# 無人機資安保障規範

## 第一部分：製造商資安成熟度查驗

## 第二部分：產品資安測試

# Cybersecurity Assurance Specification for Drone

## Part 1: Cybersecurity Maturity Inspection for Drone Maker

## Part 2: Product Cybersecurity Testing

無人機資安聯合驗測實驗室

財團法人電信技術中心

中華資安國際股份有限公司

安華聯網科技股份有限公司

鑑智實相科技股份有限公司

中華民國 111 年 12 月 30 日

# 目次

目次 ..... 1
前言 ..... 2
1. 適用範圍 ..... 3
2. 引用標準 ..... 4
3. 用語及定義 ..... 5
4. 製造商查驗項目 ..... 7
5. 無人機產品檢測 ..... 7
5.1 檢測項目及安全等級 ..... 7
5.2 系統安全 ..... 9
5.3 軟體安全 ..... 15
5.4 通訊安全 ..... 19
5.5 韌體安全 ..... 21
5.6 晶片安全 ..... 24
版本修改紀錄 ..... 27
附錄 A 安全通道（TLS）所選用的密碼套件要求 ..... 28

# 前言

無人機為具備自主飛行能力且不須人為操控的飛行器，無人機之間也具有協作功能以完成各種不同的任務，例如群飛表演、空中物流或空拍等。無人機帶來便利性的同時，其高度移動特性伴隨而來的資安風險也隨之增加，確保其資安防護能力以降低風險已是刻不容緩。本資安規範目的在於協助建立國內無人機資安檢測制度，強化無人機資安防護能力以降低安全相關疑慮。

# 1. 適用範圍

為確保無人機於開發設計階段即導入資安防護要素，本規範第一部分規範無人機製造商之資安成熟度及產品安全開發；第二部分則針對無人機（含飛航控制器、酬載模組及無人機交通管理系統模組等）、地面控制站及無人機交通管理系統等產品，制定其資安檢測項目。

本規範適用產品範圍如圖 1 所示，包含紅色方框內無人機、地面控制站及無人機交通管理系統與藍色實線表示的通訊界面；虛線表示之產品或通訊界面則不在本規範範圍。

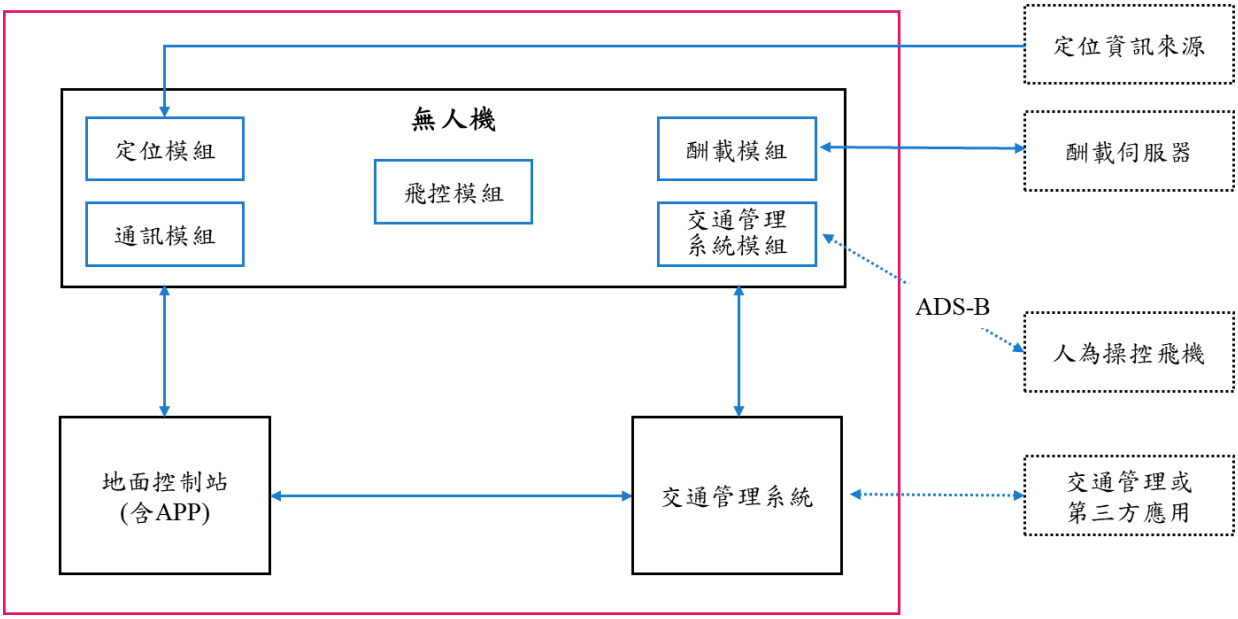


圖 1、本規範適用範圍

# 2. 引用標準

以下引用標準係本規範必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本（含補充增修）適用之。

[1] ISO/IEC 27001: “Information security management systems”.

