CNS 18031-1

遙控無人機資安檢測產業端參考指引

財團法人電信技術中心

中華民國 115 年 6 月 26 日

目錄

1. 目的

為協助遙控無人機廠商符合 CNS 18031-1:2025「無線電設備共同安全要求－第 1 部：網路連接之無線電設備」之要求，本指引說明遙控無人機於設計、開發、文件準備及送測前階段，應如何理解各項安全要求、辨識相關威脅與風險，建立可驗證之合規佐證資料，使廠商能以一致性方式說明受評估產品之系統邊界、通訊介面、安全資產、網路資產、安全機制及技術文件內容，降低因文件不足、適用性判斷不明確或實作說明無法佐證，而導致不合規之風險。

2. 引用標準

經濟部標準檢驗局，CNS 18031-1:2025 無線電設備共同安全要求－第 1 部：網路連接之無線電設備。

3. 遙控無人機資安威脅、風險與合規方針

本指引依 CNS 18031-1 之要求機制逐一說明，並於每一要求項目說明目的、「注意事項」、「合規方針」。

本指引所列圖示係為協助理解遙控無人機系統架構、安全機制及其相互關係之概念示意。圖像係使用生成式 AI 輔助製作之示意圖，僅供說明測試情境與評估概念使用；圖示不取代標準條文、產品實際技術文件或符合性判定依據。

為協助廠商由產品整體架構理解 CNS 18031-1 各安全機制之可能適用環節，本指引以遙控無人機常見之基本架構為例，說明使用者、行動 App、遙控器、無人機本體及雲端或更新服務等組成，以及各環節可能涉及之安全機制。下圖 1 係作為整體理解之示意，實際適用性仍應依產品架構、通訊方式、介面配置、儲存方式及使用情境逐項判斷。下圖 2 係作為各安全機制之概略說明，協助廠商快速掌握各機制所關注之保護重點，實際要求內容仍應以標準條文及產品設計為準。

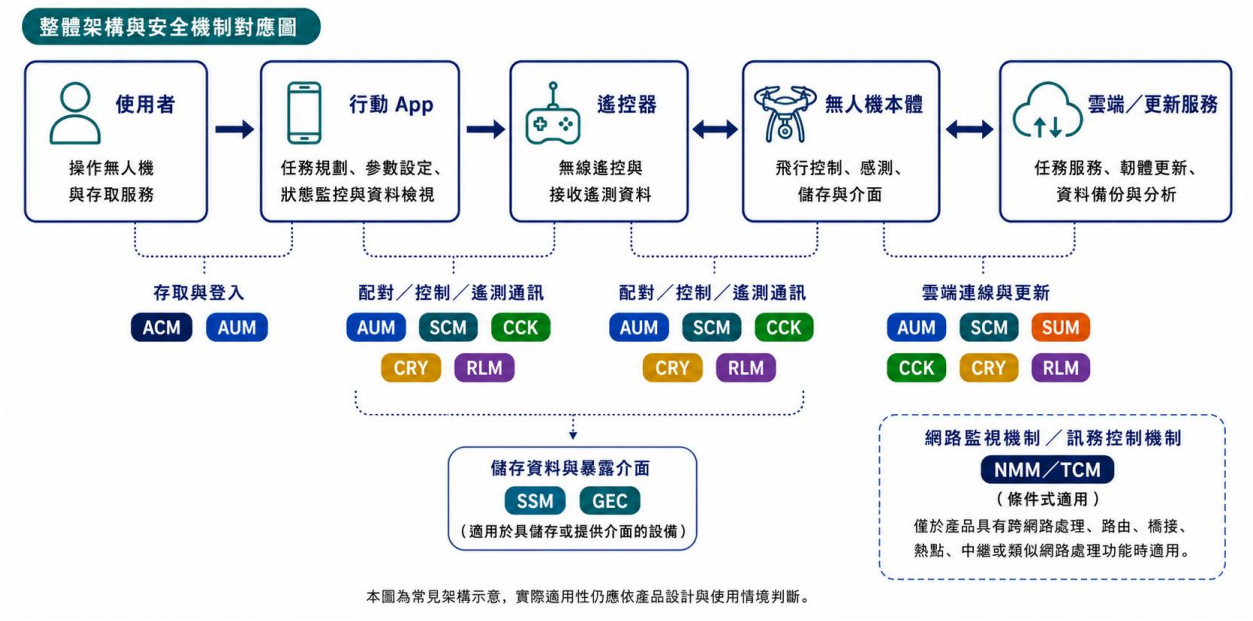

圖 1 無人機架構與安全機制對應

ACM	存取控制機制	管理使用者、裝置與權限，確保僅授權主體可存取系統與功能。
AUM	鑑別機制	驗證使用者與裝置身分，確保身分可信與會話安全。
SCM	安全通訊機制	保護通訊通道與裝置配對，防止竊聽、竄改與中間人攻擊。
CCK	機密密碼金鑰	管理金鑰強度、產生與唯一性，支援安全通訊與簽章驗證。
CRY	密碼學	提供加密、解密、簽章與驗證等密碼學服務，確保資料機密性與完整性。
RLM	韌性機制	提升系統對異常流量、DoS 攻擊與故障的抵禦與回復能力。
SUM	安全更新機制	確保韌體／軟體更新來源可信，驗證完整性並可回復。
SSM	安全儲存機制	保護機密資料與憑證於儲存中的安全性，防止未授權存取。
GEC	一般設備能力	限制暴露介面與服務，降低攻擊面並強化預設安全設定。
NMM TCM	網路監視機制／訊務控制機制（條件式適用）	進行跨網路流量監視與訊務控制，熱點／中繼等路由與處理，提供存取控制與流量管理。

圖 2 安全機制概略說明

為協助廠商理解 CNS 18031-1 各安全機制之相互關聯，本指引依各機制要求內容整理其概念性關係，如下圖 3 所示。其旨在說明各機制如何共同保護安全資產與網路資產，並非表示標準原文已明確定義固定之上下層架構或實作順序。

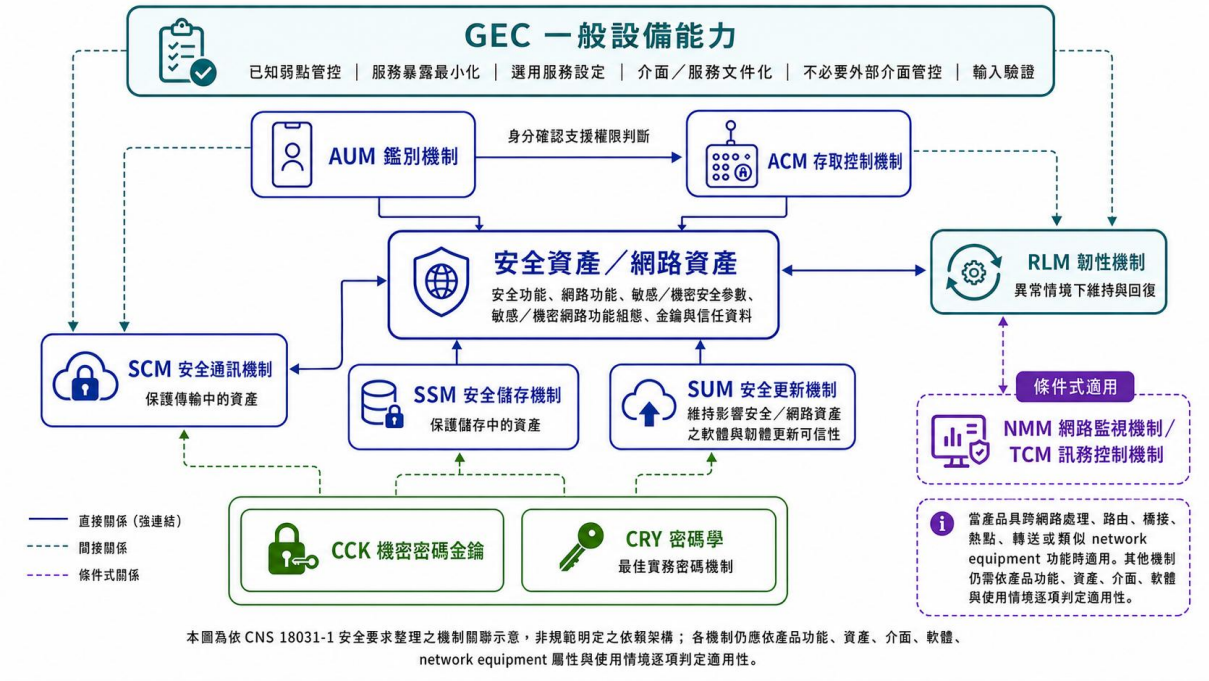

圖 3 安全機制相互關係圖

3.1 [ACM]存取控制機制

3.1.1 合規目標

[ACM] 存取控制機制主要關注設備中之安全資產與網路資產，是否僅能由經授權之實體依其權限進行存取。對遙控無人機而言，常見存取情境包含使用者透過行動應用程式、地面控制站、網頁管理介面、遙控器操作介面、維護工具或雲端服務，讀取、修改或使用與飛行控制、網路連線、設備管理、安全設定、配對資訊、更新功能或紀錄資料相關之功能與資料。

廠商應先辨識哪些安全資產與網路資產可被使用者、設備、服務或其他實體存取，並說明該存取是否需要存取控制機制；若需要，則應進一步說明該機制如何確保僅有授權實體得以存取相關資產。

ACM-1 所建立之資產、介面與存取路徑盤點，常可作為後續 AUM、SSM、SCM 及 GEC 等要求適用性判斷之重要基礎。若廠商未能清楚說明產品中有哪些資產、誰可以透過哪些介面存取及如何限制未授權存取，其他安全機制之保護範圍將較難判斷。

3.1.2 常見攻擊面

攻擊面	說明
行動應用程式/地面控制站	使用者透過 App 或地面控制站進行登入、任務設定、飛行參數設定、韌體更新、紀錄查詢或雲端同步。
網頁管理介面	遙控無人機、遙控器或地面站可能提供 Web UI，用於設定網路、帳號、安全參數或系統功能。
維護與工程介面	SSH、序列埠、維護工具、工程模式或診斷服務可能提供較高權限之系統管理能力。
雲端服務	設備可能透過雲端帳號、API、token 或服務憑證存取使用者資料、飛行紀錄、設備綁定狀態或更新服務。

3.1.3 威脅情境

遙控無人機可能涉及多種使用者、設備與服務之互動。若存取控制機制未完整設計或文件說明不足，攻擊者可能透過網路介面、使用者介面、維護介面或雲端服務，讀取、修改或使用原本不應開放之功能與資料。

威脅類型	情境說明
未授權存取	未經授權之使用者、設備或服務，透過 App、Web UI、API、維護介面或無線連線存取飛行設定、網路設定、安全設定或紀錄資料。
權限越權	一般使用者或低權限帳號可執行管理員、維護人員、製造商或雲端服務專用功能，例如修改安全設定、開啟除錯服務或變更設備綁定狀態。
未授權設定變更	攻擊者修改網路設定、連線端點、配對資訊、任務參數、飛行限制、安全功能或更新來源，使設備進入不安全或非預期狀態。
安全資產外洩	攻擊者讀取金鑰、憑證、token、配對秘密、帳號資訊或其他安全參數，進而取得後續存取能力。

3.1.4 [ACM-1] 存取控制機制之適用性

ACM-1 要求設備應使用存取控制機制管理實體對安全資產與網路資產之存取。惟若該安全或網路資產之公開存取屬於設備預期功能，或目標操作環境中之實體或邏輯措施已限制其僅能由授權實體存取，或因法規因素不允許採用存取控制機制，則可依實際情形提出不適用或例外說明。

➢注意事項

- 應先辨識設備中可被實體存取之安全資產與網路資產，例如安全設定、鑑別設定、金鑰或憑證資料、配對資訊、網路設定、通訊功能、更新功能及維護功能。
- 應逐一說明各資產可透過哪些介面被存取，例如 App、地面控制站、Web UI、API、遙控器操作介面、SSH、序列埠、雲端服務或維護工具。
- 應區分存取型態，例如讀取資料、修改資料、執行功能、啟用服務、變更設定或匯出紀錄。
- 避免僅以「一般使用者不會操作」、「介面未公開」、「需靠近設備」或「使用私有協定」作為不需要存取控制之理由。
- 若主張公開存取，應說明該公開存取係產品預期功能之一部分，且不會導致安全或網路資產受損或遭濫用。
- 若主張操作環境已限制存取，應說明該環境如何透過實體或邏輯措施確保僅授權實體可存取；對於無線介面，應特別注意其可能超出實體場域邊界。

➢合規方針

面向	建議
資產與存取關係	廠商應先釐清哪些安全資產與網路資產可被外部實體接觸，並確認每一項資產的存取來源、存取介面及存取型態。
適用性判斷	對於可被讀取、修改或使用之安全資產與網路資產，原則上應配置存取控制機制；若主張不適用，應能說明其符合公開功能、環境限制或法規限制等例外條件。
存取控制設計	對於需要保護之資產，應設計可限制未授權實體存取之機制，例如帳號權限、角色控管、設備綁定、API 授權、配對限制或作業系統權限。
例外情形處理	若某些資產不採用存取控制，應避免僅以產品設計習慣或使用者不易接觸作為理由，而應說明該資產為何可公開、如何受環境限制，或為何因法規因素不得限制。
後續要求銜接	ACM-1 的判斷結果會影響 ACM-2、AUM、SSM、SCM 等要求之適用性，因此資產與存取路徑不宜遺漏或過度概括。

3.1.5 [ACM-2] 適當存取控制機制

ACM-2 要求依 ACM-1 判定需要存取控制之安全資產與網路資產，其存取控制機制應能確保僅有授權實體得以存取受保護資產。換言之，廠商不僅需說明「有存取控制」，也需說明該機制如何判斷誰是授權實體、授權實體可執行哪些操作，以及如何避免未授權或越權存取。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 「有登入畫面」不等於已滿足 ACM-2；廠商仍應說明登入後不同實體可存取哪些資產、可執行哪些操作，以及權限如何被限制。
- 應明確區分不同實體之角色或身分，例如一般使用者、設備擁有者、飛手、管理員、維護人員、製造商服務、雲端服務或授權設備。
- 應依最小權限原則配置權限，避免一般使用者或低權限服務取得管理、維護、除錯或安全設定變更能力。
- 應注意同一資產可能透過多個介面存取，例如 App、Web UI、API 或維護工具均可能操作相同設定；各介面均應有一致且可說明之授權邏輯。
- 若具備雲端帳號、設備綁定或多使用者管理功能，應避免使用者可存取其他帳號、其他設備或其他組織之資產。
- 權限變更本身亦應受控，例如新增帳號、變更角色、解除綁定、開啟維護模式或修改 API token 等操作，應僅能由授權實體執行。

➢合規方針

面向	建議
實作類別判斷	**IC.ACM-2.RBAC：角色型存取控制** 若產品以角色配置權限，例如一般使用者、管理員、維護人員，廠商應說明各角色可存取之資產、操作範圍、最小權限配置及角色變更如何受控。
	IC.ACM-2.DAC：裁量型存取控制 若產品依個別使用者、帳號、設備、資產擁有者或授權實體設定權限，廠商應說明權限由誰授予、如何變更，以及如何避免使用者自行擴張或錯誤分享權限。
	IC.ACM-2.MAC：強制型存取控制 若產品依系統政策、安全等級、操作狀態或管理者設定之強制規則控制存取，廠商應說明政策如何建立、由誰維護，以及一般使用者無法自行放寬限制。
	IC.ACM-2.Generic：通用或其他方式 若產品採混合設計或不屬於前述類型，例如帳號權限、設備綁定、API 授權、服務端檢查及作業系統權限共同運作，廠商應說明各機制如何共同限制未授權存取。
授權邏輯	廠商應說明產品如何判斷某一實體是否有權存取特定安全或網路資產，而非僅描述登入流程。
跨介面一致性	同一資產若可透過多個介面操作，應確認各介面均採用一致之授權檢查，避免透過 API、維護工具或雲端服務繞過限制。
權限變更保護	權限設定、角色變更、設備綁定、維護模式啟用或 API token 管理等操作，應視為高風險功能並限制於授權實體執行。
未授權存取處理	對未授權或越權請求，設備或服務應拒絕執行，並視產品特性保留錯誤訊息、事件紀錄或通知機制。

