道路車輛網路安全工程產業指引
第 1 部：組織與專案之網路安全管理；分散式與持續性之網路安全活動

Industrial guideline for road vehicles cybersecurity engineering
Part 1: organizational and project dependent cybersecurity management; distributed and continual cybersecurity activities

(TTVMA IG-001:2025)

台灣區車輛工業同業公會

2025 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 ISO/SAE 21434 訂定之，內容為針對組織與專案之網路安全管理、分散式及持續性之網路安全活動，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 ISO/SAE 21434 的適用範圍，惟本指引僅針對 ISO/SAE 21434 第 5 節至第 8 節之相關要求、建議及許可事項，提供實踐指引，具體指引內容詳述於本指引第 5 節至第 8 節。

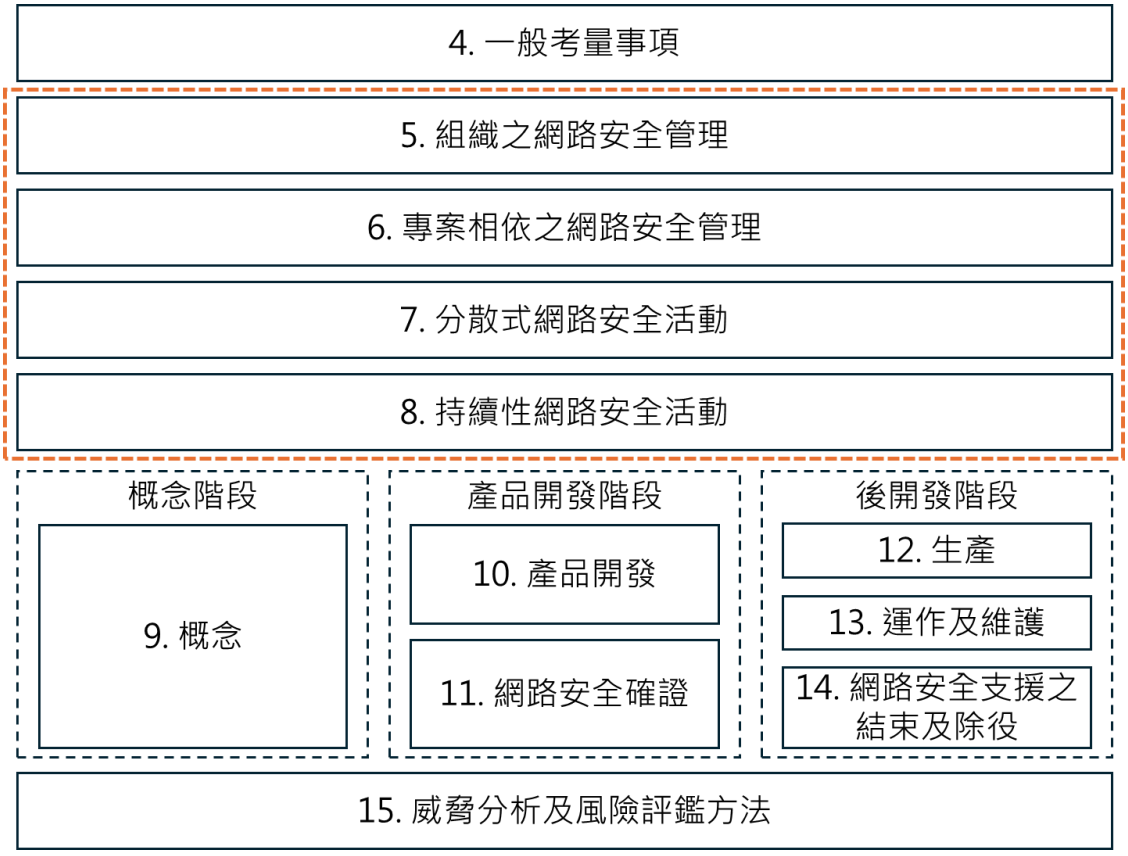


圖 1 ISO/SAE 21434 架構概觀

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 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

請參閱 ISO/SAE 21434 第 4 節，以了解該標準的涵蓋範圍及相關限制。

5. 組織之網路安全管理

5.1 一般

為啟用網路安全工程，組織需建立並維護網路安全治理及網路安全文化，包含網路安全認知管理、適任性管理及持續改善。此涉及依 ISO/SAE 21434 目標進行獨立稽核之組織規則與過程的規定。

為支援網路安全工程，組織實作網路安全管理系統，包含管理工具及應用品質管理系統。

5.2 目的

本節目的為：

(a) 定義網路安全政策及網路安全之組織規則與過程。

(b) 指派履行網路安全活動所需之責任及相對應授權。

(c) 支援網路安全的實作，包含提供資源及管理網路安全過程與相關過程間之互動。

(d) 網路安全風險管理。

(e) 建置及維護網路安全文化，包含適任性管理、認知管理及持續改善。

(f) 支援及管理網路安全資訊的共享。

(g) 建置及維護支援維護網路安全的管理系統。

(h) 提供證據以證明工具的使用不會對網路安全產生不利的影響。

(i) 組織網路安全稽核之履行。

5.3 輸入

5.3.1 先決條件

無

5.3.2 更多的支援資訊

可考量以下資訊：

- 支援品質管理標準的現有符合性證據。

例：IATF 16949 與 CNS 12681、CNS 14238、Automotive SPICE®、ISO/IEC 330xx 系列標準、ISO/IEC/IEEE 15288、以及 ISO/IEC/IEEE 12207 聯合。

5.4 要求事項及建議事項之實踐指引

5.4.1 網路安全治理

[RQ-05-01]組織應定義網路安全政策，其中包含：

(a)確認道路車輛網路安全風險。

(b)履行管理階層管理相對應網路安全風險之允諾。

備考 1：網路安全政策可包含組織目的與其他政策之鏈結。

備考 2：網路安全政策可於考量外部或內部全景的情況下，包含關於組織產品或服務組合之一般威脅情境的風險處理聲明。

- RQ-05-01 說明
  1. 強調管理層的責任：
     組織領導層應高度重視網路安全管理，具備識別與管理車輛網路安全風險的意識，並明確制定網路安全政策，以確保整體資安戰略的有效推動。
  2. 確保政策與組織戰略一致：
     網路安全政策應與組織的經營目標及實際運營需求保持一致。對內，有助於提升全體員工的安全意識與協作能力；對外，則可展現組織對網路安全的承諾，強化與利益相關方的信任關係。
  3. 制定明確的安全承諾：
     為確保網路安全政策的有效落實，組織應制定具體的安全承諾，確保涵蓋 ISO/SAE 21434 的所有要求，並納入資安管理系統的核心架構。
  4. 奠定標準實施基礎：
     網路安全政策是標準實施的核心基礎，應確保組織在符合合規要求的前提下，持續強化網路安全管理能力，推動資安機制的優化與發展。
- RQ-05-01 實踐方式
  1. 網路安全政策制定與實施考量：
     制定網路安全政策時，可從以下三個層面進行考慮，以確保管理層承諾與實施的一致性：
     (1) 整體組織層面：
     確保組織高度重視道路車輛的網路安全風險，並將其納入企業品質管理系統，作為風險治理的重要一環。

(2) OEM 管理層面：

承諾積極應對網路安全風險，並明確定義網路安全管理的範疇與責任，確保資安措施貫穿產品生命週期。

(3) 外部相關方(如供應者、最終使用者)：

使供應鏈與 OEM 的網路安全政策保持一致，提升整體網路安全水準，確保數據與系統的完整性與可控性。

2. 網路安全政策與手冊的落實：

為有效落實網路安全政策，組織應制定網路安全管理手冊，作為資安管理的核心文件，提供明確的指導方向與實施規範。手冊中應明確組織的網路安全政策，例如：

「我們承諾將網路安全視為全球業務的重要組成部分，並對產品的安全性負責。我們確保在所有產品的規劃、開發與維護階段均納入網路安全考量。此外我們的數位行銷、銷售策略，以及與供應者的合作均需符合相關網路安全要求。」

此外為確保政策落實，手冊應進一步規範組織的安全承諾，包括但不限於：

(1) 建立並落實網路安全管理流程，確保各項活動符合標準要求，並定期審查與優化。

(2) 培育並維護網路安全文化，透過持續培訓與內部溝通提升員工安全意識與技能。

(3) 提供必要的資源支援，確保網路安全風險能夠有效管理與控制。

(4) 確保安全措施貫穿產品生命週期，從產品開發、生產、運作、維護及除役(報廢)，全面落實風險控管。

(5) 促進與外部相關方的合作，確保供應鏈與合作夥伴均符合網路安全要求，降低潛在風險。

組織可根據業務需求進一步補充具體承諾，以確保政策的適用性與執行力。

- RQ-05-01 產出文件
  - ■ 網路安全管理手冊文件清單(對應 ISO/SAE 21434 之 WP-05-01)

➔一、二階文件(手冊/程序書)：網路安全管理手冊

➔三階文件(作業指導書)：無

➔四階文件(範本/表單)：無

[RQ-05-02]組織應建立並維護規則與過程，以：

(a)啟用實作 ISO/SAE 21434 之要求事項。

(b)支援相對應活動之履行。

例 1：過程定義、技術規則、指導綱要、方法及範本。

備考 3：網路安全風險管理可包含活動的工作受益考量。

備考 4：規則及過程涵蓋概念、產品開發、生產、運作、維護及除役(報廢)，包含 TARA 方法、資訊共享、網路安全監督、網路安全事故回應及觸發。

備考 5:可依 ISO 29147 規定關於脆弱性揭露之規則與過程(例:資訊共享)。

備考 6：圖 2 概述整體網路安全政策(參照[RQ-05-01])及組織特定之網路安全規則與過程(參照[RQ-05-02])、責任(參照[RQ-05-03])及資源(參照[RQ-05-04])間的關係。

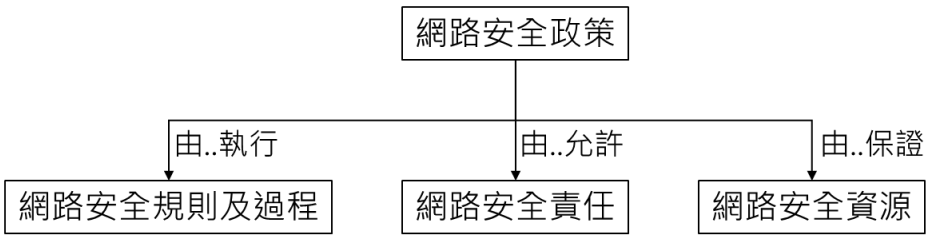


圖 2 網路安全治理

- RQ-05-02 說明
  1. 由圖 2 可知：
     (1) 網路安全政策
        A. 是整體網路安全的指導原則與最高方針。
        B. 作為核心，由上而下驅動其他三大元素(網路安全規則及過程、網路安全責任、網路安全資源)。
     (2) 網路安全規則及過程
        A. 是實踐政策的具體方式與流程。

B. 對應政策中所訂立的原則，制定實際作業準則及操作流程。

C. 藉由規則和過程來執行政策。

(3) 網路安全責任

A. 明確定義誰負責什麼的角色與責任。

B. 對應組織中各角色如何配合落實政策。

C. 透過職責界定來支持政策之推動。

(4) 網路安全資源

A. 為實施政策所需的人力、技術、工具與時間。

B. 若無資源，規則與職責即無從落實。

C. 透過資源來保障政策的落實。

2. 建立並明確車輛網路安全管理系統的組織架構，確保各層級的職責與權限劃分清晰，以提升管理與執行的有效性。

3. 依據 ISO/SAE 21434 要求，制定涵蓋各工作領域的相關流程文件、範本與指引，以確保網路安全工作的落實與標準化執行。

- RQ-05-02 實踐方式

1. 建立網路安全管理架構：

建立由上而下的網路安全管理架構，確保各層級均有明確分工：

(1) 領導層：負責制定網路安全原則與決策。

(2) 管理層：負責執行網路安全原則，監督與調整安全管理機制。

(3) 執行層：負責具體實施網路安全流程與日常管理。

2. 明確網路安全工作領域與標準文件：

確保涵蓋 ISO/SAE 21434 要求，並有明確的安全管理規範，包括：

(1) 網路安全治理(策略制定、監管機制)。

(2) 網路安全文化(意識培養、培訓計畫)。

(3) 工具管理(安全工具的開發與使用監控)。

(4) 資訊共用(內部與外部網路安全資訊流通)。

(5) 網路安全專案管理(專案風險評估與執行)。

(6) 車輛網路安全生命週期管理(從設計到報廢的安全考量)。

(7) 持續網路安全活動(監測、更新與強化安全機制)。

(8) 事件回應與應變處理(應對安全事故與風險)。

(9) 內部審查與管理評估(持續改善與標準符合性檢查)。

(10) 網路安全生產與供應鏈管理(確保供應者符合安全要求)。

為確保執行有跡可循，各領域應建立 流程文件、範本、指引 等標準文件，並列出網路安全文件清單，確保標準化操作流程與可追溯性。

3. 定義各工作領域的責任部門以及相關支援部門：

表 1 網路安全相關部門職責示意表(供參，可基於公司組織進行調整)

