道路車輛網路安全工程產業指引
第 2 部：產品生命週期之網路安全活動

Industrial guideline for road vehicles cybersecurity engineering
Part 2: product lifecycle cybersecurity activities

(TTVMA IG-002:2026)

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 9 節至第 14 節，內容為針對產品生命週期之網路安全活動，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 9 節至第 14 節之相關要求、建議及許可事項，提供實踐指引。

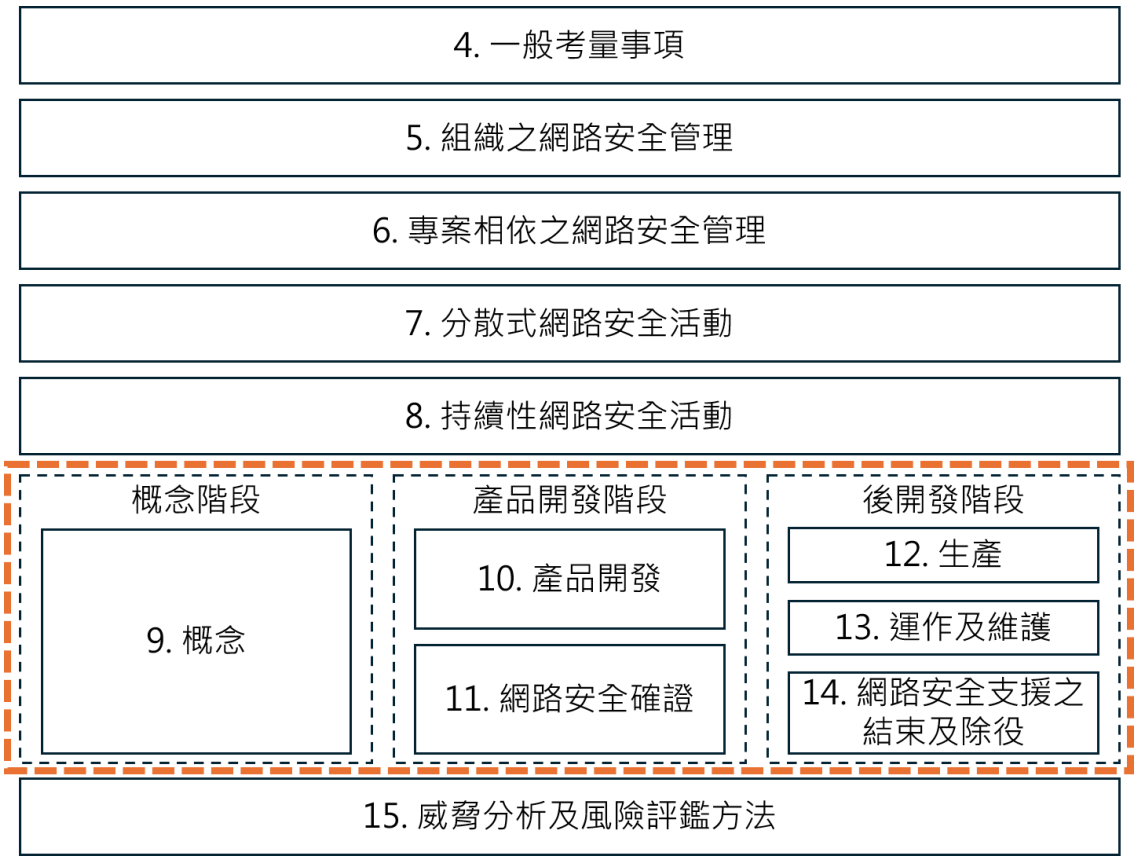

圖 1　CNS 21434 架構概觀

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 9 節至第 14 節之實踐指引

第 9 節 概念

9.1 一般

本概念階段涉及考量於項目中實作之車輛級功能。於本節中，此項目及其運作環境被識別為〝項目定義〞(參照 CNS 21434 第 9.3 節)。項目定義構成後續活動的基礎。

本節亦規定此項目之網路安全目標(參照 CNS 21434 第 9.4 節)，此是最高等級的要求事項。為此，需藉由使用 CNS 21434 第 15 節的方法以評鑑網路安全風險，(另參照 CNS 21434 附錄 H，圖 H.1)。此外，CNS 21434 第 9.4 節亦規定網路安全聲明，用於解釋風險保留或共享被認為係適足。

網路安全概念(參照 CNS 21434 第 9.5 節)係由網路安全要求事項及運作環境要求事項所組成，兩者均源自網路安全目標並基於對此項目的全面看法。

9.2 目的

本節目的為：

(a) 定義此項目、其運作環境及於網路安全全景下的互動。

(b) 規定網路安全目標及網路安全聲明。

(c) 規定網路安全概念以達到網路安全目標。

9.3 項目定義

9.3.1 輸入

9.3.1.1 先決條件

無

9.3.1.2 進一步的支援資訊

可考量以下資訊：

– 有關此項目及運作環境的既有資訊。

例：車載 E/E 系統架構，包含車載網路、車輛外部網路。參考模型及早期開發之文件。

9.3.2 要求事項及建議事項

[RQ-09-01]應識別此項目之以下資訊：

(a)項目邊界。

備考 1：項目邊界將項目與其運作環境區別。項目邊界的描述可包含與車輛內部的其他項目及/或與車輛外部之 E/E 系統介面。

(b)項目功能。

備考 2：描述項目於生命週期階段之預期行為[例：產品開發(測試)、生產、運作及維護、除役(報廢)]並包含由此項目實現之車輛功能。

(c)初步架構。

備考 3：初步架構的描述可包含項目中組件及其連接的識別，以及項目之外部介面。

備考 4：CNS 21434 中描述的項目定義，特別是項目邊界，可能與其他行為規範之項目定義不同，例：符合 ISO 26262 系列標準之功能性人身設備安全。

備考 5：可考量有關限制及適用網路安全標準的資訊。

備考 6：全景外組件(參照 CNS 21434 第 6.4.5 節)之開發可基於假設(通用)項目的定義及項目內組件功能的描述。

- RQ-09-01 說明
  1. 項目：在車輛層級實現某一功能的單個組件，或組件的集合。例如：車門控制功能涉及一個車門 ECU (Electronic Control Unit，電子控制單元)單個組件；OTA (Over-the-Air，空中下載)升級功能則涉及 OTA 平台、更新主控節點以及被更新 ECU 等多個組件。項目是網路安全風險評鑑的對象，主要包含項目邊界、項目功能以及初步架構。
  2. 項目邊界：用於劃分研究對象與運作環境的界限，明確內部與外部介面，例如車輛內部其他項目、車輛外部 E/E (Electrical/ Electronic，電子與電機)系統，這是後續 TARA 中，識別介面相關威脅情境的基礎。
  3. 項目功能：項目是按車輛級功能範疇進行劃分，功能涵蓋產品的全生命週期。例如產品開發與生產階段的韌體燒錄；營運階段的 OTA 升級與診斷服務；除役(報廢)階段的個人資料清除等。

4. 初步架構：識別項目的組件、組件之間的連接方式以及外部介面。

- RQ-09-01 實踐方式

  併同[RQ-09-02]進行闡述。

- RQ-09-01 產出文件

  併同[RQ-09-02]進行闡述。

[RQ-09-02]應描述與網路安全相關項目之運作環境資訊。

備考 7：運作環境的描述及其與項目的互動，可識別及/或分析相關的威脅情境及攻擊路徑。

備考 8：相關資訊可包含假設，例：假設此項目所依賴的每個公開金鑰基礎設施(PKI)憑證機構(CA)都得到適當的管理。

- RQ-09-02 說明

  1. 運作環境：項目之運作環境是網路安全威脅的載體，項目與環境之互動則是攻擊的「通道」。必須先明確項目在何種環境運作以及如何與環境互動，才能精準找出潛在的威脅情境與攻擊路徑。
  2. 網路安全假設：對無法完全查證，但符合產業規範或設計邏輯的安全前提作出明確判斷。假設並非憑空猜測，而是基於產業標準、供應商能力或技術實現的可信前提。 明確的假設有助於聚焦核心風險、界定安全責任範圍，並減少 TARA 中不必要的工作量。此外，網路安全假設需納入持續性網路安全活動(參照 CNS 21434 第 8 節)中進行監控，以判斷其是否持續有效。