[2] NIST 800-171A: “Assessing Security Requirements for Controlled Unclassified Information”.

[3] IEC 62443-4-1: “product security development life-cycle requirements”.

[4] IEC 62443-2-1: “Establishing an industrial automation and control system security program”.

[5] SEMI E187: “Specification for Cybersecurity of Fab Equipment”.

[6] UL 2900-1: “Standard for Software Cybersecurity for Network-Connectable Products”, Part 1: General Requirements.

[7] ANSI/CTA -2088.1: “Baseline Cybersecurity for Small Unmanned Aerial Systems”.

[8] 台灣資通產業標準協會「TAICS TR-0022 v1.0:2021 物聯網場域資安防護評估指引」

[9] 台北市電腦商業同業公會「資訊供應商資安成熟度參考指引」

[10] ITU-T X.1521: “Cybersecurity Information Exchange Vulnerability/State Exchange Common Vulnerability Scoring System (CVSS）”.

[11] Code of Federal Regulations: “§ 89.320 Minimum performance requirements for remote identification broadcast modules”.

[12] ETSI TS 103 701 V1.1.1 (2021-08): “CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements”.

[13] NIST FIPS 197: “Advanced Encryption Standard (AES)”.

[14] NIST SP 800-38A: “Recommendation for Block Cipher Modes of Operation: Methods and Techniques”.

[15] NIST SP 800-90A Rev. 1: “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”.

[16] NIST FIPS 180-4: “Secure Hash Standard (SHS)”.

# 3. 用語及定義

下列用語及定義適用於本規範。

## 3.1 無人機（Drone or Unmanned Aerial Vehicle, UAV）

指自遙控設備以信號鏈路進行飛航控制，或以導航設備執行自動駕駛操作，或其他經民航局公告之無人航空器。

## 3.2 飛航控制模組（Flying Controlling Module）

一種電路模組，用以控制及穩定無人機飛行路徑及飛行速度。

## 3.3 酬載模組（Payload Module）

因應任務執行，無人機所搭載的不同應用模組，如攝影機、通訊中繼或吊掛模組等。

## 3.4 地面控制站（Ground Control Station, GCS）

大部分位於地面，用來控制無人機飛行的軟硬體整合系統，包含通訊系統及應用程式等。

## 3.5 無人機系統（Unmanned Aerial System, UAS）

由無人機、地面控制站、通訊系統及其相關應用程式等組合而成，可執行飛行任務的系統。

## 3.6 無人機交通管理（Unmanned Aircraft System Traffic Management, UTM）系統

整合地面或空中設施及功能，提供即時空域資訊，以達到安全而有效的管理無人機飛行狀況。

## 3.7 資安成熟度（Cybersecurity Maturity）

用以評估組織是否具備有效的資安防禦機制之評估指標，以提供業務成長與運作的所有階段有效資安防護，並能持續改善。

## 3.8 安全軟體開發生命週期（Secure Software Development Life Cycle, SSDLC）

組織用於開發安全軟體過程，確保軟體生命週期之各個階段都具備安全性的程序。

## 3.9 通用漏洞評分系統（Common Vulnerability Scoring System, CVSS）

由資安事件應變小組論壇（Forum of Incident Response and Security Teams, FIRST）提供的漏洞評分系統，以衡量軟體漏洞的特徵和嚴重性進行評分，目前發展至第 3 版。

## 3.10 受測物（Unit Under Test, UUT）

本規範所稱受測物為待測之軟體、韌體、硬體、系統或通訊協定等之統稱。

# 4. 製造商查驗項目

將於後續另行公告。

# 5. 無人機產品檢測

## 5.1 檢測項目及安全等級

檢測項目包含系統安全、軟體安全、通訊安全、韌體安全及晶片安全等 5 大項目，安全等級區分為初階、中階及高階三級。檢測項目、檢測細項所對應之安全等級與適用設備如表 1，檢測細項區分為必測項目及選測項目。中階安全等級測試細項須包含所有初階及中階之必測項目；高階安全等級測試則須包含初階、中階及高階所有必測項目。廠商申請測試須檢附受測物未加密之軟體原始碼，申請中階與高階安全等級之受測物須檢附未加密韌體檔案；申請高階之受測物須檢附原始碼、Netlist 與 Layout 等設計文件、詳細運作規格及參數，並於測試過程配合軟硬體通訊介面與定位，並產生觸發訊號等實作。