部門/架構	工作領域	職責	備註
領導層	所有	➢ 負責制定組織的網路安全政策。 ➢ 組織網路安全規劃與重大決策。	由組織 CEO 等成員組成的網路安全委員會。
管理層	所有	➢ 負責規劃與實施整體網路安全架構。 ➢ 監控與考核網路安全管理系統的運行狀況。	由網路安全相關部門高層組成的指導組。
品質保證	網路安全治理	負責編寫與維護網路安全管理手冊。	
	內部稽核及管理審查	負責內部稽核與管理審查，包括制定稽核計劃、執行稽核與發佈報告。	

	工具管理	負責網路安全工具的管理與使用監控。	
人力資源	網路安全文化	負責網路安全意識與專業技術培訓。	

4. 定義各工作領域的流程文件、範本及指引：

組織應針對各工作領域制定相應的流程文件、標準範本及實施指引，以確保網路安全工作的標準化、可追溯性與可執行性。這些文件應包含但不限於：

(1) 流程文件：詳細規範各項網路安全作業的執行步驟與責任分工。

(2) 標準範本：提供各類報告、審查文件、風險評估表等標準格式，確保資訊完整性與一致性。

(3) 實施指引：提供具體操作指引，幫助不同部門理解並有效執行安全政策與流程。

5. 具體實施案例：

(1) 網路安全管理手冊

網路安全管理手冊應明確定義網路安全管理系統的組織架構與權責，確保涵蓋所有標準要求的工作範圍與相關責任部門。該手冊作為指導文件，協助組織內各層級有效協作，確保網路安全工作的順利進行。

(2) 網路安全文件清單

文件清單應包括各工作領域所需的流程文件、範本、指引等必要資料，作為執行網路安全政策的基礎，確保標準化操作流程與可追溯性。

- RQ-05-02 產出文件
  - ■ 網路安全管理系統文件清單(對應 ISO/SAE 21434 之 WP-05-01)
    - ➔一、二階文件(手冊/程序書)：網路安全管理手冊、網路安全管理流程
    - ➔三階文件(作業指導書)：無

➔四階文件(範本/表單)：網路安全管理系統文件列表

[RQ-05-03]組織應指派並傳達責任及對應之組織權力，以達成與維護網路安全。

備考 7：此關聯組織和專案相關之活動。

- RQ-05-03 說明
  1. 依據部門職責，明確定義各部門內的網路安全相關角色及其職責，確保責任劃分清晰。
  2. 網路安全角色應涵蓋：
     (1) 組織層級的網路安全管理與監督活動。
     (2) 專案層級的網路安全執行與落實活動。
- RQ-05-03 實踐方式
  1. 組織層級網路安全角色與職責

     針對組織層級網路安全活動，清晰定義各部門內網路安全相關的角色及其職責，確保管理與執行的有效性。以下為範例：

     表 2 組織層級網路安全角色及職責示意表(供參，可基於實際組織角色進行調整)

角色	部門	職責
人事專員	人力資源部	負責網路安全培訓、網路安全能力建立與文化養成
IT 工程師	IT 部	負責資訊共用和資訊安全管理
網路安全內稽人員	品質保證部	負責網路安全內部稽核以及網路安全管理評鑑
系統網路安全工程師	系統工程部	負責網路安全工具管理

  2. 專案層級網路安全角色與職責

     針對專案層級網路安全活動，定義各相關角色的職責，確保專案安全要求的落實，圖 3 為舉例：

     表 3 專案層級網路安全角色及職責示意表(供參，可基於實際組織角色進行調整)

角色	部門	職責
專案層級網路安全經理	系統部門	➢ 負責網路安全計畫的制定和維護、任務分配 ➢ 負責組織相關部門開展網路安全活動，並審查工作成果 ➢ 監控網路安全活動的執行
系統網路安全工程師	系統部門	➢ 負責概念階段的相關組件定義與 TARA 分析 ➢ 負責系統網路安全架構設計與弱點識別 ➢ 負責識別和定義系統級網路安全需求
網路安全專家	系統部門	➢ 負責相關組件定義與 TARA 分析的審查 ➢ 負責執行網路安全評鑑
系統網路安全測試工程師	系統部門	➢ 負責制定系統層級網路安全測試計劃與測試範例 ➢ 負責執行系統層級網路安全測試

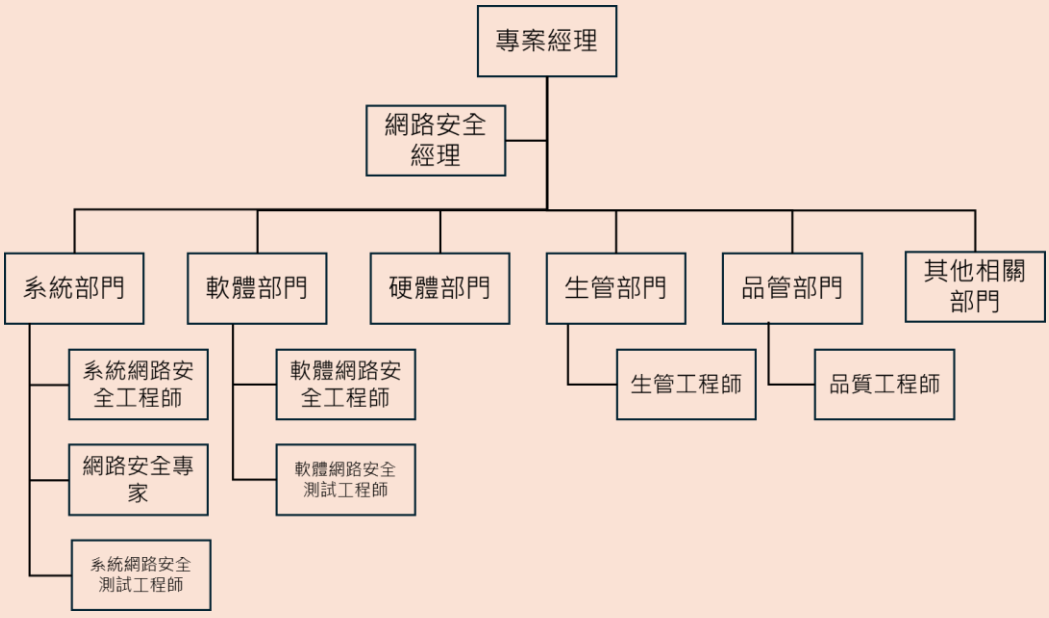


圖 3 專案層級網路安全組織示意圖

3. 實施案例：網路安全角色職責分配表

   根據網路安全管理手冊中的部門職責規範，定義各部門內與網路安全相關的角色及其職責，涵蓋組織層級與專案層級的網路安全管理活動。

   (1) 組織層級：確保各部門的網路安全治理、培訓、內稽與工具管理。

   (2) 專案層級：涵蓋網路安全計畫制定、架構設計、風險分析、評估與測試等關鍵活動。

   (3) 確保責任分工清晰：各角色能有效落實安全機制，提高整體網路安全管理能力。

- RQ-05-03 產出文件
  - ■ 網路安全角色職責分配文件清單(對應 ISO/SAE 21434 之 WP-05-01)
    - ➔一、二階文件(手冊/程序書)：網路安全管理流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全角色職責分配表

[RQ-05-04]組織應提供資源以因應網路安全問題。

備考 8：資源包含負責網路安全風險管理、開發及事件管理之人員。

例 2：履行網路安全活動之資深技術人員及合適的工具。

- RQ-05-04 說明

  資源應包括充足且具備合格能力的網路安全風險管理、開發和事件管理人員，以及支援網路安全活動所需的各類工具，這些工具需滿足組織層級與專案層級的網路安全需求，並涵蓋產品的整個生命週期。例如，網路安全測試設備、監控平台等，均屬此範疇。

- RQ-05-04 實踐方式

  組織應確保提供充足且適當的資源，以支援網路安全活動的順利推行，並透過計畫、手冊與佐證資料來確保資源可用性與有效性。

  1. 網路安全承諾與資源保障：

組織應在網路安全管理手冊中明確網路安全承諾，並確保提供足夠的資源，以支援各項網路安全活動的推展。

2. 專案層級資源識別與配置：
   在專案層級的網路安全活動實施前，應識別所需的資源，包括人員、工具、技術與財務支援，並確保其可用性，以滿足安全需求。
3. 網路安全計畫與資源規劃：
   在制定網路安全計畫時，應明確各項網路安全活動所需的資源，確保所有安全措施皆有足夠的支持，並落實至專案執行階段。
4. 資源支援的佐證資料：
   組織應提供資源配置的相關證明，例如人員部署任命、設備採購記錄、測試工具清單等，以確保資源已到位並能有效支持網路安全活動。

- RQ-05-04 產出文件
  - ■ 網路安全資源佐證資料清單(對應 ISO/SAE 21434 之 WP-05-01)
    - ➔一、二階文件(手冊/程序書)：網路安全管理流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：其他資源支持的證明資料，如人員部署任命等

[RQ-05-05]組織應識別與網路安全相關或互動之行為規範，並建立及維護此等行為規範間之溝通管道，以便：

(a)判定是否及如何將網路安全整合至既有過程中。

(b)協調相關資訊之交換。

備考 9：協調可包含在行為規範間共享過程及使用策略與工具。

備考 10：行為規範包含資訊技術安全、功能性安全及隱私。

例 3：行為規範間交換：

- 威脅情境及危害(參照 ISO 26262-1:2018 之 3.75)資訊。
- 網路安全目標及人身設備安全目標(參照 ISO 26262-1:2018 之 3.139)。

- 網路安全要求事項與功能安全性要求事項之衝突或競爭(參見 ISO 26262-1:2018 之 3.69)。

- RQ-05-05 說明

1. 組織應將網路安全活動整合到現有的營運流程中，並且要明確界定網路安全管理系統與其他現行品質管理系統(例如品質管理系統、資訊安全管理系統、隱私保護系統等)之間的相互關聯與協作。
2. 建立並維護這些系統間的有效溝通管道，例如，當網路安全需求與功能安全需求出現衝突時，應有機制來協調這些問題。

- RQ-05-05 實踐方式

1. 網路安全管理系統及品質管理系統：
   品質管理系統中的需求管理、組態管理、文件管理和變更管理等流程皆可支援網路安全管理系統。
2. 網路安全管理系統及資訊安全管理系統：
   資訊安全管理系統對車輛網路安全生命週期量產階段的產線資訊安全提出管理要求。
   資訊安全管理系統中的資產分級管理，支援網路安全管理系統中的資訊共用與保護。
3. 網路安全管理系統及軟體更新管理：
   網路安全管理系統中的事件回應流程會引用軟體更新管理，用於脆弱性修復。
4. 網路安全管理系統及隱私保護：
   網路安全管理系統風險分析中，對於資產隱私資料的影響進行評估，並結合隱私保護相關要求。
5. 網路安全管理系統及功能安全：
   (1) 概念設計階段功能安全可作為系統架構與網路安全目標識別的參考依據，透過功能失效模式分析可協助界定關鍵資產，進而支援網路安全威脅建模與風險評鑑，建立功能與網路安全整合的初步防護架構。

(2) 功能安全可以為分析網路安全威脅及風險提供支援，因為網路攻擊可以導致功能安全風險；在檢測到攻擊時，功能安全可以考慮電子/電氣系統行為相關的網路安全性原則。

(3) 產品開發階段功能安全措施可能影響網路安全，如冗餘監控可能會增加新的網路安全攻擊介面，帶來新的網路安全脆弱性；網路安全措施也可能影響功能安全，如網路安全控制措施可能導致系統反應時間延遲，進而影響功能安全機制。

(4) 營運階段功能安全機制需與網路安全事件通報與修補機制協同運作，以確保系統異常行為可及時識別與應對；網路安全更新(如 OTA)亦需確認不影響功能安全邏輯與性能，確保整體安全維持至產品除役(報廢)為止。

6. 網路安全事件導致的設計變更，可能進一步會影響功能安全。

7. 網路安全管理系統與其他系統交互如下表：

表 4 網路安全管理系統與其他系統交互示意表(供 RQ-05-05 產出文件之四階文件參考使用)

網路安全管理系統工作領域	品質管理系統 (ISO 9001/ IATF 16949)	資訊安全管理系統 (ISO 27001)	隱私保護 (ISO 27701)	功能安全管理系統 (ISO 26262)
網路安全治理	遵循文件管理流程			
網路安全文化	遵循培訓管理流程			
資訊共用		遵循資產的分級管理		
網路安全專案管理	遵循組態管理流程			
車輛網路安全生命週期管理	遵循需求管理和變更管理流程		TARA 分析中的隱私資料資產遵循隱私保護	

產品開發設計					可做為系統架構與安全目標識別參考依據，為分析威脅與風險提供支援等...
網路安全生產			遵循產線的資訊安全管理		
…					

- RQ-05-05 產出文件
  - ■ 網路安全交互規則與過程文件清單(對應 ISO/SAE 21434 之 WP-05-01)
    - ➔一、二階文件(手冊/程序書)：網路安全管理流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全管理系統與其他品質系統的交互表