3.2 [AUM]鑑別機制

3.2.1 合規目標

[AUM] 鑑別機制主要關注設備於採用存取控制機制管理安全或網路資產時，是否能確認存取實體之身分或其所宣稱之資格。對遙控無人機而言，常見鑑別情境包含使用者登入行動應用程式、地面控制站或網頁管理介面，設備與遙控器或地面站進行配對，App 或設備連線至雲端服務，維護工具連線至設備，或設備向更新服務、後台 API 及其他授權服務進行身分確認。

廠商應依 ACM-1 所需之存取控制情境，說明哪些經網路介面或使用者介面進行之存取需要鑑別機制，並說明該鑑別機制如何驗證實體所提出之身分或授權主張。

AUM 與 ACM 直接相關，ACM 著重「誰可以存取哪些資產」，AUM 進一步要求廠商說明「如何確認該實體確實是其所宣稱者」。若產品僅設有權限設計，但未能有效確認使用者、設備或服務身分，仍可能導致未授權存取或權限濫用。

3.2.2 常見攻擊面

攻擊面	說明
使用者登入流程	使用者透過 App、地面控制站、Web UI 或遙控器介面登入帳號、解鎖管理功能或存取設備設定。
設備配對流程	遙控無人機本體與遙控器、行動裝置、地面站、相機模組或其他周邊建立信任關係。
雲端帳號與 API 存取	App、地面站或設備透過帳號、token、API key、憑證或服務身分連線至雲端服務。
維護與診斷連線	維護工具、工程模式、SSH、Web 管理介面或診斷服務可能需要較高權限之鑑別。
預設通行碼或初始設定	設備於出廠預設狀態、首次啟用、初始化或恢復原廠設定後，可能使用預設通行碼或要求使用者設定新通行碼。
機器對機器鑑別	設備與更新伺服器、雲端服務、授權設備或其他組件之間可能透過憑證、金鑰或共享秘密進行鑑別。

3.2.3 威脅情境

遙控無人機通常同時存在人員登入、設備配對、雲端連線及維護連線等情境。若鑑別機制不足，攻擊者可能冒用合法使用者、合法設備、雲端服務或維護工具，取得原本不應具備之操作能力。

威脅類型	情境說明
冒用使用者	攻擊者使用猜測、竊取或重複使用之通行碼登入 App、地面站或 Web UI，存取設備設定或飛行資料。
偽裝設備或服務	攻擊者偽裝遙控器、地面站、雲端服務、更新來源或維護工具，嘗試與設備建立連線。
鑑別因子偽造或重用	攻擊者使用偽造憑證、錯誤私鑰、過期 token、舊配對資料或其他不完整鑑別資訊通過驗證。
預設通行碼濫用	多台設備共用預設通行碼，或預設通行碼可由型號、MAC 位址、序號等資料推導，導致大規模未授權存取。
暴力破解	攻擊者對登入介面、API、配對流程或維護服務重複嘗試通行碼、PIN、token 或其他鑑別資訊。
靜態鑑別資訊長期使用	通行碼、token、配對秘密或服務金鑰長期不可變更，於外洩後無法有效撤換或降低風險。

3.2.4 [AUM-1] 鑑別機制之適用性

AUM-1 要求依 ACM-1 需要存取控制之情境，若經由網路介面或使用者介面存取會讀取機密網路功能組態或機密安全參數、修改敏感網路功能組態或敏感安全參數，或使用網路功能或安全功能時，原則上應使用鑑別機制。若特定存取因產品預期功能、目標操作環境之限制，或特定唯讀功能與法規因素而不需鑑別，則應提出具體說明。

➢注意事項

- 應先銜接 ACM-1 判斷結果，確認哪些存取控制機制涉及網路介面或使用者介面。
- 應特別檢視可修改安全設定、網路設定、配對資訊、更新設定、雲端連線設定或維護功能之介面。
- 避免僅以「已在本地網路」、「需靠近設備」或「使用者一般不會操作」作為不需鑑別之理由。
- 若某些通訊或操作在初始化、配對或首次設定階段未要求鑑別，應說明其必要性、限制條件及後續信任建立方式。
- 使用者介面與網路介面之例外條件不同，廠商應避免將所有介面以同一理由概括處理。

➢合規方針

面向	建議
適用範圍銜接	以 ACM-1 已識別之受控存取為基礎，判斷哪些存取需進一步確認實體身分。
介面區分	分別檢視網路介面與使用者介面，避免因介面類型不同而遺漏鑑別需求。
高風險操作	對修改安全參數、網路組態、配對狀態、更新設定或維護功能之操作，原則上應配置鑑別機制。
例外處理	若主張不需鑑別，應能說明該功能為預期公開功能、受環境限制，或屬於特定唯讀且不影響安全之情境。
狀態差異	應考量出廠預設、首次啟用、配對、一般使用、維護模式及恢復原廠設定後之鑑別需求差異。

3.2.5 [AUM-2] 適當之鑑別機制

AUM-2 要求依 AUM-1 需要鑑別之機制，應至少基於知識、持有或固有特徵其中一類要素，驗證實體所提出之身分或資格主張。換言之，產品應能說明其鑑別機制所使用之鑑別因子，例如通行碼、PIN、設備金鑰、憑證私鑰、token、生物特徵或與受信任網路建立之共享秘密。

➢注意事項

- 鑑別機制不只限於帳號通行碼，也可能是設備憑證、金鑰、配對 token、API token、一次性通行碼或生物特徵。
- 應明確說明每一種鑑別機制使用哪一類鑑別因子，而非僅描述「有登入」或「有配對」。
- 若使用受信任網路或配對關係作為鑑別依據，應說明該信任關係如何建立及如何防止未授權設備加入。
- 若同一產品同時有人員登入與設備對設備連線，應分別說明其鑑別方式。
- 應避免使用空白通行碼、固定通用通行碼、無限制共享 token 或僅以設備名稱作為身分確認方式。

➢合規方針

面向	建議
鑑別因子確認	對每個需鑑別之存取情境，明確說明使用知識、持有或固有特徵中何種因子。
人員與設備區分	人員登入、設備配對、雲端服務連線及維護工具連線，應依其特性採取合適鑑別方式。
信任關係建立	若鑑別依賴配對或受信任網路，應確保信任關係建立過程本身具備合理限制。
鑑別範圍	應說明鑑別成功後可存取之功能與資產，並與 ACM 權限設計一致。
可用性考量	若產品具特殊使用情境，例如飛行中不得中斷操作，應設計不影響安全與可用性之鑑別流程。

3.2.6 [AUM-3] 鑑別符確證

AUM-3 要求依 AUM-1 需要之鑑別機制，應依操作環境中可取得之資訊，驗證所使用鑑別符之相關屬性。因此，產品不應只確認「有提供鑑別資訊」，而應確認該鑑別資訊是否完整、有效、屬於正確實體，且未被偽造或不當重用。標準中也以通行碼、憑證私鑰及其他鑑別符作為實作類別說明。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 若使用通行碼，應確認完整通行碼被驗證，而非只檢查部分字元、部分欄位或特定格式。
- 若使用憑證或私鑰，應注意憑證鏈、有效期間、用途、信任來源、主體識別及撤銷或替代驗證機制。
- 若使用 token、API key、配對秘密或設備金鑰，應確認其是否與正確帳號、設備、服務或工作階段綁定。
- 應避免接受過期、撤銷、未受信任、屬於其他設備或其他帳號之鑑別符。

➢若設備離線或無可靠時間來源，應說明如何處理憑證有效期間、撤銷狀態或時間相關驗證限制。

➢ 合規方針

面向	建議
實作類別判斷	**IC.AUM-3.Password：通行碼型鑑別符** 若產品以通行碼或 PIN 作為鑑別符，廠商應說明完整通行碼如何被驗證，並避免只檢查部分內容、接受錯誤通行碼或接受其他使用者通行碼。
	IC.AUM-3.CertificatePrivateKey：憑證私鑰型鑑別符 若產品以私鑰與受信任憑證進行鑑別，廠商應說明憑證鏈、信任根、有效期間、主體識別、私鑰持有關係及撤銷或替代驗證方式。
	IC.AUM-3.Generic：通用或其他方式 若產品使用 token、API key、SSH key、對稱金鑰、生物特徵、配對秘密或其他方式，廠商應說明其有效性、歸屬實體、防偽造能力及失效條件如何被驗證。
驗證屬性定義	依鑑別符類型定義需驗證之屬性，例如通行碼完整性、憑證鏈、token 有效性、設備綁定或工作階段關聯。
偽造防護	鑑別機制應拒絕偽造、不完整、過期、未受信任或與實體不匹配之鑑別符。
綁定關係	鑑別符應與正確使用者、設備、服務或工作階段建立關聯，避免不同實體間重複使用。
環境限制	若操作環境無法取得完整驗證資訊，應說明限制條件及替代控制方式。
與通訊安全銜接	若鑑別訊息經由網路傳輸，應避免被重送或攔截後再次使用。

3.2.7 [AUM-4] 變更鑑別符

AUM-4 要求依 AUM-1 需要之鑑別機制，應允許變更鑑別符；惟若存在衝突之安全目標，使特定鑑別符不宜或不能變更，則應提出具體說明。此要求主要避免通行碼、token、配對秘密、金鑰或其他鑑別資訊長期固定使用，導致外洩後無法降低風險。

➢注意事項

- 使用者通行碼、管理通行碼、API token、配對資訊、維護憑證或服務金鑰若外洩，應有合理的更新、撤銷或重建方式。
- 變更鑑別符時，應確認舊鑑別符不再有效，避免新舊鑑別資訊同時可用而造成風險。
- 若鑑別符為設備根信任、硬體內建金鑰或製造過程注入之不可變秘密，應說明不可變更之安全理由與保護措施。
- 變更流程本身應受保護，避免未授權實體可變更他人通行碼、解除綁定或重設設備信任關係。
- 若變更可能影響飛行安全或任務不中斷需求，應設計適當時機或延後機制。

➢合規方針

面向	建議
可變更性	對使用者、設備、服務及維護相關鑑別符，應評估是否支援變更、撤銷或重新配對。
變更授權	鑑別符變更應僅允許授權實體執行，並避免未授權重設或接管。
舊值失效	鑑別符變更後，舊通行碼、舊 token、舊配對資料或舊憑證應不再授予存取能力。
不可變更理由	若鑑別符不可變更，應說明其衝突安全目標、生命週期風險及替代防護。
操作安全	變更流程應避免在飛行中或安全關鍵狀態下強制執行，除非產品已考量其安全影響。

3.2.8 [AUM-5] 通行碼強度

AUM-5 要求若 AUM-1 所需之鑑別機制使用通行碼，則出廠預設通行碼應為每台設備唯一並符合強度最佳實務，或要求使用者於首次使用前或首次使用時變更；非出廠預設通行碼則應於首次使用前或連網前由使用者設定、由授權實體於受限網路內定義，或由設備依強度最佳實務產生並僅提供予授權實體。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 應避免多台設備共用相同預設通行碼，或使用可由型號、序號、MAC 位址、產品名稱推導之通行碼。
- 若採首次使用強制變更，應確保在設定通行碼前，受保護功能或網路連線不會暴露於未授權存取。
- 若設備自動產生通行碼，應使用適當隨機性來源，並確保通行碼只傳達給授權實體。
- 通行碼強度不應只以複雜字元規則判斷，亦應考量長度、不可預測性、是否重複使用及使用情境。
- 若使用 PIN 也是須檢視的通行碼之一。

➢合規方針

面向	建議
實作類別判斷	**IC.AUM-5-1.UniqueBestPractice：唯一且符合最佳實務之出廠預設通行碼** 若產品不強制使用者於首次使用時變更預設通行碼，廠商應說明每台設備通行碼之唯一性、不可推導性、隨機來源及強度。
	IC.AUM-5-1.EnforceSettingFirstUse：首次使用前或首次使用時強制變更出廠預設通行碼 若產品採此方式，廠商應說明使用者在變更前無法持續以預設通行碼存取受保護功能。
	IC.AUM-5-2.SettingFirstUse：首次使用前或連網前由使用者設定非出廠預設通行碼 若產品要求使用者自行設定通行碼，廠商應說明通行碼設

面向	建議
	定發生於何時，以及未設定前如何限制網路連線或高風險功能。
	IC.AUM-5-2.DefinedAuthEntity：由授權實體於受限網路內定義非出廠預設通行碼 若通行碼由管理者、維護人員或受授權系統設定，廠商應說明該實體如何被授權，以及設定流程如何限制於受控網路或受控環境。
	IC.AUM-5-2.EquipmentGenerated：由設備產生非出廠預設通行碼並僅提供授權實體 若產品由設備自動產生通行碼，廠商應說明通行碼之隨機性、強度，以及如何確保通行碼只傳達給授權實體。
通行碼情境分流	廠商應先區分產品使用的是出廠預設通行碼、首次設定通行碼、使用者自訂通行碼、設備產生通行碼，或由授權實體設定之通行碼，再分別判斷適用要求。
通行碼強度原則	通行碼設計不宜僅依複雜字元規則判斷，亦應考量長度、不可預測性、唯一性、是否可由公開資訊推導，以及該通行碼保護之功能風險。
未完成設定前之保護	若產品要求首次設定或首次變更通行碼，應避免在通行碼完成設定前開放高風險功能、管理介面或未受保護之網路連線。
通行碼傳遞限制	出廠通行碼或設備產生通行碼應僅提供給授權實體，避免透過公開資訊、不安全通道或容易被推導之方式暴露。

3.2.9 [AUM-6] 暴力防護

AUM-6 要求依 AUM-1 需要之鑑別機制，應能抵抗暴力破解攻擊。防護方式可包含失敗嘗試延遲、嘗試次數限制、鑑別符複雜度、多因子、允許清單、警示或記錄等機制；標準亦將時間延遲、嘗試次數限制、鑑別符複雜度及其他方法列為實作類別方向。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 暴力破解防護不只適用於使用者登入，也可能適用於 API、配對流程、維護介面及機器對機器鑑別。

- 若採用帳號鎖定或暫停登入，應避免攻擊者利用大量錯誤嘗試造成合法使用者無法登入。
- 若僅依賴通行碼複雜度，應能說明該複雜度足以抵抗實際使用情境下之猜測攻擊。
- 對於無線或遠端可接觸之鑑別介面，應優先考量速率限制、失敗計數、延遲或警示機制。
- 應注意不同介面之防護一致性，例如 App 有限制，但 API 或維護介面未限制，仍可能形成弱點。

➢合規方針

面向	建議
實作類別判斷	**IC.AUM-6.TimeDelay：時間延遲** 若產品透過錯誤嘗試後延遲下一次鑑別，廠商應說明延遲條件、延遲時間、累進方式及適用介面。
	IC.AUM-6.LimitedAttemps：嘗試次數限制 若產品限制連續錯誤次數或暫停登入，廠商應說明限制門檻、解除條件，以及如何避免合法使用者被長時間阻斷。
	IC.AUM-6.AuthenticatorComplexity：鑑別符複雜度 若主要依賴通行碼、PIN、token、金鑰、憑證或多因子強度抵抗猜測攻擊，廠商應說明強度規則及其適用情境。
	IC.AUM-6.Generic：通用或其他方式 若採用允許清單、風險偵測、警示、設備綁定、IP 限制、行為分析或混合方式，廠商應說明實際防護邏輯與適用範圍。
防護範圍	應涵蓋人員登入、API、設備配對、維護連線及機器對機器鑑別等可被反覆嘗試之情境。
可用性	防護機制應避免被濫用造成合法使用者或設備長時間無法使用。
異常處理	對大量失敗嘗試宜具備記錄、警示、事件處理或其他可追蹤機制。

3.3 [SUM] 安全更新機制

3.3.1 合規目標

[SUM] 安全更新機制主要關注設備中影響安全或網路資產之軟體，是否具備可維護、可修補且不易被攻擊者濫用之更新能力。對遙控無人機而言，常見更新對象可能包含遙控無人機本體韌體、遙控器韌體、地面控制站軟體、行動應用程式、通訊模組韌體、相機或感測器模組韌體，以及與雲端服務、維護工具或安全功能相關之軟體組件。

廠商應辨識哪些軟體會影響安全或網路資產，並說明其是否具備更新機制；若具備更新機制，應進一步說明更新檔案之完整性、真實性如何被驗證，以及安全更新是否能以自動化、排程或經使用者核准方式完成。