- RQ-09-01、RQ-09-02 實踐方式

  以 CNS 21434 附錄 H.2 的「頭燈系統」為例進行項目定義：

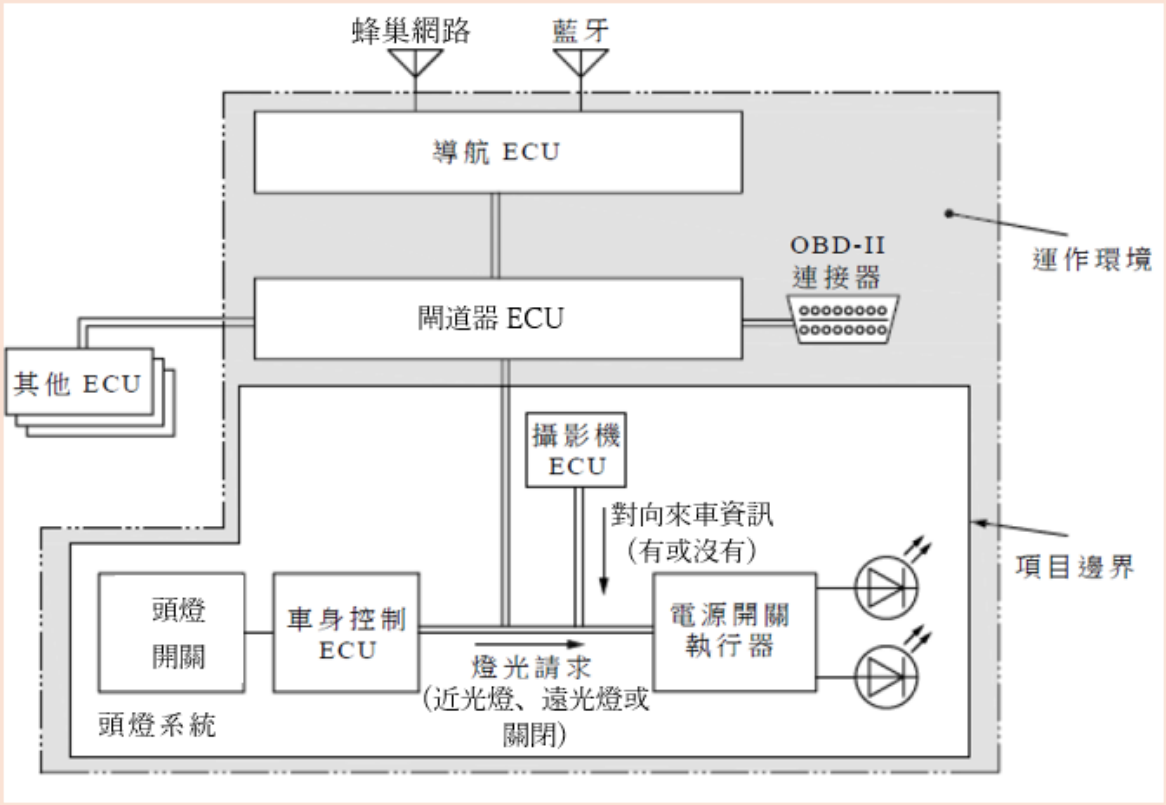

圖 1　CNS 21434 附錄 H.2 頭燈系統項目範例

1. 定義項目邊界與運作環境：劃分項目與運作環境。運作環境為項目邊界以外的部分，例如包含與項目連接的閘道器 ECU (Gateway ECU)及導航 ECU。其中導航 ECU 包含藍牙和蜂巢網路的外部介面，閘道器 ECU 包含 OBD 外部介面，ECU 之間透過車載網路(如 CAN)通訊相連。
2. 定義項目功能：例如駕駛員可透過開關直接控制頭燈；遠光燈開啟時若偵測到對向來車，則自動切換為近光燈；對向車駛離後自動切回遠光燈。
3. 繪製初步架構：識別相關組件，如攝影機 ECU(感知對向車輛)、頭燈開關(駕駛員手動控制)、車身控制 ECU(保留訊號並輸出燈光控制請求)、電源開關執行器(執行遠近光切換)，並標示資料流向(如對向車存在與否的訊號及燈光控制指令)。
4. 制定網路安全假設：組織根據自身產品特性與實務經驗制定，並需明確假設的依據及適用邊界。例如：
   (1)當前業界共識安全的密碼學演算法、方案與通訊協定，目前無法被直接破解。

(2)開發由可信賴的人員進行，即建立的韌體是可信的。

(3)LIN (Local Interconnect Network，區域互聯網路)匯流排僅傳輸非安全、非關鍵資料，且依附於主節點(如 CAN)的安全防護，暫不考量對其進行額外防護。

- RQ-09-01、RQ-09-02 產出文件
  - ■ 項目定義(對應 CNS 21434 之 WP-09-01)。
    - ➔一、二階文件(手冊/程序書)：無。
    - ➔三階文件(作業指導書)：項目定義作業指導書。
    - ➔四階文件(範本/表單)：項目定義範本(內含項目邊界、功能、架構、運作環境描述與網路安全假設)。

9.4 網路安全目標

9.4.1 輸入

9.4.1.1 先決條件

應提供以下資訊：

ー 項目定義[WP-09-01]。

9.4.1.2 進一步的支援資訊

可考量以下資訊：

ー 網路安全事件[WP-08-03]。

9.4.2 要求事項及建議事項

[RQ-09-03]應履行基於項目定義的分析，其中涉及：

(a)依 CNS 21434 第 15.3 節之資產識別。

(b)依 CNS 21434 第 15.4 節之威脅情境識別。

(c)依 CNS 21434 第 15.5 節之衝擊評級。

(d)　依 CNS 21434 第 15.6 節之攻擊路徑分析。

(e)依 CNS 21434 第 15.7 節之攻擊可行性評級。

(f) 依 CNS 21434 第 15.8 節判定之風險值。

備考 1：若項目定義沒有為分析提供充足的資訊，則可使用假設資訊。

- RQ-09-03 說明

  參照 CNS 21434 第 15 節。

- RQ-09-03 實踐方式

  參照 CNS 21434 第 15 節。
- RQ-09-03 產出文件
  - TARA(對應 CNS 21434 之 WP-09-02)，併同 [RQ-09-06]進行闡述。

[RQ-09-04]依[RQ-09-03]的結果，應依 CNS 21434 第 15.9 節判定每種威脅情境之風險處理選項。

備考 2：依變更管理，藉由消除風險來源以避免風險可能會導致項目發生變更(參照 CNS 21434 第 5.4.4 節)。

- RQ-09-04 說明
  1. 依據[RQ-09-03]透過 TARA 分析得出每個威脅情境的風險值後，組織應根據該風險值做出對應的處理決定。
  2. 處理決定的選項主要包含迴避、降低、分擔及保留，以下進行說明：
     (1) 迴避風險：即移除風險產生的根本原因，例如更換硬體架構、取消某項高風險功能等。此類決定往往會帶來設計上的變更，這種變更不能隨意進行，必須遵循組織本身的變更管理流程。
     (2) 降低風險：即透過技術或管理手段(如導入加密演算法、防火牆等)降低風險發生的機率，或減輕風險造成之影響，將風險值降到可接受的範圍內。
     (3) 分擔風險：即透過合約、協議等方式，將風險的責任與管控義務分擔給有能力的第三方(如供應商、保險公司等)，組織自身不再直接承擔該風險的主要責任。
     (4) 保留風險：即評估後認為風險處於可接受範圍，無需採取額外的防護措施，直接承受該風險。
- RQ-09-04 實踐方式

1. 在組織內部的 TARA 指引中，必須明確定義風險處理原則，以指導工程師在面對不同風險等級時，能做出一致的相關風險處理決定。舉例如下表的對應矩陣：

表 1　風險處理原則

風險等級	風險處理原則
嚴重或高	風險迴避/降低/分擔
中	風險迴避/降低/分擔
低或非常低	風險迴避/降低/分擔/保留

- RQ-09-04 產出文件
  - TARA(對應 CNS 21434 之 WP-09-02)，併同 [RQ-09-06]進行闡述。

[RQ-09-05]若威脅情境的風險處理決定包含降低風險，則應規定 1 或多個對應之網路安全目標。

備考 3：網路安全目標係保護資產免受威脅情境的要求事項。

備考 4：若適用，可為網路安全目標判定 CAL(參照 CNS 21434 附錄 E)。

備考 5：可為項目的任何生命週期階段規定網路安全目標。

- RQ-09-05 說明
  1. 針對某一具體的網路威脅情境，若風險處理決定選用降低風險，則必須制定一個或多個對應的網路安全目標。一般網路安全目標的描述方式示例為：保護[某資產]的[某網路安全性質]。
  2. 組織可視需要，針對網路安全目標設定 CAL(Cybersecurity Assurance Level，網路安全保證等級)。藉由導入 CAL 等級，可為網路安全目標增加可量化的允收準則，以利後續查證與確證風險緩解措施之有效性。惟依據 CNS 21434，CAL 之應用屬可選擇(非強制性)項目。
- RQ-09-05 實踐方式
  1. 在 TARA 的範本中，如果選用降低風險的風險處理決定，直接在表中生成對應的網路安全目標。

表 2　TARA 網路安全目標

資產	網路安全性質	…	風險值	處理決定	網路安全目標
CAN 通訊訊息	可用性		高	降低	保護 CAN 通訊訊息的可用性

- RQ-09-05 產出文件
  - ■ 網路安全目標(對應 CNS 21434 之 WP-09-03)，併同[RQ-09-06]進行闡述。

[RQ-09-06]若威脅情境的風險處理決定包含：

(a)分擔風險。

(b)因[RQ-09-03]分析期間使用的 1 或多項假設而保留風險，則應規定 1 或多項對應的網路安全聲明。

備考 6：網路安全聲明可考量用於網路安全監督。

- RQ-09-06 說明
  1. 針對某一具體的網路威脅情境，若風險處理決定選用分擔風險或保留風險，則必須制定一個或多個對應的網路安全聲明。
  2. 網路安全聲明並非「無條件」地接受風險，而是必須基於特定條件對風險進行保留。

     例如：基於組織的風險處理原則，該風險值被評定為低，因此接受該風險。

     例如：基於車載區域互聯網路(如 LIN)其技術本質僅用於傳輸車窗、雨刷等非安全且非關鍵功能的資料，且其運作環境以依賴於主系統既有的安全防護假設(如 CAN)，在評估其影響極低的前提下，組織可決定接受並保留此風險。
  3. 由於網路安全風險是持續動態變化的，因此網路安全聲明也必須納入 CNS 21434 第 8 節的網路安全監督活動中，以定期評估該網路安全聲明與前提假設是否持續有效。
- RQ-09-06 實踐方式

1. 在 TARA 的範本中，如果選用分擔或保留風險的風險處理決定，直接在表中生成對應的網路安全聲明。

表 3　TARA 網路安全聲明

資產	網路安全性質	…	風險值	處理決定	網路安全聲明
CAN 通訊訊息	完整性		低	保留	基於風險處理原則，該風險值極低，接受該風險

- RQ-09-03、RQ-09-04、RQ-09-05、RQ-09-06 產出文件
  - ■ 網路安全聲明(對應 CNS 21434 之 WP-09-04) 。
    - ➔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)：TARA 指引(參考車輛公會公告之「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」，須包含資產識別、威脅情境識別、衝擊評級、攻擊路徑分析、攻擊可行性評級、風險值判定及風險處理決定之執行方法，以及網路安全目標訂定方式、CAL 判定基準、風險分擔或保留之網路安全聲明撰寫規範)。
    - ➔四階文件(範本/表單)：TARA 報告(參考車輛公會公告之「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」，記錄各威脅情境之最終風險值判定結果，以及風險處理決定、威脅情境對應之網路安全目標與 CAL 等級、風險分擔或保留之理由與相關假設)。

[RQ-09-07]應履行查證以確認：

(a) 關於項目定義[RQ-09-03]之結果的正確性(correctness)及完整性(completeness)。

(b) 關於[RQ-09-03]結果之[RQ-09-04]的風險處理決定的完整性、正確性及一致性(consistency)。

(c) 關於[RQ-09-04]的風險處理決定之[RQ-09-05]的網路安全目標及[RQ-09-06]的網路安全聲明的完整性、正確性及一致性。

(d)此項目的所有網路安全目標[RQ-09-05]及網路安全聲明[RQ-09-06]的一致性。

- RQ-09-07 說明
  1. 必須執行相關的查證活動，以確認項目定義、風險評鑑、處理決定、網路安全目標和網路安全聲明之間達到準確、完整且具追溯性的邏輯一致性，避免出現邏輯漏洞、資訊錯誤與前後矛盾。查證的方式可採用如文件審查。
  2. 針對(a)項目與風險評鑑的查證：
     (1) 正確性：風險評鑑的結論是否確實符合實際的威脅情境與資產特徵。
     (2) 完整性：所有資產是否被完整識別，有無遺漏。
  3. 針對(b)風險評鑑與處理決定的查證：
     (1) 正確性：是否所有被識別出的風險點，都已指定了對應的風險處理決定。
     (2) 完整性：處理決定是否與風險的等級相匹配。
     (3) 一致性：決定邏輯和分析結果之間是否存在衝突。
  4. 針對(c)處理決定與目標/聲明的查證：
     (1) 完整性：是否所有的風險處理決定都有產生對應的網路安全目標或網路安全聲明。
     (2) 正確性:產出的目標或聲明是否與組織訂定的風險處理原則相符。
     (3) 一致性：目標或聲明的內容方向，是否與處理決定的方向一致。
  5. 針對(d)目標與聲明之間的查證：
     一致性：例如，針對同一個威脅情境的風險處理決定，不能出現既有網路安全目標又有網路安全聲明，這種自相矛盾的表述。
- RQ-09-07 實踐方式
  1. 在 TARA 的查證執行過程中，應依據上述要求，逐項進行審查。

表 4　TARA 查證範本

查證內容	審查結果	發現之問題項	負責人
風險評鑑結果與對應的項目之間，是否具備正確性	[通過/不通過]		
風險評鑑結果與對應的項目之間，是否具備完整性	[通過/不通過]		
….			