表 1、檢測項目及對應之安全等級與適用設備

| 檢測項目 | 檢測細項 | 安全等級 | | | 適用設備 | | |
|---|---|---|---|---|---|---|---|
| | | 初階 | 中階 | 高階 | UAV | GCS | UTM |
| 5.2 系統安全 | 5.2.1 身分鑑別 | V | | | V | V | V |
| | 5.2.2 身分權限存取控制 | V | | | | V | V |
| | 5.2.3 網路服務埠檢測 | V | | | V | V | V |
| | 5.2.4 衛星定位系統強化能力 | | | V | V | | |
| | 5.2.5 衛星定位系統抗干擾能力 | | V | | V | | |
| | 5.2.6 遠端識別碼（Remote Identification, Remote ID）資訊之完整性（選測） | O | O | O | V | | |
| | 5.2.7 系統異常流量 | V | | | V | | V |
| | 5.2.8 酬載模組測試 | V | | | V | | |
| | 5.2.9 數據儲存安全 | V | | | V | | V |
| | 5.2.10 對無人機之存取認證機制 | | V | | | V | V |
| 5.3 軟體安全 | 5.3.1 軟體物料清單 | V | | | V | V | V |
| | 5.3.2 弱點掃描 | V | | | V | V | V |
| | 5.3.3 原碼掃描 | | V | | V | V | V |
| | 5.3.4 取得行動應用 App 基本資安標章 | | V | | | V | |
| | 5.3.5 惡意程式 | V | | | V | V | V |
| | 5.3.6 軟體更新加密保護 | | V | | | | V |
| | 5.3.7 軟體更新安全通道 | | V | | V | V | V |
| 5.4 通訊安全 | 5.4.1 無線通訊安全 | V | | | V | V | V |
| | 5.4.2 傳輸介面加密 | V | | | V | V | V |
| | 5.4.3 Wi-Fi Deauthentication（限具備 Wi-Fi 功能） | | V | | V | V | |
| 5.5 韌體安全 | 5.5.1 工程除錯介面 | | | V | V | V | |
| | 5.5.2 未公開揭露應用程式 | | | V | V | V | |
| | 5.5.3 韌體已知漏洞檢測 | | V | | V | V | |
| | 5.5.4 韌體更新加密保護 | | V | | V | V | |
| | 5.5.5 韌體更新安全通道 | | V | | V | V | |
| 5.6 晶片安全 | 5.6.1 密碼模組旁道洩漏防護（選測） | | | O | V | | |
| | 5.6.2 錯誤注入攻擊（選測） | | | O | V | | |
| | 5.6.3 AES 加密演算法（選測） | | | O | V | | |
| | 5.6.4 RSA 2048 加密演算法（選測） | | | O | V | | |
| | 5.6.5 確定性亂數產生器（DRBG）（選測） | | | O | V | | |
| | 5.6.6 非確定性亂數產生器（NRBG）（選測） | | | O | V | | |

註：本表以「V」標示表示必測項目，以「O」標示表示選測項目

## 5.2 系統安全

### 5.2.1 身分鑑別

5.2.1.1 測試目的

測試受測物之身分鑑別機制與通行碼強度是否具備防止暴力破解的能力與具備登入權限有效時間之限制。

5.2.1.2 測試方法

(1) 登入受測物之輸入錯誤達 3 次，確認是否鎖定至少 5 分鐘不得登入。

(2) 登入受測物之連續輸入錯誤達 10 次，確認該組帳號是否遭停用。

(3) 受測物登入成功後閒置達 15 分鐘後，確認是否會須強制登出與要求重新登入。

(4) 登入受測物所使用的通行碼，確認是否使用預設之通行碼，且通行碼設置規則應具備高複雜度（符合 8 碼以上長度，且包含大小寫字母、特殊符號、數字設定），並不使用具明顯含意之通行碼。