安全更新機制亦與其他機制密切相關，例如更新來源與更新通訊可能涉及 SCM 安全通訊機制；更新檔案簽章與驗證涉及 CRY 密碼技術；更新權限與維護流程可能涉及 ACM 存取控制及 AUM 鑑別機制。因此，廠商應避免僅說明「產品可以更新」，而應說明更新對象、更新路徑、驗證方式、失敗處理及使用者互動方式。

3.3.2 常見攻擊面

攻擊面	說明
韌體更新流程	遙控無人機本體、遙控器、通訊模組、相機模組或感測器模組透過 App、地面站、雲端或維護工具進行韌體更新。
更新檔案下載	設備或 App 從雲端服務、更新伺服器、維護電腦或本地儲存媒體取得更新檔案。
更新來源驗證	設備需確認更新來源為授權來源，避免安裝攻擊者提供之更新檔案。
更新檔案驗證	更新檔案於下載、傳輸或儲存過程中可能遭竄改，設備需驗證完整性與真實性。
回復、降版與失敗處理	更新失敗、斷電、通訊中斷或降版更新可能使設備進入不安全或不可用狀態。
自動化更新設定	使用者同意、更新通知、排程更新、飛行前更新、維護時更新或雲端推送更新，均可能影響安全與可用性。

3.3.3 威脅情境

遙控無人機系統通常由多個軟體與韌體組件組成，且部分組件可能透過網路、App、地面站或維護工具進行更新。若更新機制設計不足，攻擊者可能利用更新流程導入惡意軟體、阻止安全修補、安裝舊版脆弱版本，或使設備在更新過程中進入不可用狀態。

威脅類型	情境說明
無法修補已知弱點	影響安全或網路資產之韌體或軟體無法更新，導致已知漏洞於產品生命週期中持續存在。
更新檔案遭竄改	攻擊者修改韌體、App 套件、設定檔或更新包，使設備安裝非原廠授權內容。
偽造更新來源	攻擊者偽裝更新伺服器、維護工具或雲端服務，誘使設備或 App 接受未授權更新。
降版攻擊	攻擊者使設備安裝舊版但具有已知弱點之軟體，藉此繞過後續安全修補。
更新中斷或失敗	更新過程斷電、斷線或驗證失敗，可能造成設備無法開機、功能異常或回復至不安全狀態。
使用者延遲更新	安全更新需高度人工操作或通知不明確，導致使用者長期未安裝修補程式。

3.3.4 [SUM-1] 更新機制之適用性

SUM-1 要求設備應對影響安全或網路資產之軟體提供至少一種更新機制。惟若該軟體因功能安全理由不得更新、屬於不可變更之軟體，或已有替代措施可於設備生命週期內保護受影響之安全或網路資產，則可依實際情形提出不適用或例外說明。

➢注意事項

- 應先盤點設備中會影響安全或網路資產之軟體與韌體，包括主控韌體、通訊模組、更新元件、安全功能、維護功能及相關應用程式。
- 應避免只說明「產品支援 OTA 更新」；應說明哪些軟體元件可透過該機制更新，哪些不可更新，以及不可更新之理由。
- 若主張某些軟體不可更新，應區分是因功能安全、技術上不可變更、硬體記憶體限制，或其他替代措施所致。
- 若以替代措施取代更新能力，應說明該措施如何在設備生命週期中持續保護受影響資產，而非僅以「風險低」概括說明。
- 應注意供應商模組或第三方元件是否影響安全或網路資產；若會影響，仍應說明其更新或替代維護方式。

➢合規方針

面向	建議
軟體範圍判斷	廠商應辨識哪些軟體、韌體或元件會影響安全或網路資產，並納入更新機制適用性判斷。
更新能力配置	對於需維護之軟體，應提供可在產品生命週期內修補安全問題之更新機制。
不可更新理由	若特定軟體不可更新，應能說明其功能安全、不可變更性或其他限制，並確認不會造成未受控風險。
替代措施	若不提供更新機制，應以替代措施保護受影響資產，例如隔離、補償控制、更換策略或生命週期管理。
元件責任邊界	對第三方模組或供應商元件，應釐清廠商是否能取得更新、如何部署更新，以及由誰負責維護。

3.3.5 [SUM-2] 安全更新

SUM-2 要求依 SUM-1 所需之更新機制，僅能於安裝時具備有效完整性與真實性之軟體。因此，設備應能確認更新檔案未被竄改，且確實來自授權來源或授權實體，而非僅依檔名、版本號、下載位置或使用者操作即允許安裝。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 更新檔案之完整性與真實性應在安裝時被驗證，不能只在下載前或伺服器端宣稱已驗證。
- 常見方式包含數位簽章、安全通訊通道、授權實體之存取控制搭配雜湊驗證，或其他可達成相同效果之機制。
- 若使用數位簽章，應說明信任根、簽章演算法、簽章驗證位置及未通過驗證時之處理方式。
- 若依賴安全通訊通道取得更新，仍應說明更新來源如何被鑑別，以及傳輸過程如何避免偽造或竄改。
- 應避免允許未簽章、測試版、工程或降版之更新繞過正式驗證流程。
- 若更新檔案包含機密密碼金鑰或其他機密安全參數，應另行考量傳輸與儲存之機密性保護。

➢合規方針

面向	建議
實作類別判斷	**IC.SUM-2.AuthIntVal.Sign：簽章驗證** 若產品以數位簽章驗證更新檔案，廠商應說明簽章如何產生與驗證、信任根如何建立，以及未通過簽章驗證時如何拒絕安裝。
	IC.SUM-2.AuthIntVal.SecChan：安全通道驗證 若產品主要依賴安全通訊通道取得更新，廠商應說明更新通道如何提供端點鑑別、完整性保護與來源可信性，並確認更新內容不會在通道外被替換。
	IC.SUM-2.AuthIntVal.AccContMech：存取控制機制驗證 若產品依賴授權實體或受控環境提供更新檔案，廠商應說明誰可提供、選擇或安裝更新，以及該權限如何被限制與驗證。

面向	建議
	IC.SUM-2.AuthIntVal.Generic：通用或其他方式 若產品採混合設計或其他驗證方式，例如簽章搭配安全通道、雜湊搭配受控來源、供應商 OTA 模組或硬體安全啟動鏈，廠商應說明整體驗證邏輯及其如何同時支持完整性與真實性。
驗證時間點	驗證應在安裝時或安裝前之可信任流程中完成，且驗證失敗時不得繼續安裝。
信任基礎	應明確說明簽章、憑證、金鑰、受信任來源或授權更新者之建立方式。
例外流程控管	工程模式、維護模式、離線更新或替代軟體安裝流程，亦應具備可說明之安全限制。
版本與降版控制	若允許降版，應評估舊版弱點風險；若不允許，應說明版本檢查或 anti-rollback 設計。

3.3.6 [SUM-3] 自動更新

SUM-3 要求依 SUM-1 所需之每一更新機制，設備應能在無需人為介入下更新軟體，或可由人員核准後排程安裝，或在需避免操作環境中非預期損害時，由人員核准或監督後觸發安裝。此要求重點在於提高安全更新部署效率，同時兼顧遙控無人機之安全與可用性。

➢注意事項

- 自動化更新不必然等於完全自動安裝；對遙控無人機而言，因飛行安全、任務不中斷或相容性需求，可能需採通知、核准、排程或維護時段安裝。
- 應避免安全更新完全仰賴使用者自行到網站下載、手動比對版本或手動複製檔案，導致修補率不足。
- 更新檢查、通知、下載、排程、安裝及重啟流程應簡化，並避免影響飛行中或安全關鍵操作。
- 若更新需人員核准，應說明何時通知、如何核准、是否可延後，以及延後是否會造成安全風險。
- 若產品由多個組件組成，應注意遙控無人機本體、遙控器、App、地面站及模組之更新協調與版本相容性。
- 應考量更新失敗、驗證失敗、斷電、斷線或儲存空間不足時之處理方式。

➢合規方針

面向	建議
自動化程度	依產品特性選擇自動下載安裝、通知後安裝、排程安裝或人員監督觸發安裝。
安全與可用性	對飛行中、任務中或安全關鍵狀態，應避免非預期強制更新；可安排於起飛前、維護時或閒置狀態執行。
更新通知	當安全更新可用時，應讓使用者或管理者能以明確方式得知並啟動更新流程。
版本一致性	對多組件產品，應避免遙控無人機本體、遙控器、App 或地面站版本不相容而造成安全或功能異常。
更新失敗處理	更新失敗時應具備合理處理方式，例如保留原版本、回復、重試或提示使用者採取維護措施。
定期檢查	產品宜具備初始化後或定期檢查安全更新之能力，以降低已知弱點長期未修補風險。

3.4 [SSM] 安全儲存機制

3.4.1 合規目標

[SSM] 安全儲存機制主要關注設備中持續儲存之安全資產與網路資產，是否受到適當保護，以避免未授權讀取、竄改、刪除或其他不當存取。對遙控無人機而言，常見需檢視之儲存內容可能包含帳號資訊、通行碼或雜湊值、配對資訊、金鑰、憑證、token、網路設定、雲端連線設定、更新設定、安全功能組態、維護設定、飛行限制參數及其他會影響設備安全或網路功能之資料。

廠商應先辨識哪些安全資產與網路資產會被持續儲存在設備中，並依其風險說明是否需要安全儲存機制。若該資產需要保護，應進一步說明所採取之完整性保護與機密性保護方式。

SSM 機制與 ACM、AUM、CCK 及 CRY 具有關聯性，例如安全資產若透過存取控制限制讀取或修改，需對應 ACM；若涉及帳號、通行碼或憑證，需對應 AUM；若涉及機密密碼金鑰，則需對應 CCK 與 CRY。廠商應避免僅以「資料存在設備內部」或「一般使用者無法直接看到」作為安全儲存之理由，而應具體說明資料儲存位置、保護機制及未授權存取時之防護效果。

3.4.2 常見攻擊面

攻擊面	說明
內部儲存空間	遙控無人機本體、遙控器、地面站或模組內部之非揮發性儲存媒體（如 Flash、eMMC、EEPROM 等），可能儲存設定、金鑰、憑證、帳號或紀錄資料。
行動應用程式儲存	App 可能於手機或平板中保存登入狀態、token、設備綁定資料、任務資料、地圖快取或飛行紀錄。
地面控制站或維護工具	PC 端軟體可能儲存設備連線資料、帳號資訊、維護設定、更新檔案、log 或診斷資料。
外接或可移除媒體	SD 卡、USB 隨身碟、記憶卡或匯出檔案可能保存飛行紀錄、設定檔、任務資料或更新檔。
雲端與本機同步資料	設備、App 或地面站可能將設定、帳號 token、飛行紀錄、任務資料或設備狀態同步至雲端或本機。
維護與除錯資料	工程模式、診斷功能、crash dump、debug log 或維修紀錄可能包含敏感設定、token、路徑、憑證或其他安全相關資訊。

3.4.3 威脅情境

遙控無人機可能在多個組件中持續儲存安全資產與網路資產。若儲存保護不足，攻擊者可能透過實體接觸、檔案系統存取、App 資料擷取、備份還原、維護介面或除錯功能，讀取或修改原本應受保護之資料。

威脅類型	情境說明
未授權讀取	攻擊者取得設備、記憶卡、App 本機資料或維護檔案後，讀取帳號 token、配對資料、憑證、金鑰或網路設定。
未授權竄改	攻擊者修改儲存於設備內之安全設定、飛行限制、網路組態、更新來源、配對資料或權限設定。
金鑰或憑證外洩	儲存保護不足導致機密密碼金鑰、私鑰、憑證或共享秘密被擷取，進一步影響通訊、更新或鑑別安全。
設定檔替換	攻擊者以偽造或修改後之設定檔取代原設定，使設備連線至錯誤端點、停用安全功能或接受未授權設備。
log 或 dump 洩漏	維護紀錄、錯誤紀錄或除錯輸出中包含 token、帳號、路徑、金鑰片段或敏感設定。
可移除媒體濫用	SD 卡或 USB 中之設定、紀錄或更新資料未受保護，遭複製、修改或重放使用。

3.4.4 [SSM-1] 安全儲存機制之適用性

SSM-1 要求設備對持續儲存於設備上之安全資產與網路資產，原則上應使用安全儲存機制加以保護。惟若目標操作環境中之實體或邏輯措施，已確保儲存於設備上之安全或網路資產僅能由授權實體存取，則可依實際情形提出不適用或例外說明。

➢注意事項

- 應先辨識哪些安全資產與網路資產會被持續儲存在設備中，而非只列出產品主要功能資料。
- 應注意「設備」可能不只包含遙控無人機本體，也可能包含遙控器、地面控制站、行動應用程式、維護工具或隨產品提供之模組。
- 應區分資料是短暫存在記憶體中，或會持續儲存於各類非揮發性儲存空間（如 Flash、檔案系統、資料庫、設定檔或外接媒體）中。對於涉及安全或敏感之資料，亦應考量是否採用適當之保護機制或安全儲存環境（如 Secure Element、TPM、TEE 或應用程式沙盒）加以保護。

- 避免僅以「資料在設備內部」、「使用者不會拆機」或「檔案名稱不可讀」作為安全儲存之理由。
- 若主張操作環境已限制存取，應說明該環境限制如何避免未授權實體接觸儲存內容；若設備可能遺失、轉手或送修，亦應納入考量。
- 若某些資料儲存在可移除媒體或可匯出檔案中，應特別說明是否屬於設備持續儲存範圍，以及如何避免被未授權讀取或修改。

➢合規方針

面向	建議
儲存資產辨識	廠商應先確認哪些安全資產與網路資產會被持續儲存，並判斷其是否需受安全儲存機制保護。
儲存位置判斷	應釐清資料儲存於何種組件、媒體或邏輯位置，例如設備內部儲存、App 本機資料、維護工具或外接媒體。
保護需求判斷	對儲存資產應判斷其是否需要完整性保護、機密性保護，或兩者皆需要。
例外情形處理	若主張不需安全儲存機制，應說明該資產如何受操作環境之實體或邏輯措施保護。
多組件一致性	遙控無人機本體、遙控器、App、地面站及維護工具若皆儲存相關資產，應分別檢視其保護需求。
生命週期考量	設備初始化、配對、一般使用、維修、恢復原廠設定、轉手及報廢等階段，皆應考量儲存資料之保護與清除。

3.4.5 [SSM-2] 安全儲存機制之適當完整性保護

SSM-2 要求依 SSM-1 需要之安全儲存機制，應保護其所持續儲存之安全資產與網路資產的完整性。因此，設備應能防止未授權修改，或至少能偵測安全資產與網路資產是否遭到未授權竄改。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 完整性保護不等同於機密性保護；即使資料不需要保密，仍需要避免被竄改。
- 需特別關注安全設定、網路組態、配對狀態、更新來源、飛行限制、權限設定及安全功能開關等資料。

- 完整性保護可透過數位簽章、訊息驗證碼、雜湊搭配信任根、存取控制、硬體保護或其他機制達成。
- 若採用存取控制作為完整性保護，應說明未授權實體如何被防止修改該資料。
- 若資料遭竄改後僅於下次啟動才偵測，應說明偵測時點、處理方式及是否會造成安全風險。
- 若資料儲存在外接媒體或可匯出/匯入檔案中，應注意匯入時是否驗證完整性。

➢合規方針

面向	建議
實作類別判斷	**IC.SSM-2.DigitalSignature：數位簽章** 若產品以簽章保護儲存資料完整性，廠商應說明簽章涵蓋哪些資料、信任根如何建立，以及驗證失敗時如何處理。
	IC.SSM-2.AccessControl：存取控制 若產品主要透過權限限制防止儲存資料被修改，廠商應說明哪些實體可修改資料、授權條件為何，以及未授權實體如何被阻擋。
	IC.SSM-2.OTProgrammable：一次性可程式化保護 若產品將特定安全資料或組態寫入一次性可程式化區域，廠商應說明該資料為何不應被修改、寫入時機，以及如何避免後續遭竄改。
	IC.SSM-2.HardwareProtection：硬體保護 若產品透過安全元件、TPM、TEE、Secure Element、受保護儲存區或硬體隔離保護完整性，廠商應說明硬體保護邊界及其如何防止或偵測未授權修改。
	IC.SSM-2.Generic：通用或其他方式 若產品採用訊息驗證碼、雜湊搭配信任根、檔案系統保護、供應商安全儲存方案或混合方式，廠商應說明完整性驗證邏輯、保護範圍及失敗處理。
需保護資料判斷	對會影響安全功能或網路功能之持續儲存資料，應判斷其是否需要完整性保護，例如安全設定、網路組態、配對狀態、更新來源、權限設定或飛行限制參數。
驗證與處理時間點	廠商應說明完整性保護在何時生效，例如寫入時、讀取時、匯入時、啟動時或使用前驗證，並說明驗證失敗時如何處理。