- RQ-09-07 產出文件
  - ■ 網路安全目標查證報告(對應 CNS 21434 之 WP-09-05) 。
    - ➔一、二階文件(手冊/程序書)：無。
    - ➔三階文件(作業指導書)： TARA 查證指引。
    - ➔四階文件(範本/表單)：TARA 查證報告。

9.5 網路安全概念

9.5.1 輸入

9.5.1.1 先決條件

應提供以下資訊：

- 項目定義[CNS 21434 之 WP-09-01]。
- 網路安全目標[CNS 21434 之 WP-09-03]。
- 網路安全聲明 [CNS 21434 之 WP-09-04]。

9.5.1.2 進一步的支援資訊

可考量以下資訊：

- TARA [CNS 21434 之 WP-09-02]。

9.5.2 要求事項及建議事項

[RQ-09-08]應描述技術及/或運作網路安全控制措施與其為達到網路安全目標而進行的互動，同時考量：

(a) 項目之功能間的依賴性。

(b)網路安全聲明。

備考 1：描述可包含：

– 達成網路安全目標的條件，例：預防洩漏、偵測及監督洩漏，

– 專門用於因應威脅情境的特定層面功能，例：使用安全的通訊通道。

備考 2：此描述可用於評估設計並判定網路安全確證的目標。

- RQ-09-08 說明
  1. 網路安全控制措施是指用於修正風險值的措施。為了實現網路安全目標，將風險值降低到可接受範圍內，必須定義技術性及/或操作性層面的控制措施。
     (1) 技術層面：安全啟動(Secure Boot)、防火牆、安全通訊協定等。
     (2) 操作層面：如漏洞修復機制、安全日誌審查、人員安全培訓等
  2. 考量相依性與聲明，說明如下：
     (1) 項目之功能間的依賴性：指安全措施生效或執行所需的前置條件或配套功能。例如：建立加密通道依賴於金鑰管理功能。
     (2) 網路安全聲明：用於明確該安全控制措施能達成的安全目標範圍或前提假設。
  3. 這些安全控制措施的描述可作為設計審查的依據，以驗證網路安全設計是否充分，同時作為 CNS 21434 第 11 節的基準。
- RQ-09-08 實踐方式
  - ■ 併同[RQ-09-10]進行闡述。
- RQ-09-08 產出文件
  - ■ 併同[RQ-09-10]進行闡述。

[RQ-09-09]網路安全目標應依[RQ-09-08]的描述，定義此項目之網路安全要求事項及運作環境要求事項。

備考 3：網路安全要求事項可取決或包含項目之特定功能，例：更新能力或於運作期間獲得使用者同意的能力。

備考 4：運作環境的要求事項可於項目外實現，但須包含於項目之網路安全確證中，以確認是否達成相對應的網路安全目標。

備考 5：作為運作環境一部分之其他項目的要求事項， 可為該等項目之網路安全要求事項。

- RQ-09-09 說明
  1. 基於[RQ-09-08]對控制措施的描述，需進一步定義具體的網路安全要求事項。這讓網路安全目標從抽象概念轉變為可執行、可查證的規則。
  2. 網路安全要求可以是針對項目本身的需求，例如 ECU 應具備安全啟動功能、ECU 應安全儲存金鑰等；也可以是針對運作環境的需求，例如診斷儀應具備權限管理功能、雲端伺服器應安全儲存金鑰等。
- RQ-09-09 實踐方式
  - ■ 併同[RQ-09-10]進行闡述。
- RQ-09-09 產出文件
  - ■ 併同[RQ-09-10]進行闡述。

[RQ-09-10]應配置於項目之網路安全要求事項，若適用，亦應配置於 1 或多個組件。

備考 6：網路安全控制措施的描述補充網路安全要求事項及運作環境要求事項 之規格及配置，其全部併同構成網路安全的概念。

- RQ-09-10 說明
  1. 網路安全要求事項的實現需依託於具體的產品，因此應分配給項目，以及其下的一個或多個組件。例如在車輛級，將要求分配給特定的 ECU；在 ECU 層級，則分配給特定的軟硬體組件模組。
  2. 網路安全控制措施描述的是做什麼(What)，網路安全要求事項描述的是如何做(How)，兩者與運作環境要求共同構成了完整的網路安全概念。
- RQ-09-10 實踐方式
  1. 應將目標、控制措施、具體要求與分配對象進行對應，如表 5 範例。

表 5　網路安全概念

網路安全目標	網路安全控制措施	網路安全要求事項	需求分配
保護 OTA 升級封包的機密性	採用加密通道	車端與雲端平台的連線應採用 TLS 1.2 以上之安全通訊協定	雲端平台/T-Box

- RQ-09-08、RQ-09-09、RQ-09-10 產出文件
  - ■ 網路安全概念 (對應 CNS 21434 之 WP-09-06)。
    - ➔一、二階文件(手冊/程序書)：無。
    - ➔三階文件(作業指導書)：網路安全概念流程(須包含網路安全控制措施描述方式、網路安全要求事項與運作環境要求事項之定義方法、以及要求事項配置至組件之規則)。
    - ➔四階文件(範本/表單)：網路安全概念報告(記錄技術與運作控制措施描述、網路安全要求事項清單、運作環境要求事項、及各要求事項對應之組件配置結果)。

[RQ-09-11]應查證[RQ-09-08]、[RQ-09-09]及[RQ-09-10]的結果，以確認：

(a) 關於網路安全目標的完整性、正確性及一致性。

(b) 關於網路安全聲明之一致性。

- RQ-09-11 說明
  1. 必須執行相關的查證活動，以確認網路安全控制措施、網路安全要求事項以及需求分配之間形成準確、完整且具追溯性的邏輯一致性，避免出現邏輯漏洞、資訊錯誤或前後矛盾。查證的方式通常採用文件審查。
  2. 針對網路安全目標，查證需涵蓋三大面向：
     (1) 一致性：確認網路安全目標、控制措施、要求事項以及需求分配之間沒有衝突，邏輯前後連貫。

(2)完整性：確認所有的網路安全目標都已被涵蓋與處理，沒有遺漏。

(3)正確性：確認對應的網路安全控制措施和要求事項是合理的，且在技術上確實能夠達成對應的網路安全目標。

3. 網路安全聲明的一致性：網路安全聲明本質上是對風險的保留，因此無須為其產生相對應的網路安全控制措施及要求事項。

- RQ-09-11 實踐方式

1. 應將目標、控制措施、具體要求與分配對象進行對應，如表 6 範例。

表 6　網路安全概念查證報告

查證內容	審查結果	發現之問題項	負責人
網路安全控制措施與對應的網路安全目標，是否具備一致性	[通過/不通過]		
網路安全控制措施與對應的網路安全目標，是否具備完整性	[通過/不通過]		
….			

- RQ-09-11 產出文件

■ 網路安全概念查證報告(對應 CNS 21434 之 WP-09-07) 。

➔一、二階文件(手冊/程序書)：無。

➔三階文件(作業指導書)：網路安全概念查證指引。

➔四階文件(範本/表單)：網路安全概念查證報告。

第 10 節 產品開發

10.1 一般

本節描述網路安全要求事項及架構設計的規格(參照 CNS 21434 第 10.4.1 節)。此外，本節描述整合及查證活動(參照 CNS 21434 第 10.4.2 節)。

此等網路安全活動會反覆履行，直至不需進一步精細化網路安全控制措施。

網路安全規格係經由查證活動定義及確認，以實現網路安全概念。

CNS 21434 圖 9 說明產品開發活動如何適用基於 V 模型之工作流程示例，其中 CNS 21434 第 10.4.1 節對應於 V 模型的左側，第 10.4.2 節對應於右側。在此例中，在項目級下假設有兩個抽象(概念)層，即組件級及子組件級。此工作流程可擴展至涵蓋任何之抽象(概念)級。

可適用與 V 模型不同的開發方式或方法(例：敏捷式軟體開發)。

CAL 可用於衡量本節中活動的深度及嚴謹度，亦可用於此等活動的方法(參照 CNS 21434 附錄 E)。

10.2 目的

本節目的為：

(a) 定義網路安全規格。

備考 1：可包含現有架構設計中不存在的網路安全相關組件的規格。

(b) 查證定義的網路安全規格是否符合更高級的架構抽象(概念)的網路安全規格。

(c) 識別組件的弱點。

備考 2：CNS 21434 第 8 節描述脆弱性分析及管理。

(d) 提供證據以證明組件的實作及整合之結果符合網路安全規格。

10.3 輸入

10.3.1 先決條件

應提供以下資訊：

- 來自更高級架構抽象(概念)之網路安全規格 CNS 21434 之[WP-10-01]。

備考 1：可能限定於正在開發組件相關之資訊，例：

- 配置於正在開發組件之網路安全要求事項。
- 正在開發組件之外部介面規格。
- 關於正在開發組件的運作環境之假設資訊。

備考2:對於最高級架構抽象(概念)的開發,使用項目之網路安全概念CNS 21434 之[WP-09-06]及項目定義 CNS 21434 之[WP-09-01],而非更高級的架構抽象(概念)網路安全規格。