5.2.1.3 預期結果

(1) 涉及機敏性內容需提供身分驗證機制，如：每次登入需輸入帳號及通行碼。

(2) 登入受測物之輸入錯誤達 3 次，則鎖定至少 5 分鐘不得登入。

(3) 登入受測物之輸入錯誤連續達 10 次，則該組帳號須遭停用。

(4) 登入受測物成功後，閒置超過 15 分鐘應要求重新登入。

(5) 受測物使用非預設通行碼，通行碼設置規則具備高複雜度（符合 8 碼以上長度，且包含大小寫字母、特殊符號、數字設定），且不具明顯含意。

### 5.2.2 身分權限存取控制

5.2.2.1 測試目的

測試受測物可根據不同身分角色帳號有其不同對應的存取權限。

5.2.2.2 測試方法

(1) 測試設備連線並登入受測物之管理介面，建立 2 組以上帳號，並分別指派不同權限。

(2) 使用新建帳號分別登入受測物管理介面，並以授權及非授權給該帳號之功能進行功能驗證，確認是否能進行操作。

5.2.2.3 預期結果

(1) 受測物應具備不同身分角色帳號有其不同對應的存取權限。

(2) 以不同權限之帳號分別登入受測物，該帳號僅能對符合其授權之功能進行操作，如為非授權功能則無法進行操作。

### 5.2.3 網路服務埠檢測

5.2.3.1 測試目的

確保受測物沒有存在非預期之網路服務埠。

5.2.3.2 測試方法

(1) 將測試設備連接受測物，啟用受測物廠商所宣告之網路服務。

(2) 使用網路埠掃描工具，對受測物執行 TCP 與 UDP 埠 0～65535 之掃描。

(3) 核對掃描結果所呈現之網路服務與對應埠。

(4) 比對受測物送審資料中所聲明之網路服務與對應埠。

5.2.3.3 預期結果

受測物所開啟之網路服務與對應埠，與送審資料之內容相符。

### 5.2.4 衛星定位系統強化能力

5.2.4.1 測試目的

查驗受測無人機應具備定位強化機制，確保衛星定位系統訊號異常時，具備妥善應變作為，以避免偽造衛星定位系統訊號使無人機接收錯誤位置資訊，可能導致無人機被劫持或影響無人機本身衛星定位系統相關功能，包括禁航區限制（no-fly zone）、自動回航（Return to home）、跟隨 （Follow me）、自動巡航（Waypoint）等。

5.2.4.2 測試方法

(1) 將無人機升空飛行，使用衛星定位系統偽造工具產生離目前定位差距高於 200 公里之異常距離，以及透過軟體定義無線設備發送偽造衛星定位系統訊號欺騙無人機。

(2) 確認無人機遭受攻擊後是否有偏離原有的飛行路線。

(3) 確認無人機遭受攻擊後是否啟動故障處理機制進行迫降或返航模式。

5.2.4.3 預期結果

(1) 無人機不受偽造衛星定位系統訊號影響，仍維持正確的飛行路線。

(2) 或者無人機啟動故障處理機制進行迫降，或進入返航模式強迫無人機返回起飛地。

### 5.2.5 衛星定位系統抗干擾能力

5.2.5.1 測試目的

確保受測無人機在衛星定位系統干擾下仍可正常運行，或可啟動容錯轉移模式以抗干擾，展現通訊韌性。

5.2.5.2 測試方法

(1) 啟動受測無人機及地面控制站，並開啟衛星定位系統干擾器確認無人機是否仍可正常運行。

(2) 確認無人機是否具有無訊號迫降或返航故障處理機制。

5.2.5.3 預期結果

(1) 受測無人機運行未受衛星定位系統干擾，或啟動容錯轉移模式以抗干擾且可正常運行。

(2) 若無項次（1）之功能，無人機應啟動故障處理機制進行迫降或返航模式，強迫無人機返回起飛地。以避免當衛星定位系統信號受干擾，無人機將無法正確接收位置資訊，可能導致無人機無法正常運作或空中碰撞。

### 5.2.6 遠端識別碼（Remote Identification, Remote ID）資訊之完整性（選測項目）

5.2.6.1 測試目的

查驗受測無人機 Remote ID 模組利用的 Wi-Fi 或藍牙等無線射頻技術，所傳送之資訊（如無人機 ID、無人機位置及緯度、無人機速度、控制台位置與仰角、時間戳與緊急狀態等）具備防竄改能力。