5.4.2 網路安全文化

[RQ-05-06]組織應培育及維護強健之網路安全文化。

備考 1：參照 ISO/SAE 21434 附錄 B 之示例。

- RQ-05-06 說明

  組織需建立使成員都具備高度的安全意識與責任感，避免因觀念薄弱而導致的安全脆弱性。ISO/SAE 21434 附錄 B 中有具體舉例供參，若企業具備強而有力的網路安全文化，那與網路安全有關的決定與責任歸屬將是可以追溯，網路安全保障是最高優先，對於落實網路安全與否應賞罰分明等，而該文化的形成是需要制度與組織方法約束，由上而下實踐。
- RQ-05-06 實踐方式

如同說明，網路安全文化的建立方法因不同組織而異，需要各部門去組織與落實，以人員培養的角度來看，提升團隊對於網路安全的瞭解與素養，可以透過新人培訓、專題講座、案例分享、讀書會等方式來推動，具體內容可參照[RQ-05-08]。

- RQ-05-06 產出文件

  參照[RQ-05-08]。

[RQ-05-07]組織應確保指派網路安全角色及責任之人員具備履行之適任性與認知。

備考 2：適任性、認知及訓練計畫可包含：

- 關於網路安全之組織規則及過程，包含網路安全風險管理。
- 關於網路安全相關行為規範之組織規則及過程，例：功能性安全與隱私。
- 領域知識。
- 系統工程。
- 網路安全相關方法、工具及指導綱要。
- 已知攻擊方法和網路安全控制措施。

- RQ-05-07 說明

  組織需確保所有負責網路安全工作的人員，不僅要有執行這些任務所需的技能和知識，還要有充分的安全意識。

  1. 具備能力：

     相關人員應接受適當的培訓，並具備完成網路安全任務所需的專業技能和技術知識。例如：能夠識別和應對網路威脅、瞭解安全工具的操作等。

  2. 具備意識：

     除完成任務外，還需理解網路安全對整個組織和產品安全的重要性。例如：意識到疏忽或操作不當可能導致嚴重的資安事件。

- RQ-05-07 實踐方式

  參照[RQ-05-08]。

- RQ-05-07 產出文件

參照[RQ-05-08]。

[RQ-05-08]組織應建置並維護持續改善過程。

例：持續改善過程，包含：

- 從先前經驗中學習，包含藉由網路安全監督所收集之網路安全資訊，及對內部及外部網路安全相關資訊之觀察。
- 從網路安全相關資訊中學習關於此場域相似應用之產品。
- 後續網路安全活動中應用衍生改善。
- 對適當人員傳達有關網路安全習得之經驗。
- 依據[RQ-05-02]檢查組織規則及過程之適足性。

備考 3：持續改善適用於 ISO/SAE 21434 之所有網路安全活動。

- RQ-05-08 說明
  1. 企業應建立車輛網路安全文化，同時進行網路安全文化活動。
  2. 網路安全文化是企業內部關於網路安全的涵義達成的共識。
  3. 網路安全文化包括網路安全意識，網路安全能力以及持續改善。
  4. 安全文化意識管理、培訓紀錄、稽核報告等可以作為網路安全文化的實施證據。
- RQ-05-08 實踐方式

  企業應建立車輛網路安全文化，同時進行網路安全文化活動。
  1. 建立與維護網路安全能力管理流程：

     定義網路安全相關人員能力要求，確保被分配網路安全角色和職責的人員具有 ISO/SAE 21434 和企業網路安全要求方面的能力。能力要求範例如：

     (1) 參與網路安全相關培訓。

     (2) 獲得網路安全相關能力認證。

     (3) 具備的網路安全相關專案經驗等。
  2. 網路安全培訓管理：

規範和執行網路安全培訓管理，使員工對網路安全文化、政策等瞭解與認同，並提高網路安全相關角色專業技術能力。可參考品質管理系統人員培訓管理辦法。

3. 網路安全管理系統持續改善流程：

(1) 規範企業網路安全管理系統持續改善流程，主要流程可包括：持續改善項目的收集、改善項目需求分析、制定改善計畫及改善效果評估等。

(2) 持續改善的來源可包括：內外部稽核發現、品質系統運行中發現的問題、風險或機會、專案經驗教訓等。

- RQ-05-06、RQ-05-07、RQ-05-08 產出文件
  - ■ 網路安全能力管理、意識管理及持續改善的佐證文件清單(對應 ISO/SAE 21434 之 WP-05-02)
    - ➔一、二階文件(手冊/程序書)：網路安全能力管理流程、網路安全培訓管理流程、網路安全管理系統持續改善流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全能力管理矩陣、網路安全能力評估紀錄、培訓計畫、培訓管理紀錄、持續提升的證明

5.4.3 資訊共享

[RQ-05-09]組織應定義在組織內部或外部要求、允許或禁止與網路安全相關資訊共享之情況。

備考：共享資訊之情況可基於：

- 可共享之資訊型式。
- 共享之核可過程。
- 刪減資訊之要求事項。
- 來源屬性之規則。
- 特定方之通訊型式。
- 脆弱性揭露程序(參照 5.4.1 備考 5)。
- 對接收方處理高度敏感資訊之要求事項。

- RQ-05-09 說明

  組織應基於上述進行盤點與確認，以明確定義共用資訊，並按[RC-05-10]落實管理。
- RQ-05-09 實踐方式

  參照[RC-05-10]。
- RQ-05-09 產出文件

  參照[RC-05-10]。

[RC-05-10]組織宜依[RQ-05-09]與其他方共享資料之資訊安全管理一致。

例：公眾的、內部的、機密的、第三方機密的安全分類等級之一致性。

- RC-05-10 說明
  1. 網路安全有關的資訊需要規範管理，避免資訊的洩露和濫用。如未披露的脆弱性資訊因為洩露而被駭客利用，造成網路安全事件。
  2. 網路安全資訊的管理包括內部共享以及外部共享。
  3. 該要求的實施可參考 ISO 27001。
- RC-05-10 實踐方式
  1. 網路安全資訊共享管理流程：
     (1) 企業應明確網路安全資訊定義及範圍，建立並維護網路安全資訊資產。網路安全資訊資產可以包括：
        I. 流程文件(如範本、流程規定)。
        II. 專案資料(如測試資料)。
        III. 文件資料。
        IV. 市場資料。
     (2) 企業應建立網路安全資訊資產評級標準及流程，安全分類級別如公共、內部、機密、協力廠商機密等。
     (3) 企業應建立網路安全資訊共享管理制度，可包括：
        I. 審核流程。
        II. 不同級別資訊的共享管道管理規定。

III. 接收方的安全性原則要求。

- RC-05-10 產出文件
  - ■ 網路安全資訊共享管理文件清單(對應 ISO/SAE 21434 之 WP-05-01)
    - ➔一、二階文件(手冊/程序書)：網路安全資訊共享管理文件流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：無

5.4.4 管理系統

[RQ-05-11]組織應依標準或等效規約，建置及維護品質管理系統，以支持網路安全工程，並處理：

例 1：IATF 16949 與 CNS 12681 聯合使用。

(a)變更管理。

備考 1：網路安全變更管理適用範圍為管理項目及其組件之變更，以持續滿足適用之網路安全目標與要求事項，例：依生產控制計畫審查生產過程之變更，預防此變更引入新的脆弱性。

(b)文件化管理。

備考 2：工作產出可組合或對映至不同的文件化儲存庫。

(c)組態管理。

(d)需求事項管理。

- RQ-05-11 說明

  品質管理系統中的變更管理、文件化管理、組態管理和需求事項管理可以支援網路安全工程。

  1. 變更管理流程：
     (1) 網路安全工程應遵循品質管理系統的變更管理流程。
     (2) 網路安全相關角色需要參與變更的影響評估。
     (3) 變更影響分析中需要考慮對於網路安全相關產物的影響，比如產品變更影響相關組件的定義，進而影響網路安全目標和需求。
  2. 文件化管理流程：

網路安全相關文件應遵循品質管理系統的文件管理流程。

3. 組態管理流程：
   網路安全專案應遵循品質管理系統的組態管理流程。
4. 需求事項管理流程：
   網路安全需求應遵循品質管理系統的需求管理流程。

- RQ-05-11 實踐方式
  參照[RC-05-13]。
- RQ-05-11 產出文件
  參照[RC-05-13]。

[RQ-05-12]於產品的網路安全支援結束前，現場維護產品網路安全所需的組態資訊應保持可用，以確保可採取補救措施行動。

備考 3：構建環境之歸檔對於確保組態資訊之後續使用是有用的。

例 2：材料清單、軟體組態。

- RQ-05-12 說明
  1. 在後開發階段對產品的網路安全進行維護，例如脆弱性修復。在產品開發、生產階段相關的組態資訊，須保留直至產品的網路安全支援結束。
  2. 組態資訊包括與產品網路安全相關的關鍵資料，如產品硬體和軟體的版本資訊。這些資訊是維護車輛網路安全的基礎，用於快速定位脆弱性、分析攻擊路徑，並制定針對性的修復措施。
  3. 保持可透過生產系統和流程定義來保證。
- RQ-05-12 實踐方式
  1. 生產系統透過建立可靠的管理系統，確保資訊可追溯性且未被竄改。例如使用加密存儲和存取權限控制來保護組態資料的完整性。
  2. 流程定義通過文件化和標準化管理流程，如定期組態資料備份、系統升級或變更時同步更新組態資訊等。
- RQ-05-12 產出文件
  參照[RC-05-13]。

[RC-05-13]宜建立生產過程之網路安全管理系統，以支援 ISO/SAE 21434 第 12 節之活動。

例 3：IEC 62443-2-1。

- RC-05-13 說明
  1. 為防止在生產過程中引入脆弱性，宜建立生產過程的網路安全管理體系，維護安全的生產環境。
  2. 生產過程的網路安全管理系統可採取縱深防禦的方法，如實體環境防護、安全的工廠網路架構、工廠系統安全、伺服器終端安全等。
- RC-05-13 實踐方式

  ISO 27001 及 IEC 62443-2-1 等可以作為實踐參考。
- RQ-05-11、RQ-05-12、RC-05-13 產出文件
  - ■ 組織品質管理系統的佐證文件清單(對應 ISO/SAE 21434 之 WP-05-03)
    - ➔一、二階文件(手冊/程序書)：QMS 品質管理相關流程(變更管理、文件管理、組態管理、要求管理)
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：品質管理系統相關實施證明

5.4.5 工具管理

[RQ-05-14]應管理可能影響項目或組件網路安全之工具。

例 1：用於概念或產品開發之工具，例：基於模型之開發、靜態檢查、查證工具。

例 2：生產過程中使用之工具，例：燒錄器、產線終端測試設備。

例 3：用於維護之工具，例：車載診斷工具或可再程式設計工具。

備考：此類管理可藉以下方式建立：

- 具備勘誤表之使用手冊的應用。
- 保護避免意外使用或行動。
- 工具使用者之存取控制。
- 工具之鑑別。

- RQ-05-14 說明

  工具管理目的在於確保使用於開發與測試過程的工具不會對網路安全產生負面影響，可透過上述之備考來進行管理。
- RQ-05-14 實踐方式

  參照[RQ-05-14]備考。
- RQ-05-14 產出文件

  參照[RC-05-15]。

[RC-05-15]直至產品之網路安全支援結束前，支援網路安全事件補救措施行動(參照 ISO/SAE 21434 第 13.3 節)之適當環境宜為可重現。

例 4：用於可重現及管理脆弱性之測試、軟體建構與開發環境。

例 5：用於建構產品之軟體的工具鏈及編譯器。

- RC-05-15 說明
  1. 使用的工具不應對產品的網路安全產生不利的影響，如不會由於工具的原因，而給產品引入脆弱性。
  2. 應保留相關的網路安全工具，以支援網路安全事件發生時的補救行動，直至產品的網路安全支援結束。
- RC-05-15 實踐方式

  網路安全相關工具管理流程：
  1. 定義網路安全相關工具的管理範圍，建立網路安全相關工具清單，以便有效管理工具使用情況。如用於概念或產品開發的工具，在生產過程中使用的工具及用於維護的工具等。
  2. 開展工具的網路安全影響分析，如工具網路安全相關的狀態、誤操作或組態錯誤的安全影響等。
  3. 建立網路安全相關工具的管理策略，如許可權管理、存取控制、工具變更等。
  4. 開展網路安全工具日常的維護保養，如定期的脆弱性掃描、除役(報廢)時敏感性資料的清除等。
- RQ-05-14、RC-05-15 產出文件

■ 網路安全工具管理文件清單(對應 ISO/SAE 21434 之 WP-05-04)

➔一、二階文件(手冊/程序書)：網路安全相關工具管理流程

➔三階文件(作業指導書)：無

➔四階文件(範本/表單)：網路安全相關工具清單、網路安全相關工具影響評估報告、網路安全相關工具管理實施證據

5.4.6 資訊安全管理

[RC-05-16]工作產出宜依資訊安全管理系統進行管理。

例：工作產出可儲存於檔案伺服器上，預防未經授權的變更或刪除。

- RC-05-16 說明

  網路安全相關的工作產出宜依據資訊安全管理系統進行管理，例如存放於檔案伺服器上，並透過存取控制或權限管理等策略，確保工作產出不會被未授權的人員更改或刪除。

- RC-05-16 實踐方式

  可參考資訊安全管理系統相關要求。

- RC-05-16 產出文件

  ■ 網路安全工具管理文件清單(對應 ISO/SAE 21434 之 WP-05-03)