10.3.2 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]。
- 網路安全概念 CNS 21434 之[WP-09-06]。
- 既有之架構設計。
- 已經建立之網路安全控制措施。
- 再利用的組件中已知之弱點及脆弱性。

10.4 要求事項及建議事項

10.4.1 設計

[RQ-10-01]網路安全規格之定義應基於:

(a)來自更高級架構抽象(概念)之網路安全規格。

(b)選擇實作之網路安全控制措施(若適用)。

例1:使用具有嵌入式硬體信任錨之個別微控制器,實現安全金鑰儲存功能並隔離非安全外部連接之信任錨。

備考1:網路安全控制措施可從受信任的型錄中選擇。

(c)既有之架構設計(若適用)。

備考2:網路安全規格包含與履行已定義網路安全要求事項相關之已定義架構設計相關子組件間的介面規格,包含其使用、靜態及動態層面。

備考3:定義網路安全規格時,可考量後開發階段之網路安全內涵,例:金鑰儲存的安全管理、停用除錯介面、刪除個人可識別資訊之程序。

備考 4：網路安全規格可包含與滿足網路安全要求事項相關之組態及校準參數的識別，以及其設定或允許值範圍，例：硬體安全模組整合之正確組態。

備考 5：可考量實作網路安全控制措施所需組件之能力，例：處理器效能、記憶體資源。

- RQ-10-01 說明

1. 定義網路安全規格時，應基於較高層級架構抽象(概念)，即高階架構概念設計的網路安全規格。系統設計時，應先遵循高層級架構之要求，再逐層向下分解與細化具體規格，以避免底層規格與頂層架構產生衝突。例如，ECU 的網路安全規格需基於車輛級的規格，而 ECU 內部組件之規格，則需基於系統層級之網路安全規格。
2. 網路安全控制措施選用：擬實施的網路安全控制措施，建議優先從產業標準的可信清單中選取(如 NIST SP 800-53 安全控制清單或 UNECE R155 附錄 5 的威脅緩解措施)。
3. 制定網路安全規格時，應考量既有硬體、軟體及模組架構之特性與限制。在制定安全規格時應結合既有硬體的特點(例如該 MCU 是否帶有硬體安全模組 HSM 或加密硬體加速器)，來選擇適合的輕量級密碼學演算法，避免算力不足而導致車輛功能嚴重延遲。
4. 網路安全規格應詳細描述具體要求事項的實作過程，可包含：
   (1)涉及的密碼學演算法及其長度和類型；
   (2)透過相關靜態/動態視圖說明其實作過程；
   (3)涉及的組態和校準參數(包含其設定值或允許的數值範圍)；
   (4)為實現網路安全功能所需之非功能性要求(如處理器效能、記憶體資源等)。
   (5)若部分網路安全機制的實作發生在後開發階段(如生產、運作與維護或除役)，應考量後開發階段的網路安全規範。

- RQ-10-01 實踐方式

併同[RQ-10-03]進行闡述。

- RQ-10-01 產出文件

  併同[RQ-10-03]進行闡述。

[RQ-10-02]定義的網路安全要求事項應配置於架構設計之組件。

- RQ-10-02 說明

  網路安全規格中的網路安全要求事項，應分配至架構設計中的具體組件(如硬體、作業系統、HSM 模組等)以落實相關要求。
- RQ-10-02 實踐方式

  併同[RQ-10-03]進行闡述。
- RQ-10-02 產出文件

  併同[RQ-10-03]進行闡述。

[RQ-10-03]若適用，應規定組件開發後確保網路安全之程序。

例 2：正確整合及初始化網路安全措施，並於整個生產過程中維護網路安全之程序。

- RQ-10-03 說明

  1. 組件開發完成後，仍須制定專門之程序，以確保其後續在生產、部署、運作、維運或除役等後開發階段，持續維持網路安全。在適用情況下，應制定相關程序，包含網路安全控制措施的正確整合與初始化程序，於整個生產階段持續保障網路安全。
  2. 以每一裝置配置唯一金鑰為例，若產線初始化程序定義不當或隨機性不足，可能導致不同裝置產生相同密鑰，進而產生網路安全風險，因此，應透過適當的整合與初始化程序，確保密鑰配置之唯一性及安全性。
- RQ-10-01、RQ-10-02、RQ-10-03 實踐方式

  研發團隊應將網路安全規格文件化，並清晰定義每項方案之細節與分配，如表 7 範例：

表 7　網路安全規格報告

XX ECU 網路安全規格	
方案名稱	001 安全啟動
對應網路安全要求	ECU 韌體應採取安全啟動驗證完整性
分配對象	HSM 模組
詳細方案描述	安全啟動的時序：XXXX 相關的時序圖、架構圖如下：XXX
實施階段	研發階段
備註	…

- RQ-10-01、RQ-10-02、RQ-10-03 產出文件
  - ■ 網路安全規格(對應 CNS 21434 之 WP-10-01)、後開發網路安全要求事項(對應 CNS 21434 之 WP-10-02)。
    - ➔一、二階文件(手冊/程序書)：無。
    - ➔三階文件(作業指導書)：網路安全開發作業指導書(內含網路安全規格定義方法、控制措施選用規則、要求事項配置至組件之規則、後開發階段網路安全程序之定義規則)
    - ➔四階文件(範本/表單)：網路安全規格報告(記錄各方案名稱、對應要求事項、分配對象、詳細方案描述及實施階段，並包含後開發階段各組件須執行之網路安全程序要求)。

[RQ-10-04]若使用之設計、建模或程式設計記法或語言用於網路安全規格或實作，則在選擇記法或語言時應考量以下因素：

(a)語法及語義上明確且易於理解的定義。

(b)支援達到模組化、抽象(概念)及封裝。

(c) 支援使用結構化之建構。

(d)支援安全設計及實作技術之使用。

(e)整合既有組件之能力。

例 3：使用另一種語言編寫的函式庫、框架、軟體組件。

(f) 針對因語言使用不當而導致脆弱性之韌性。

例 4：針對緩衝區溢位之韌性。

備考 6：針對軟體開發，實作包含使用程式設計語言編撰程式碼。

- RQ-10-04 說明

1. 執行網路安全相關開發活動(如架構設計、威脅建模、程式設計)時，選擇語言或符號應遵循系統性準則。網路安全並非事後附加之功能，而應自設計規格階段就內建於系統與軟體的核心屬性中。在設計決策時選對工具和程式設計語言，是實現該目標的基礎保障。
2. 針對[RQ-10-04] (a)到(f)之考量面向，以下進行說明：
   (1)針對(a)：避免因語言定義模糊，導致開發人員產生理解偏差，進而編寫出帶有安全漏洞的程式碼。設計階段應選擇具有明確語法與語意定義之語言，以降低誤解與實作偏差之風險。
   (2)針對(b)：藉由模組化將系統分解為職責單一、獨立性較高、依賴性較低的獨立單元; 透過抽象(概念)隱藏複雜的實作細節，僅揭露必要的介面，以降低攻擊面，防止攻擊者未授權操作內部狀態之風險。透過封裝限制對內部資料的直接存取，是維護資料完整性、防止非法竄改之關鍵機制。
   (3)針對(c)：結構化建構指順序、選擇、迴圈及明確之函式或方法呼叫，應避免或建議審慎使用無條件跳轉語句(如 goto 等)。結構化程式碼具備較佳之可讀性、可分析性、可測試性與可維護性，有助於早期發現邏輯錯誤與網路安全缺陷。
   (4)針對(d)：設計階段應選擇能適配防禦性程式設計、輸入驗證、邊界檢查等安全技術的語言，優先選擇預設安全(Secure by default)的語言(例如利用 Java 的垃圾回收機制來避免記憶體管理錯誤)。
   (5)針對(e)：須考量與使用其他語言編寫之函式庫(Library)、框架、軟體組件、中介軟體或作業系統 API(包含既有程式碼 Legacy code)之互動與整合能力，以減少因重複開發而衍生的漏洞風險。
   (6)針對(f)：設計時宜優先選擇容錯性強之語言。相較於 C、C++等允許直接操作記憶體的語言，Python、Java 等高階語言通常具備受管理執行環境、自動記憶體管理及邊界檢查等機制，可降低緩衝區溢位(Buffer overflow)及其他記憶體安全問題等常見脆弱性。

- RQ-10-04 實踐方式

  併同[RQ-10-05]進行闡述。
- RQ-10-04 產出文件

  併同[RQ-10-05] 進行闡述。

[RQ-10-05]適用於網路安全之設計、建模或程式設計語言的準則(參照[RQ-10-04])，若語言本身無法闡明，則應由設計、建模及編碼指導綱要或開發環境保護。

例 5：使用 MISRA C:2012 或 CERT C 於〝C〞程式設計語言中進行安全編碼。

例 6：適用於設計、建模及程式設計語言之準則：

- 語言子集合之使用。
- 強型式之實施。
- 使用防禦實作技術。

- RQ-10-05 說明

  1. 本項要求為[RQ-10-04]之補充。當所選用之程式設計語言(如 C 語言)本身存在安全侷限，或建模工具無法完整涵蓋[RQ-10-04]所列之安全準則時，應採取額外保障措施，透過適當之設計、建模或編碼指導綱要，以及開發環境設定加以補足。相關措施可包含限制使用語言子集、實施強型別化及導入防禦性實作技術；於使用 C 語言時，可採用或遵循 MISRA C、CERT C 或其他適用之公認安全編碼規範等產業權威規範。
  2. 針對開發環境，要求利用工具鏈自動或半自動地檢查並執行[RQ-10-04]的準則(如導入靜態程式碼分析工具、動態測試工具等)。
- RQ-10-04、RQ-10-05 實踐方式

  1. 組織應依以下三個階段落實網路安全相關開發活動：

     (1)設計與建模：制定系統性策略，明確規範專案選用之程式設計語言或建模工具，並依據[RQ-10-04] (a)至(f)所列因素進行評估，確保其支援安全設計與實作。

(2)實作階段：依據 RQ-10-05，當所選語言或工具本身無法完整涵蓋 RQ-10-04 所定義的準則時，應為每種語言和工具採納公認的安全指南(如 MISRA C 或 CERT C)，並將其轉化為組織內部的「安全編碼規範」作為編碼指導綱要。