5.2.6.2 測試方法

(1) 檢視無人機設備文件或拆解無人機，確認具有 Remote ID 模組與功能。

(2) 側錄並分析無人機 Remote ID 模組傳送之資訊，確認資訊經傳送或儲存過程中無法竄改，確保資料的完整性。

5.2.6.3 預期結果

無人機具備 Remote ID 功能，且相關傳送資訊具備防竄改機制，確保資料的完整性。

### 5.2.7 系統異常流量

5.2.7.1 測試目的

確保受測物無異常流量存在。

5.2.7.2 測試方法

(1) 對受測物進行最大運行時間或至少 24 小時的流量側錄。

(2) 比對側錄結果是否與廠商宣告之對外連線對象相符。

5.2.7.3 預期結果

與廠商宣告之對外連線對象相符。

### 5.2.8 酬載模組測試

5.2.8.1 測試目的

避免無人機之酬載模組（如網路攝影機）存在資安漏洞或未揭露之程式。

5.2.8.2 測試方法

(1) 查驗資安檢測證明所示之合格酬載模組與受測物版本相同，例如：TAICS 頒發之 IP camera 資安標章。

(2) 若受測物無資安檢測證明，須執行本規範 5.2.1、5.2.3 及 5.3.1 測試項目。

5.2.8.3 預期結果

(1) 酬載模組已取得既有資安檢測通過證明；

(2) 或通過本規範 5.2.1、5.2.3、及 5.3.1 測試。

### 5.2.9 數據儲存安全

5.2.9.1 測試目的

查驗受測物之飛行紀錄等機敏資料，應加密處理後儲存。機敏資料包括但不限於身分鑑別資訊（如使用者帳號、通行碼）及含有使用者隱私之資料，包括受測物所拍攝之影像及用戶資訊。此外，廠商應提供機敏資料之定義說明。

5.2.9.2 測試方法

(1) 連線並登入受測物，依廠商提供之數據資料儲存位置，檢查儲存內容之數據資料部份是否經加密處理。

(2) 確認匯出受測物之飛行紀錄等資料，檢查是否經加密處理。

5.2.9.3 預期結果

廠商提供之飛行紀錄等資料儲存位置，儲存內容之數據資料部分應採用 NIST SP 800-140Cr1 所核可之加密處理機制進行加密。

### 5.2.10 對無人機之存取認證機制

5.2.10.1 測試目的

測試受測物之認證機制是否可被避開，讓攻擊者獲得系統的控制與存取功能，進而登載並讓非法無人機完成對受測物的存取認證。

5.2.10.2 測試方法

(1) 利用與合法連線中的相同 Token 進行 API 請求，於登出後進行重送請求攻擊，確認能否取得資訊。

(2) 確認受測物有無針對合法登入之 Session 進行逾時管理或限制該系統允許多重登入。

(3) 確認受測物 Session 是否會具定時或於登入後更新之機制。

(4) 確認非法無人機是否能透過任何方式來避開受測物認證以完成授權成為合法設備。

5.2.10.3 預期結果

(1) 利用已取得之 Token 於登出後重送請求無法取得受測物資訊。

(2) 非法無人機無法利用合法的 Session 來進行傳遞測試，具 Session 逾時管理與禁止多重登入、Session 會定時或在登入後更新、啟用 Cookie 的安全屬性等方式，無法避開認證與亦無法存取受測物。

## 5.3 軟體安全

### 5.3.1 軟體物料清單

5.3.1.1 測試目的

審閱受測物是否具備軟體物料清單（SBOM）。

5.3.1.2 測試方法

審閱受測物之軟體物料清單，軟體物料清單內容欄位應包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者及時間戳記。

5.3.1.3 預期結果

受測物具備軟體物料清單且內容包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者及時間戳記。

### 5.3.2 弱點掃描

5.3.2.1 測試目的

確保受測物之作業系統與網路服務不能含有 CVSS 風險等級為高（High，即 7 分以上）之 CVE 漏洞。

5.3.2.2 測試方法

(1) 將測試電腦連接受測物。

(2) 使用具作業系統與網路服務之弱點掃描工具，並以最高管理（root）權限之帳號對受測物執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，確認作業系統與網路服務是否存在 CVSS 風險等級為高（High，即 7 分以上）之 CVE 漏洞。

5.3.2.3 預期結果

(1) 受測物之作業系統與網路服務不存在 CVSS 風險等級為高（High，即 7 分以上）之 CVE 漏洞。

(2) 當檢測出之資安風險漏洞不具有 CVSS v3.0（或更新版本）評分時，以 CVSS v2 評分為依據。

### 5.3.3 原碼掃描

5.3.3.1 測試目的

避免受測物存在資安漏洞或未揭露之程式。

5.3.3.2 測試方法

(1) 使用原碼掃描工具，對受測物之原始碼進行掃描

(2) 檢視該原碼掃描工具所產生之報告，確認作業系統與網路服務是否存在 CWE/SANS TOP 25 最新版本軟體缺陷。

5.3.3.3 預期結果

受測物之原始碼不存在 CWE/SANS TOP 25 最新版本軟體缺陷。

### 5.3.4 取得行動應用 App 基本資安標章

5.3.4.1 測試目的

避免受測物之行動應用 App 存在資安漏洞或未揭露之程式。

5.3.4.2 測試方法

確認取得 MAS 標章之行動應用 App，與受測物之行動應用 App 版本相同。

5.3.4.3 預期結果

受測物之行動應用 App 與取得 MAS 標章之行動應用 App 版本相同。

### 5.3.5 惡意程式

5.3.5.1 測試目的

確保受測物無惡意程式。

5.3.5.2 測試方法

使用惡意程式檢測工具進行完整系統掃描。

5.3.5.3 預期結果

未發現惡意程式。

### 5.3.6 軟體更新加密保護

5.3.6.1 測試目的

查驗飛控模組之軟體有經過加密保護。

5.3.6.2 測試方法

(1) 使用具軟體拆解功能之工具，對模組之軟體進行拆解。

(2) 檢視該軟體更新檔是否可被解析出檔案系統目錄。

(3) 若軟體更新檔無法被解析出檔案系統目錄，審閱可證明所使用加密演算法之書面資料。

(4) 若軟體更新檔未加密，確認系統通行碼資料的保密機制是否採用 NIST SP 800-140Cr1, CMVP Approved Security Functions 所核可之安全功能。