面向	建議
未授權修改防護	安全儲存機制應能防止或偵測未授權修改，避免設備接受遭竄改之安全參數、網路組態或設定檔。
匯入資料檢查	若產品支援匯入設定檔、任務檔、維護檔或更新相關檔案，應確認匯入前具備完整性或授權檢查。
異常狀態處理	當偵測到儲存資料遭竄改、驗證失敗或格式異常時，設備應有明確處理方式，例如拒絕載入、回復安全預設值、要求重新設定或記錄事件。

3.4.6 [SSM-3] 安全儲存機制之適當機密性保護

SSM-3 要求依 SSM-1 需要之安全儲存機制，若其持續儲存機密安全參數或機密網路功能組態，應保護該資料之機密性。因此，若資料一旦被讀取會導致安全功能、網路功能或後續鑑別、通訊、更新機制受損，則應採取適當保護以避免未授權揭露。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 應先判斷哪些儲存資料具機密性需求，例如私鑰、共享秘密、API token、登入 token、配對秘密、Wi-Fi 通行碼、雲端憑證、更新服務憑證或維護通行碼。
- 機密性保護可透過加密、存取控制、硬體保護、安全元件、TEE、TPM 或其他等效機制達成。
- 若使用加密，應說明金鑰如何產生、儲存、衍生、輪替及銷毀，避免加密金鑰與加密資料以相同方式暴露。
- 若使用作業系統或 App 沙盒保護，應說明其保護邊界及是否足以防止未授權實體讀取。
- 應避免將機密資料寫入 log、crash dump、匯出檔、備份檔或除錯輸出。
- 若設備支援恢復原廠設定、轉手、維修或報廢，應考量機密資料是否能被清除或失效。

➢合規方針

面向	建議
實作類別判斷	**IC.SSM-3.Encryption：加密保護** 若產品以加密保護儲存資料機密性，廠商應說明加密範圍、金鑰產生與保存方式，以及未授權實體即使取得儲存內容也無法解讀。
	IC.SSM-3.AccessControl：存取控制 若產品主要透過權限限制避免機密資料被讀取，廠商應說明哪些實體可讀取資料、授權條件為何，以及未授權實體如何被阻擋。
	IC.SSM-3.HardwareProtection：硬體保護 若產品使用安全元件、TPM、TEE、Secure Element、受保護儲存區或硬體隔離保護機密資料，廠商應說明硬體保護邊界及其如何防止資料被未授權讀取。
	IC.SSM-3.Generic：通用或其他方式 若產品採用 App 沙盒、作業系統金鑰鏈、供應商安全儲存服務、白盒保護、混合式加密與存取控制等方式，廠商應說明實際防揭露邏輯、保護範圍及限制條件。
機密資料判斷	廠商應辨識哪些持續儲存之安全參數或網路功能組態，若被讀取會造成安全或網路風險，例如私鑰、共享秘密、token、通行碼、配對秘密或雲端憑證。
防揭露設計	對具機密性需求之資料，應採用加密、受控存取、硬體保護或安全儲存區等方式降低外洩風險。
金鑰與保護邊界	若機密資料以加密方式保護，應說明加密金鑰與受保護資料之關係，避免金鑰與資料以相同風險暴露。
洩漏路徑控管	應檢視 log、除錯資訊、備份、匯出檔與維護資料，避免機密資料以其他形式外洩。
清除與失效	設備重置、解除綁定、轉手、維修或報廢時，機密資料應被清除、更新或失效。

3.5 [SCM] 安全通訊機制

3.5.1 合規目標

[SCM] 安全通訊機制主要關注設備透過網路介面與其他實體通訊時，涉及安全或網路資產之資料是否受到適當保護。對遙控無人機而言，常見通訊包含遙控無人機本體與遙控器、地面控制站、行動應用程式、雲端服務、維護工具或更新伺服器間之資料交換。若該通訊內容包含控制指令、遙測資訊、網路設定、配對資訊、金鑰相關資料、帳號或 token、任務參數或更新相關資料，即可能落入本機制之檢視範圍。

本機制之合規目標，並非要求所有通訊內容均以相同方式加密，而是要求廠商能辨識哪些安全或網路資產會透過網路介面傳輸，並依其風險與使用情境，說明是否需要安全通訊機制，以及該機制如何提供完整性、真實性、機密性及重送攻擊防護。

SCM 機制與 ACM、AUM、SUM、SSM、CCK 及 CRY 均有關聯。例如通訊端點之身分確認可能涉及 AUM，通訊內容之授權存取可能涉及 ACM，更新檔案傳輸可能涉及 SUM，金鑰與密碼演算法則需對應 CCK 與 CRY。因此，廠商應避免僅說明「通訊有加密」，而應具體說明通訊情境、保護資產、使用協定、端點鑑別方式及安全保護範圍。

3.5.2 常見攻擊面

攻擊面	說明
無線控制鏈路	遙控無人機本體與遙控器或地面控制站間之控制指令、遙測資訊、狀態回報及任務參數傳輸。
App 與設備連線	使用者透過 App 設定遙控無人機、查看狀態、上傳任務或下載紀錄時所使用之 Wi-Fi、藍牙或其他連線。
雲端服務或後台 API	設備或 App 與雲端平台間進行帳號登入、資料同步、飛行紀錄上傳、任務資料下載或設備管理。
軟體或韌體更新通道	遙控無人機本體、遙控器、地面站或 App 取得更新檔案、版本資訊或更新指示之通訊。
維護與診斷介面	工程模式、維修工具、測試端口或遠端診斷服務所使用之網路連線。
設備間配對通訊	遙控無人機本體與遙控器、行動裝置、地面站、相機模組或其他周邊建立信任關係時之通訊。

3.5.3 威脅情境

遙控無人機通訊多半具有無線傳輸、遠端操作、即時控制及跨組件互動等特性。攻擊者若位於無線電涵蓋範圍、同一區域網路、受害者行動裝置所在網路，或能接觸雲端通訊路徑，即可能嘗試對通訊內容進行竊聽、竄改、偽造或重送。

威脅類型	情境說明
竊聽	攻擊者被動監聽控制鏈路、遙測資料、影像串流、配對資料或雲端 API 通訊，取得敏感資訊或推論產品運作方式。
中間人攻擊	攻擊者介入設備與 App、地面站、雲端服務或更新來源之通訊，嘗試偽裝合法端點或變更通訊內容。
訊息竄改	攻擊者修改控制指令、任務參數、網路設定、配對資料或更新相關訊息，使設備接收錯誤或未授權資料。
訊息偽造	攻擊者偽裝遙控器、地面控制站、雲端服務或維護工具，向遙控無人機或相關組件傳送未授權指令。
重送攻擊	攻擊者錄製先前合法通訊內容，於後續時點重送，使接收端重複接受過期指令、登入訊息或配對資料。
通訊降級	攻擊者誘使設備使用較弱、不安全或未受保護之通訊模式，降低原本應有之保護效果。

3.5.4 [SCM-1] 安全通訊機制之適用性

SCM-1 要求設備透過網路介面與其他實體通訊安全或網路資產時，原則上應使用安全通訊機制加以保護。惟若該傳輸已由目標環境之實體或邏輯措施保護，或該安全或網路資產之暴露屬於建立或管理連線之一部分，且已搭配其他措施用以鑑別連線或信任關係，則可依實際情形提出不適用或例外說明。

➢注意事項

- 應先列出所有網路介面及其通訊情境，例如遙控無人機與遙控器、地面控制站、App、雲端服務、維護工具及更新伺服器間之通訊。
- 應逐一判斷通訊內容是否包含安全或網路資產，例如控制指令、任務參數、配對資訊、帳號 token、網路設定、更新資訊或其他安全功能相關資料。
- 避免僅以「私有協定」、「一般使用者無法解析」或「無線距離有限」作為排除安全通訊機制之理由。
- 若主張例外，應提出可驗證之環境限制、邏輯限制或信任建立措施。
- 應注意不同設備狀態下之通訊差異，例如出廠預設、初始化、配對、一般飛行、維護模式及更新模式，可能涉及不同通訊路徑與保護需求。
- SCM-1 是 SCM-2、SCM-3 及 SCM-4 的基礎；若通訊介面、資產及情境未完整列出，後續完整性、真實性、機密性及重送攻擊防護之判斷也會受影響。

➢合規方針

面向	建議
通訊情境辨識	廠商應釐清哪些網路介面會與其他實體通訊，並確認各通訊情境是否傳輸安全或網路資產。
適用性判斷	若通訊涉及安全或網路資產，原則上應配置安全通訊機制；若主張不適用，應能說明其例外依據。
連線建立情境	若某些資料係建立連線、配對或信任關係所需之公開資訊，應說明其暴露目的及後續鑑別或信任建立方式。
環境限制	若依賴操作環境之實體或邏輯保護，應確認該限制足以避免通訊內容暴露予未授權實體。
保護範圍銜接	應將 SCM-1 判斷結果作為 SCM-2、SCM-3 及 SCM-4 之基礎，避免後續保護項目遺漏。

3.5.5 [SCM-2] 安全通訊機制之適當完整性及真實性保護

SCM-2 要求依 SCM-1 需要安全通訊機制保護之通訊，應採用最佳實務保護所傳輸安全資產與網路資產之完整性及真實性。因此，接收端應能確認訊息未遭未授權竄改，並可確認訊息來源或通訊端點係經授權或受信任者；若因互通性需求偏離最佳實務，應提出理由與補償措施。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 加密不等同於完整性與真實性保護；若通訊僅避免被讀取，但無法確認來源或偵測竄改，仍可能不足以支持 SCM-2。
- 控制指令、任務參數、飛行模式設定、網路設定、配對資訊、更新指示及雲端 API 回應，均應優先檢視是否需要完整性與真實性保護。
- 應說明初始信任關係如何建立，例如憑證、預置金鑰、配對程序、第二通道交換、第三方信任服務或其他等效機制。
- 若產品採用標準通訊安全協定或機制，例如 TLS、DTLS、WPA、SSH 或 IPsec，應進一步說明其使用版本、安全設定、對端身分驗證方式，以及是否已停用已知不安全之版本、演算法或設定選項。
- 若為私有協定，應說明訊息認證、端點鑑別、完整性驗證及金鑰管理方式，而非僅說明協定未公開。
- 若因互通性需支援較弱或舊版協定，應說明該模式之限制條件、啟用方式及補償措施。

➢合規方針

面向	建議
實作類別判斷	**IC.SCM-2.ManufSecret：製造商秘密或預置秘密** 若產品以製造商預先配置之秘密、共享金鑰或設備內建秘密建立真實性與完整性保護，廠商應說明秘密如何產生、配置、保護、區分設備或批次，以及外洩時如何降低影響。
	IC.SCM-2.SecChanExchange：安全通道交換 若產品透過安全通道建立或交換後續通訊所需之金鑰、參數或信任資訊，廠商應說明安全通道如何建立、端點如何驗證，以及通道外資料是否仍受保護。
	IC.SCM-2.PKI-based：PKI 憑證式機制 若產品以憑證、憑證鏈或公開金鑰基礎建設確認通訊端點，廠商應說明信任根、憑證驗證、有效期間、主體識別及撤銷或替代驗證方式。
	IC.SCM-2.ThirdPartyTrust：第三方信任服務 若產品依賴雲端服務、身分服務、授權伺服器或第三方信任機制確認端點或訊息來源，廠商應說明第三方信任關係、責任邊界及阻斷服務時之處理方式。
	IC.SCM-2.Generic：通用或其他方式 若產品採用訊息認證碼、數位簽章、AEAD、私有安全協定、供應商安全通訊模組或混合方式，廠商應說明完整性與真實性保護邏輯、保護範圍及限制條件。
保護範圍判斷	廠商應先確認哪些通訊內容需要完整性與真實性保護，例如控制指令、任務參數、飛行模式設定、網路設定、配對資料、更新指示或雲端 API 回應。
接收端驗證	接收端在接受資料、執行指令或變更設定前，應能確認訊息未遭未授權修改，且訊息來源或通訊端點為授權或受信任者。
信任建立與維持	廠商應說明通訊端點間之信任關係如何建立、如何維持，以及當金鑰、憑證、配對資料或信任來源異常時如何處理。
偏離最佳實務處理	若因互通性或產品限制需支援較弱或舊版協定，應限制其使用範圍，並說明補償措施及預設安全設定。

3.5.6 [SCM-3] 安全通訊機制之適當機密性保護

SCM-3 要求在通訊內容有機密性保護需求時，安全通訊機制應採用最佳實務保護所傳輸安全資產與網路資產之機密性。此要求並非代表所有通訊均必須加密，而是要求廠商能判斷哪些通訊內容若被竊聽，會造成安全功能受損、網路資源誤用或敏感資訊外洩，並對該通訊採取適當保護。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 應先區分哪些通訊內容具機密性需求，例如帳號憑證、登入 token、配對秘密、金鑰交換資料、Wi-Fi 設定、雲端 API token、任務資料、維護診斷資料或更新相關敏感資訊。
- 機密性保護可在通道層、訊息層或端對端層實作，但應說明保護起點與終點。
- 鏈路層加密不一定涵蓋所有通訊情境；例如雲端 API、維護介面、更新下載或 App 與設備間之本地連線仍需個別確認。
- 若資料需長期保密，應注意金鑰交換方式、金鑰更新、前向保密及密碼技術最佳實務。
- 若某些資料被判定不需機密性保護，仍應說明該資料即使被讀取也不會造成安全或網路資產受害之理由。
- 應避免將帳號、通行碼、token、金鑰材料或敏感設定以明文形式傳輸於登入、配對、維護或更新流程中。

➢合規方針

面向	建議
實作類別判斷	**IC.SCM-3.MessageEnc：訊息加密** 若產品針對單一訊息、資料物件或應用層 payload 加密，廠商應說明哪些欄位或資料被加密、加密端點為何，以及中間節點是否可接觸明文。
	IC.SCM-3.ChannelEnc：通道加密 若產品透過 TLS、DTLS、VPN、SSH、IPsec、WPA 或其他安全通道保護通訊，廠商應說明通道建立、端點驗證、協定版本、密碼套件及是否防止降級。
	IC.SCM-3.Generic：通用或其他方式 若產品採用端對端加密、混合式加密、供應商安全通訊模組、私有加密協定或其他方法，廠商應說明實際防揭露邏輯、保護範圍及限制條件。
機密資料判斷	廠商應辨識哪些通訊內容若被讀取，會造成安全功能、網路功能或後續存取風險，例如帳號憑證、權杖、配對秘密、金鑰資料、任務資料或維護資料。
保護邊界	應明確說明機密性保護之起點、終點及中間節點是否可能接觸明文。
金鑰處理	應說明加密所需金鑰如何建立、交換、保存及更新，並與 CCK、CRY 之要求保持一致。
不安全通訊限制	應停用或限制明文傳輸及不安全降級，避免敏感資訊經由替代路徑外洩。
例外判斷	若主張不需機密性保護，應說明資料內容、公開性、使用情境及風險判斷。

3.5.7 [SCM-4] 安全通訊機制之適當重送保護

SCM-4 要求依 SCM-1 需要安全通訊機制保護之通訊，應採用最佳實務避免安全資產與網路資產在傳輸過程中受到重送攻擊。若重複傳輸不會造成重送攻擊威脅，或因互通性需求必須偏離最佳實務，則應於文件中說明原因、影響範圍及相關補償措施。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 重送攻擊不只發生於登入流程，也可能發生於控制指令、模式切換、任務參數下發、返航指令、雲台控制、配對流程、更新指示及管理設定變更等情境。
- 若某些訊息允許重複傳送，應說明重複傳送不會造成狀態改變、權限提升、錯誤控制或其他安全影響。
- 用於防止重送之欄位，例如序號、時間戳記、一次性數值（nonce）或工作階段識別值，應納入完整性保護範圍，避免攻擊者修改該欄位後繞過檢查。
- 接收端亦應維護防重送視窗（anti-replay window），以拒絕重複、過期或超出允許範圍之訊息；亦應說明接收端如何處理重複、過期、不連續、超出視窗或不屬於目前工作階段之訊息。
- 無線通訊可能存在封包遺失或亂序，防重送設計應兼顧實際通訊特性，避免為了容錯而接受明顯重複或過期訊息。
- 重新配對、斷線重連、工作階段切換或時間同步異常時，應確認舊訊息不會被新工作階段接受。