(3)查證階段：在 CI/CD 流程或開發環境中，整合靜態程式碼分析工具或動態測試工具，以強制檢查並驗證 RQ-10-04 所定義的語言選用準則及 RQ-10-05 所採納的安全編碼規範之執行狀況。

- RQ-10-04、RQ-10-05 產出文件
  - ■ 產生之建模、設計或程式設計語言及編碼指導綱要(對應 CNS 21434 之 WP-10-03)。
    - ➔一、二階文件(手冊/程序書)：無。
    - ➔三階文件(作業指導書)：網路安全開發作業指導書(內含語言與工具選用準則、安全編碼規範採納規則)。
    - ➔四階文件(範本/表單)： 網路安全編碼規範(記錄組織內部採納之安全編碼規範，如 MISRA C 或 CERT C 的適用規則與例外處理方式)。

[RC-10-06]宜建立可信之設計及實作原則，以避免引入弱點或將弱點最小化。

備考 7：網路安全架構設計的設計原則，例：NIST Special Publication 800-160 Vol. 1 之附錄 F.1。

- RC-10-06 說明
  1. 採用產業公認、經過實務檢驗的安全設計原則，涵蓋架構設計與程式碼實作，從源頭設計端避免和減少弱點的引入。
  2. 依據所建議之參考 NIST SP 800-160 Vol.1 系統可信安全設計原則，可導入如最小權限原則、縱深防禦、清晰的抽象(概念)與介面等，將安全性內建於系統架構中。
- RC-10-06 實踐方式

在架構設計審查階段，宜從網路安全的維度考量相關的安全設計原則，並透過檢核表逐一確認架構是否符合這些防禦理念。

- RC-10-06 產出文件
  - ➔一、二階文件(手冊/程序書)：無。
  - ➔三階文件(作業指導書)：網路安全開發作業指導書。
  - ➔四階文件(範本/表單)：安全架構設計原則檢查表(記錄各專案設計階段導入安全設計原則之評估結果)。

[RQ-10-07]應分析[RQ-10-01]中定義的架構設計以識別弱點。

備考 8：可考量再利用組件之已知弱點及脆弱性。

備考 9：對已識別的弱點進行脆弱性分析(參照 CNS 21434 第 8.5 節)，並對已識別的脆弱性進行管理(參照 CNS 21434 第 8.6 節)。然而，亦可藉由更改架構設計來解決已識別的弱點，無需履行脆弱性分析。

- RQ-10-07 說明
  1. 架構設計完成後，應針對架構進行網路安全維度的分析，以判斷架構是否存在弱點或脆弱性。此條款是對[RC-10-06]的驗證與補充。
  2. 分析方式應包含檢查再利用組件(如第三方函式庫、開源組件、既有模組)本身是否存在已知的安全弱點或脆弱性，並將其納入架構弱點分析中。
  3. 識別出的弱點，可依據 CNS 21434 第 8 節之脆弱性管理流程執行；在某些情況下，弱點可直接透過修改架構設計被消除(如架構分層不合理導致的權限外洩，直接調整分層規則即可)，而無需對弱點進行進一步的脆弱性分析。
- RQ-10-07 實踐方式

  需針對架構進行盤點，並記錄弱點來源與處理方式，如表 8 範例：

表 8　架構弱點分析報告

弱點名稱	弱點描述	弱點來源	脆弱性分析/處理方案
遠端程式碼執行	某開源通訊模組版本過舊	第三方組件	評估不具備攻擊可行性，不會升級為脆弱性，列入持續監控
…			

- RQ-10-07 產出文件

  併同 [RC-10-12] 進行闡述。

[RQ-10-08]應查證定義的網路安全規格，以確保完整性、正確性及與更高級架構抽象(概念)之網路安全規格的一致性。

備考 10：查證方法可包含：

- 審查。
- 分析。
- 模擬。
- 原型。

- RQ-10-08 說明

  1. 為了確認已定義之網路安全規格，查證應涵蓋以下項目：
     (1) 完整性：全面盤點並檢查底層網路安全規格，是否已完整涵蓋由較高層級(如車輛級或系統層級)所分配下來的所有網路安全要求事項、邊界假設及運作限制，確保安全需求無任何遺漏。
     (2) 正確性：逐條審查網路安全規格在技術上是否精準、表述明確且無爭議、符合邏輯，並確認其具備可實作性與可查證性。
     (3) 一致性：確認網路安全規格於不同層級之分解、細化及配置過程中，各組件的要求事項彼此間不存在相互矛盾或衝突的情形。
     (4) 在進行完整性與一致性審查時，規格應建立雙向追溯關係(Bidirectional Traceability)。向上追溯需確保每條底層規格

皆能找到對應的高層級要求作為依據；向下追溯則確保高層級的每項網路安全概念，皆有具體的低層級規格落實。

- RQ-10-08 實踐方式

利用如文件審查、雙向追溯分析等方法，填寫安全規格查證報告之範例如下，以確認各項規格是否滿足完整性、正確性與一致性。

表 9　網路安全規格查證報告

查證內容	審查結果	發現之問題項	負責人
網路安全規格的完整性			
網路安全規格的正確性			
….			

- RQ-10-08 產出文件

■ 網路安全規格查證報告(對應 CNS 21434 之 WP-10-04)。

➔一、二階文件(手冊/程序書)：網路安全整合與查證程序書(內含網路安全規格查證之啟動時機、跨部門審查與簽核權責、雙向追溯分析之要求機制)。

➔三階文件(作業指導書)：安全整合與查證作業指導書(內含規格正確性與完整性評估方法，雙向追溯檢核表以及模擬查證之執行方法，進行規格之完整性、正確性及一致性查核細則)。

➔四階文件(範本/表單)：網路安全規格查證報告。

10.4.2 整合及查證

[RQ-10-09]整合及查證活動應查證組件之實作與整合是否滿足定義的網路安全規格。

- RQ-10-09 說明

組件開發完成後，應透過查證活動來確認實際的開發成果(如程式碼、硬體配置等)完全符合所定義的網路安全規格。即針對組件進行的符合性測試。

- RQ-10-09 實踐方式

併同[RQ-10-10]進行闡述。

- RQ-10-09 產出文件

  併同[RC-10-12]進行闡述。

[RQ-10-10] [RQ-10-09]之整合及查證活動應考量以下規定：

(a) 定義之網路安全規格。

(b) 用於系列生產之組態(若適用)。

(c) 具有充足的能力支援所定義之網路安全規格中規定的功能。

(d) [RQ-10-05]的建模、設計及編碼指導綱要的符合性(若適用)。

備考 1：可包含車輛整合及查證。

備考 2：查證方法可包含：

- 要求事項式測試。
- 介面測試。
- 來源利用評估。
- 控制流及資料流之查證。
- 動態分析。
- 靜態分析。

備考 3：若採用測試查證，測試案例及測試環境的選擇可考量：

- 達到查證目的之測試整合等級。
- 基於對所選測試環境之分析，於後續整合活動期間履行額外測試之必要性，例：由於與處理器仿真或開發環境相比，造成最終整合目標處理器之資料字組與位址字組的位元寬度不同。

備考 4：導出測試案例的方法可包含：

- 要求事項分析。
- 等同類別之產生及分析。
- 邊界值分析。
- 基於知識或經驗之錯誤猜測。

- RQ-10-10 說明

  1. 針對(a)定義之網路安全規格：整合與查證活動是針對網路安全規格的符合性進行查證。網路安全規格是明確且具備追溯性的查

證標準，規格中的每一條具體要求，都應有對應的測試案例來驗證其是否被落實。

2. 針對(b)用於系列生產之組態：查證活動應在「預計用於量產」的軟硬體配置環境下進行。若僅在開發階段的模擬環境中測試，可能會導致實際運作環境中的安全問題被遺漏，使部分攻擊面無法被有效驗證。
3. 針對(c)支援網路安全規格中規定的功能：由於加密、鑑別及其他網路安全控制措施可能消耗處理能力、記憶體、儲存空間或網路頻寬，應評估其對系統或組件效能、資源使用及既有功能運作之影響，並採用適當之非功能性查證方法。
4. 針對(d)建模、設計及編碼指導綱要的符合性：查證活動中需要驗證開發過程是否遵循了組織定義的相關指南(例如 MISRA C 或 CERT C)。此類規範通常可透過靜態程式碼分析工具進行查證。
5. 針對查證方法以及測試案例的匯出方法，標準中給出了具體建議但並不強制，組織可依據實際專案需求選擇適合的方法。

- RQ-10-09、RQ-10-10 實踐方式

1. 應將目標、控制措施、具體要求與分配對象進行對應，如表 10 範例。

表 10　網路安全整合與查證測試報告

網路安全規格	查證方法	測試案例匯出方法	測試案例	查證通過條件	結果
加密儲存的資料，應僅能被相關的應用程式讀取和使用。	基於要求事項的測試	基於要求事項的分析	透過功能所需情境之外的應用程式嘗試存取加密資料，檢查是否成功。	滿足上述目標，不存在偏差。	通過

- RQ-10-10 產出文件

  併同[RC-10-12]進行闡述。

[RQ-10-11]若採用測試查證，則應使用定義的測試涵蓋範圍度量指標評估測試涵蓋範圍，以判定測試活動之充分性。

備考 5：標準測試涵蓋範圍度量指標可能不足以滿足網路安全， 例：軟體聲明之涵蓋範圍。

- RQ-10-11 說明

  1. 若採用測試作為查證方法，應於測試規範或測試報告中建立量化的測試涵蓋率(Coverage)度量機制。透過明確的量化數據，客觀評估網路安全測試活動是否已全面涵蓋所有已定義的安全需求與架構路徑。
  2. 測試涵蓋率的度量結果應區分為「安全需求涵蓋率」與「程式碼結構涵蓋率」兩個維度，並與專案初始定義之測試目標進行嚴格比對：
     (1) 安全需求涵蓋率：用以確保所有設計階段定義之網路安全要求事項，皆有對應的測試案例予以驗證。
     (2) 程式碼結構涵蓋率：用以評估測試案例執行時，對組件原始碼的覆蓋深度。最基礎的語句涵蓋率(Statement Coverage)，指動態測試時實際被執行到的原始碼語句佔總語句之百分比衡量標準較為寬鬆。即使達到 100% 語句涵蓋率，仍可能遺漏關鍵的分支判定或異常安全路徑。因此，應增加如分支涵蓋率(Branch Coverage)、條件涵蓋率(Condition Coverage)、路徑涵蓋率(Path Coverage)等測試指標。