(5) 若軟體更新檔未加密，確認是否存在金鑰。

(6) 若軟體更新檔未加密，確認是否存在所宣告之外的 email 資料。

(7) 若軟體更新檔未加密，確認是否存在所宣告相連伺服器外之 IP 資料。

(8) 若軟體更新檔未加密，確認是否存在所宣告相連伺服器外之 URL 資料。

5.3.6.3 預期結果

(1) 軟體具備更新功能。

(2) 軟體更新檔案無法被解析出檔案系統目錄，且加密演算法採用 NIST SP 800-140Cr1, CMVP Approved Security Functions 所核可之安全功能。

(3) 軟體之程式碼與安裝檔內其他檔案，無檢出通行碼資料。

(4) 軟體之程式碼與安裝檔內其他檔案，無檢出加解密演算法之金鑰，或加解密金鑰不能被解密回復。

(5) 軟體之程式碼與安裝檔內其他檔案，不存在非公開 email 資料。

(6) 軟體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之 IP 資料。

(7) 軟體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之 URL 資料。

### 5.3.7 軟體更新安全通道

5.3.7.1 測試目的

查驗模組之軟體線上更新採用安全通道，同時能鑑別安全通道所使用憑證之正確性及有效性。

5.3.7.2 測試方法

(1) 使用安全通道掃描工具，對更新伺服器進行掃描。

(2) 比對掃描結果，檢視伺服器所支援的密碼套件，是否符合附錄 A 之要求。

(3) 將測試電腦（或行動裝置）連接模組，並啟動更新。

(4) 側錄更新伺服器與模組間之封包，檢視所側錄之封包是否採用安全通道。

(5) 再次啟動更新。

(6) 於更新伺服器發送憑證予模組期間，攔截更新伺服器憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式及憑證簽章。

(7) 發送已竄改之憑證予模組，於安全通道建立的交握過程中側錄封包，檢視模組是否接受此憑證。

5.3.7.3 預期結果

(1) 軟體具備更新功能。

(2) 模組之線上更新路徑通過安全通道，且安全通道僅支援附錄 A 中所建議之密碼套件。

(3) 若更新伺服器之憑證公鑰或憑證資訊被竄改，安全通道建立不成功。

## 5.4 通訊安全

### 5.4.1 無線通訊安全

5.4.1.1 測試目的

系統使用之無線通訊傳輸應加密，且應使用符合國際標準規範（例如: 4G/5G 等）的加密方式，不得使用客製化演算法。另外，傳輸過程不得包含系統機敏性之資料。

5.4.1.2 測試方法

(1) 使用安全通道檢測工具或側錄網路封包檢測是否符合該無線通訊安全要求之加密機制。

(2) 檢視傳輸過程是否包含帳號、通行碼、API Tokens、設定檔、程式原始碼、金鑰等系統機敏資訊。

5.4.1.3 預期結果

(1) 無線傳輸使用符合國際規範之加密機制。

(2) 傳輸過程無包含系統機敏性資料等。

### 5.4.2 傳輸介面加密

5.4.2.1 測試目的

確保受測物之傳輸介面具備 TLS v1.2 以上之加密連線機制，以避免禁航區資訊、無人機飛行路線及圖像等敏感性資料遭受竊取或竄改。

5.4.2.2 測試方法

(1) 連線並登入每一設備並同時抓取封包，確認是否加密傳輸。

(2) 使用工具掃描確認是否採用 TLS v1.2 以上之加密連線機制。

(3) 登入受測物確認系統敏感性資料之傳輸，是否皆密文且經過加密傳輸。

5.4.2.3 預期結果

(1) 受測物之傳輸具備 TLS v1.2 以上之加密連線機制。

(2) 網路傳輸過程無檢出敏感性資料，例如：帳號、通行碼、API Tokens、設定檔、程式原始碼、金鑰等。

### 5.4.3 Wi-Fi Deauthentication（限具備 Wi-Fi 功能）

5.4.3.1 測試目的

針對 Wi-Fi based 無人機，測試遭利用 IEEE 802.11 之 deauthentication Frame 取消或解除其認證之攻擊時，無人機應有適當處理機制。