  ➔一、二階文件(手冊/程序書)：資訊安全管理文件相關流程

  ➔三階文件(作業指導書)：無

  ➔四階文件(範本/表單)：資訊安全管理證明

5.4.7 組織網路安全稽核

[RQ-05-17]應獨立履行網路安全稽核，以判斷組織流程是否達到 ISO/SAE 21434 之目的。

備考 1：網路安全稽核可包含或合併於品質管理系統標準進行之稽核中，例如 IATF 16949 與 CNS 12681 聯合使用。

備考 2：獨立性為基於 ISO 26262 系列等。

備考 3：稽核之履行人員可為組織內部或外部。

備考 4：為確保組織流程保持網路安全之適切性，可定期履行稽核。

備考 5：圖 6 說明與其他網路安全活動相關之組織網路安全稽核。

- RQ-05-17 說明
  1. 企業應開展獨立的網路安全稽核，以判斷組織流程達到網路安全目標。
  2. 企業應按照定義的網路安全稽核流程實施稽核。
- RQ-05-17 實踐方式

  網路安全稽核流程：
  1. 建立網路安全稽核流程，以保證車輛網路安全管理系統規範運行。
  2. 應確保網路安全稽核員的獨立性、能力和資格要求。
  3. ISO/PAS 5112 緊密銜接 ISO/SAE 21434，可以作為支持和指導稽核過程的參考與依據。
- RQ-05-17 產出文件
  - 組織網路安全稽核文件清單(對應 ISO/SAE 21434 之 WP-05-05)
    - ➔一、二階文件(手冊/程序書)：網路安全稽核流程
    - ➔三階文件(作業指導書)：網路安全稽核指引(參照 ISO/PAS 5112)
    - ➔四階文件(範本/表單)：網路安全稽核計劃、網路安全稽核報告

6. 專案相依之網路安全管理

6.1 一般

本節說明有關特定專案之網路安全開發活動管理的要求事項。

專案相依之網路安全管理包含責任配置(參照 ISO/SAE 21434 第 6.4.1 節)及網路安全活動規劃(參照 ISO/SAE 21434 第 6.4.2 節)。ISO/SAE 21434 以通用方式定義要求事項，以便適用於各種項目與組件。此外，可應用基於理由闡述並於網路安全計畫中定義的裁適(參照 ISO/SAE 21434 第 6.4.3 節)。可使用裁適之範例包含：

- 再利用(參照 ISO/SAE 21434 第 6.4.4 節)。
- 全景外之組件(參照 ISO/SAE 21434 第 6.4.5 節)。
- 使用現成組件(參照 ISO/SAE 21434 第 6.4.6 節)。
- 更新(參照 ISO/SAE 21434 第 13.4 節)。

項目及組件之再利用係可能的開發策略，無論是否對項目、組件或其運作環境進行修改，都可應用此策略。然而，修改可能會引入原始項目或組件未考量到之脆弱性。此外，已知的攻擊可能亦發生變化，例：

- 攻擊技術之演進。
- 新出現的脆弱性，例：從網路安全監督(參照 ISO/SAE 21434 第 8.3 節)及/或網路安全事件評估(參照 ISO/SAE 21434 第 8.4 節)中學習。
- 自最初開發至今之資產變化。

若原始項目或組件是依 ISO/SAE 21434 開發，則此項目或組件之再利用將基於現有的工作產出。若項目或組件最初並非依 ISO/SAE 21434 開發，則亦可基於現有文件提供理由闡述再利用。

組件可以於全景外開發，即基於假設的全景。在與顧客約定或達成商業協議前，組織可為不同的應用程式及不同的顧客開發通用組件。供應者可對全景及預期的用途提出假設。於此基礎上，供應者可得出全景外的開發需求。

例：全景外可開發的微控制器。

現成組件是指不為特定顧客開發之組件，可在不修改其設計或實作的情況下使用，例：第三方軟體函式庫，開源軟體組件。不預先假設現成的組件是依 ISO/SAE 21434 開發。

圖 4 顯示，現成組件及全景外的組件都可依 ISO/SAE 21434 整合至項目或組件中。整合可能牽涉類似於 ISO/SAE 21434 第 6.4.4 節中再利用分析之活動，若進行變更以因應無效之假設，則適用變更管理(參照 ISO/SAE 21434 第 5.4.4 節)。可針對欲整合之組件及/或作為整合目標之組件或項目進行變更。

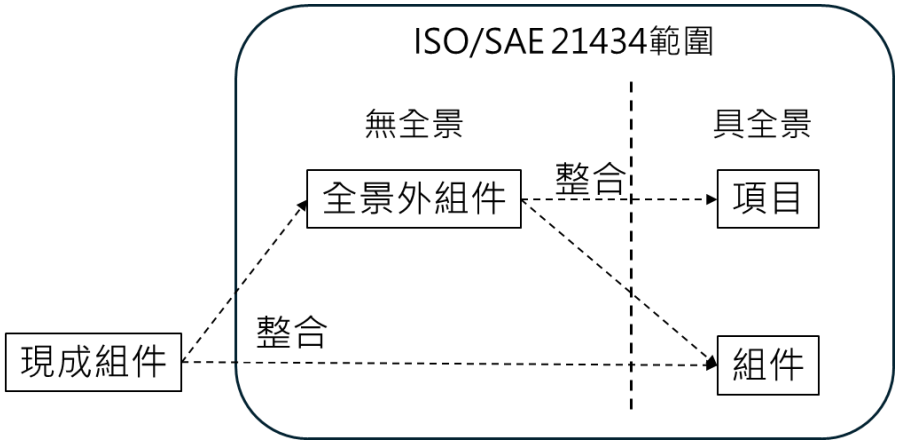


圖 4 現成組件與全景外組件之整合

網路安全案例(參照 ISO/SAE 21434 第 6.4.7 節)為網路安全評鑑及後開發(post-development)釋出的輸入。

網路安全評鑑(參照 ISO/SAE 21434 第 6.4.8 節)應獨立的判斷項目或組件之網路安全，且為後開發釋出與否決定的輸入(參照 ISO/SAE 21434 第 6.4.9 節)。

6.2 目的

本節目的為：

(a)指派有關專案之網路安全活動的責任。

(b)規劃網路安全活動，包含已裁適之網路安全活動的定義。

(c)產生網路安全案例。

(d)履行網路安全評鑑(若適用)。

(e)從網路安全的角度決定項目或組件是否可釋出供後開發用。

6.3 輸入

6.3.1 先決條件

無。

6.3.2 更多支援資訊

可考量以下資訊：

- 組織網路安全稽核報告[ISO/SAE 21434 之 WP-05-03]。
- 專案計畫。

6.4 要求事項及建議事項之實踐指引

6.4.1 網路安全責任

[RQ-06-01]應依[RQ-05-03]指派及傳達關於專案網路安全活動之責任。

備考：在可進行溝通並可取得相關資訊前提下，網路安全活動的責任是可被移轉的。

- RQ-06-01 說明
  1. 識別網路安全相關專案中的所有網路安全活動。
  2. 定義每個網路安全活動的角色和職責。
- RQ-06-01 實踐方式

  網路安全計畫流程：
  1. 在啟動和確定涉及網路安全的專案組織架構圖時，分配網路安全相關角色，如專案網路安全經理、網路安全測試工程師。
  2. 明確每個角色的職責和能力要求。
  3. 指定具體人員擔任相關角色，並評定人員是否滿足該角色之能力要求。
- RQ-06-01 產出文件

  參照[RQ-06-12]。

6.4.2 網路安全計畫

[RQ-06-02]為決定項目或組件所需的網路安全活動，應分析此項目或組件以判定：

(a)此項目或組件是否與網路安全相關。

備考 1：ISO/SAE 21434 附錄 D 提供可用於評鑑網路安全相關性之方法及準則。

備考 2：若此項目或組件被判定為與網路安全無關，則不存在網路安全活動，因此網路安全計畫便不會持續。

(b)若項目或組件與網路安全相關，則不論此項目或組件是否為新開發或再利用。

(c)是否依 ISO/SAE 21434 第 6.4.3 節進行裁適。

- RQ-06-02 說明
  1. 在制定網路安全計畫前，應進行分析並確定專案中的相關項目或組件是否與網路安全相關，具體分析過程和方法可參考 ISO/SAE 21434 附錄 D。
  2. 若該專案中的相關項目或組件與網路安全無關，則無需制定網路安全計畫。
  3. 若該專案的相關項目或組件與網路安全相關，則判斷該專案的相關項目或組件是新開發還是再利用。
  4. 若該專案的相關項目或組件是再利用，則按照 ISO/SAE 21434 第 6.4.3 節的要求進行活動裁適。
- RQ-06-02 實踐方式

  網路安全計畫流程：
  1. 參考 ISO/SAE 21434 中附錄 D 開展網路安全相關性分析，產出網路安全相關性分析報告。
  2. 若相關項目或組件與網路安全相關，則定義網路安全活動，網路安全活動可按以下參考展開，包括但不限於：
     (1) 網路安全管理活動：
        I. 網路安全裁適分析。
        II. 網路安全案例。
        III. 網路安全評估。
        IV. …
     (2) 網路安全支援活動：
        I. 組態管理，
        II. 分散式開發。
        III. …

(3) 網路安全生命週期活動：

I. 概念。

II. 產品開發。

III. 網路安全確認。

IV. ...

3. 參照 ISO/SAE 21434 第 6.4.3 節對以上活動進行裁適。

- RQ-06-02 產出文件

  參照[RQ-06-12]。

[RQ-06-03]網路安全計畫應包含：

(a)活動之目的。

(b)對其他活動或資訊之依賴性。

(c)負責履行活動之當責人員。

(d)履行活動所需之資源。

(e)活動的起點或終點，以及預期持續時間。

(f)識別欲產生之工作產出。

- RQ-06-03 說明

  網路安全計畫應按上述考量，按產品生命週期評估過程中各階段訴求，與相應所需的投入、對應之產出。

- RQ-06-03 實踐方式

  參照[RQ-06-05]。

- RQ-06-03 產出文件

  參照[RQ-06-12]。

[RQ-06-04]開發及維護網路安全計畫且依網路安全計畫追蹤網路安全活動進展的責任，應依[RQ-05-03]和[RQ-05-04]進行指派。

- RQ-06-04 說明

  計畫中需參照[RQ-05-03]網路安全職責分配與授權機制，來明確分配網路安全職責與授權，以及[RQ-05-04]組織應提供解決網路安全

問題的資源，包括充足且具備合格能力的人員、支援網路安全活動所需的各類工具等，來給予支援。

- RQ-06-04 實踐方式

  參照[RQ-06-05]。

- RQ-06-04 產出文件

  參照[RQ-06-12]。

[RQ-06-05]網路安全計畫應為：

(a)於開發專案計畫中參引。

(b)包含於專案計畫中，以便可區別網路安全活動。

備考 3：網路安全計畫可包含對其他計畫(例：專案計畫)的相互參引，此等計畫亦需位於組態管理之下(另參照[RQ-06-09])。

- RQ-06-05 說明

  1. 網路安全計畫應包含每個活動的完整內容，包括[RQ-06-03]中規定的相關輸入。
  2. 應明確制定、維護網路安全計畫及追蹤網路安全活動的各相關角色與職責。
  3. 網路安全計畫是主專案計畫的重要組成部分，可參考以下方式管理：
     (1) 單獨管理：
     獨立於主專案計畫，但在需要時被引用。
     (2) 合併管理：
     融合於主專案計畫中，並在其中清楚標示網路安全相關工作活動。

- RQ-06-03、RQ-06-04、RQ-06-05 實踐方式

  網路安全計畫流程：

  1. 定義網路安全計畫中每個活動的內容。
  2. 定義制定網路安全計畫、維護網路安全計畫以及網路安全計畫活動追蹤的相關角色和職責。

3. 定義網路安全計畫與主專案計畫的對應階段和里程碑，將網路安全計畫中的活動對應到主專案計畫的相應階段和里程碑。如 A 階段完成網路安全概念，B 階段完成網路安全設計和查證，C 階段進行網路安全相關的缺陷修復。

- RQ-06-05 產出文件

  參照[RQ-06-12]。

[RQ-06-06]網路安全計畫應依 ISO/SAE 21434 第 9、10、11 及 15 節之相關要求事項，於概念及產品開發階段時，規定網路安全所需的活動。

- RQ-06-06 說明

  在產品開發階段，需按 ISO/SAE 21434 第 9、10、11 和 15 節進行網路安全所需相關活動。

- RQ-06-06 實踐方式

  參照[RQ-06-07]。

- RQ-06-06 產出文件

  參照[RQ-06-12]。

[RQ-06-07]當識別履行的活動發生變更或精細化時，應更新網路安全計畫。

備考 4：網路安全計畫可於開發過程中逐步完善。例：網路安全計畫可依網路安全活動的結果進行更新，如同 TARA(參照 ISO/SAE 21434 第 15 節)。

- RQ-06-07 說明

  網路安全計畫需要動態更新，確保隨著開發進度和新資訊的出現，計畫內容能夠精確反應當前需求和目標。

  1. 網路安全計畫中應包含 ISO/SAE 21434 中第 9、10、11 和 15 節所要求的網路安全活動，確保符合相關規範和要求。
  2. 網路安全計畫需隨著開發過程的進展持續更新，以保持內容的完整性和適用性。例如：