➢合規方針

面向	建議
實作類別判斷	**IC.SCM-4.SeqNumb：序號機制** 若產品以遞增序號、封包編號或 anti-replay window 防止重送，廠商應說明序號如何產生、驗證、重置，以及接收端如何處理重複、過期或超出視窗之訊息。
	IC.SCM-4.TimeStamp：時間戳機制 若產品以時間戳判斷訊息新鮮性，廠商應說明時間來源、允許時間範圍、時間同步方式，以及設備離線或時間異常時如何處理。
	IC.SCM-4.OneTimeEncKey：一次性加密金鑰 若產品以一次性金鑰、單次工作階段金鑰或每訊息金鑰避免舊訊息重用，廠商應說明金鑰如何產生、使用、失效及防止重複使用。
	IC.SCM-4.Generic：通用或其他方式 若產品採用其他方式避免舊訊息被再次利用，例如一次性數值（nonce）、挑戰－回應機制、工作階段識別值、短效且不可重複使用之 token，或通訊協定本身提供之防重播機制，廠商應說明設備如何確認收到的訊息不是舊訊息重送，也不是被攻擊者複製後再次傳送的訊息。
重送風險判斷	廠商應辨識哪些通訊若被重送，可能造成狀態改變、控制異常、權限濫用或安全功能受損。
完整性綁定	防重送相關欄位應與訊息內容一併納入完整性保護範圍，例如透過訊息驗證碼（MAC）、數位簽章、具關聯資料之認證式加密（AEAD, Authenticated Encryption with Associated Data）或其他完整性保護機制。
接收端處理	接收端應拒絕重複、過期、不屬於目前工作階段或不符合序號規則之訊息。
工作階段管理	應說明連線建立、重新連線、序號初始化、時間同步及工作階段切換時之處理邏輯。
例外判斷	若特定訊息不需防重送保護，應說明該訊息重複傳送不會造成安全影響。

3.6 [RLM] 韌性機制

3.6.1 合規目標

[RLM] 韌性機制主要關注設備面對網路介面遭受阻斷服務攻擊時，是否能降低攻擊對網路功能與設備可用性之影響，並於攻擊結束後回復至廠商所定義之狀態。對遙控無人機而言，常見情境包含遙控無人機本體、遙控器、地面控制站、行動應用程式或雲端連線遭受大量封包、異常連線、重複請求或其他造成資源耗盡之異常流量影響，導致控制通訊、遙測回傳、設備管理、更新檢查或雲端同步功能受到干擾。

本機制之合規目標，並非要求遙控無人機在所有阻斷服務攻擊情境下仍能維持所有功能正常，而是要求廠商能針對與網路介面相關之風險，說明產品如何降低阻斷服務攻擊對必要功能、網路資源及設備狀態之影響；若攻擊造成部分功能不可用，亦應說明設備進入何種定義狀態，以及攻擊結束後如何回復至廠商所定義之操作狀態。

RLM 群組與 AUM-6、TCM、NMM 及 GEC 具有關聯。例如 AUM-6 主要處理鑑別機制遭暴力破解時之防護，TCM 可能涉及訊務控制或流量限制，NMM 則可能協助偵測異常網路狀態，GEC 也會涉及外部介面與暴露服務之管理。因此，廠商應避免只說明「設備可重新開機」或「網路中斷後會恢復」，而應說明針對網路介面遭受阻斷服務攻擊影響時之緩解、維持與回復策略。

3.6.2 常見攻擊面

攻擊面	說明
無線控制鏈路	攻擊者對遙控無人機與遙控器或地面站間之通訊介面發送大量封包、異常封包或干擾性連線請求，影響控制或遙測通訊。
本地網路服務	遙控無人機、遙控器或地面站提供之 Web UI、API、串流服務、配對服務或維護服務，可能遭大量請求或異常連線消耗資源。
雲端連線	App、設備或地面站與雲端服務間之登入、同步、更新檢查或資料上傳，可能受到大量請求、連線失敗或阻斷服務影響。
更新與維護通道	韌體更新、診斷連線或遠端維護服務若遭阻斷，可能影響安全更新部署或維護功能可用性。
設備內部資源	CPU、記憶體、連線數、socket、佇列、儲存空間或電力資源可能因異常網路流量而耗盡。
中繼或 Mesh 通訊	若遙控無人機或地面設備參與中繼、Mesh 或多設備網路，單一設備遭攻擊可能影響其他設備之網路功能。

3.6.3 威脅情境

遙控無人機常需在有限硬體資源、無線通訊環境及即時操作需求下運作。若網路介面缺乏韌性設計，攻擊者可能透過大量請求、洪水攻擊、惡意連線或資源耗盡攻擊，降低設備可用性或使重要功能無法正常運作。

威脅類型	情境說明
洪水攻擊	攻擊者對 Wi-Fi、乙太網路、API 或服務埠發送大量封包，使設備無法正常處理合法通訊。
連線資源耗盡	攻擊者建立大量連線、半開連線或重複請求，占用連線表、記憶體、CPU 或服務佇列。
廣播/群播封包異常	區域網路或中繼網路中出現大量廣播、群播或重複封包，影響設備網路功能。
阻斷服務	雲端服務、更新服務或維護服務遭阻斷，使設備無法同步資料、檢查更新或完成授權流程。
安全功能受干擾	大量錯誤登入、異常配對或惡意 API 請求影響鑑別、授權、監視或事件紀錄功能。
回復失敗	攻擊結束後設備未能恢復正常網路狀態，需人工重置或持續處於錯誤狀態。

3.6.4 [RLM-1] 韌性機制之適用性與適當性

RLM-1 要求設備應使用韌性機制，以降低阻斷服務攻擊對網路介面之影響，並於攻擊後回復至定義狀態。惟若該網路介面僅用於不與其他網路互通之區域網路，或網路中其他設備已提供足夠保護，可避免阻斷服務攻擊造成重要網路功能喪失，則可依實際情形提出不適用或例外說明。RLM-1 同時涵蓋適用性與適當性，因此廠商不僅需說明是否需要韌性機制，也需說明該機制如何降低攻擊影響並支援回復。

➢注意事項

- 應先列出設備所有網路介面，例如 Wi-Fi、藍牙、行動通訊、乙太網路、更新通道、雲端連線或維護網路介面。
- 應判斷各網路介面是否可能暴露於阻斷服務攻擊，包含大量封包、異常請求、連線耗盡或阻斷服務情境。
- 應避免僅以「攻擊機率低」、「無線距離有限」或「使用者不會開啟此功能」作為不需要韌性機制之理由。

- 若主張介面僅用於區域網路且不與其他網路互通，應說明其網路邊界、互通限制及實際操作情境。
- 若主張由網路中其他設備提供阻斷服務防護，應說明該設備或環境如何提供足夠保護，以及遙控無人機設備本身是否仍會喪失必要功能。
- 應定義設備在攻擊期間與攻擊結束後之狀態，例如維持基本通訊、保留既有連線、降級服務、丟棄異常流量、重新建立連線或回復正常操作。
- 韌性機制不應妨礙必要功能，例如合法控制指令、遙測資料、安全更新或維護功能；若採用流量限制或連線限制，應注意誤阻合法通訊之風險。

➢合規方針

面向	建議
網路介面判斷	廠商應逐一檢視設備之網路介面，判斷其是否可能受阻斷服務攻擊影響，以及是否需韌性機制。
必要功能定義	應說明攻擊期間需維持或優先保護之功能，例如控制連線、遙測回傳、安全狀態、更新能力或管理功能。
緩解機制	可依產品特性採用封包過濾、連線限制、速率限制、廣播/群播流量異常保護、資源保留、佇列管理或服務隔離等措施。
定義狀態	應定義設備於攻擊期間可能進入之狀態，以及攻擊結束後應回復之操作狀態。
回復能力	攻擊停止後，設備應能自動或依合理程序恢復必要網路功能，避免長時間停留於錯誤或不可用狀態。
誤阻控制	韌性機制應避免過度限制合法通訊，尤其是控制、遙測、更新、維護或安全事件處理相關流量。
例外判斷	若主張不適用，應說明介面僅限封閉區域網路，或由其他網路設備提供足夠保護之具體依據。

3.7 [NMM] 網路監視機制

3.7.1 合規目標

[NMM] 網路監視機制主要適用網路設備，確認其是否具備監視其所處理之跨網路流量的能力，以偵測可能與阻斷服務攻擊相關之異常流量或異常封包型態。對遙控無人機而言，若設備僅作為一般終端連接至網路，例如遙控無人機本體連線至遙控器、App 或雲端服務，通常應先判斷該產品是否具備轉送或橋接等「網路設備」特質。

遙控無人機適用 NMM 的情境，包括遙控器或地面站同時連接遙控無人機與網際網路、行動裝置或地面站作為網路分享節點、遙控無人機系統提供中繼或 Mesh 網路功能、設備作為多個網段之間的閘道，或產品具備轉送其他設備封包之功能。

廠商在產品具備「網路設備」特質時，應說明其如何監視所處理之跨網路流量，並偵測可能導致部分或全部阻斷服務之異常流量、封包型態或網路行為。

3.7.2 常見攻擊面

攻擊面	說明
遙控器或地面站作為閘道	遙控器或地面站同時連接遙控無人機、本地網路及網際網路，並可能轉送設備、App 或雲端服務間之流量。
熱點或網路分享功能	遙控器、地面站或行動裝置提供 Wi-Fi 熱點、橋接或網路分享，使其他設備透過其連線。
中繼或 Mesh 網路	多台遙控無人機、地面站或中繼設備共同形成網路，部分設備可能轉送其他節點之資料。
多網段任務系統	遙控無人機系統同時連接控制網路、影像傳輸網路、維護網路或雲端網路，並處理跨網路資料流。
行動通訊或專網接入設備	若遙控無人機相關設備具備基地台、行動網路接入、行動封包資料處理（如 GPRS 或其他行動數據封包機制）或類似網路轉送能力，可能需檢視跨網路流量監視。
維護或測試網路橋接	維護工具或測試設備在維修、診斷或更新時，可能臨時將設備網路與外部網路連接。

3.7.3 威脅情境

若遙控無人機之某組件具備跨網路處理、橋接或轉送流量之功能，該組件可能不是阻斷服務攻擊的最終目標，而是攻擊流量通過或被放大的節點。若缺乏網路監視機制，設備可能無法辨識異常流量，導致整體系統、其他網路設備或後端服務受到影響。

威脅類型	情境說明
異常封包量	大量封包於短時間內通過遙控器、地面站、閘道或中繼節點，可能影響控制、影像或雲端通訊。
非預期網段流量	設備收到來自未設定網路，或目的地超出其設定網路範圍之封包，可能代表錯誤路由、惡意掃描或異常轉送。
遭修改之封包	攻擊者傳送格式異常、欄位不一致或疑似遭竄改封包，使設備或被轉送端點資源耗盡。
ICMP / ARP 濫用	攻擊者透過 ICMP、ARP 或類似網路層封包造成掃描、洪泛、快取污染或網路壅塞。
行動網路封包濫用	若設備具備行動通訊、專網接入、基地台、閘道或其他行動網路流量處理功能，異常封包、大量連線或非預期協定流量可能影響設備或相關網路資源。
中繼節點被濫用	遙控無人機、地面站或中繼設備被用來轉送攻擊流量，使其他節點、服務或網路遭受阻斷服務攻擊影響。

3.7.4 [NMM-1] 網路監視機制之適用性及適當性

NMM-1 要求若設備屬於網路設備，則設備應提供網路監視機制，用以偵測其所處理之不同網路間流量中，可能與阻斷服務攻擊相關之指標。此要求同時涵蓋適用性與適當性，因此廠商不僅需判斷設備是否屬於網路設備，也需說明若適用，其監視機制如何分析跨網路流量並偵測異常行為或封包型態。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 應先判斷受評估設備是否屬於網路設備；若設備會在不同網路間轉送、路由、橋接或處理流量，通常需進一步檢視 NMM-1。
- 遙控無人機本體若僅作為終端設備連線至遙控器、App 或雲端服務，不一定屬於本要求所稱網路設備；但若其具備中繼、Mesh、熱點、路由或轉送其他設備流量之功能，則應重新評估。
- 應說明設備處理哪些網路之間的流量，例如遙控無人機控制網路、地面站網路、維護網路、行動網路、雲端網路或其他任務網路。
- 網路監視機制可採行為式或規則/型態式偵測，重點在於能偵測與阻斷服務相關之異常流量或封包型態。
- 應注意監視對象為「設備所處理之跨網路流量」，而非單純設備自身登入紀錄或一般系統 log。
- 若採用 ICMP、ARP、GTP 或其他特定封包監視/過濾機制，應說明其適用條件、監視範圍及異常判斷邏輯。
- 若產品依賴外部網路設備進行監視，應說明責任邊界；但若受評估設備本身屬於網路設備，仍應說明其自身是否具備必要監視能力或為何可由外部機制滿足需求。

➢合規方針

面向	建議
實作類別判斷	**IC.NMM-1.GTPFiltering：GTP 相關流量監視** 若設備處理行動網路核心、專網閘道、基地台或類似場域中之 GTP 或相關行動網路封包，廠商應說明其如何監視異常 GTP 流量或封包型態；一般僅使用 LTE/5G 模組連網之終端設備，通常不應直接以此類別概括。
	IC.NMM-1.IPPacketFiltering：IP 封包監視 若設備透過 IP 封包、來源/目的位址、協定、連接埠、封包數量或異常封包型態進行監視，廠商應說明監視條件、門檻及異常判斷邏輯。
	IC.NMM-1.Generic：通用或其他方式 若產品採用行為式監視、流量統計、網路異常偵測、供應商網路管理模組或混合方式，廠商應說明其如何偵測可能導致阻斷服務或網路功能喪失之異常流量。
網路設備判斷	廠商應先判斷產品或其組件是否會在不同網路間處理、轉送、橋接或路由流量，並據此判斷 NMM-1 是否適用。
跨網路流量識別	若適用，應釐清設備處理哪些網路之間的流量，以及該等流量與安全或網路資產之關聯。
監視結果處理	應說明偵測異常後如何處理，例如記錄、警示、觸發流量控制、限制特定封包或提供管理者資訊。
不適用判斷	若主張不適用，應具體說明設備不屬於網路設備，或不處理不同網路間之流量，而非僅以產品名稱或使用情境概括排除。

3.8 [TCM] 訊務控制機制

3.8.1 合規目標

[TCM] 訊務控制機制主要關注設備若屬於網路設備，是否能對其所轉送或處理之網路流量採取適當控制，以避免惡意、異常或未授權流量危害其所服務或控制之網路資產與安全資產。對遙控無人機而言，若遙控無人機本體僅作為一般終端設備連線至遙控器、App、地面站或雲端服務，通常需先判斷其是否實際具有網路設備性質；若產品具備閘道、路由、橋接、中繼、熱點分享、Mesh 或跨網路流量處理功能，則可能需要進一步檢視 TCM-1。

本機制之合規目標，並非要求所有遙控無人機均具備防火牆或完整網路安全閘道能力，而是要求在產品具備網路設備功能時，廠商能說明其如何控制所轉送之流量，例如依來源位址、目的位址、網路區域、協定型態、流量規則或網域隔離方式，避免設備成為攻擊流量的轉送節點，或使異常流量影響其他網路、服務或設備。

TCM 與 NMM、RLM 具有密切關係。NMM 偏向「監視與偵測」跨網路流量中的異常；TCM 則偏向「管理、限制、阻擋或隔離」跨網路流量；RLM 則關注設備在受到阻斷服務攻擊或異常網路影響時的韌性與回復能力。廠商應避免只說明「有監控流量」，而應進一步說明是否具備實際控制、阻擋、丟棄、隔離或限制流量之能力。

