 OBD 介面的本機存取權限。 2) 攻擊者從 OBD 介面發送惡意控制訊號。 3) 閘道器 ECU 將惡意訊號轉發給電源開關執行器。 4) 電源開關執行器非預期地關閉頭燈。	本機	低	

…	…	…			

表 16　彙總的攻擊可行性評級(基於「攻擊潛在性」的評價方式)

威脅情境	攻擊路徑分析		威脅情境							彙總攻擊可能性
	編號	攻擊路徑	花費時間	專業知識	所需資訊	機會窗口	設備	總分數	攻擊可行性等級	
攻擊者對 CAN 匯流排發送阻絕服務攻擊，導致車身控制器無法獲取對向車輛訊號，無法觸發遠光燈切換。	1	1) 攻擊者透過蜂巢網路介面攻陷導航 ECU。 2) 攻擊者透過被攻陷的導航 ECU 發送惡意控制訊號。 3) 閘道器 ECU 將惡意訊號轉發給電源開關執行器。 4) 攻擊者用大量高優先權的封包癱瘓 CAN 匯流排通訊。	1	8	7	0	4	20	低	低 *(取攻擊路徑中最高的攻擊可行性評級)*
	2	1) 攻擊者在車輛駐車解鎖時，將一個支援藍牙的 OBD 轉接頭連接到 OBD 介面。 2) 攻擊者透過藍牙介面攻陷駕駛員的智慧型手機。	1	8	7	4	4	24	低	

		3) 攻擊者透過智慧型手機和藍牙 OBD 適配器向閘道器 ECU 發送訊息。 4) 網路 ECU 將惡意資訊轉發給電源開關執行器。 5) 攻擊者用大量高優先權的封包癱瘓 CAN 匯流排通訊。								
…	…	…								

表 17　風險值判定矩陣

衝擊評級	攻擊可行性評分			
	非常低	低	中等	高
嚴重	2	3	4	5
主要	1	2	3	4
中等	1	2	2	3
可忽略	1	1	1	1

表 18　風險值判定結果

威脅情境	彙總的攻擊可行性評級	彙總的損害情境衝擊評級	風險值
攻擊者偽造「頭燈請求」訊號，破壞該訊號資料通訊的完整性，導致前照燈非預期地關閉。	高	嚴重	5

攻擊者對 CAN 匯流排發送阻絕服務攻擊，導致車身控制器無法獲取對向車輛訊號，無法觸發遠光燈切換。	低	中等	2

- RQ-15-15、RQ-15-16 產出文件
  - ■ 風險值(對應 CNS 21434 之 WP-15-07)。
    - ➔ 一、二階文件(手冊/程序書)：無。
    - ➔ 三階文件(作業指導書)：TARA 指引(須包含風險矩陣對應關係、彙總的攻擊可行性評級、彙總之損害情境的衝擊評級，以及風險值判定矩陣)。
    - ➔ 四階文件(範本/表單)：TARA 報告(記錄各威脅情境之最終風險值判定結果)。

15.9 風險處理決定

15.9.1 輸入

15.9.1.1 先決條件

應提供以下資訊：

- 項目定義 CNS 21434 之[WP-09-01]。
- 威脅情境 CNS 21434 之[WP-15-03]。
- 風險值 CNS 21434 之[WP-15-07]。

15.9.1.2 進一步的支援資訊

可考量以下資訊：

- 網路安全規格 CNS 21434 之[WP-10-01]。
- 項目或組件或類似項目或組件之先前風險處理決定。
- 衝擊評級及相關衝擊類別 CNS 21434 之[WP-15-04]。
- 攻擊路徑 CNS 21434 之[WP-15-05]。
- 攻擊可行性評級 CNS 21434 之[WP-15-06]。

15.9.2 要求事項及建議事項

[RQ-15-17]對於每種威脅情境，應考慮其風險值，確定以下 1 或多個風險處理選項：

(a) 迴避風險。

例 1：藉由移除風險來源、判定不開始或繼續產生風險的活動以迴避風險。

(b) 降低風險。

(c) 分擔風險。

例 2：透過契約分擔風險或購買保險進行風險轉移。

(d) 保留風險。

備考：保留風險及分擔風險的理由闡述記錄為網路安全聲明，並依 CNS 21434 第 8 節規定接受網路安全監督及脆弱性管理。

- RQ-15-17 說明

  對於每個威脅情境，應根據其風險值，決定採取以下一種或多種風險處理選項：

  (1) 迴避風險：透過移除風險源，決定不開始或停止進行會產生風險的活動來消除風險的可能性。例如，為應對來自外部網路的入侵威脅，直接在架構上斷開與外部的通訊連線。

  (2) 降低風險：透過對脆弱性採取網路安全控制措施來減少威脅發生的機率或降低安全風險。例如：為防止資料外洩，而實作安全加密演算法。

  (3) 分擔風險：將風險分擔或轉移給其他實體，例如透過合約或協議將風險轉移給供應者或保險公司。需注意並非所有風險皆可轉移。

  (4) 保留風險：若評估風險值的影響較小，無需採取額外的安全措施來降低風險，可直接接受該風險。若選擇保留風險或分擔風險，必須將其理由記錄為網路安全聲明，並依據第 8 節的要求納入持續的網路安全監督與脆弱性管理。因為網路安全風險是動態變化的，若外部環境變化導致風險等級升高，需重新啟

動並調整處置決策。組織內部可根據產品定義與風險容忍度，預先制定針對不同風險值的風險處理原則。

- RQ-15-17 實踐方式

於 TARA 指引中定義風險處理原則，並於 TARA 報告中記錄每個威脅情境的處理決策與理由，如下表範例：

表 18　風險處理原則

風險值	風險處理方法			
	迴避風險	降低風險	分擔風險	保留風險
5	√	√	√	
4	√	√	√	
3	√	√	√	
2	√	√	√	√
1		√		√

表 19　風險處理決定

威脅情境	彙總的攻擊可行性	彙總的衝擊	風險值	風險處理決定	理由
攻擊者偽造「頭燈請求」訊號，破壞資料通訊的完整性，導致前照燈非預期關閉。	高	嚴重	5	降低風險	風險值較高，必須採取控制措施降低風險。
攻擊者對 CAN 匯流排發送阻絕服務攻擊，導致無法獲取對向車輛訊號。	低	中等	2	保留風險	風險值較低，符合組織風險處理原則，保留風險並納入網路安全聲明進

					行日常監控。

- RQ-15-17 產出文件
  - ■ 風險處理決定(對應 CNS 21434 之 WP-15-08)。
    - ➔一、二階文件(手冊/程序書)：無。
    - ➔ 三階文件(作業指導書)：TARA 指引(須定義風險處理原則)。
    - ➔四階文件(範本/表單)：風險處理決定表(須記錄每個威脅情境，其選擇使用迴避、降低、分擔或保留風險之處理決定)及網路安全聲明(若選擇分擔或保留風險之處理決定，提供理由與相關假設)。