(1) 專案初期：根據主專案計畫制定初版網路安全專案計畫。

(2) TARA 分析後：根據識別出的網路安全目標和網路安全聲明，更新網路安全專案計畫。

(3) 系統架構完成後：根據再利用分析、供應者管理等資訊，進一步更新網路安全專案計畫。

- RQ-06-06、RQ-06-07 實踐方式

  網路安全計畫流程：

  1. 定義網路安全計畫中的網路安全活動，根據 ISO/SAE 21434 第 9、10、11 和 15 節的相關要求，指定概念、產品開發階段網路安全所需的活動，可參考[RQ-06-02]實踐方式。
  2. 隨著開發過程的不斷進行，網路安全計畫須不斷更新。

- RQ-06-07 產出文件

  參照[RQ-06-12]。

[PM-06-08]依 ISO/SAE 21434 第 15.8 節的分析判定的風險值為 1 之威脅情境，可省略 ISO/SAE 21434 第 9.5、10 及 11 節之符合性。

備考 5：若此等威脅情境可能對網路安全產生影響，儘管可能不如 ISO/SAE 21434 中定義的嚴格，仍須對相對應風險進行處理。

備考 6：可依網路安全案例中定義之理由闡述此類風險處理的充分性。其理由闡述可基於品質管理標準之符合性，例如 IATF 16949 與 CNS 12681 聯合使用，並組合其他措施，例：

- 網路安全認知保證。
- 品質人員之網路安全訓練。
- 組織品質管理系統中定義的網路安全特定措施。

- PM-06-08 說明

  1. 綜合考慮風險與成本，對於風險值為 1 的威脅場景，允許不採取額外的網路安全控制措施，但對於風險仍需進行處理，如論證該風險可接受的理由，同時納入網路安全聲明進行監控。

2. 該風險是否接受可以在網路安全案例中進行論證，論證理由可以是基於符合品質管理標準，該風險處於受控狀態。

- PM-06-08 實踐方式

  對於威脅分析和風險評估方法產生的威脅場景的風險值為 1，則可以省略相應的網路安全活動及作業產出。該要求可以定義在流程文件中，即對於低風險的威脅場景可以進行接受，但是需要在網路安全案例中論述接受的理由，同時納入網路安全聲明進行持續的網路安全監控。

- PM-06-08 產出文件

  參照[RQ-06-12]。

[RQ-06-09]網路安全計畫中已識別之工作產出，應進行更新及維護其準確性，直至後開發釋出為止。

- RQ-06-09 說明

  網路安全計畫中的作業產出(例如風險評估報告、測試報告等)應隨著項目的進展不斷反應最新的安全需求和風險狀況，直到產品發行完成。意即網路安全工作不僅限於開發階段的初期分析，而是應在整個開發過程中持續進行，以確保產品在任何階段都能滿足安全要求。

- RQ-06-09 實踐方式

  網路安全計畫中的作業產出應納入組態管理，以進行更新，同時為維護其準確度，應進行安全的儲存，建立存取控制，許可權限管理等安全措施。

- RQ-06-09 產出文件

  參照[RQ-06-12]。

[RQ-06-10]若網路安全活動為分散式，則顧客與供應者應依 ISO/SAE 21434 第 7 節各自定義關於個別網路安全活動與介面有關之網路安全計畫。

- RQ-06-10 說明

若網路安全開發活動涉及到多方合作，顧客和供應者需要各自訂自己的網路安全開發計畫，制定計畫的依據來自雙方協定好的工作分工和職責分工，具體內容可參考 ISO/SAE 21434 第 7 節的相關規定。

- RQ-06-10 實踐方式
  規劃分散式網路安全活動，符合 ISO/SAE 21434 第 7 節的要求。
- RQ-06-10 產出文件
  參照[RQ-06-12]。

[RQ-06-11]網路安全計畫應依 ISO/SAE 21434 第 5.4.4 節進行組態管理及文件化管理。

- RQ-06-11 說明
  組態管理指的是對所有與網路安全相關的工作成果、文件、工具和資源進行嚴格控制，確保它們在整個開發過程中保持一致性和可追溯性。文件化管理則要求將所有關鍵的安全文件進行詳細記錄，以便於日後的查驗和審核，並保證網路安全措施在整個開發過程中得到有效實施。
- RQ-06-11 實踐方式
  參照[RQ-06-12]。
- RQ-06-11 產出文件
  參照[RQ-06-12]，

[RQ-06-12]網路安全計畫中已識別之工作產出應依 ISO/SAE 21434 第 5.4.4 節進行組態管理、變更管理、需求事項管理及文件化管理。

- RQ-06-12 說明
  1. 在產品開發設計凍結之前的整個開發過程中，網路安全開發計畫中的工作產出需要被更新和維護，確保狀態跟專案整體保持一致。

2. 針對網路安全計畫中的工作產出應制定相關確認措施，以保證其準確性，如評估和審查。
3. 按照組態管理和文件化管理流程對網路安全計畫實施管理。
4. 按照組態管理、變更管理、需求事項管理和文件化管理流程對網路安全計畫中確定的作業產出進行管理。

- RQ-06-11、RQ-06-12 實踐方式

1. 針對網路安全計畫中的工作產出，應制定相關確認措施以保證其準確性，如審查和檢查。
2. 網路安全計畫中確定的工作產出應遵循組態管理、變更管理、需求事項管理和文件化管理，例如需求開發及管理工作，遵循需求事項管理規定。
3. 網路安全計畫應遵循組態管理和文件化管理。

- RQ-06-01 至 RQ-06-12 產出文件
  - ■ 網路安全計畫文件清單(對應 ISO/SAE 21434 之 WP-06-01)
    - ➔一、二階文件(手冊/程序書)：網路安全計畫程序書
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全相關性分析報告、網路安全計畫範本

6.4.3 裁適

[PM-06-13]可裁適網路安全活動。

- PM-06-13 說明

1. 裁適指的是根據組織的特定需求、產品特性、開發環境或法規要求，對標準中的網路安全要求進行適當的調整，以確保其可行性與適用性。
2. 裁適並不代表削減安全要求，而是根據實際情況，調整方法、範圍或細節，確保標準能夠有效應用於不同類型的車輛或零組件開發過程。

- PM -06-13 實踐方式

參照[RQ-06-14]。

- PM -06-13 產出文件

  參照[RQ-06-22]。

[RQ-06-14]若網路安全活動為已裁適，則應提供與審查裁適的充分性且足以達到 ISO/SAE 21434 相關目的之理由闡述。

備考：因活動係由供應鏈中另一個體履行，而未履行，則不視為裁適活動，而視為分散式網路安全活動(參照 ISO/SAE 21434 第 7 節)。然而，分散式網路安全活動亦可能導致聯合裁適(參照 ISO/SAE 21434 第 7.4.3 節)。

- RQ-06-14 說明

  1. 網路安全活動可以被裁適，但前提是需要提供裁適理由並接受審查。裁適理由如：
     (1) 結構簡單，硬體架構設計活動被裁適。
     (2) 專案中的組件基於再利用、全景外的組件、現成組件等。
  2. 分散式的網路安全活動可以實施聯合裁適，如供應者所開發的產品網路安全風險較低，其網路安全測試在顧客同意的情況下可以被裁適。
  3. 裁適包括省略網路安全活動，以及補充相關網路安全活動。

- PM-06-13、RQ-06-14 實踐方式

  網路安全活動裁適分析流程：

  網路安全活動可以被裁適，對應的裁適理由需要提供並審查。

- RQ-06-14 產出文件

  參照[RQ-06-22]。

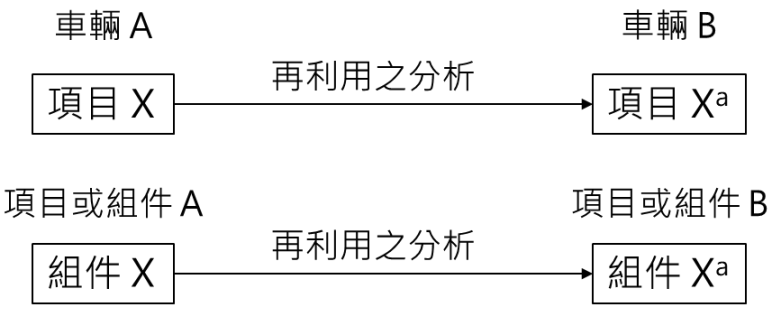
6.4.4 再利用

[RQ-06-15]若某個項目或組件已開發且滿足以下條件，則應進行再利用分析：

(a)已規劃修改。

(b)規劃將於另一個運作環境中再利用。

例 1：因於新的運作環境中安裝既有之項目或組件，或升級與其互動的其他項目或組件，而導致對環境的修改(參照圖 5)。



註(a)：可依再利用之分析結果進行變更。

圖 5 再利用之分析示例

(c)已規劃不修改的再利用，且有關此項目或組件之資訊有相關變更。

例 2：已知攻擊及脆弱性或威脅情境發生變更。

備考 1：判定是否可再利用時，需考量既有之工作產出。

備考 2：修改可包含設計修改及/或實作修改，其中：

- 設計修改可能來自需求事項的修改，例：功能或效能增強。
- 實作修改可能是因軟體修正或新生產或維護工具之使用而導致，例：模組式開發。

備考 3：若組態資料或校準資料的變更，導致衝擊項目或組件的功能行為、資產或網路安全性質，則此變更被視為修改。

- RQ-06-15 說明

  再利用之目的與意義為：

  1. 確保適用性：檢查原本的安全設計是否仍然適用於新的應用環境。
  2. 識別新風險：即使該項目或組件曾經滿足安全要求，在新的使用情境下可能會產生新的威脅或脆弱性
  3. 提高開發效率：如果確認安全性無虞，可以減少不必要的重新開發，提高組件的可重複使用性。

- RQ-06-15 實踐方式

  參照[RQ-06-17]。

- RQ-06-15 產出文件
  參照[RQ-06-22]。

[RQ-06-16]項目或組件的再利用之分析應：

(a)識別項目或組件及其運作環境的修改。

(b)分析修改對網路安全的影響，包含對網路安全聲明及先前所作假設的有效性影響。

例 3：對網路安全要求事項、設計及實作、運作環境、假設與運作模式的有效性、維護、對已知攻擊的耐受性以及已知脆弱性或資產暴露的影響。

(c)識別受影響或遺失之工作產出。

例 4：TARA 考量新的或修改之資產、威脅情境或風險值。

(d)於網路安全計畫中規定符合 ISO/SAE 21434 所需之網路安全活動(參照 ISO/SAE 21434 第 6.4.2 節)。

備考 4：此可能意味著裁適(參照 ISO/SAE 21434 第 6.4.3 節)。

- RQ-06-16 說明
  再利用需要進行分析，確保其適用性、安全性及合規性，避免因環境變更而產生安全風險。
- RQ-06-16 實踐方式
  參照[RQ-06-17]。
- RQ-06-16 產出文件
  參照[RQ-06-22]。

[RQ-06-17]組件的再利用分析應評估是否：

(a)此組件能滿足要整合之項目或組件配置之網路安全要求事項。

(b)既有文件足以支援整合至一個項目或另一個組件中。

- RQ-06-17 說明
  1. 該再利用的組件進行修改分析。
  2. 根據修改的變化點，識別受影響的或者缺失的工作產出。

3. 根據修改的變化點，識別對於網路安全聲明和網路安全假設的影響。
4. 現成組件是否滿足將被整合的相關項目或組件所分配的網路安全需求，現有文件或證據是否充分，如果不充分，需要補充相關的網路安全活動及作業產出。

- RQ-06-15、RQ-06-16、RQ-06-17 實踐方式

網路安全裁適分析流程：

1. 再利用的相關項目或組件修改分析清單。

表 5 再利用的相關項目或組件修改分析示意清單(以下供參，可依實際需求進行調整)

序號	檢查項目		結果 (是/否)	受影響或缺失的工作產出	備註 (如需補充額外的網路安全活動)
1	計畫進行的修改				
2	操作環境的變化	不同車輛			
		不同相關組件或組件			
3	相關資訊變化	已知攻擊和脆弱性的變化			
		威脅場景的變化			
4	設計修改	需求修改			
5	實施修改	軟體的修正			
		新的生產或維護工具			

6	配置資料的修改				
7	校準資料的修改				
…					

2. 相關項目或組件修改對網路安全聲明和假設的影響分析查檢表。

表 6 影響分析查檢示意表(以下供參，可依實際需求進行調整)

序號	分配的網路安全需求	是否滿足安全影響分析	受影響或缺失的工作產出	備註(如需補充額外的網路安全活動)
1				
2				

3. 現成組件是否滿足將被整合的相關項目或組件所分配的網路安全需求。

表 7 網路安全需求示意表(以下供參，可依實際需求進行調整)

序號	分配的網路安全需求	是否滿足安全影響分析	受影響或缺失的工作產出	備註(如需補充額外的網路安全活動)
1				
2				

- RQ-06-17 產出文件

參照[RQ-06-22]。

6.4.5 全景外之組件

[RQ-06-18]針對全景外開發組件之預期用途及全景(包含外部介面)之假設，應記錄於對應的工作產出中。

- RQ-06-18 說明

確保全景外的組件在不同環境中的安全性與可追溯性：

1. 確保組件的安全性可追溯：即使組件是獨立開發的，未來使用時仍然能夠理解其安全限制與需求。

2. 降低整合風險：記錄清楚的背景假設有助於避免與其他系統整合時發生安全問題。
3. 提升再利用性：讓組件的開發者與使用者都能清楚瞭解其適用範圍，提高其在不同專案中的可用性。