5.4.3.2 測試方法

(1) 啟動無人機並發送 Wi-Fi Deauthentication Attack 訊號，來確認無人機是否會因取消認證而與控制器傳輸失敗

(2) 確認無人機 Wi-Fi 規格是否使用 WPA2 同等或以下版本之保護設置。

(3) 確認無人機是否具備訊號喪失即啟動返回機制。

5.4.3.3 預期結果

(1) 針對 Wi-Fi based 無人機，當遭利用 IEEE 802.11 之 deauthentication Frame 取消或解除其認證之攻擊時，無人機應持續維持正常運作與飛行。若無法達成，無人機應啟動故障處理機制進行迫降或返航模式，強迫無人機返回起飛地。

(2) 或 Wi-Fi 加密規格非 WEP 和 WPA PSK（WPA 1）。

(3) 或無人機除了具備 Wi-Fi 模式外也同時有 SDR 模式可自動切換。

## 5.5 韌體安全

### 5.5.1 工程除錯介面

5.5.1.1 測試目的

避免受測物之韌體存在未揭露或未受適當保護控制介面。

5.5.1.2 測試方法

(1) 依廠商提供說明文件及工具，拆解受測物之韌體檔案。

(2) 使用反編譯工具分析韌體。

(3) 分析是否存在工程除錯介面或未受適當保護之控制介面（未公開揭露，但可直接存取飛控模組之管理介面的方式）。

5.5.1.3 預期結果

經測試未檢出未公開揭露或未受適當保護之工程除錯或控制介面。

### 5.5.2 未公開揭露應用程式

5.5.2.1 測試目的

避免待測試之韌體存在資安漏洞或未揭露應用程式。

5.5.2.2 測試方法

(1) 依廠商提供說明文件及工具，拆解受測物之韌體檔案。

(2) 使用反編譯工具分析韌體。

(3) 分析是否存在資安漏洞或未揭露應用程式（未公開揭露，但卻存在的應用程式）。

5.5.2.3 預期結果

經測試未檢出資安漏洞或未公開揭露應用程式。

### 5.5.3 韌體已知漏洞檢測

5.5.3.1 測試目的

測試受測物韌體是否存在高風險 CVE 漏洞。

5.5.3.2 測試方法

(1) 使用韌體掃描工具，對受測物之韌體進行掃描。

(2) 檢視韌體掃描功能之工具所產生之報告，確認韌體內軟體套件未檢出 CVSS 風險等級為高（High，即 7 分以上）之 CVE 漏洞。

5.5.3.3 預期結果

受測物韌體未檢出 CVSS 風險等級為高（High，即 7 分以上）之 CVE 漏洞。

### 5.5.4 韌體更新加密保護

5.5.4.1 測試目的

查驗飛控模組之韌體有經過加密保護。

5.5.4.2 測試方法

(1) 使用具韌體拆解功能之工具，對模組之軟韌體進行拆解。

(2) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(3) 若韌體更新檔無法被解析出檔案系統目錄，審閱可證明所使用加密演算法之書面資料。

(4) 若韌體更新檔未加密，確認系統通行碼資料的保密機制是否採用 NIST SP 800-140Cr1, CMVP Approved Security Functions 所核可之安全功能。

(5) 若韌體更新檔未加密，確認是否存在金鑰。

(6) 若韌體更新檔未加密，確認是否存在所宣告之外的 email 資料。

(7) 若韌體更新檔未加密，確認是否存在所宣告相連伺服器外之 IP 資料。

(8) 若韌體更新檔未加密，確認是否存在所宣告相連伺服器外之 URL 資料。

5.5.4.3 預期結果

(1) 韌體具備更新功能。

(2) 韌體更新檔案無法被解析出檔案系統目錄，且加密演算法採用 NIST SP 800-140Cr1, CMVP Approved Security Functions 所核可之安全功能。

(3) 韌體之程式碼與安裝檔內其他檔案，無檢出通行碼資料。

(4) 韌體之程式碼與安裝檔內其他檔案，無檢出加解密演算法之金鑰，或加解密金鑰不能被解密回復。

(5) 若韌體更新檔未加密，確認是否存在所宣告之外的 email 資料。

(6) 韌體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之 IP 資料。

(7) 韌體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之 URL 資料。

### 5.5.5 韌體更新安全通道

5.5.5.1 測試目的

查驗模組之韌體線上更新採用安全通道，同時能鑑別安全通道所使用憑證之正確性及有效性。

5.5.5.2 測試方法

(1) 使用安全通道掃描工具，對更新伺服器進行掃描。

(2) 比對掃描結果，檢視伺服器所支援的密碼套件，是否符合附錄 A 之要求。

(3) 將測試電腦（或行動裝置）連接模組，並啟動更新。

(4) 側錄更新伺服器與模組間之封包，檢視所側錄之封包是否採用安全通道。

(5) 再次啟動更新。

(6) 於更新伺服器發送憑證予模組期間，攔截更新伺服器憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式及憑證簽章。