3.8.2 常見攻擊面

攻擊面	說明
遙控器或地面站作為閘道	遙控器或地面站同時連接遙控無人機、本地網路及網際網路，並可能轉送設備、App 或雲端服務間之流量。
熱點或網路分享功能	遙控器、地面站或行動裝置提供 Wi-Fi 熱點、橋接或網路分享，使其他設備透過其連線。
中繼或 Mesh 網路	多台遙控無人機、地面站或中繼設備共同形成網路，部分設備可能轉送其他節點之資料。
多網段任務系統	遙控無人機系統同時連接控制網路、影像傳輸網路、維護網路或雲端網路，並處理跨網路資料流。
行動通訊或專網接入設備	若遙控無人機相關設備具備基地台、行動網路接入、行動封包資料處理（如 GPRS 或其他行動數據封包機制）或類似網路轉送能力，可能需控制進出該網路之流量。
維護或測試網路橋接	維護工具或測試設備在維修、診斷或更新時，可能臨時將設備網路與外部網路連接。

3.8.3 威脅情境

若遙控無人機系統之某組件具備跨網路轉送或路由能力，該組件可能被攻擊者利用作為流量轉送、攻擊放大或繞過網路邊界之節點。若缺乏訊務控制機制，惡意或未授權流量可能經由該設備進入其他網路或服務，影響整體系統可用性與網路安全。

威脅類型	情境說明
惡意流量轉送	被入侵或遭濫用之設備將惡意封包轉送至其他遙控無人機、地面站、雲端服務或營運網路。
未授權網段存取	攻擊者透過遙控器、地面站或中繼節點，嘗試存取不應互通之控制網路、維護網路或任務網路。
來源/目的位址濫用	攻擊者偽造來源位址、使用未授權目的位址，或利用設備轉送不符合預期網路路徑之封包。
網域隔離失效	飛行控制、資料傳輸、維護管理或使用者操作等不同用途之通訊與功能未適當隔離，導致低信任網路或低權限功能可影響高信任功能。
攻擊流量放大	設備轉送大量異常封包，使其他網路節點、雲端 API 或後端服務受到阻斷服務攻擊影響。
維護橋接濫用	維護或測試模式下臨時開啟之橋接功能未受限制，使外部網路可接觸原本隔離之設備網路。

3.8.4 [TCM-1] 訊務控制機制之適用性及適當性

TCM-1 要求若設備屬於網路設備，應提供網路訊務控制機制。訊務控制機制可包含以 IP datagram 監視與規則為基礎之控制，例如依異常型態、惡意流量、來源位址或目的位址進行丟棄或阻擋；亦可包含不同網路網域間之完整實體或邏輯分離，或其他等效控制方式。

➢注意事項

- 本機制具有不同實作類別，廠商應依產品實際採用之機制判斷所屬類別，並提供產品相關實際設計與保護邏輯之說明。
- 應先判斷受評估產品或其元件是否屬於網路設備；若設備會在不同網路間轉送、路由、橋接或處理流量，通常需進一步檢視 TCM-1。
- 遙控無人機本體若僅作為終端設備連線至遙控器、App 或雲端服務，不一定屬於本要求所稱網路設備；但若具備中繼、Mesh、熱點、路由、橋接或轉送其他設備流量之功能，則應重新評估。
- 應說明設備處理哪些網路之間的流量，以及該流量可能影響哪些安全或網路資產。
- 訊務控制不應只停留在「可觀察流量」；若適用，應能說明如何依規則、位址、網域、協定或其他條件限制、阻擋、丟棄、隔離或重新導向流量。
- 若採用網域隔離作為訊務控制，應說明不同網域之間是否完全禁止轉送，或僅允許特定受控流量。
- 若採用 IP datagram 規則，應說明來源位址、目的位址、協定型態、異常型態或惡意流量如何被識別與處理。
- 若產品依賴外部路由器、防火牆、基地台或網路管理設備進行訊務控制，應說明責任邊界；但若受評估設備本身屬於網路設備，仍需說明其自身控制能力或為何可由外部機制合理涵蓋。
- 注意維護模式、測試模式、工程模式或臨時橋接功能是否可能繞過正常訊務控制。

➢合規方針

面向	建議
實作類別判斷	**IC.TCM-1.DatagramRules：封包/資料報規則控制** 若產品依來源位址、目的位址、協定、連接埠、封包型態或異常流量特徵進行阻擋、丟棄或限制，廠商應說明規則條件與處理方式。
	IC.TCM-1.TrafficSeparation：流量分離 若產品透過實體或邏輯方式分離控制網路、維護網路、使用者網路、影像網路或雲端網路，廠商應說明隔離邊界、允許通訊條件及例外流量控管方式。
	IC.TCM-1.Generic：通用或其他方式 若產品採用限速、閘道政策、服務隔離、供應商網路管理機制、SDN 規則或混合方式，廠商應說明實際控制邏輯及如何避免未授權或異常流量影響其他網路。
網路設備判斷	廠商應先判斷產品或組件是否會在不同網路間轉送、橋接、路由或處理流量，並據此判斷 TCM-1 是否適用。
流量範圍界定	若適用，應釐清設備控制或服務哪些網路間流量，以及該流量與安全或網路資產之關聯。
控制動作定義	訊務控制不應只停留在觀察流量；廠商應說明可採取哪些處理動作，例如阻擋、丟棄、限制、隔離、重新導向或觸發事件紀錄。
模式一致性	維護模式、工程模式、測試模式或臨時橋接功能，應避免繞過正常訊務控制規則。
不適用判斷	若主張不適用，應具體說明設備不屬於網路設備，或不處理不同網路間之流量。

3.9 [CCK] 機密密碼金鑰

3.9.1 合規目標

[CCK] 機密密碼金鑰主要關注設備中用於密碼演算法或密碼協定之機密金鑰，是否具備足夠安全強度、是否以適當方式產生，以及預先安裝之金鑰是否避免使用可被推導或多設備共用之靜態預設值。對遙控無人機而言，常見情境包含控制鏈路加密金鑰、訊息認證金鑰、韌體更新簽章驗證相關金鑰、設備配對金鑰、雲端連線憑證私鑰、VPN 或 TLS 相關私鑰，以及安全儲存或資料加密所使用之金鑰。

本機制之合規目標，並非要求廠商公開機密金鑰內容，而是要求廠商能清楚說明產品中有哪些機密密碼金鑰、各金鑰用於何種安全機制、其演算法與金鑰長度是否符合最佳實務、金鑰如何產生或預先安裝，以及是否存在多台設備共用或可由公開資訊推導之靜態金鑰。

CCK 群組與 SCM、SSM、SUM、AUM 及 CRY 具有高度關聯。例如安全通訊可能使用通訊金鑰，安全儲存可能使用資料加密金鑰，安全更新可能涉及簽章驗證或更新通道金鑰，鑑別機制則可能涉及憑證私鑰或設備金鑰。因此，廠商應避免只說明「使用加密」或「採用 TLS」，而應能說明相關機密金鑰之用途、強度、產生方式與生命週期管理。

3.9.2 常見攻擊面

攻擊面	說明
控制鏈路與遙測通訊	遙控無人機本體、遙控器或地面站之間可能使用對稱金鑰、工作階段金鑰或訊息認證金鑰保護控制指令與遙測資料。
設備配對與信任建立	遙控無人機與遙控器、App、地面站或周邊模組建立信任關係時，可能涉及預置金鑰、配對金鑰、憑證私鑰或共享秘密。
雲端服務連線	設備或 App 與雲端服務通訊時，可能使用 TLS 私鑰、client certificate、API 金鑰或其他服務憑證。
安全更新流程	韌體或軟體更新機制可能使用簽章驗證金鑰、更新通道金鑰或設備端信任根確認更新來源與內容。
安全儲存	設備、App 或地面站可能使用資料加密金鑰保護本機儲存之 token、憑證、設定、配對資料或飛行紀錄。

攻擊面	說明
製造與預先安裝流程	生產線可能於設備中注入預設金鑰、憑證或設備識別金鑰，若管理不當，可能造成多台設備共用或可被推導。
除錯、維護與測試模式	測試金鑰、開發金鑰或維護金鑰若殘留於正式產品，可能被攻擊者用於繞過正式安全機制。

3.9.3 威脅情境

機密密碼金鑰若強度不足、產生方式不當、被多設備共用或未妥善保護，攻擊者可能藉由猜測、暴力破解、從公開資訊推導、分析韌體、讀取儲存內容或取得單一設備後擴大攻擊其他設備。

威脅類型	情境說明
金鑰強度不足	金鑰長度過短、演算法過時或安全強度不足，使攻擊者可透過暴力破解或密碼分析取得金鑰。
隨機性不足	金鑰由弱亂數、固定種子、可預測資料或不足熵來源產生，導致不同設備或不同工作階段之金鑰可被推導。
多設備共用金鑰	多台遙控無人機、遙控器或地面站使用相同預置金鑰，攻擊者取得一台設備金鑰後可攻擊同型號其他設備。
可由公開資訊推導	金鑰由 MAC 位址、序號、型號、產品名稱或其他可觀察資訊推導，導致攻擊者可在未取得設備內部資料前推算金鑰。
開發或測試金鑰殘留	正式產品中保留開發金鑰、測試憑證、預設私鑰或範例金鑰，使攻擊者可偽造通訊、更新或配對。
金鑰用途不明	文件未說明金鑰用途、演算法、長度、來源或使用範圍，導致無法判斷是否符合最佳實務或是否影響其他安全機制。

3.9.4 [CCK-1] 適當之 CCK

CCK-1 要求用於保護安全或網路資產之機密密碼金鑰，應符合密碼技術最佳實務所需之安全強度；若某一金鑰僅用於特定安全機制，且已於 ACM、AUM、SCM、SUM 或 SSM 等相關章節中辨識並辯證其偏離最佳實務之理由，則可依實際情形提出例外說明。CCK-1 評估時會要求說明機密金鑰所使用之密碼演算法、金鑰長度與安全強度。

➢注意事項

- 應先盤點產品中所有機密密碼金鑰，包括預先安裝金鑰、設備產生金鑰、工作階段金鑰、通訊金鑰、資料加密金鑰、訊息認證金鑰及憑證私鑰。
- 應避免只說明「使用 AES」、「使用 TLS」或「使用加密」，而應說明相關機密金鑰之演算法、金鑰長度、用途及保護對象。
- 應確認金鑰安全強度與其保護之資產風險相符，例如控制指令、更新驗證、雲端鑑別或安全儲存所需之安全強度可能不同。
- 若使用舊版演算法、短金鑰或為支援互通性而偏離最佳實務，應說明偏離原因、使用範圍、風險及補償措施。
- 應避免將通行碼、token、API key 或其他非密碼演算法運作所需秘密全部混稱為 CCK；但若其實際用於密碼協定或密碼演算法，仍應納入判斷。

➢合規方針

面向	建議
金鑰盤點	廠商應辨識產品中用於密碼演算法或密碼協定之機密金鑰，並說明其用途、所在元件及保護對象。
演算法與長度	每一機密金鑰應對應其使用之密碼演算法、金鑰長度及預期安全強度，避免使用過時或不足強度之設計。
風險對應	金鑰安全強度應與其保護之安全或網路資產相稱，特別是控制通訊、更新驗證、設備鑑別與安全儲存等高影響情境。
偏離最佳實務	若金鑰使用偏離最佳實務，應能連回對應之 ACM、AUM、SCM、SUM 或 SSM 要求，說明偏離原因、限制條件及補償措施。
文件一致性	CCK-1 所列金鑰應與 SCM、SSM、SUM、AUM、CRY 等章節中提及之加密、簽章、通訊或鑑別機制一致。

3.9.5 [CCK-2] CCK 產生機制

CCK-2 要求機密密碼金鑰之產生應符合密碼技術最佳實務；若特定機密金鑰僅用於某一安全機制，且其偏離已於 ACM、AUM、SCM、SUM 或 SSM 等相關章節中辨識並辯證，則可依實際情形提出例外說明。標準說明金鑰安全強度高度取決於亂數來源、亂數產生器，以及金鑰產生、派生或建立演算法。

➢注意事項

- 應區分金鑰是由設備本身產生、由製造流程注入、由雲端服務產生、由配對流程建立，或由既有秘密衍生而來。
- 若金鑰由設備產生，應說明亂數來源、亂數產生器、熵來源、初始化方式及是否符合適用最佳實務。
- 若金鑰係透過金鑰派生或金鑰交換機制產生，應說明所使用之金鑰衍生函數（KDF, Key Derivation Function）或金鑰交換協定、其輸入資料、鹽值（salt）、一次性數值（nonce）或脈絡資訊（context）之使用方式，以及產生後金鑰之用途。
- 應避免使用固定種子、可預測值、序號、MAC 位址、時間戳單獨作為金鑰產生依據。
- 若使用第三方晶片、作業系統、SDK 或安全元件產生金鑰，仍應取得足以說明其亂數或金鑰產生能力之資料。

➢合規方針

面向	建議
產生來源判斷	廠商應說明每一 CCK 是由設備產生、製造注入、雲端產生、配對建立或由其他金鑰衍生。
亂數來源	若依賴亂數產生金鑰，應確保亂數來源具足夠熵，並說明其初始化、健康檢查或安全強度依據。
產生與衍生演算法	若使用金鑰產生、金鑰協議或金鑰衍生機制，應採用符合最佳實務之演算法與參數。
可預測性避免	金鑰產生不應主要依賴公開、固定或可預測資訊，避免攻擊者由設備屬性或環境資訊重建金鑰。
生命週期銜接	金鑰產生後，應與金鑰儲存、使用、輪替、撤銷及銷毀流程一致，避免產生安全金鑰但後續管理失效。
偏離最佳實務	若特定安全機制因互通性或產品限制而採用非最佳實務產生方式，應能連回相關要求之偏離辯證。

3.9.6 [CCK-3] 防止預先安裝 CCK 之靜態預設值

CCK-3 要求預先安裝於設備中之機密密碼金鑰，應避免使用所有設備相同、可由設備屬性推導或系統性重用之靜態預設值;原則上應使預先安裝之 CCK 對每台設備具實質唯一性。惟若該金鑰僅用於受授權實體控制條件下建立初始信任關係，或該金鑰作為共享參數是設備預期功能所必需，則可依實際情形提出不適用或例外說明。標準亦指出，唯一性係指不應被系統性重用或可由同產品其他設備推導，例如不應由製造商名稱、型號或 MAC 位址等設備屬性輕易推得。

➢注意事項

- 應盤點所有於製造、燒錄、出廠、初始化或部署前已存在於設備中之機密密碼金鑰。
- 應避免讓同型號、多批次或多台設備共用相同私鑰、共享秘密、更新金鑰、配對金鑰或預置通訊金鑰。
- 即使金鑰不易由使用者介面取得，若其存在於韌體、映像檔、設定檔、測試資料或公開可下載檔案中，仍可能被攻擊者分析取得。
- 若主張金鑰不需具設備間唯一性，應具體說明其僅用於受控條件下建立初始信任，或其作為共享參數確實為設備預期功能所必需。
- 開發、測試、維護或範例金鑰不應殘留於正式出貨產品中，除非有明確限制與合理辯證。

➢合規方針

面向	建議
預先安裝金鑰辨識	廠商應列出所有在設備交付使用前已存在之 CCK，並說明其用途、安裝階段及所在組件。
設備間唯一性	預先安裝 CCK 原則上應對每台設備具實質唯一性，避免多台設備共用相同金鑰或可由公開屬性推導。
靜態預設值避免	不應將相同固定金鑰、範例金鑰、測試金鑰或硬編碼金鑰用於正式產品之安全機制。
例外情形處理	若預先安裝金鑰需共用，應說明其是否僅用於授權實體控制條件下之初始信任建立，或是否為設備預期功能所必要之共享參數。
製造與供應鏈控管	金鑰注入、燒錄、憑證簽發、批次管理及出貨流程應避免金鑰外洩、重複配置或錯誤使用。
後續替換或失效	若預置金鑰僅用於初始化或首次配對，應說明後續是否會替換、失效或限制使用範圍。

3.10 [GEC] 一般設備能力

3.10.1 合規目標

[GEC] 一般設備能力主要關注設備在軟硬體組成、暴露介面、暴露服務、使用者文件、外部介面及輸入處理等基礎能力上，是否具備降低攻擊面及避免已知弱點被利用之能力。對遙控無人機而言，常見檢視對象包含遙控無人機本體韌體、遙控器韌體、地面控制站軟體、行動應用程式、通訊模組、作業系統、開源套件、雲端連線組件、維護服務、除錯介面、USB/ UART/ JTAG 等實體介面，以及所有可由外部介面輸入之資料。