- RQ-10-11 實踐方式

  1. 於網路安全整合與查證測試規範中定義測試涵蓋率指標，如語句涵蓋率，分支涵蓋率，條件涵蓋率等。
  2. 於網路安全整合與查證測試報告中，統計對應的指標是否滿足要求。

- RQ-10-11 產出文件
  - ➔一、二階文件(手冊/程序書)：網路安全整合與查證測試流程。
  - ➔三階文件(作業指導書)：無。
  - ➔四階文件(範本/表單)：網路安全整合與查證測試規範、網路安全整合與查證測試報告。

[RC-10-12]宜履行測試，以確認組件中剩餘的未識別弱點及脆弱性已最小化。

備考 6：不必要的功能可能包含弱點。

備考 7：測試方法可包含：

- 功能測試。
- 脆弱性掃描。
- 模糊測試。
- 滲透測試。

備考 8：針對已識別弱點進行脆弱性分析(參照 CNS 21434 第 8.5 節)，並對已識別脆弱性進行管理(參照 CNS 21434 第 8.6 節)。然而，若可藉由更改架構設計解決已識別的弱點，則無需履行脆弱性分析。

- RC-10-12 說明
  1. 宜展開專業的網路安全測試，以主動識別組件中遺留的未識別弱點或脆弱性。
  2. 測試方法可以包含功能測試、脆弱性掃描、模糊測試以及滲透測試。
- RC-10-12 實踐方式

  併同[RQ-10-13]進行闡述。
- RQ-10-07、RQ-10-09、RQ-10-10、RQ-10-11、RC-10-12 產出文件
  - ■ 產品開發過程中發現之弱點(對應 CNS 21434 之 WP-10-05)、網路安全整合與查證測試規範(對應 CNS 21434 之 WP-10-

06)、網路安全整合與查證測試報告(對應 CNS 21434 之 WP-10-07)。

➔一、二階文件(手冊/程序書)：網路安全整合與查證程序書。

➔三階文件(作業指導書)：網路安全整合與查證作業指導書(內含架構弱點分析方法、整合查證執行規則、測試涵蓋範圍度量指標定義、功能測試/脆弱性掃描/模糊測試/滲透測試之執行方法、以及 CAL 對應之測試深度基準)、網路安全整合與查證測試規範(針對特定專案定義測試項目、測試方法與涵蓋範圍要求)。

➔四階文件(範本/表單)：架構弱點分析報告(記錄識別之弱點及處理方式)、網路安全整合與查證測試報告。

[RQ-10-13]若未依[RC-10-12]履行測試，則應提供理由闡述。

備考 9：理由闡述可包含以下考量因素：

- 存取組件攻擊面的可行性。
- (直接或間接)存取此組件的能力，並組合其他組件之危害。
- 組件之簡單性。

- RQ-10-13 說明

1. 本項要求係針對[RC-10-12]建議事項的裁適規範。由於各組件的風險程度與複雜度不同，組織可以對測試活動進行適度裁適(如調整或免除部分測試)，但應提出明確、合理的裁適理由與評估依據。
2. 若選擇了裁適，可基於以下考量：
   (1)存取組件攻擊面的可能性：評估組件實體或邏輯介面的暴露程度、存取條件及所處之網路安全區域。例如：某 ECU 雖僅具備 CAN 匯流排介面，但仍應審慎評估其是否可經由診斷介面(OBD-II)、中央閘道器或其他遠端通訊路徑被間接存取，不宜僅因介面類型而直接判定其風險較低。
   (2)(直接或間接)存取組件的能力：評估攻擊者突破防線所需的攻擊路徑與前置條件。例如：若攻擊者應先攻陷車載資訊娛樂系統(IVI)並破解閘道器防護後，才能間接存取目標 ECU，可

將該攻擊路徑與前置條件納入評估，但不應僅因攻擊步驟較多而直接免除相關測試。

(3) 組件的簡易性：組件功能簡單，無複雜的軟體邏輯，幾乎不存在漏洞風險，針對該 ECU 的網路安全測試可以裁適。

(4) 應將基於上述考量條件的「裁適理由」明確記錄下來，以供後續審查。

- RC-10-12、RQ-10-13 實踐方式

  網路安全測試流程：定義網路安全測試相關的活動，包括測試活動的裁適分析與審查流程。

- RQ-10-13 產出文件

  ➔一、二階文件(手冊/程序書)：網路安全整合與查證程序書(內含 RC-10-12 裁適之判斷準則)。

  ➔三階文件(作業指導書)：無。

  ➔四階文件(範本/表單)：裁適理由說明(記錄未履行測試之具體理由，包含攻擊面可能性、組件存取難度及組件簡易性之評估結果)。

第 11 節 網路安全確證

11.1 一般

本節描述此項目於車輛級之網路安全確證活動(參照 CNS 21434 圖 9)。此項目被考量於車輛級之運作環境及預計用於系列生產的組態中。

11.2 目的

本節之目的為：

(a) 確證網路安全目標及網路安全聲明。

(b)確認此項目達成網路安全目標。

(c) 確認未存在不合理之風險。

11.3 輸入

11.3.1 先決條件

應提供以下資訊：

- 項目定義 CNS 21434 之[WP-09-01]。
- 網路安全目標 CNS 21434 之[WP-09-03]。
- 網路安全聲明 CNS 21434 之[WP-09-04](若適用)。

11.3.2 進一步的支援資訊

可考量以下資訊：

- 網路安全概念 CNS 21434 之[WP-09-06]。
- 產品開發之工作產出(參照 CNS 21434 第 10.5 節)。

11.4 要求事項及建議事項

[RQ-11-01]考量系列生產組態項目於車輛級之確證活動應確認：

(a) 網路安全目標對於威脅情境及對應風險之適足性。

備考 1：若於確證過程中識別網路安全目標未闡明任何風險，則可依 CNS 21434 第 9.4 節闡明。

(b)達到此項目之網路安全目標。

(c) 網路安全聲明之有效性。

(d)運作環境要求事項之有效性(若適用)。

備考 2：確證活動可包含：

- 藉由審查 CNS 21434 第 9.5 節及第 10 節之工作產出以確認網路安全目標的達成。
- 滲透測試以證明網路安全目標之適足性及達成。
- 經由 CNS 21434 第 9 節及第 10 節所識別之所有風險的管理審查。

備考 3：CAL 可用於衡量滲透測試之深度及嚴謹度(參照 CNS 21434 附錄 E)。

備考 4：針對[RQ-11-01]確證活動期間識別出的弱點進行脆弱性分析(參照 CNS 21434 第 8.5 節)，並對識別出的脆弱性進行管理(參照 CNS 21434 第 8.6 節)。

- RQ-11-01 說明

1. 網路安全確證與查證的區別在於，網路安全確證旨在確認項目(Item)於車輛級的生產配置組態下，是否能有效抵禦概念階段所識別出的威脅情境，並證實其確實滿足頂層之網路安全目標以及網路安全聲明。相對地，查證則是確認開發過程是否滿足設計階段的技術規範與要求，其評估對象主要為獨立組件或子系統。
2. 網路安全確證活動可以包含以下幾種方式：
   (1) 工作產出的審查：透過審查概念階段(CNS 21434 第 9 節)及產品開發階段(CNS 21434 第 10 節)的工作產出進行車輛級網路安全確證，確保工作產出的完整性、正確性及一致性，作為滿足網路安全目標的證據。
   (2) 滲透測試：從外部攻擊者(或稱駭客)的角度，在車輛級的真實運作環境中模擬真實的攻擊，確認網路安全目標的達成以及網路安全聲明的有效性。
   (3) 審查已管理的風險：審查車型專案概念階段及開發階段所有已識別且進行管理的風險，確認經技術緩解或管理手段處理後，產品的殘餘風險已處於合理且可接受之範圍。
3. 網路安全保障等級(CAL)專案所定義的 CAL 等級，將直接決定滲透測試的執行深度與嚴謹度基準(參照 CNS 21434 附錄 E)。如

果 CAL 等級越高，表示滲透測試人員所需的專業能力要求就越高。

- RQ-11-01 實踐方式

  併同[RQ-11-02]進行闡述。

- RQ-11-01 產出文件

  併同[RQ-11-02]進行闡述。

[RQ-11-02]應提供選擇確證活動的理由闡述。

- RQ-11-02 說明

  組織內部可定義網路安全確證活動的選取與裁適原則，並針對每項確證活動的實施或省略，提供具體的理由與評估依據。例如：組織可於程序書中將「車輛級進階滲透測試」定義為依條件執行的項目；若該專案之風險評鑑環節中包含高風險或嚴重等級之威脅情境，則必須選做滲透測試作為確證依據。

- RQ-11-01、RQ-11-02 實踐方式

  1. 需記錄所選擇的確證活動與理由，並將執行步驟與結果記錄下來，如表 11 範例：

表 11　網路安全確證活動報告

網路安全目標/網路安全聲明	確證活動	理由	執行方法	執行結果	發現事項
XX 車型網路安全目標清單	滲透測試	由於風險評鑑環節包含高風險威脅情境	詳見 XX 滲透測試報告	詳見 XX 滲透測試報告	詳見 XX 滲透測試報告問題單

- RQ-11-01、RQ-11-02 產出文件
  - 網路安全確證報告(對應 CNS 21434 之 WP-11-01)
    - ➔一、二階文件(手冊/程序書)：網路安全確證活動程序書(內含確證活動選取準則、測試裁適理由之評估與撰寫規範)。
    - ➔三階文件(作業指導書)：網路安全確證作業指導書(內含工作產出審查檢核表、滲透測試執行方法與 CAL 對應之測試深度基準、以及已管理風險之審查執行規則)。
    - ➔四階文件(範本/表單)：網路安全確證報告。

第 12 節 生產

12.1 一般

生產包含車輛級之項目或組件的製造及組裝。建立生產控制計畫係為確保後開發的網路安全要求事項可應用於項目或組件，並確保於生產過程中不會引入脆弱性。

12.2 目的

本節之目的為：

(a) 應用於後開發之網路安全要求事項。

(b)預防於生產過程中引入脆弱性。

12.3 輸入

12.3.1 先決條件

應提供以下資訊：

- 釋出之後開發報告 CNS 21434 之[WP-06-04]。
- 後開發之網路安全要求事項 CNS 21434 之[WP-10-02]。

12.3.2 進一步的支援資訊

無

12.4 要求事項及建議事項

[RQ-12-01]應產生適用於後開發之網路安全要求事項的生產控制計畫。

備考 1：生產控制計畫可作為整體生產計畫之一部分。

- RQ-12-01 說明

  網路安全要求事項除適用於開發階段外，亦包含需於生產、運作、維護或除役等後開發階段落實之要求事項。因此，組織應於生產階段前制定生產控制計畫，以確保適用的後開發階段網路安全要求事項能於生產過程中予以落實。生產控制計畫可納入組織既有之整體生產計畫。