(7) 發送已竄改之憑證予模組，於安全通道建立的交握過程中側錄封包，檢視模組是否接受此憑證。

5.5.5.3 預期結果

(1) 韌體具備更新功能。

(2) 模組之線上更新路徑通過安全通道，且安全通道僅支援附錄 A 中所建議之密碼套件。

(3) 若更新伺服器之憑證公鑰或憑證資訊被竄改，安全通道建立不成功。

## 5.6 晶片安全

### 5.6.1 密碼模組旁道洩漏防護（選測項目）

5.6.1.1 測試目的

確保受測物不會透過旁道分析而洩漏密鑰。

5.6.1.2 測試方法

(1) 依據廠商提供之原始碼、Netlist 與 layout 之設計文件、運作規格及參數，建立測試儀器與受測物之連線。

(2) 完成軟硬體通訊介面定位並產生觸發訊號。

5.6.1.3 預期結果

(1) 受測物加密過程中，不得洩漏密鑰。

(2) 受測物使用之密碼演算法須符合 NIST 相關標準。

### 5.6.2 錯誤注入攻擊（選測項目）

5.6.2.1 測試目的

確保受測物具備錯誤注入攻擊防護

5.6.2.2 測試方法

(1) 依據廠商提供之原始碼、Netlist 與 layout 之設計文件、運作規格及參數，建立測試儀器與受測物之連線。

(2) 完成軟硬體通訊介面定位並產生觸發訊號。

5.6.2.3 預期結果

(1) 受測物加密過程應能阻擋注入攻擊。

(2) 受測物使用之密碼演算法須符合 NIST 相關標準。

### 5.6.3 AES 加密演算法（選測項目）

5.6.3.1 測試目的

確保 AES 128, 192, 256 於電子密碼本（Electronic codebook, ECB）模式與密碼區塊連結（Cipher-block chaining, CBC）模式之密碼演算法正確性。

5.6.3.2 測試方法

依 NIST SP 197 及 SP 800-38A 相關規範進行驗證。

5.6.3.3 預期結果

廠商所提交的結果符合實驗室實測結果。

### 5.6.4 RSA 2048 加密演算法（選測項目）

5.6.4.1 測試目的

確保 RSA 2048 with SigGen 9.31 on sha-224, 256, 384, 512 密碼演算法正確性。

5.6.4.2 測試方法

依 NIST PUB 180-4 進行驗證。

5.6.4.3 預期結果

廠商所提交的結果符合實驗室實測結果。

### 5.6.5 確定性亂數產生器（Deterministic Random Bit Generator, DRBG）（選測項目）

5.6.5.1 測試目的

確保 DRBG with Hash_DRBG on sha-224, 256, 384, 512 之正確性。

5.6.5.2 測試方法

依據 NIST SP 800-90A 規範進行驗證。

5.6.5.3 預期結果

廠商所提交的結果符合實驗室實測結果。

### 5.6.6 非確定性亂數產生器（Non-deterministic Random Bit Generators, NRBG）（選測項目）

5.6.6.1 測試目的

確認 NRBG 產生器亂度（Entropy）符合標準。

5.6.6.2 測試方法

依據 NIST 800-90B/C 進行驗證。

5.6.6.3 預期結果

廠商所提交的結果符合實驗室做出的結果。

# 版本修改紀錄

| 版本 | 日期 | 摘要 |
|---|---|---|
| v1.0 | 2022/12/30 | 出版 |
| | | |
| | | |
| | | |

# 附錄 A 安全通道（TLS）所選用的密碼套件要求

## A.1 TLSv1.2

(1) TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384

(2) TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384

(3) TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305

(4) TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

(5) TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256

(6) TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256

(7) TLS_ECDHE_ECDSA_WITH_AES256_SHA384

(8) TLS_ECDHE_RSA_WITH_AES256_SHA384

(9) TLS_ECDHE_ECDSA_WITH_AES128_SHA256

(10) TLS_ECDHE_RSA_WITH_AES128_SHA256

## A.2 TLSv1.3

(1) TLS_AES_128_GCM_SHA256

(2) TLS_AES_256_GCM_SHA384

(3) TLS_CHACHA20_POLY1305_SHA256

(4) TLS_AES_128_CCM_SHA256

(5) TLS_AES_128_CCM_8_SHA256