本機制之合規目標，並非要求廠商證明產品完全不存在任何弱點或介面，而是要求廠商能說明產品軟硬體組成是否已盤點、是否存在公開已知可利用弱點、預設狀態下是否僅暴露必要服務、選用服務是否可由授權使用者設定、使用者文件是否揭露必要網路介面與服務、實體外部介面是否具備必要性，以及外部輸入是否經過適當驗證。

GEC 群組與前述多個要求群組具有基礎關聯。例如暴露服務會影響 ACM、AUM、SCM 及 RLM 之判斷；外部介面會影響 GEC-5 與 GEC-6；軟硬體弱點管理會影響 SUM 安全更新與整體風險處理。因此，廠商應避免僅以「產品功能正常」或「無對外服務」概括說明，而應具體盤點軟硬體、介面、服務、文件與輸入處理方式。

3.10.2 常見攻擊面

攻擊面	說明
軟體與韌體元件	遙控無人機本體、遙控器、地面站、App、通訊模組或安全模組可能含作業系統、函式庫、開源套件、SDK 或第三方元件。
預設暴露網路介面	出廠預設狀態下可能開啟 Wi-Fi AP、藍牙、乙太網路、行動通訊、API、Web UI、配對服務或串流服務。
暴露服務	SSH、Telnet、FTP、HTTP、RTSP、MQTT、mDNS、UPnP、診斷 API、維護服務或更新服務若開啟，可能形成攻擊入口。
選用服務	非基本操作必要，但為特定使用情境提供之服務，例如遠端診斷、雲端同步、影像串流、開發者 API 或維護功能。
實體外部介面	USB、UART、JTAG/SWD、SD 卡、CAN、S.Bus、Payload 接口、擴充槽、實體按鍵或維護端口可能被用於資料輸入或系統存取。
外部輸入資料	控制指令、任務檔、更新檔、設定檔、API 請求、感測器資料、影像檔、log 匯入或雲端下載資料皆可能影響安全或網路功能。

3.10.3 威脅情境

遙控無人機若未掌握軟硬體組成、未管理公開已知弱點，或出廠預設狀態下暴露過多服務，攻擊者可能透過已知漏洞、未必要服務、未文件化介面或未驗證輸入取得存取能力、造成服務異常或影響安全功能。

威脅類型	情境說明
已知弱點利用	攻擊者利用作業系統、通訊模組、Web 服務、開源套件或第三方 SDK 中已公開且可利用之弱點。
預設服務暴露	出廠預設狀態下開啟非必要服務，例如 SSH、Telnet、FTP、診斷 API 或測試服務，使攻擊面擴大。
選用服務濫用	遠端維護、雲端同步、開發者 API 或影像串流等選用功能無法停用，導致使用者無法依風險降低暴露面。
文件不足	使用者文件未說明預設開啟之網路介面與服務，導致使用者無法正確配置網路環境或辨識暴露風險。
實體介面濫用	攻擊者透過 USB、UART、JTAG、SD 卡或維護端口讀取資料、注入設定、進入除錯模式或修改系統狀態。
輸入資料攻擊	攻擊者送入畸形封包、異常 API 請求、惡意設定檔、錯誤任務檔或特殊字元，造成解析錯誤、注入、緩衝區溢位或安全功能繞過。

3.10.4 [GEC-1] 最新軟體及硬體，無眾所周知之可利用脆弱性

GEC-1 要求設備不應包含會影響安全或網路資產之公開已知可利用弱點；惟若該弱點在設備特定條件下無法被利用、已採取緩解措施並由廠商提出殘餘風險評估與接受理由，或已基於風險接受流程提出後續處理計畫，則可依實際情形提出說明。標準亦指出，廠商需能辨識設備所使用之軟硬體，以及查詢公開弱點資料庫來確認是否存在可利用弱點。

➢注意事項

- 應盤點產品中所有會影響安全或網路資產之軟體、韌體、硬體與第三方元件。
- 應避免僅說明「已使用最新版本」或「未發現弱點」，而應說明弱點查詢範圍、查詢來源、版本資訊及判斷日期。
- 若存在公開已知弱點，應判斷該弱點是否可於產品實際條件下被利用，而非只依 CVSS 分數作結論。
- 若主張弱點不可利用，應說明其前提，例如受影響功能未啟用、介面未暴露、需特定權限、需特定環境或已由其他機制阻擋。
- 若主張已降低至可接受殘餘風險或接受風險，應說明風險評估、緩解措施、接受理由及後續處理計畫。
- 供應商模組、通訊晶片、作業系統映像檔、App SDK 或開源套件若影響安全或網路功能，仍應納入弱點盤點與處理。

➢合規方針

面向	建議
軟硬體盤點	廠商應建立軟體、韌體、硬體及第三方元件清單，並標示版本、供應商、用途及是否影響安全或網路資產。
弱點查詢	應針對相關元件查詢公開弱點來源，如 NVD、供應商公告、開源專案公告、晶片商安全公告或其他可信弱點資訊來源。
可利用性判斷	對已知弱點應判斷其是否能於產品實際配置、暴露介面、啟用功能及操作環境下被利用。
風險處理	若弱點可影響安全或網路資產，應採修補、停用功能、限制暴露、補償控制、版本更新或風險接受等處理方式。
生命週期管理	產品上市後仍應維持弱點監控與安全更新能力，使新揭露弱點可被追蹤與處理。
文件一致性	GEC-1 之軟硬體與弱點盤點結果，應能與 SUM 更新機制、GEC-2 暴露服務及 GEC-4 使用者文件內容相互對應。

3.10.5 [GEC-2] 限制經由相關網路介面暴露之服務

GEC-2 要求設備於出廠預設狀態下，僅能暴露為設備設定或基本操作所必要，且會影響安全或網路資產之網路介面及透過網路介面暴露之服務。因此，預設狀態下不應開啟非必要之網路服務或介面，以避免增加攻擊面。

➢注意事項

- 應以「出廠預設狀態」檢視網路介面與服務，而非只檢視使用者完成設定後的狀態。
- 應列出所有暴露之網路介面與服務，例如 Wi-Fi AP、藍牙配對服務、Web UI、API、RTSP、SSH、mDNS、MQTT、更新服務或診斷服務。
- 應判斷每一暴露服務是否為設備設定或基本操作所必要；若不是，應避免預設開啟。
- 應避免以「服務有通行碼」、「服務僅供維護」或「一般使用者不會使用」作為預設暴露的充分理由。
- 若某服務僅在初始化或配對期間必要，應說明其開啟時機、關閉條件及是否會在完成設定後持續暴露。
- 若產品因多用途平台或作業系統預設服務而暴露網路服務，仍應確認該服務是否屬於產品基本操作或設定必要。

➢合規方針

面向	建議
預設狀態盤點	廠商應以出廠預設狀態盤點所有暴露之網路介面與服務。
必要性判斷	每一暴露服務應能對應至設備設定流程或基本操作需求，避免預設開啟非必要服務。
服務最小化	非必要之遠端管理、診斷、測試、開發、檔案傳輸或除錯服務，原則上不應於出廠預設狀態暴露。
初始化限制	只在初始化、配對或首次設定期間必要之服務，應具備限制開啟時間、完成後關閉或改為受控狀態之設計。
風險連動	暴露服務若影響安全或網路資產，應與 ACM、AUM、SCM、RLM 等要求之保護措施一致。
預設組態控管	產品版本變更、客製化設定或不同銷售型號，應避免因預設組態差異而新增未文件化或非必要服務。

3.10.6 [GEC-3] 選項服務及相關暴露網路介面之組態

GEC-3 要求若選用網路介面或透過網路介面暴露之選用服務會影響安全或網路資產，且屬於出廠預設狀態之一部分，則應提供授權使用者可啟用與停用該網路介面或服務之選項。該設定功能本身亦宜受 ACM 與 AUM 相關要求保護。

➢注意事項

- 應區分「基本操作必要服務」與「選用服務」。選用服務雖可能為預期功能之一部分，但不一定每個使用者或每個部署情境都需要。
- 若選用服務於出廠預設狀態存在，且會影響安全或網路資產，應允許授權使用者啟用或停用。
- 應避免將選用服務設計為永久開啟且無法關閉，尤其是遠端維護、雲端同步、診斷 API、影像串流或開發者服務。
- 啟用或停用選用服務之操作，應限制於授權使用者，避免未授權實體開啟高風險服務。
- 若服務停用後會影響產品功能，應清楚告知影響範圍，避免使用者誤關造成不可預期行為。
- 若選用服務因安全、法規或營運需求不得由使用者停用，應提出具體理由及替代風險控制措施。

➢合規方針

面向	建議
選用服務辨識	廠商應識別哪些網路介面或服務屬於選用功能，並判斷其是否影響安全或網路資產。
啟用/停用能力	對適用之選用服務，應提供授權使用者啟用與停用之設定能力。
授權控制	啟用或停用選用服務應受存取控制與鑑別保護，避免未授權實體改變服務狀態。
狀態可見性	使用者或管理者應能辨識選用服務目前是否啟用，以及啟用後可能暴露之介面或功能。
功能影響說明	停用選用服務可能影響雲端同步、遠端維護、影像串流或診斷功能時，應提供明確說明。
預設策略	對高風險選用服務，宜採預設關閉或最小暴露策略，並於需要時由授權使用者啟用。

3.10.7 [GEC-4] 暴露之網路介面及經由網路介面暴露的服務之文件

GEC-4 要求設備之使用者文件應包含出廠預設狀態下所有暴露網路介面，以及所有透過網路介面暴露之服務的說明。其目的在於讓使用者理解設備連線能力與可能攻擊面，並能正確配置設備與周邊網路環境。

➢注意事項

- 使用者文件應說明出廠預設狀態下會暴露哪些網路介面與服務，而不是只描述主要功能。
- 文件內容應足以讓使用者理解該介面或服務之用途、啟用狀態及基本風險。
- 應避免將暴露服務只記載於內部技術文件，卻未於使用者可取得之文件中揭露。
- 若不同型號、韌體版本、地區版本或產品模式之預設暴露服務不同，文件應能反映差異。
- 若服務於初始化、配對或維護模式中短暫暴露，也應視情況於文件中說明。
- GEC-4 文件內容應與 GEC-2、GEC-3 實際服務盤點一致，避免文件列出服務與實際掃描結果不符。

➢合規方針

面向	建議
文件揭露範圍	使用者文件應列出出廠預設狀態下所有暴露網路介面與透過網路介面暴露之服務。
服務用途說明	每一暴露服務應說明其用途，例如設定、配對、控制、串流、更新、雲端同步或維護。
使用者可理解性	文件應以使用者或管理者可理解之方式說明連線能力，而非僅列內部代碼或工程名稱。
組態差異管理	不同產品版本、韌體版本、模式或地區設定造成的暴露差異，應在文件或版本資料中可追溯。
風險與設定提示	對可設定或可停用之服務，文件應提醒使用者如何依部署需求調整，並說明停用可能影響。
與實際狀態一致	使用者文件所列介面與服務，應與出廠預設狀態實際暴露情形一致。

3.10.8 [GEC-5] 非必要之外部介面

GEC-5 要求設備僅應暴露其預期功能所必要之實體外部介面。依標準說明，非必要介面已透過實體保護、硬體封鎖或韌體停用，則可視為未暴露；而實體外部介面可能包含供內部系統通訊使用之介面、使用者介面及機器介面。

➢注意事項

- 應盤點所有實體外部介面，例如 USB、UART、JTAG/SWD、SD 卡、CAN、S.Bus、網路埠、擴充槽、按鍵、螢幕等連接器。
- 應說明每一實體外部介面與產品預期功能之關係；若介面僅為開發、測試或製造使用，正式產品中應避免暴露。
- 應避免將「介面沒有標示」、「使用者不會知道」或「需要特殊線材」作為必要性理由。
- 若實體介面已停用、封鎖、移除或被外殼阻擋，應說明其狀態及使用者是否仍可接觸。
- 若介面因維修、擴充或法規要求而保留，應說明其預期用途、限制條件與安全控制。
- 應注意介面雖非網路介面，仍可能透過資料匯入、除錯、命令列、韌體更新或設定修改影響安全或網路資產。

➢合規方針

面向	建議
介面盤點	廠商應列出所有實體外部介面，包含使用者可見介面、維護介面、擴充介面及機器介面。
必要性判斷	每一暴露實體介面應能對應至產品預期功能、設定、維護、擴充或安全需求。
開發介面處理	開發、測試、除錯或製造用介面於正式產品中應移除、停用、封鎖或限制存取。
暴露狀態控制	對不需暴露之介面，應以外殼、封膠、停用韌體功能、移除接點、禁用服務或其他方式降低可接觸性。
使用情境說明	若介面用於維護、Payload 擴充、資料匯入或緊急回復，應說明適用情境與限制條件。
與其他要求銜接	可能接收輸入或提供存取能力之外部介面，應同步考量 GEC-6 輸入驗證、ACM 存取控制及 AUM 鑑別。

3.10.9 [GEC-6] 輸入確證

GEC-6 要求設備對透過外部介面接收、且可能影響安全或網路資產之輸入，應進行驗證。標準說明輸入驗證應檢查語法、長度、內容，以及語意正確性；不當輸入驗證亦可能導致越界寫入、注入、路徑穿越等弱點。

➢注意事項

- 應先辨識哪些外部介面會接收輸入，例如網路 API、控制協定、任務檔、更新檔、設定檔、App 表單、維護命令、SD 卡匯入、USB 或周邊模組資料。
- 應判斷哪些輸入可能影響安全或網路資產，例如安全設定、網路組態、權限狀態、更新流程、配對資訊、控制指令或通訊行為。
- 輸入驗證不應只檢查格式，也應檢查長度、範圍、型別、結構、允許值、狀態條件及語意合理性。
- 對來自網路、外接媒體、周邊模組或非受信任來源之輸入，應特別注意畸形資料、特殊字元、超長欄位、負數、錯誤 offset、異常檔案結構或不合理參數。
- 驗證應盡可能在資料處理早期進行，避免無效或惡意輸入在系統內部繼續傳遞。
- 若輸入驗證失敗，應拒絕處理或採安全失敗行為，避免進入未定義狀態、當機、重啟迴圈或接受部分錯誤設定。

➢合規方針

面向	建議
輸入來源盤點	廠商應列出所有外部介面可接收之輸入來源，並判斷其是否可能影響安全或網路資產。
語法驗證	應檢查輸入格式、長度、型別、欄位結構、檔案格式、header、JSON/XML 結構或協定格式是否符合預期。
語意驗證	應檢查輸入值是否在合理範圍內，是否符合目前設備狀態，是否屬於允許值，以及是否與操作情境相符。
允許清單	對可列舉之輸入值、命令、檔案類型、參數或狀態轉換，宜採允許清單方式，拒絕未定義或非預期輸入。
失敗處理	輸入驗證失敗時，設備應拒絕處理、回傳錯誤、記錄事件或採安全預設行為，避免部分套用錯誤資料。
邊界條件	應特別檢視超長、空值、負值、重複欄位、錯誤 offset、畸形封包、特殊字元及異常檔案大小等邊界情境。
與安全功能銜接	涉及控制指令、更新檔、配對資料、安全設定或網路組態之輸入，應與 ACM、AUM、SUM、SSM、SCM 等要求之保護措施一致。

3.11 [CRY] 密碼學

3.11.1 合規目標

[CRY] 密碼學主要關注設備用於保護安全或網路資產之密碼演算法、密碼協定、密碼參數及密碼技術組態，是否符合其使用情境下之最佳實務。對遙控無人機而言，常見密碼技術應用包含控制鏈路加密、訊息認證、韌體更新簽章驗證、安全通訊協定、安全儲存加密、設備鑑別、憑證驗證、金鑰交換及金鑰產生等。

本機制之合規目標，並非要求廠商自行發明密碼技術，也不是要求所有功能採用同一套演算法，而是要求廠商能清楚說明產品中哪些安全或網路資產受到密碼技術保護、採用哪些密碼演算法或協定、保護目標為何，以及所採用之密碼技術為何可被視為符合目前最佳實務。

CRY 機制與 AUM、SUM、SSM、SCM 及 CCK 密切相關。AUM 可能使用通行碼、憑證或 token 進行鑑別；SUM 可能使用簽章或安全通道驗證更新；SSM 可能使用加密或完整性驗證保護儲存資料；SCM 可能使用 TLS、DTLS、VPN、訊息加密或訊息認證保護通訊；CCK 則關注機密密碼金鑰本身之強度與產生方式。因此，廠商應避免只寫「使用加密」或「使用標準協定」，而應能說明該密碼技術之保護目標、使用位置、參數設定及最佳實務依據。