- RQ-06-18 實踐方式

  參照[RQ-06-20]。
- RQ-06-15 產出文件

  參照[RQ-06-22]。

[RQ-06-19]對於全景外組件之開發，網路安全要求事項應基於[RQ-06-18]的假設。

- RQ-06-19 說明

  參照[RQ-06-20]。
- RQ-06-19 實踐方式

  參照[RQ-06-20]。
- RQ-06-19 產出文件

  參照[RQ-06-22]。

[RQ-06-20]對於全景外開發組件的整合，應確證[RQ-06-18]的網路安全聲明及假設。

- RQ-06-19、RQ-06-20 說明
  1. 全景外的組件是指不是在特定專案背景下，並由協力廠商開發的組件，它的開發是基於對預期使用場景和環境的假設。
  2. 由於全景外的組件不是在特定專案背景下開發的，所以該組件網路安全需求的開發需要基於假設，否則無法展開威脅分析。
  3. 整合全景外的組件時，由於實際運行環境可能跟開發環境不一致，可能會導致一些網路安全問題，所以網路安全聲明和假設的有效性需要被確證。
- RQ-06-18、RQ-06-19、RQ-06-20 實踐方式

  網路安全裁適分析流程：

全景外的裁適分析

表 8 全景外的裁適分析示意表(以下供參，可依實際需求進行調整)

序號	網路安全聲明/假設	是否有效	省略或補充的網路安全活動及工作產出	備註
1				
2				

- RQ-06-19、RQ-06-20 產出文件

  參照[RQ-06-22]。

6.4.6 現成組件

[RQ-06-21]整合現成組件時，應收集及分析網路安全相關文件，以判定是否：

(a)能夠滿足配置之網路安全要求事項。

(b)此組件適合預期用途之特定應用全景。

(c)既有文件係足以支援網路安全活動。

- RQ-06-21 說明

  要求在整合現成組件時，應透過標準分析來確認其適用性與安全性，確保組件在新系統中的正確配置、適用性與安全合規性。

- RQ-06-21 實踐方式

  參照[RQ-06-22]。

- RQ-06-21 產出文件

  參照[RQ-06-22]。

[RQ-06-22]若既有文件不足以支援現成組件之整合，則應識別及履行符合 ISO/SAE 21434 之網路安全活動。

例：有關脆弱性的文件不足。

備考：此可能意味著裁適(參照 ISO/SAE 21434 第 6.4.3 節)。

- RQ-06-22 說明

1. 現成組件是指一種大眾市場產品，可能並非針對車輛網路安全的特定要求而設計，如藍牙模組。
2. 由於現成組件是一種大眾市場產品，所以需要蒐集和分析其網路安全相關的文件，評估是否滿足分配的網路安全需求以及是否適用於預期用途的應用環境，如果不滿足，該組件可能會被棄用或需補充相關的網路安全活動，如擴展整合與查證測試。

- RQ-06-21、RQ-06-22 實踐方式

  網路安全裁適分析流程：

  現成組件的裁適分析

  表 9 現成組件的裁適分析示意表(以下供參，可依實際需求進行調整)

序號	分配的網路安全需求/預期用途的具體應用環境	是否滿足安全影響分析	省略或補充的網路安全活動及工作產出	備註
1				
2				

- PM-06-13 至 RQ-06-22 產出文件
  - ■ 網路安全計畫文件清單(對應 ISO/SAE 21434 之 WP-06-01)
    - ➔一、二階文件(手冊/程序書)：網路安全計畫程序書、網路安全裁適分析程序書
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全計畫範本、網路安全裁適分析報告

6.4.7 網路安全案例

[RQ-06-23]應產生網路安全案例，為項目或組件之網路安全提供論點，並由工作產出支援。

備考 1：論點的某部分可為內隱的(例：若從工作產出匯集中可以明顯看出部分論點，則可以省略該部分論點)。

備考 2：於分散式開發中，項目之網路安全案例可為顧客及供應者的網路安全案例的組合，亦可參考自各方產生的工作產出之證據。使項目之整體論點可得到各方論點的支援。

備考 3：網路安全案例考量後開發之網路安全要求事項[ISO/SAE 21434 之 WP-10-02]。

- RQ-06-23 說明

  建立網路安全案例的過程是一個論證的過程，主要包括三個元素：

  1. 網路安全目標和相關網路安全要求。
  2. 網路安全論證。
  3. 網路安全工作產出。

  基於網路安全工作產出，透過過程和產品論證，判斷專案達到的網路安全程度。網路安全案例的論證範圍包括整個產品的生命週期。

- RQ-06-23 實踐方式

  表 10 網路安全案例示意(以下供參，可依實際需求進行調整)

階段	(如相關組件定義)
目標	(如定義相關組件、其運行環境及其在網路安全背景下的相互作用)
過程論證	(論點應清楚地描述如何滿足 ISO/SAE 21434 要求清單，並清楚地識別論點的來源，即從哪些證據中得到這個論點)
產品論證	(所有工作產出皆通過查證審核，工作過程與公司品質管理流程一致)
證據	(網路安全相關工作產出)
結論	(通過/不通過/有前提或條件通過) 註：「有前提或條件通過」之一般認定原則為，論證過程發現問題為一般不符合項，該問題未對過程或者產品造成嚴重偏差，且該不符合項已制定相關整改計畫，即可認定為有前提或條件通過。

- RQ-06-23 產出文件

  ■ 網路安全案例文件清單(對應 ISO/SAE 21434 之 WP-06-02)

  ➔一、二階文件(手冊/程序書)：網路安全案例程序書

  ➔三階文件(作業指導書)：無

➔四階文件(範本/表單)：網路安全案例範本

6.4.8 網路安全評鑑

[RQ-06-24]是否對某個項目或組件履行網路安全評鑑的決定，應適用基於風險作法理由闡述之支援。

備考 1：理由闡述可基於：

- TARA 結果(參照 ISO/SAE 21434 第 15 節)。
- 欲開發項目或組件之複雜度。
- 組織規則及過程定義之準則(參照 ISO/SAE 21434 第 5.4.1 節)。

備考 2：若未履行網路安全評鑑，則應於網路安全案例中記錄其理由闡述。

- RQ-06-24 說明

  需依據風險導向方法來決定是否對某個項目或組件執行網路安全評鑑，確保資源分配合理，並透過明確的風險理由來支持決策，提高安全性與可追溯性。
- RQ-06-24 實踐方式

  參照[RQ-06-24]備考。
- RQ-06-24 產出文件

  參照[RQ-06-32]。

[RQ-06-25] [RQ-06-24]之理由闡述應進行獨立審查。

備考 3：獨立性方案可基於 ISO 26262 系列標準。

- RQ-06-25 說明

  需要獨立審查之目的與意義在於：

  1. 提升決策的公正性與可信度，由獨立審查方查證基於風險導向方法所作出的決策，確保不受偏見影響。
  2. 確保風險評估的準確性，避免因主觀判斷或疏忽，導致未對高風險項目執行必要的網路安全評鑑。
  3. 提高合規性與可追溯性，符合 ISO/SAE 21434 中的合規要求，並確保所有安全決策都有明確的審查與記錄，以便後續追蹤。
- RQ-06-25 實踐方式

參照[RQ-06-25]備考。

- RQ-06-25 產出文件

  參照[RQ-06-32]。

[RQ-06-26]網路安全評鑑應判斷項目或組件之網路安全性。

備考 4：可用的證據由記錄網路安全活動的結果提供，即工作產出(參照 ISO/SAE 21434 附錄 A)。

備考 5：圖 6 說明組織之網路安全稽核、專案級之網路安全評鑑及其他網路安全活動間的關係。

備考 6：網路安全評鑑可逐步履行，促成早先已識別議題之解決方案。

備考 7：網路安全評鑑可重複履行或補充履行，例：因變更、先前的網路安全評鑑提出負面建議時，或發現脆弱性時。

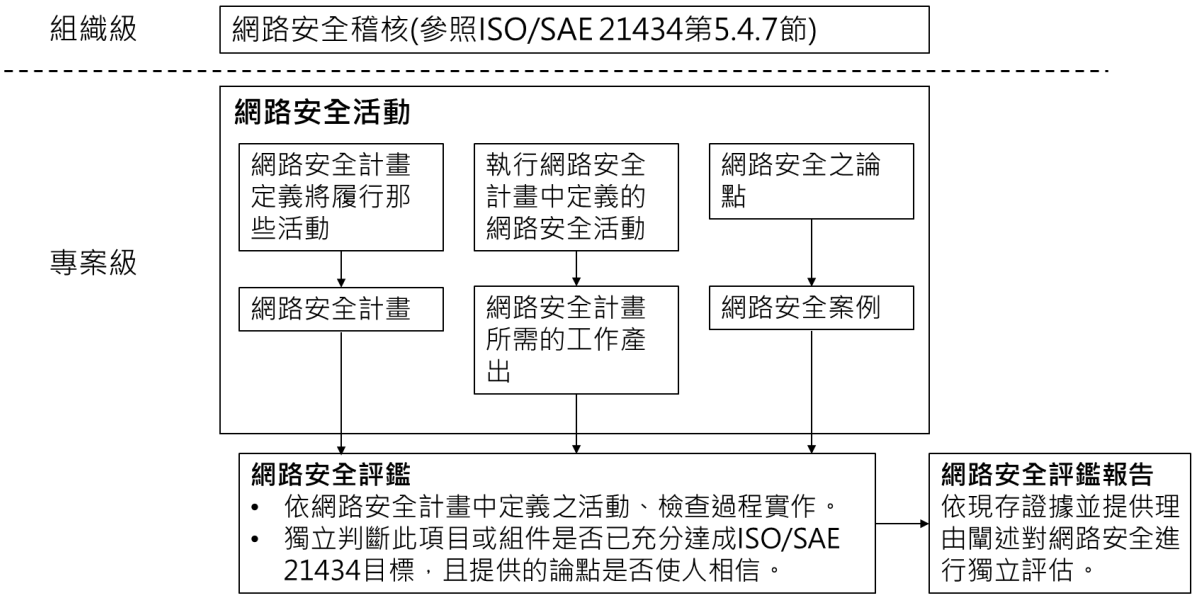


圖 6 與其他網路安全活動相關之網路安全評鑑

- RQ-06-26 說明

  併同[PM-06-29]、[RQ-06-30]進行闡述。

- RQ-06-26 實踐方式

  併同[PM-06-29]、[RQ-06-30]進行闡述。

- RQ-06-26 產出文件

  參照[RQ-06-32]。

[RQ-06-27]應依[RQ-06-01]指派負責計畫及履行獨立網路安全評鑑之人員。

備考 8：獨立性方案可基於 ISO 26262 系列標準。

例：來自組織內不同團隊或部門的人員(例：品保人員)或來自獨立組織的人員。

- RQ-06-27 說明

  確保評鑑過程的獨立性與客觀性、提升網路安全評鑑的品質與準確性，以及確保合規要求。

- RQ-06-27 實踐方式

  參照[RQ-06-28]。

- RQ-06-27 產出文件

  參照[RQ-06-32]。

[RQ-06-28]履行網路安全評鑑之人員應具備：

(a)存取相關資訊及工具。

(b)與履行網路安全活動人員進行合作。

- RQ-06-28 說明

  1. 應定義制定網路安全評鑑計畫和實施網路安全評鑑的人員，其中網路安全評鑑員需要保證獨立性。
  2. 為保證網路安全評鑑的順利進行，評鑑員需要獲得足夠的許可權及相關人員的配合。

- RQ-06-27、RQ-06-28 實踐方式

  網路安全評鑑流程：

  1. 應定義制定網路安全評鑑計畫和實施網路安全評估的角色，同時網路安全評估員需要保證獨立性。
  2. 評鑑員應獲得足夠的許可權以及相關人員的配合。

- RQ-06-28 產出文件

  參照[RQ-06-32]。

[PM-06-29]網路安全評鑑可基於對 ISO/SAE 21434 目的是否達成之判斷。

- PM-06-29 說明
  併同[RQ-06-26]、[RQ-06-30]進行闡述。
- PM-06-29 實踐方式
  併同[RQ-06-26]、[RQ-06-30]進行闡述。
- PM-06-29 產出文件
  參照[RQ-06-32]。

[RQ-06-30]網路安全評鑑範疇應包含：

(a)網路安全計畫及網路安全計畫中識別之所有工作產出。

(b)網路安全風險之處理。

(c)為專案履行實作之網路安全控制措施及網路安全活動的合宜性與有效性。

備考 9 : 合宜性及有效性可藉由使用先前出於查證目的而履行的審查判斷。

(d)展現實現 ISO/SAE 21434 目的的理由闡述(若提供)。

備考 10：考量[PM-06-13]，負責產生工作產出的人員可提供達到 ISO/SAE 21434 對應目標的理由闡述，以促進網路安全評鑑。

備考 11：滿足所有相對應要求事項係達到 ISO/SAE 21434 目的之充分理由闡述。

- RQ-06-26、PM-06-29、RQ-06-30 說明
  1. 網路安全稽核與網路安全評鑑的差異：網路安全稽核的對象是組織層級，檢查組織是否依 ISO/SAE 21434 的要求建立相關流程品質系統，並按照品質系統流程執行；網路安全評鑑的對象若是專案層級，透過評估既有證據及相關論證，判斷相關項目或組件達到的網路安全水準。
  2. 網路安全評鑑的對象包括網路安全計畫，計畫中確認的工作產出以及網路安全案例。
  3. 網路安全評鑑可以分階段進行，以儘早解決所發現的問題。