- RQ-12-01 實踐方式

  併同[RQ-12-01]、[RQ-12-02]、[RQ-12-03]進行闡述。

- RQ-12-01 產出文件

  併同[RQ-12-01]、[RQ-12-02]、[RQ-12-03]進行闡述。

[RQ-12-02]生產控制計畫應包含：

(a) 適用於後開發之網路安全要求事項之步驟順序。

(b)生產工具及設備。

(c) 網路安全控制措施，以預防生產過程中未經授權之變更。

例 1：預防對保存軟體之生產伺服器履行實體存取之實體控制措施。

例 2：適用密碼學技術及/或存取控制之邏輯控制措施。

(d)確認符合後開發網路安全要求事項之方法。

備考 2：方法可包含檢驗及校準檢查。

備考 3：為製造項目或組件並安裝硬體及軟體，生產過程可使用特權存取。若生產後仍以未經授權的方式存取，可能會在項目或組件中引入脆弱性。

- RQ-12-02 說明

  1. 適用生產階段的網路安全需求：例如出廠前刪除特權帳戶以及停用、封鎖或限制對外的除錯介面，以縮減潛在攻擊面。
  2. 生產控制計畫的核心內容宜與組織既有之品質管理及生產管理機制(如 IATF 16949 流程)整合，用以規劃及落實生產階段之網路安全要求事項，其內容可包括下列項目：
     (1) 步驟順序：制定標準化的操作流程以落實後開發階段網路安全需求。
     (2) 工具與設備：明確界定並管控生產所需的工具、伺服器和工作終端等設備。
     (3) 網路安全控制措施：採用適當之實體與邏輯控制措施，防止生產過程中發生未經授權之變更。實體控制如透過門禁及實體區域管制，限制對儲存生產軟體之伺服器的實體存取；邏輯控制則透過加密、身分鑑別及權限控管進行防護，防止生產過程中發生未經授權的修改。

(4)確認方法：採用檢驗、測試、紀錄審查、工具校準檢查或其他適當方法，確認適用之後開發網路安全要求事項已於生產過程中正確落實。

- RQ-12-02 實踐方式

  併同[RQ-12-01]、[RQ-12-02]、[RQ-12-03]進行闡述。

- RQ-12-02 產出文件
  - ■ 生產控制計畫(對應 CNS 21434 之 WP-12-01)併同[RQ-12-01]、[RQ-12-02]、[RQ-12-03]進行闡述。

[RQ-12-03]應實作生產控制計畫。

- RQ-12-03 說明

  生產控制計畫應確實執行。在製造產品或組件並安裝軟硬體的過程中，生產流程往往需要使用特權存取權限。若產品出廠或生產完成後，該特權權限被以未經授權的方式惡意使用，將會在產品或組件中引入嚴重的安全脆弱性。因此，必須嚴格落實控制計畫以防範此類後開發階段的風險。

- RQ-12-01、RQ-12-02、RQ-12-03 實踐方式

  1. 應定義開發與生產端之間的網路安全介面，並落實以下生產控制計畫的執行步驟：
     (1)需求轉化與確認：接收來自開發端的需求後，需確認如何在生產過程中實現(例如：出廠前刪除特權帳戶以及停用、封鎖或限制對外的除錯介面，以縮減潛在攻擊面)。
     (2)計畫制定：根據確認的網路安全需求，制定一份完整的生產控制計畫，內容需涵蓋步驟順序、生產工具與設備之管理、防止未經授權修改的實體與邏輯安全控制措施，以及確認方法。
     (3)生產執行與變更管控：嚴格按照計畫執行生產作業，並透過人工檢驗(如目視檢查除錯介面是否移除)或設備自動檢測(如透過檢測腳本驗證特權帳戶是否確實刪除)等方式，確認生產

階段的網路安全需求已完全被滿足，且整個過程無未經授權的修改。

- RQ-12-01、RQ-12-02、RQ-12-03 產出文件
  - ➔一、二階文件(手冊/程序書)：生產階段網路安全管理程序書(內含生產控制計畫制定規範、開發與生產端介面定義)。
  - ➔三階文件(作業指導書)：生產線網路安全配置與查核作業指導書(內含產線實體與邏輯安全控制基準、特權帳戶刪除步驟、金鑰安全燒錄規範、除錯介面移除方法及設備校準原則)。
  - ➔四階文件(範本/表單)：生產控制計畫與執行查核表(內含各項安全需求之落實步驟與最終檢驗證據)

第 13 節 運作及維護

13.1 一般

本節描述網路安全事故回應(參照 CNS 21434 第 13.3 節)及場域之項目或組件的更新(參照 CNS 21434 第 13.4 節)。當組織調用網路安全事故回應作為脆弱性管理(參照 CNS 21434 第 8.6 節)之一部分時，就會發生網路安全事故回應。

更新係於後開發對項目或組件進行的變更，可包含附加資訊，例：技術規格、整合手冊、使用者手冊。組織可以因各種原因提出更新，例：闡明脆弱性或安全議題，提供功能改善。涉及更新之工作產出將被記錄為其他節之工作產出。變更管理(參照 CNS 21434 第 5.4.4 節)涵蓋概念、產品開發或生產階段中項目或組件的修改，本節不贅述。

13.2 目的

本節目的為：

(a) 判定並實作網路安全事故之補救措施。

(b) 於生產後項目或組件更新期間及更新後維護網路安全，直至網路安全支援結束。

13.3 網路安全事故回應

13.3.1 輸入

13.3.1.1 先決條件

無

13.3.1.2 進一步的支援資訊

可考量以下資訊：

- 與引起網路安全事故回應之脆弱性相關的網路安全資訊。
- 脆弱性分析 CNS 21434 之[WP-08-05]。

13.3.2 要求事項及建議事項

[RQ-13-01]對於每個網路安全事故，應產生網路安全事故回應計畫，其中包含：

(a) 補救措施。

備考 1：補救措施依 CNS 21434 第 8.6 節中的脆弱性管理判定。

(b)溝通計畫。

備考 2：溝通計畫的產生可涉及內部關注方，例：行銷或公共關係、產品開發團隊、法律、顧客關係、品質管理、採購。

備考 3：溝通計畫可包含內部及外部溝通夥伴(例：開發者、研究人員、一般公眾、權責機構)之識別，及為此等受眾發展特定資訊。

(c) 指派補救措施之責任。

備考 4：責任可具有：

- 受影響項目或組件之專業知識，包含舊有的項目及組件。
- 組織知識(例：業務流程、溝通、採購、法規)。
- 決定之權責機構。

(d)記錄與網路安全事故相關之新網路安全資訊程序。

備考 5：可依 CNS 21434 第 8.3 節蒐集新的網路安全資訊，例：有關以下資訊：

- 受影響組件。
- 相關事故及脆弱性。
- 鑑識資料，例：資料日誌、碰撞感測器資料。
- 終端用戶抱怨。

(e)確定進展之方法。

例：衡量進展之指標為：

- 受影響項目或組件得到補救的百分比。
- 補救措施影響項目或組件之百分比。

(f) 網路安全事故回應結束的準則。

(g)結束行動。

- RQ-13-01 說明

  網路安全事故(例如資料外洩、系統遭受破壞)會帶來營運、合規與聲譽等風險。制定網路安全事故回應計畫之目的，在於確保事件發生時能迅速、有效地進行處置，以最大程度降低損害並恢復業務、減少負面影響，同時滿足合規要求。

- RQ-13-01 實踐方式

1. CNS 21434 中要求針對每一個網路安全事故，應制定專屬的網路安全事故回應計畫，主要內容必須包括：
   (1) 補救措施：針對網路安全事故的根源(例如脆弱性、惡意程式)依據 CNS 21434 第 8.6 節，定義適當之臨時措施、長期措施以及恢復措施。例如：臨時關閉連網功能以避免事件擴大；長期措施如對脆弱性進行修補程式修復；針對已發生的不良後果進行恢復(如資料備份恢復等)。補救措施應與脆弱性管理活動連結，並評估其有效性及可能衍生之影響，避免同類事故再次發生。
   (2) 溝通計畫：明確規範事故發生後的內部與外部溝通，包括溝通的時間點、窗口、內容、方式以及相關利害關係人等。例如：發生網路安全事故後需即時向主管機關報告。
   (3) 指派補救措施之責任：依據技術專業與業務範疇指派應變負責人，明確不同角色在補救過程中的分工。如技術團隊負責分析脆弱性並修復受影響的組件；業務團隊負責提供業務流程並協調內外部溝通；管理層負責事件處理的決策。
   (4) 記錄與網路安全事故相關之新網路安全資訊：在事故發生與處理過程中，要持續記錄與網路安全事故相關的新網路安全資訊(如資料日誌、碰撞感測器數據等)，保證完整準確。
   (5) 確定進展之方法：用可量化的指標衡量資訊安全事故處理的進度(如受影響項目或組件得到補救的百分比)，方便團隊追蹤進度與評估效果。
   (6) 網路安全事故回應結束的準則：明確判斷事件已經得到控制，可以結束回應流程的條件。例如所有受影響的系統已恢復正常運作。
   (7) 結束行動：如網路安全事故的總結、更新相關流程文件及加強人員培訓等。

- RQ-13-01 產出文件
  - ■ 網路安全事故回應計畫(對應 CNS 21434 之 WP-13-01)併同[RQ-13-02]進行闡述。

[RQ-13-02]應實作網路安全事故回應計畫。

- RQ-13-02 說明

  網路安全事故回應計畫必須被確實執行。若僅制定計畫而未在事故發生時嚴格執行，將無法有效控制安全事故的損害擴大與蔓延。因此，應確實落實計畫中的補救措施、溝通計畫與結案行動。

- RQ-13-02 實踐方式

  1. 當事件發生時，團隊需依據流程定義建立並記錄相關的回應措施與責任分配，如表 12 範例

     表 12　網路安全事故回應計畫

網路安全事故回應計畫	
網路安全事故回應項目	內容說明/執行紀錄
事故描述及嚴重等級判定	描述事故現象、影響範圍，並判定嚴重等級 (如 Critical/High/Medium/Low)
事故回應團隊	定義參與處理之技術、業務與管理層人員(明確記錄各窗口之職責指派與聯絡通報管道)