3.11.2 常見攻擊面

攻擊面	說明
控制與遙測通訊	遙控無人機本體、遙控器、地面站或 App 間之控制指令、狀態回報、任務資料與遙測資訊可能依賴加密、訊息認證或安全通訊協定保護。
雲端與後台 API	App、設備或地面站與雲端服務之登入、資料同步、設備管理、授權檢查或飛行紀錄上傳，可能使用 TLS、token、憑證或簽章機制。
韌體與軟體更新	更新檔案、更新指示、版本資訊或更新來源可能透過數位簽章、雜湊、憑證鏈或安全通道確認完整性與真實性。
安全儲存	設備、App 或地面站可能使用加密、訊息驗證碼、簽章或系統金鑰鏈保護金鑰、憑證、權杖、配對資料、設定檔或紀錄資料。
設備配對與鑑別	遙控無人機與遙控器、App、地面站、雲端或維護工具建立信任時，可能使用金鑰交換、憑證、共享秘密、挑戰回應或密碼衍生機制。

攻擊面	說明
硬體安全模組或加速器	通訊晶片、安全元件、TEE、TPM、Secure Element 或硬體加密加速器可能內建特定密碼演算法或信任根。
私有協定或供應商 SDK	若產品使用私有控制協定、供應商通訊模組、OTA SDK 或第三方安全函式庫，仍需確認其密碼技術與設定是否符合最佳實務。

3.11.3 威脅情境

若產品使用過時、已知不安全、參數不足或設定錯誤之密碼技術，即使名義上具備加密、簽章或安全通訊機制，仍可能無法有效保護安全或網路資產。

威脅類型	情境說明
弱演算法使用	使用已不適合特定安全目的之演算法或協定，導致攻擊者可解密通訊、偽造訊息、繞過驗證或破解雜湊。
錯誤協定設定	使用安全協定但允許弱式密碼套件、不安全版本、降級連線、不驗證憑證或未檢查主體識別。
私有密碼設計	廠商自行設計加密或簽章方式，缺乏公開分析或安全證據，可能存在未被發現之設計缺陷。
密碼技術過時	產品生命週期較長，但密碼演算法、協定或硬體信任根無法更新，可能在使用期間內變得不符合最佳實務。
保護目標不清	文件未說明密碼技術要提供機密性、完整性、真實性、不可否認性或金鑰建立，導致無法判斷其適當性。
偏離最佳實務未辯證	因互通性、舊設備相容或硬體限制使用較弱機制，但未說明限制條件、風險與補償措施。

3.11.4 [CRY-1] 密碼學最佳實務

CRY-1 要求設備用於保護安全或網路資產之密碼技術，應符合最佳實務；若某項密碼技術係用於特定安全機制，且該偏離已於 ACM、AUM、SCM、SUM 或 SSM 等相關章節中辨識並提出辯證，則可依實際情形提出例外說明。標準指引中亦提到，可參考 ISO/IEC、SOG-IS、ETSI、ENISA、NIST SP 800 系列及 BSI TR-02102-1 等公開密碼技術指引或密碼目錄判斷最佳實務。

➢注意事項

- 應先盤點產品中所有用於保護安全或網路資產之密碼技術，包括演算法、協定、密碼套件、金鑰交換、簽章、雜湊、訊息驗證碼、AEAD、隨機數產生及金鑰派生機制。
- 應避免只說明「使用 AES」、「使用 TLS」或「使用加密」，而應說明其保護目標、使用情境、協定版本、參數設定及最佳實務依據。
- 應避免自行設計未經公開分析或缺乏安全證據之密碼演算法或協定；若採用新密碼技術，應提供其適用於該使用情境之證據。
- 若使用舊版協定、弱式演算法或為互通性支援而偏離最佳實務，應說明偏離原因、限制範圍、風險與補償措施，並對應至相關要求之辯證。
- 應考量產品預期生命週期。若密碼技術可更新，應與 SUM 安全更新能力銜接；若因硬體信任根、安全元件或加速器限制而不可更新，應確認其建議使用壽命足以涵蓋產品預期生命週期。
- 應確認密碼技術與 CCK 所列機密密碼金鑰之演算法、金鑰長度、安全強度及用途一致。

➢合規方針

面向	建議
密碼技術盤點	廠商應列出所有用於保護安全或網路資產之密碼技術，包含演算法、協定、密碼套件、簽章、雜湊、訊息驗證碼、AEAD、金鑰交換、金鑰派生及亂數產生。
保護目標說明	每一項密碼技術應說明其保護目標，例如機密性、完整性、真實性、防重送支援、金鑰建立、金鑰衍生或更新驗證。
最佳實務依據	應以可信密碼技術指引、公開密碼目錄、標準、供應商安全文件或密碼分析證據，說明所採用技術符合使用情境下之最佳實務。
參數與組態	使用標準協定或演算法時，應說明版本、模式、密碼套件、曲線、參數、金鑰長度、憑證驗證設定及是否停用不安全選項。
偏離處理	若因互通性、舊設備支援或硬體限制偏離最佳實務，應限制適用範圍，並於相關 ACM、AUM、SCM、SUM 或 SSM 要求中提出辯證與補償措施。
密碼敏捷性	產品宜具備因應密碼技術過時、弱點揭露或協定淘汰之更新或替換能力；若不可更新，應說明其生命週期與風險控制。
與其他章節一致	CRY-1 所列密碼技術，應能與 AUM、SUM、SSM、SCM、CCK 章節中提到之鑑別、更新、儲存、通訊與金鑰管理機制互相對應。

4. 技術文件與概念性評鑑撰寫指引

CNS 18031-1 各要求之評鑑準則通常包含必要資訊、實作類別、決策樹、概念性評鑑、功能完備性評鑑及功能充分性評鑑等內容。對產業端而言，合規準備之重點不僅在於安全機制本身，亦在於技術文件能否清楚說明該機制與標準要求之對應關係、適用性判斷，以及其如何由產品設計與使用情境加以支持。

本章節主要目的在於協助廠商理解概念性評鑑文件之撰寫邏輯。概念性評鑑不應僅視為表格填寫，而應被視為以產品事實與合理說明支持適用性與符合性判斷之過程。廠商撰寫時，應清楚區分描述(Description)與辯證(Justification)兩種資訊功能，避免以結論取代事實描述，或以概略說明取代適用性判斷理由。

本章不逐項列舉各要求之建議佐證資料。各要求可準備之文件、紀錄或其他佐證內容，已於第三章各項「合規方針」中依要求分別說明。本章重點在於協助廠商將既有產品設計、技術文件、介面盤點、資產盤點及功能說明，轉化為概念性評鑑表中可理解、可追溯且可支持判斷之描述與辯證。

4.1 概念性評鑑之定位

概念性評鑑主要檢視廠商所提供之描述與理由是否足以支持 CNS 18031-1 要求之適用性判斷及安全機制說明。其重點在於：文件是否完整描述受評估之資產、介面、功能、通訊情境及安全機制；決策樹路徑是否與產品事實一致；辯證(Justification)是否能合理支持該路徑之選擇。

因此，概念性評鑑並非單純回答「YES」、「NO」或「NA」。若廠商主張某項要求適用，應說明產品採用何種安全機制、該機制保護哪些資產，以及適用於哪些介面、功能或通訊情境；若主張某項要求不適用，則應說明不適用之依據，例如產品功能、通訊內容、操作環境、實體或邏輯限制、互通性需求或其他合理理由。

4.2 描述（Description）撰寫原則

描述(Description)係對產品事實、設計、功能或安全機制之客觀說明，宜回答「是什麼」、「在哪裡」、「如何運作」、「適用於哪些情境」等問題。描述不應直接寫成結論，例如「本產品符合 GEC-2」或「本產品具備安全通訊」，而應具體說明產品實際具備哪些介面、服務、功能、機制或限制。

描述宜至少包含下列內容：

- 受評估對象，例如遙控無人機本體、遙控器、行動應用程式、地面控制站、雲端服務、維護工具或其他元件。
- 涉及之介面或功能，例如網路介面、使用者介面、機器介面、維護介面、更新功能、配對功能或管理功能。
- 涉及之安全或網路資產，例如安全設定、網路組態、控制指令、配對資訊、帳號權杖、金鑰、憑證或更新資訊。
- 採用之安全機制或限制條件，例如存取控制、鑑別、加密、簽章、服務停用、介面限制、輸入驗證或例外條件。
- 適用狀態或操作情境，例如出廠預設、首次啟用、配對、一般操作、維護模式、更新模式或恢復原廠設定後狀態。

4.3 辯證（Justification）撰寫原則

辯證(Justification)係說明「為什麼可作成此判斷」之理由，宜回答「為何適用」、「為何不適用」、「為何此設計足以降低風險」、「為何該例外可被接受」等問題。辯證應建立在描述之產品事實上，並結合要求目的、威脅情境及風險影響進行說明。

常見不良寫法包括僅寫「本產品已具備防護」、「本產品不適用」、「此功能為內部使用」或「使用者無法操作」等結論，卻未說明具體產品事實與判斷依據。較佳寫法應具備可追溯性，例如明確指出該判斷基於哪一個介面、哪一項功能、哪一種產品狀態、哪一項安全機制或哪一項限制條件。

若廠商主張某要求不適用，辯證應特別注意：不適用不是因為廠商未設計相關機制，而是因為該要求依產品功能、資產、介面或使用情境確實不需適用；若缺乏充分理由，通常不宜以「NA」處理。

4.4 描述與辯證之對應原則

概念性評鑑表中，描述與辯證應相互支撐。描述負責說明「產品實際是什麼樣子」，辯證則說明「基於這些產品事實，為什麼可作成此判斷」。

資訊類型	功能	撰寫重點
描述 (Description)	描述產品事實與設計方式	說明受評估組件、介面、服務、資產、安全機制、設定狀態或操作情境。
辯證 (Justification)	說明判斷理由與風險降低邏輯	說明為何要求適用或不適用、為何該設計可降低風險、為何例外情形可被接受。
決策樹路徑	對應評鑑表之判斷流程	說明依產品事實所選擇之路徑，例如適用、符合、不適用或例外處理。
實作類別	對應標準所列之實作方式	若該要求列有實作類別，應說明產品實際設計較接近哪一類，而非僅填寫代碼名稱。

4.5 完整範例：[GEC-2] 限制經由相關網路介面暴露之服務

以下範例係依概念性評鑑表格之欄位格式填寫，用以示範廠商如何針對出廠預設狀態下之網路介面與暴露服務，描述產品事實、選擇決策樹路徑，並撰寫合理之辯證說明。本範例並非要求所有遙控無人機均具有相同介面或服務，廠商應依自身產品之出廠預設狀態、網路介面、服務暴露情形及必要性判斷進行填寫。

4.5.1 範例情境

範例產品以一般消費型或商用小型遙控無人機系統，其中包含遙控無人機本體、遙控器及行動應用程式。使用者於首次啟用時，行動應用程式需與遙控器或遙控無人機本體建立連線，以完成設備綁定、基本設定及控制鏈路建立。產品亦具備控制或遙測通訊與即時影像預覽功能。

此外，產品可能具有維護診斷服務，供原廠或授權維修人員於維修情境中使用。該類服務若非設備設定或基本操作所必要，原則上不應於出廠預設狀態下對外暴露。

4.5.2 技術文件填寫範例

名稱	網路介面及透過網路介面暴露之服務的說明	是出廠預設狀態的一部分嗎？	是否為基本操作所需？	是否為設備設定時所需？	是否屬於可選服務／可選介面？	DT.GEC-2.DN-1 該網路介面或服務在出廠預設狀態下是否可用？	DT.GEC-2.DN-2 該網路介面或服務是否會影響安全／網路資產？	DT.GEC-2.DN-3 該網路介面或服務是否為設備設定或基本操作所必需？	E.Just.DT.GEC-2	DT Result
App 連線介面	遙控器或遙控無人機本體於首次啟用時提供本地無線連線介面，供行動應用程式連線並完成設備綁定、基本設定及控制鏈路建立。	YES	YES	YES	NO	YES	YES	YES	App 連線介面為使用者完成首次啟用、設備綁定與基本設定所必要，亦為後續建立控制鏈路與設備操作流程之一部分。該介面雖於出廠預設狀態下可用，且會影響網路資產，但其屬於設備設定與基本操作所必需之網路介面，符合 GEC-2 對必要介面之允許條件。	PASS

名稱	網路介面及透過網路介面暴露之服務的說明	是否出廠預設狀態的一部分嗎？	是否為基本操作所需？	是否為設備設定時所需？	是否屬於可選服務／可選介面？	DT.GEC-2.DN-1 該網路介面或服務在出廠預設狀態下是否可用？	DT.GEC-2.DN-2 該網路介面或服務是否會影響安全／網路資產？	DT.GEC-2.DN-3 該網路介面或服務是否為設備設定或基本操作所必需？	E.Just.DT.GEC-2	DT Result
控制/遙測通訊服務	遙控無人機本體與遙控器間提供控制指令與遙測資訊交換服務，用於飛行控制、設備狀態回報及基本操作。	YES	YES	NO	NO	YES	YES	YES	控制/遙測通訊服務係遙控無人機基本操作所必要，若未提供該服務，使用者將無法進行飛行控制、狀態監看或基本操作。該服務雖於出廠預設狀態下可用，且會影響網路資產，但其為設備正常運作不可或缺之通訊服務，符合 GEC-2 要求。	PASS

名稱	網路介面及透過網路介面暴露之服務的說明	是出廠預設狀態的一部分嗎？	是否為基本操作所需？	是否為設備設定時所需？	是否屬於可選服務／可選介面？	DT.GEC-2.DN-1 該網路介面或服務在出廠預設狀態下是否可用？	DT.GEC-2.DN-2 該網路介面或服務是否會影響安全／網路資產？	DT.GEC-2.DN-3 該網路介面或服務是否為設備設定或基本操作所必需？	E.Just.DT.GEC-2	DT Result
影像預覽串流服務	遙控無人機本體或遙控器提供即時影像預覽串流，供行動應用程式或地面控制介面顯示飛行畫面與任務視覺資訊。	YES	YES	NO	NO	YES	YES	YES	本範例產品之預期功能包含即時影像預覽，該服務為使用者執行飛行操作、構圖、任務監看或避障輔助所需之基本功能。該影像串流服務雖於出廠預設狀態下可用，且可能影響網路資產，但其屬於產品基本操作所必要之服務，符合 GEC-2 要求。	PASS

名稱	網路介面及透過網路介面暴露之服務的說明	是出廠預設狀態的一部分嗎？	是否為基本操作所需？	是否為設備設定時所需？	是否屬於可選服務／可選介面？	DT.GEC-2.DN-1 該網路介面或服務在出廠預設狀態下是否可用？	DT.GEC-2.DN-2 該網路介面或服務是否會影響安全／網路資產？	DT.GEC-2.DN-3 該網路介面或服務是否為設備設定或基本操作所必需？	E.Just.DT.GEC-2	DT Result
維護診斷服務	設備供原廠或授權維修人員使用之維護診斷服務，可用於檢視設備狀態、調整維護參數或進行故障分析。	YES	NO	NO	YES	YES	YES	NO	維護診斷服務雖供原廠或授權維修使用，但並非設備設定或基本操作所必要；且其於出廠預設狀態下即透過網路介面暴露，並可能影響安全或網路資產，因此無法支持 GEC-2 之 PASS 判斷。。	FAIL

4.5.3 範例撰寫說明

在此範例中，App 連線介面與控制/遙測通訊服務屬於遙控無人機設定與基本操作所必要，因此即使於出廠預設狀態下可用，仍可支持 GEC-2 之 PASS 判斷。

影像預覽串流服務是否屬於基本操作所必要，應依產品預期功能判斷。若該產品定位為具備即時影像預覽之遙控無人機，且飛行操作或任務執行需依賴該畫面，則可說明其為基本操作必要服務；若該服務僅為選用功能，則應重新評估其是否可於出廠預設狀態下暴露。

維護診斷服務則用來示範 FAIL 情境。該維護診斷服務雖供原廠或授權維修使用，但並非設備設定或基本操作所必要；且其於出廠預設狀態下即透過網路介面暴露，並可能影響安全或網路資產，因此無法支持 GEC-2 之 PASS 判斷。若產品設計中該維護服務僅於授權維修流程、維護模式或受控環境下啟用，且出廠預設狀態未暴露，則應依其實際暴露狀態與必要性重新判斷。