4. 網路安全評鑑可以被重複或補充執行，如由於變化，先前的網路安全評鑑結果提出負面建議，或指出存在脆弱性。
5. 網路安全評鑑目的，可以是 ISO/SAE 21434 的目標是否達成。

- RQ-06-26、PM-06-29、RQ-06-30 實踐方式

  網路安全評鑑流程：

  1. 應定義網路安全評鑑目的，如 ISO/SAE 21434 的目標是否實現。
  2. 應定義網路安全評鑑的輸入文件，包括網路安全計畫，計畫中確認的工作產出以及網路安全案例。
  3. 應定義網路安全評鑑計畫，如分階段多次評鑑或後開發釋出前一次評鑑。
  4. 應定義網路安全評鑑的範圍，具體內容參照[RQ-06-30]。

- RQ-06-30 產出文件

  參照[RQ-06-32]。

[RQ-06-31]網路安全評鑑報告應包含項目或組件網路安全之接受、有條件接受或拒絕的建議事項。

備考 12：評鑑報告還可包含持續改善之建議事項。

- RQ-06-31 說明

  併同[RQ-06-32]進行闡述。

- RQ-06-31 實踐方式

  併同[RQ-06-32]進行闡述。

- RQ-06-31 產出文件

  參照[RQ-06-32]內容落實。

[RQ-06-32]若依[RQ-06-31]提供有條件接受之建議事項，則網路安全評鑑報告應包含接受之條件。

- RQ-06-31、RQ-06-32 說明

  網路安全評估報告包括接受，有條件接受和拒絕；針對有條件接受，對應的條件需要說明。

- RQ-06-31、RQ-06-32 實踐方式

  網路安全評鑑報告：

  針對有條件接受，在網路安全評鑑報告中應說明評鑑方法及闡述相應的條件。

- RQ-06-24 至 RQ-06-32 產出文件
  - ■ 網路安全評鑑報告文件清單(對應 ISO/SAE 21434 之 WP-06-03)
    - ➔一、二階文件(手冊/程序書)：網路安全評鑑流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全評鑑計畫、網路安全評鑑報告

6.4.9 後開發釋出

[RQ-06-33]於後開發釋出前應提供以下工作產出：

(a)網路安全案例[ISO/SAE 21434 之 WP-06-02]。

(b)若適用，網路安全評鑑報告[ISO/SAE 21434 之 WP-06-03]。

(c)後開發的網路安全要求事項[ISO/SAE 21434 之 WP-10-02]。

- RQ-06-33 說明

  產品後開發釋出前，需要相關工作產出進行網路安全評鑑，確保產品在釋出前達到網路安全標準要求，避免發生安全風險與合規問題。

- RQ-06-33 實踐方式

  併同[RQ-06-34]進行闡述。

- RQ-06-33 產出文件

  參照[RQ-06-34]內容落實。

[RQ-06-34]項目或組件後開發釋出應滿足以下條件：

(a)網路安全案例提供之具有說服力的網路安全論點。

(b)經網路安全評鑑確認之網路安全案例(若適用)。

(c)已接受後開發階段之網路安全要求事項。

備考：變更可能導致須對後開發釋出重新評估，例：網路安全聲明之變更。

- RQ-06-34 說明
  1. 後開發階段的釋出需對網路安全案例、網路安全評鑑報告(若適用)及後開發階段的網路安全需求進行審查，審查通過後，才能最終發佈。
  2. 網路安全案例為網路安全提供具說服力的論證，如網路安全案例按照流程文件實施，且經過審查。
  3. 網路安全評鑑報告的結論應是通過或有條件通過(若適用)。
  4. 後開發階段的網路安全需求需要與相關責任方進行確認，並且被接受。如生產階段的網路安全需求應與生產階段網路安全負責人進行確認，並且被接受。
- RQ-06-33、RQ-06-34 實踐方式

  網路安全後開發釋出流程：

  應定義網路安全後開發之發佈里程碑節點的輸入以及釋出條件。
- RQ-06-33、RQ-06-34 產出文件
  - ■ 後開發釋出報告文件清單(對應 ISO/SAE 21434 之 WP-06-04)
    - ➔一、二階文件(手冊/程序書)：網路安全後開發釋出流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全後開發釋出報告

7. 分散式網路安全活動

7.1 一般

若項目或組件之網路安全活動責任為分散的，則可適用本節。

本節說明分散式網路安全活動之管理，適用於：

(a)於分散式活動中開發之項目及組件。

(b)顧客與供應者間之互動。

(c)協議適用於顧客/供應者介面之所有階段。

內部供應者之管理方式與外部供應者相同。

例：第一層組織可為開發期間 OEM 之供應者，而於另一種契約關係中，第一層組織可為組件之第二層組織的顧客。圖 7 對此進行說明。

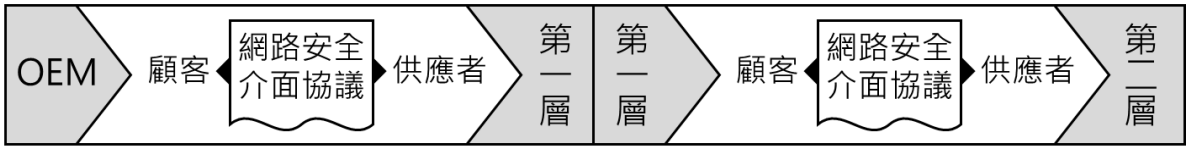


圖 7 供應鏈中顧客/供應者關係之使用案例

7.2 目的

本節目的係定義顧客與供應者間分散式網路安全活動之互動、依賴性及責任。

7.3 輸入

無。

7.4 要求事項及建議事項之實踐指引

7.4.1 供應者能力

[RQ-07-01]應評估候選供應者依 ISO/SAE 21434 開發及(若適用)履行後開發活動之能力。

備考 1：此評估支援供應者之選擇，可基於供應者符合本標準的能力，或基於對先前已實作有關網路安全工程之其他標準的評估。

- RQ-07-01 說明

  併同[RC-07-02]進行闡述。

- RQ-07-01 實踐方式

  併同[RC-07-02]進行闡述。

- RQ-07-01 產出文件

參照[RC-07-02]。

[RC-07-02]為支援顧客對供應者能力的評估，供應者宜提供網路安全能力的紀錄。

備考 2：網路安全能力的紀錄可包含：

- 組織於網路安全方面的能力證據(例：開發、後開發、治理、品質及資訊安全之網路安全之最佳實務)。
- 持續網路安全活動(參照 ISO/SAE 21434 第 8 節)及網路安全事件回應(參照 ISO/SAE 21434 第 13 節)之證據。
- 先前網路安全評鑑報告的彙總。

- RQ-07-01、RC-07-02 說明
  1. 選擇供應者時應評估供應者的網路安全能力。
  2. 供應者網路安全能力的評估內容可以包括組織有關的網路安全能力證據，持續的網路安全活動和網路安全事件回應以及以前的網路安全評鑑報告。
- RQ-07-01、RC-07-02 實踐方式

  供應者能力評估表：

  供應者能力評估表中應有網路安全等級的相關評估指標。
- RQ-07-01、RC-07-02 產出文件
  - ■ 供應者網路安全能力紀錄文件清單
    - ➔一、二階文件(手冊/程序書)：網路安全供應者管理流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：供應者能力評估表

7.4.2 詢價

[RQ-07-03]顧客向候選供應者提出的報價請求應包含：

(a)符合 ISO/SAE 21434 之正式請求。

(b)預期供應者依 ISO/SAE 21434 第 7.4.3 節承擔網路安全責任。

(c)與供應者報價之項目或組件相關的網路安全目標及/或網路安全需求事項。

例：與訊息鑑別相關之網路安全需求事項。

- RQ-07-03 說明

  在正式的報價文件中增加網路安全相關要求，以合約的形式約束雙方的職責，同時提前考慮基於保障網路安全而帶來的成本因素。

- RQ-07-03 實踐方式

  報價請求(RFQ)：

  1. 遵守 ISO/SAE 21434 的正式請求。
  2. 網路安全職責。
  3. 網路安全目標及/或網路安全要求。

- RQ-07-03 產出文件

  ■ 報價請求文件清單

  ➔一、二階文件(手冊/程序書)：網路安全供應者管理流程

  ➔三階文件(作業指導書)：無

  ➔四階文件(範本/表單)：報價請求(RFQ)

7.4.3 職責一致

[RQ-07-04]顧客與供應者應於網路安全介面協議中規定分散式網路安全活動，包含：

(a)指派顧客與供應者之網路安全聯絡人。

(b)識別由顧客與供應者分別履行之網路安全活動。

例 1：由顧客於車輛級履行之網路安全確證。

例 2：關於後開發網路安全活動之分配。

例 3：涉及供應者開發之組件或工作產出的網路安全評鑑，可由第三方、顧客或供應者履行。

(c)若適用，依 ISO/SAE 21434 第 6.4.3 節聯合裁適網路安全活動。

(d)共享之資訊及工作產出。

備考 1：共用資訊可包含：

- 分配、審查及網路安全議題回饋機制。
- 脆弱性及其他網路安全相關發現事項之資訊交換程序，例：關於風險。

- 與介面相關之過程、方法及工具，以確保顧客與供應者間之相容性，例：正確處理資料及保護用於傳遞資料的通訊網路。
- 角色定義。
- 溝通及記錄項目或組件變更之方法，包含潛在的重申 TARA。
- 要求事項管理工具的一致性。
- 網路安全評鑑結果。

(e)有關分散式網路安全活動之期程。

(f)項目或組件之網路安全支援結束的定義。

- RQ-07-04 說明

  應建立網路安全介面協議，包括：

  1. 雙方介面窗口，即顧客和供應者之網路安全聯絡人。
  2. 定義介面協議中的網路安全活動，網路安全活動應涵蓋整個產品的生命週期(適用)，包括概念、設計、網路安全確認、生產、持續的網路安全活動(包括脆弱性管理)、售服、終止網路安全支援和除役(報廢)。同時針對每個網路安全活動，分配顧客和供應者的職責，可通過 RSICA 表進行職責分配。
  3. 網路安全活動可以進行裁適與調整，具體可參考 ISO/SAE 21434 第 6.4.3 節。
  4. 分散式開發過程中，顧客和供應者之間需要進行工作產出和資訊的相容性，應建立相關的共享機制，包括共享的資訊，傳輸的方式及使用的工具等。
  5. 針對每個活動應定義開始和結束時間，同時定義專案的里程碑節點。
  6. 網路安全活動中應包括終止網路安全支援的定義。

- RQ-07-04 實踐方式

  併同[RC-07-08]進行闡述。

- RQ-07-04 產出文件

  參照[RC-07-08]。

[RC-07-05]於分散式網路安全活動開始前，顧客與供應者宜共同議定網路安全介面協議。

- RC-07-05 說明
  網路安全介面協議應在分散式網路安全活動開始前由顧客和供應者共同商定。
- RC-07-05 實踐方式
  併同[RC-07-08]進行闡述。
- RC-07-05 產出文件
  參照[RC-07-08]。

[RQ-07-06]若具有需依[RQ-08-07]進行管理之已識別脆弱性，顧客及供應者應就該等措施之行動及責任達成意見一致。

- RQ-07-06 說明
  介面協議中定義的網路安全活動應包括脆弱性管理，涉及脆弱性資訊的報告、脆弱性的分析、處置及關閉等。
- RQ-07-06 實踐方式
  併同[RC-07-08]進行闡述。
- RQ-07-06 產出文件
  參照[RC-07-08]。

[RQ-07-07]若要求事項不清楚、不可行、或與其他網路安全或其他行為規範的要求事項相衝突，則顧客與供應者應各自通知對方，以便採取合適之決定及行動。

- RQ-07-07 說明
  介面協議中應定義顧客和供應者的溝通計畫和方式，便於及時管理網路安全相關需求。
- RQ-07-07 實踐方式
  網路安全介面協議：
  介面協議中應定義顧客和供應者的溝通計畫和方式，如定期會議等。

- RQ-07-07 產出文件

  參照[RC-07-08]。

[RC-07-08]宜於責任指派矩陣中規定責任。

備考 2：可使用 RASIC 表，參照 ISO/SAE 21434 附錄 C。

- RC-07-08 說明

  針對每個網路安全活動，需清楚定義顧客和供應者的職責，可使用 RASIC 表進行責任分配。

- RQ-07-04 至 RC-07-08 實踐方式

  1. 網路安全介面協議。
  2. 定義顧客和供應者在網路安全方面的聯絡窗口。
  3. 確定由顧客和供應者分別開展的網路安全活動以及每個活動雙方職責的分配，網路安全活動應包括脆弱性管理和終止網路安全支援。
  4. 定義顧客和供應者之間工作產出和資訊的一致性要求。
  5. 定義分散式網路安全活動的里程碑。
  6. 網路安全介面協議應在分散式網路安全活動開始前由客戶和供應者共同商定。
  7. 介面協議參考 ISO/SAE 21434 附錄 C。