- RQ-13-01、RQ-13-02 產出文件

  ➔一、二階文件(手冊/程序書)：網路安全事故應變與處置程序書(內含事故回應計畫制定規範、應變小組召集流程，並對事故處理過程中的所有技術操作、決策變更、通報時間點與修補進度，進行全程的紀錄留存與時序追蹤管控規範)。

  ➔三階文件(作業指導書)：無。

  ➔四階文件(範本/表單)：網路安全事故回應計畫範本(內含補救措施規劃欄位、事故描述及嚴重等級判定、事故回應團隊配置、職

責分配矩陣及結案準則檢核項)與執行紀錄表(內含事故及嚴重等級判定、事故回應團隊參與人員之實際填寫內容與執行紀錄、處理進度指標以及最終結案簽核證據)。

13.4 更新

13.4.1 輸入

13.4.1.1 先決條件

應提供以下資訊：

- 釋出之後開發報告 CNS 21434 之[WP-06-04]。

13.4.1.2 進一步的支援資訊

可考量以下資訊：

- 網路安全事故回應計畫 CNS 21434 之[WP-13-01]。
- 後開發網路安全要求事項 CNS 21434 之[WP-10-02]相關的更新。

13.4.2 要求事項及建議事項

[RQ-13-03]車輛內的更新及更新相關能力應依 CNS 21434 進行開發。

- RQ-13-03 說明

  網路安全事件的修復措施往往需要透過車輛的更新功能來實現(例如 OTA 升級、診斷儀升級及 USB 升級等)。然而，在車輛更新的過程中，系統極易受到駭客的攻擊(例如駭客竄改更新封包，導致車輛失控、資料外洩等)。因此，車輛內的更新機制和與更新有關的能力，都必須視為一個完整的專案，按照 CNS 21434 的規定進行開發與防護。

- RQ-13-03 實踐方式

  1. 針對車輛內的更新機制和與更新有關的能力，應參照 CNS 21434 第 9 節至第 11 節的要求進行完整的開發及測試。例如：必須針對車輛的 OTA 升級功能進行項目定義，並完整展開 TARA 分析等網路安全活動。
  2. TARA 分析與 CNS 21434 第 9 節的關聯：當我們劃定項目定義後，首先就是執行 TARA 分析。

(1) 識別威脅與風險：透過 TARA 的系統化方法(如識別資產、威脅情境、計算攻擊可行性與衝擊)，找出系統潛在的風險值。

(2) 推導安全目標與概念：依據 TARA 算出的風險值，組織會做出風險處置決策(如決定降低風險或保留風險)。為了降低這些被 TARA 識別出來的高風險，CNS 21434 要求必須制定對應的網路安全目標，並進一步展開為包含具體控制措施的網路安全概念。

3. TARA 分析與 CNS 21434 第 10 節的關聯：產品設計與軟硬體開發，完全受到 TARA 分析結果與 CNS 21434 第 9 節工作產出影響。

(1) 落實安全規格：工程師必須根據 TARA 推導出的網路安全概念，在架構設計中細化出具體的網路安全規格，並將需求分配給軟體和硬體去實作防禦機制(如：加密、安全啟動等)。

(2) 架構與弱點的再分析：在架構設計與程式碼開發過程中，若識別出新的系統弱點(如開源軟體脆弱性)，也需要回頭運用 TARA 裡的威脅分析與攻擊路徑評估邏輯，來判斷這些新弱點是否會構成真實的攻擊威脅，並進行修補。

4. TARA 分析與 CNS 21434 第 11 節的關聯：在產品即將量產出貨前，需要回頭檢視 TARA 的風險是否被有效排除。

(1) 確證防禦的有效性：在車輛級確證活動(通常包含滲透測試等)，必須用來證明系統真的達成了網路安全目標，並且充分覆蓋了當初 TARA 分析中所識別出的威脅情境與對應風險。

(2) 確認無不合理風險：確證階段必須確保經過 CNS 21434 第 10 節後，TARA 所算出的風險已經被降至可接受範圍，系統不存在不合理的殘餘風險。

- RQ-13-03 產出文件

  ➔一、二階文件(手冊/程序書)：無。

➔三階文件(作業指導書)：安全架構設計作業指導書(參考 CNS 21434 第 10 節，RC-10-06 產出文件)、安全整合及查證作業指導書(參考 CNS 21434 第 10 節，RQ-10-08 產出文件)。

➔四階文件(範本/表單)：TARA 報告(對應 CNS 21434 之 WP-09-02)、網路安全規格查證報告(對應 CNS 21434 之 WP-10-04)、網路安全確證報告(對應 CNS 21434 之 WP-11-01)。

第 14 節 網路安全支援之結束及除役(報廢)

14.1 一般

除役(報廢)不同於網路安全支援的結束。組織可終止對某個項目或組件之網路安全支援，但此項目或組件仍可依場域設計運作。除役(報廢)及網路安全支援的結束皆帶來網路安全內涵，但此等內涵需分開考量。

除役(報廢)可能發生於組織不知情之情況，且除役(報廢)程序無法強制履行，因此除役(報廢)措施超出 CNS 21434 範圍。

於概念及產品開發階段需考量網路安全支援之結束及除役(報廢)。

14.2 目的

本節之目的為：

(a) 傳達網路安全支援結束。

(b)啟用與網路安全有關的項目及組件的除役(報廢)。

14.3 網路安全支援之結束

14.3.1 輸入

無

14.3.2 要求事項及建議事項

[RQ-14-01]當組織決定結束對某個項目或組件之網路安全支援時，應產生與顧客進行溝通之程序。

備考 1：溝通可以根據供應商與顧客之間的契約要求事項進行處理。

備考 2：與車主的溝通可以藉由公告的方式進行。

- RQ-14-01 說明
  1. 當產品因技術汰換或合約到期而終止網路安全生命週期時，組織必須建立明確的告知機制。車廠與車主之間可透過官方管道進行公告；供應商與客戶(車廠)之間則應依據合約條款執行正式通知，以確保雙方責任邊界清晰。
  2. 終止網路安全支援之常見情境包括產品停產、技術架構更新後不再維護、已知安全漏洞不再提供修補等。在上述情境下，組織可依內部程序正式啟動網路安全支援結束流程，並同步進行對外溝通。

3. 終止支援時，應明確界定溝通對象、溝通內容及溝通方式。例如，車廠與車主之間可透過官方公告進行說明；供應商與客戶之間則通常以正式函文或電子郵件方式進行通知與確認。
4. 網路安全支援結束相關條件，通常應於專案初期由供應商與客戶透過合約方式加以約定，包括支援範圍、支援期限、責任分工及聯絡窗口等內容，以確保後續終止過程具備合規性與可追溯性。

- RQ-14-01 實踐方式

  終止網路安全支援之通知內容，至少包含下列事項：

  1. 終止網路安全支援之原因；
  2. 受影響之產品或元件範圍；
  3. 終止支援所造成之影響說明，以及可行之替代方案(如有)；
  4. 聯絡窗口與相關聯絡方式。

- RQ-14-01 產出文件
  - 網路安全支援結束的溝通程序(對應 CNS 21434 之 WP-14-01)
    - ➔一、二階文件(手冊/程序書)：網路安全支援結束管理程序書(內含終止網路安全支援之評估時機、跨部門權責分工與對內外通報溝通機制)。
    - ➔三階文件(作業指導書)：網路安全支援結束作業指導書(內含終止原因之評估標準、受影響產品範圍盤點方法、替代或升級方案之評估基準，以及通知發布之標準作業流程)。
    - ➔四階文件(範本/表單)：網路安全支援結束通知與執行紀錄表(內含結束原因、受影響之產品或元件範圍、影響說明、聯絡窗口，以及實際向顧客或供應商發送通知之證據留存)。

14.4 除役(報廢)

14.4.1 輸入

14.4.1.1 先決條件

應提供以下資訊：

- 後開發之網路安全要求事項 CNS 21434 之[WP-10-02]。

14.4.1.2 進一步的支援資訊

無

14.4.2 要求事項及建議事項

[RQ-14-02]應提供與除役(報廢)相關之後開發網路安全要求事項。

備考：與此要求事項相關的適切文件(例：說明書、使用者手冊)可啟動網路安全除役(報廢)。

- RQ-14-02 說明

1. 組織應識別產品於除役(報廢)或所有權移轉情境下所需遵循之網路安全要求，以確保資料安全與權限控管之完整性，防範殘留資訊避免遭惡意利用。具體的技術要求應包含：
   (1) 如何清除個人資料(包含車載設備端與雲端系統之連動資料)。
   (2) 如何停用或註銷生產階段殘留之特權帳號。
   (3) 如何移除、登出或重設系統之存取控制機制。
   (4) 如何安全地撤銷或抹除 ECU 內的密碼學金鑰，確保廢棄或替換下來的組件無法被用於攻擊其他系統。

   上述要求之具體落實方式，應透過產品說明書、使用者手冊或官方公告等形式明確告知使用者，以確保資料安全與權限控管之完整性。

- RQ-14-02 實踐方式

1. 應明確定義產品於除役(報廢)或所有權移轉情境下之網路安全要求與操作方法，並依據對象區分為「外部使用者」與「內部維修體系」，以確保使用者能正確執行相關安全措施：
   (1) 針對外部使用者：於手冊中編列專章，定義產品於除役(報廢)或所有權移轉情境下之網路安全操作方法(如刪除個人資料、解除車機綁定等)。
   (2) 針對內部或授權維修體系：當車輛進廠替換組件或進行除役(報廢)時，維修人員應依循內部安全清除程序，填寫並留存

《產品除役(報廢)執行檢核表》，確保生產與維運階段殘留之敏感資訊及金鑰已徹底抹除。

- RQ-14-02 產出文件
  - ➔一、二階文件(手冊/程序書)：產品除役(報廢)網路安全管理程序書(內含車輛或組件除役(報廢)、所有權移轉時之網路安全風險管理政策與啟動時機)。
  - ➔三階文件(作業指導書)：產品除役(報廢)安全清除作業指導書(內含個人隱私資料之抹除步驟、特權帳號之註銷方法、存取控制機制重設、回復原廠設定、密碼學金鑰撤銷與記憶體安全抹除的技術指引和規範)。
  - ➔四階文件(範本/表單)：產品說明書/使用者手冊(內含提供給外部使用者之安全除役操作指引)與產品除役(報廢)執行檢核表(若由廠內/授權維修廠回收時之實體與邏輯清除查核紀錄)。