- RQ-07-04 至 RC-07-08 產出文件

  ■ 網路安全介面協議文件清單(對應 ISO/SAE 21434 之 WP-07-01)

  ➔一、二階文件(手冊/程序書)：網路安全供應者管理流程

  ➔三階文件(作業指導書)：無

  ➔四階文件(範本/表單)：網路安全介面協議

8. 持續性網路安全活動

8.1 一般

持續的網路安全活動於生命週期的所有階段履行，並且可於特定專案外完成。

網路安全監督(參照 ISO/SAE 21434 第 8.3 節)收集且分析網路安全資訊，並依定義的觸發進行分類。

網路安全事件評估(參照 ISO/SAE 21434 第 8.4 節)判定網路安全事件是否存在某個項目或組件的弱點。

脆弱性分析(參照 ISO/SAE 21434 第 8.5 節)檢查弱點並評鑑特定弱點是否可被利用。

脆弱性管理(參照 ISO/SAE 21434 第 8.6 節)追蹤並監視項目及組件中已識別脆弱性之處理，直至網路安全支援結束。

8.2 目的

本節目的為：

(a)監督網路安全資訊以識別網路安全事件。

(b)評估網路安全事件以識別弱點。

(c)從弱點中識別脆弱性。

(d)管理已識別的脆弱性。

8.3 網路安全監督

8.3.1 輸入

8.3.1.1 先決條件

應提供以下資訊：

- [ISO/SAE 21434 之 WP-05-01]中包含用於觸發開發之規則及過程。

8.3.1.2 進一步的支援資訊

可考量以下資訊：

- 項目定義[ISO/SAE 21434 之 WP-09-01]。
- 網路安全聲明[ISO/SAE 21434 之 WP-09-04]。
- 網路安全規格[ISO/SAE 21434 之 WP-10-01]。
- 威脅情境[ISO/SAE 21434 之 WP-15-03]。
- 過去的脆弱性分析[ISO/SAE 21434 之 WP-08-05]。

- 從場域收到的資訊。

例：脆弱性掃描報告、修復資訊、消費者使用資訊。

8.3.2 要求事項及建議事項之實踐指引

[RQ-08-01]網路安全資訊之收集應選擇來源。

備考 1：可選擇內部及/或外部來源。

備考 2：內部來源可包含 ISO/SAE 21434 第 8.3.1.2 節中所列之來源。

備考 3：外部來源可包含：

- 研究人員。
- 商業或非商業來源。
- 組織供應鏈。
- 組織之顧客。
- 政府來源。

例：最先進的攻擊方法之來源。

- RQ-08-01 說明
  1. 由於網路安全的威脅來源和攻擊手段不斷變化，企業應建立持續的網路安全監控以確保產品在整個生命週期內的網路安全風險是可控的。
  2. 企業應根據自身產品特點，識別網路安全資訊收集的來源，來源可以包括內部和外部。
- RQ-08-01 實踐方式

  可建立網路安全資訊監控流程，明確監控來源，包括監控來源的類型(內部/外部)、具體來源管道(如網站、平台或系統等)、監控頻率、當責人員等資訊。
- RQ-08-01 產出文件
  - ■ 網路安全監控來源清單(對應 ISO/SAE 21434 之 WP-08-01)

    ➔一、二階文件(手冊/程序書)：持續的網路安全監控流程

    ➔三階文件(作業指導書)：無

    ➔四階文件(範本/表單)：網路安全監控來源清單

[RQ-08-02]應定義及維護網路安全資訊分類之觸發。

備考 4：觸發可包含關鍵字、組態資訊參考、組件或供應者名稱。

- RQ-08-02 說明

  併同[RQ-08-03]進行闡述。

- RQ-08-02 實踐方式

  併同[RQ-08-03]進行闡述。

- RQ-08-02 產出文件

  ■ 觸發機制清單(對應 ISO/SAE 21434 之 WP-08-02)

  ➔一、二階文件(手冊/程序書)：持續網路安全監控流程

  ➔三階文件(作業指導書)：無

  ➔四階文件(範本/表單)：觸發機制清單

[RQ-08-03]應收集及分類網路安全資訊，以判定網路安全資訊是否成為 1 或多個網路安全事件。

- RQ-08-02、RQ-08-03 說明

  網路安全資訊分類之觸發，用於分析確認網路安全資訊是否與某一項目或組件相關。觸發機制可包括使用的軟硬體組件、供應者的產品、密碼演算法等，如某個脆弱性受影響的產品名稱與觸發清單中某產品相匹配，則該網路安全資訊將分類為網路安全事件。

- RQ-08-02、RQ-08-02 實踐方式

  透過網路安全資訊監控流程：

  1. 定義與產品相關的觸發機制。
  2. 收集和分類網路安全資訊。

- RQ-08-03 產出文件

  ■ 網路安全事件清單(對應 ISO/SAE 21434 之 WP-08-03)

  ➔一、二階文件(手冊/程序書)：持續網路安全監控流程

  ➔三階文件(作業指導書)：無

  ➔四階文件(範本/表單)：網路安全事件清單

8.4 網路安全事件評估

8.4.1 輸入

8.4.1.1 先決條件

應提供以下資訊：

- 網路安全事件[ISO/SAE 21434 之 WP-08-03]。
- 後開發之網路安全要求事項[ISO/SAE 21434 之 WP-10-02](若適用)。
- 依[RQ-05-12]之組態資訊。

8.4.1.2 進一步的支援資訊

可考量以下資訊：

- 項目定義[ISO/SAE 21434 之 WP-09-01]。
- 網路安全規格[ISO/SAE 21434 之 WP-10-01]。
- 過往的脆弱性分析[ISO/SAE 21434 之 WP-08-05]。

8.4.2 要求事項及建議事項之實踐指引

[RQ-08-04]應評估網路安全事件，以識別項目及/或組件中的弱點。

備考 1：此活動可與[RQ-08-03]之分類聯合。

備考 2：若存在弱點並有可用的補救措施(例：供應者針對組件中的脆弱性提供修補程式)，組織可將補救措施(參照 ISO/SAE 21434 第 8.6 節)作為假設的脆弱性進行處理，無需任何其他活動。

備考 3 : 威脅情境[ISO/SAE 21434 之 WP-15-03]可依評估結果進行更新。

- RQ-08-04 說明
  1. 弱點是導致不良行為的缺陷或特徵，可能包括設計過程缺陷(如架構設計不合理)，實施過程缺陷(如軟硬體缺陷)，運作過程缺陷(如錯誤的組態)及過時的功能(如過時的加密演算法)等。
  2. 應對網路安全事件進行評估，以發現項目及/或組件中的弱點。
  3. 如有已存在的弱點補救措施，可直接進行弱點修復，而無需進行後續的弱點分析、脆弱性管理等活動。
  4. TARA 是動態更新的，需根據弱點評估的結果去更新 TARA 中的威脅場景。
- RQ-08-04 實踐方式

  網路安全事件弱點分析報告：

1. 應對網路安全事件進行弱點分析，識別出項目及/或組件中的弱點。
2. 若不存在弱點，則對網路安全資訊持續監控；若存在弱點，則進行弱點補救措施。

- RQ-08-04 產出文件
  - ■ 網路安全事件弱點分析報告文件清單(對應 ISO/SAE 21434 之 WP-08-04)
    - ➔一、二階文件(手冊/程序書)：持續網路安全監控流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：網路安全弱點分析報告

8.5 脆弱性分析

8.5.1 輸入

8.5.1.1 先決條件

應提供以下資訊：

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

備考：若對項目履行脆弱性分析，則應使用項目定義。若對組件履行脆弱性分析，則應使用網路安全規格。

8.5.1.2 進一步的支援資訊

可考量以下資訊：

- 網路安全事件之弱點[ISO/SAE 21434 之 WP-08-04]。
- 產出開發期間發現的弱點[ISO/SAE 21434 之 WP-10-05]。
- 過去的脆弱性分析[ISO/SAE 21434 之 WP-08-05]。
- 攻擊路徑[ISO/SAE 21434 之 WP-15-05]。
- 查證報告[ISO/SAE 21434 之 WP-10-04]及[ISO/SAE 21434 之 WP-10-07]。
- 過去網路安全事故之資訊。

8.5.2 要求事項及建議事項之實踐指引

[RQ-08-05]應分析弱點以識別脆弱性。

備考 1：分析可包含：

- 架構分析。
- 依 ISO/SAE 21434 第 15.6 節進行攻擊路徑分析。
- 依 ISO/SAE 21434 第 15.7 節進行攻擊可行性評級。

備考 2：可履行根本原因分析，以判定導致弱點成為脆弱性之可能性的任何基本因素。

例 1：若攻擊路徑分析發現不存在攻擊路徑，則此弱點不被視為脆弱性。

例 2：利用此弱點的攻擊可行性評級非常低，則此弱點不被視為脆弱性。

- RQ-08-05 說明

  併同[RQ-08-06]進行闡述。
- RQ-08-05 實踐方式

  併同[RQ-08-06]進行闡述。
- RQ-08-05 產出文件

  參照[RQ-08-06]。

[RQ-08-06]對於未被識別為脆弱性之弱點，應提供理由闡述。

- RQ-08-05、RQ-08-06 說明

  弱點與脆弱性的差異在於是否存在攻擊路徑及攻擊可行性的等級。若弱點不存在攻擊路徑或存在攻擊路徑，但是攻擊可行性很低，則弱點不會成為脆弱性。脆弱性的分析方法可參考 TARA 流程。
- RQ-08-05、RQ-08-06 實踐方式

  脆弱性分析報告：

  1. 判斷弱點是否構成攻擊路徑，如不構成攻擊路徑，則該弱點不升級為脆弱性；若弱點構成攻擊路徑，便繼續評估攻擊路徑的可行性等級。
  2. 評估攻擊路徑的可行性等級，若攻擊可行性等級很低，則該弱點不升級為脆弱性；反之，則該弱點升級為脆弱性，進入後續的脆弱性管理流程。
- RQ-08-05、RQ-08-06 產出文件

  ■ 脆弱性分析報告文件清單(對應 ISO/SAE 21434 之 WP-08-05)

➔一、二階文件(手冊/程序書)：無

➔三階文件(作業指導書)：無

➔四階文件(範本/表單)：脆弱性分析報告

8.6 脆弱性管理

8.6.1 輸入

8.6.1.1 先決條件

應提供以下資訊：

- 脆弱性分析[ISO/SAE 21434 之 WP-08-05]。

8.6.1.2 進一步的支援資訊

無

8.6.2 要求和建議事項之實踐指引

[RQ-08-07]應對每個脆弱性進行脆弱性管理：

(a)依 ISO/SAE 21434 第 15.9 節評鑑及處理相對應之網路安全風險，以確保不存在不合理的風險。

(b)藉由應用獨立於 TARA 之可用補救措施來消除脆弱性

例：開源軟體的修補程式。

備考 1：若脆弱性管理導致項目或組件發生變更，則依[RQ-05-11]應用變更管理。

備考 2：有關脆弱性資訊可於分散式網路安全活動之全景下共享(參照 ISO/SAE 21434 第 7.4.3 節，例：共享攻擊路徑的知識)，亦可共享給其他關注方(參照 ISO/SAE 21434 第 5.4.3 節)。

- RQ-08-07 說明

  併同[RQ-08-08]進行闡述。
- RQ-08-07 實踐方式

  併同[RQ-08-08]進行闡述。
- RQ-08-07 產出文件

  參照[RQ-08-08]。

[RQ-08-08]若依 ISO/SAE 21434 第 15.9 節做出的風險處理決定需要網路安全事故回應，則應適用 ISO/SAE 21434 第 13.3 節。

備考 3：網路安全事故回應過程可獨立於 TARA 應用。

- RQ-08-07、RQ-08-08 說明
  1. 脆弱性的處理可以按照 TARA 的方法進行處理，也可以獨立於 TARA 的方法進行處理。
  2. 脆弱性的修復若涉及到項目或組件的變更，則按照[RQ-05-11]變更管理流程執行。
  3. 脆弱性資訊應按照 ISO/SAE 21434 第 5.4.3 節中資訊共享要求進行內外部的共享。
  4. 依據對脆弱性的處置決定，確定是否須要進行網路安全事件回應，若需要，則參考網路安全事件回應計畫。
- RQ-08-07、RQ-08-08 實踐方式

  脆弱性管理流程：
  1. 識別脆弱性影響範圍，如涉及的產品類型、批次、型號、版本等。
  2. 針對脆弱性進行風險評鑑，評估脆弱性風險等級。
  3. 判斷脆弱性是否觸發網路安全事件，若觸發網路安全事件，則參考網路安全事件回應計畫。
  4. 若未觸發網路安全事件，則進行脆弱性修復。
  5. 脆弱性修復後的跟蹤及持續監控。
- RQ-08-07、RQ-08-08 產出文件
  - ■ 脆弱性管理流程文件清單(對應 ISO/SAE 21434 之 WP-08-06)
    - ➔一、二階文件(手冊/程序書)：脆弱性管理流程
    - ➔三階文件(作業指導書)：無
    - ➔四階文件(範本/表單)：脆弱性管理報告