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

第三部分：晶片安全測試

Cybersecurity Assurance Specification for Drone

Part 1: Cybersecurity Maturity Inspection for Drone Maker

Part 2: Product Cybersecurity Testing

Part 3: Chip Security Testing

無人機資安聯合驗測實驗室

中華民國 112 年 6月 28 日

目次

前言

國家科學及技術委員會科技辦公室於 111 年 11 月 1 日召開「無人載具資安檢驗能量建構討論會議」，邀集數位發展部、經濟部工業局、財團法人電信技術中心及相關資安業者共同研商成立「無人機資安聯合驗測實驗室」（下稱聯合實驗室），後續委由聯合實驗室草擬「無人機資安保障規範」（下稱本規範），並由數位發展部、交通部民用航空局以及公共工程委員會共同成立「無人機技術工作小組」，針對本規範進行審閱討論，亦透過「無人機資安保障規範說明與交流會議」與無人機業者溝通並取得共識，爰完成本規範。

本規範之「無人機」即民用航空法之「遙控無人機」，係指自遙控設備以信號鏈路進行飛航控制，或以自動駕駛操作，或其他經交通部民用航空局公告之無人航空器，已運用在群飛表演、空中物流或空拍等，應用領域相當多元。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。本資安規範目的在於協助建立國內無人機資安檢測制度，以降低其所面臨之資安風險，提升無人機資通安全防護能力。

1. 適用範圍

本規範第一部分為製造商資安成熟度查驗（參閱第 4 章）、第二部分為產品資安測試（參閱第 5 章）及第三部分為晶片安全測試（參閱第 6 章），皆為獨立之內容，申請者視需求可個別選擇驗測。本規範第一部分係規範無人機製造商之資安成熟度及產品安全開發，確保無人機於開發設計階段即導入資安防護要素；第二部分則針對無人機與地面控制站等產品，制定其資安檢測項目；第三部分測試項目僅針對無人機使用之加解密晶片模組，惟其係供申請者自行選測，無涉初階、中階或高階無人機產品資安檢測項目。

本規範適用產品範圍如圖 1 所示，包含實線方框內無人機之飛行控制系統、定位模組、通訊模組，以及地面控制站（含 App）與實線表示之通訊界面；虛線表示之產品或通訊界面則不在本規範適用範圍內。

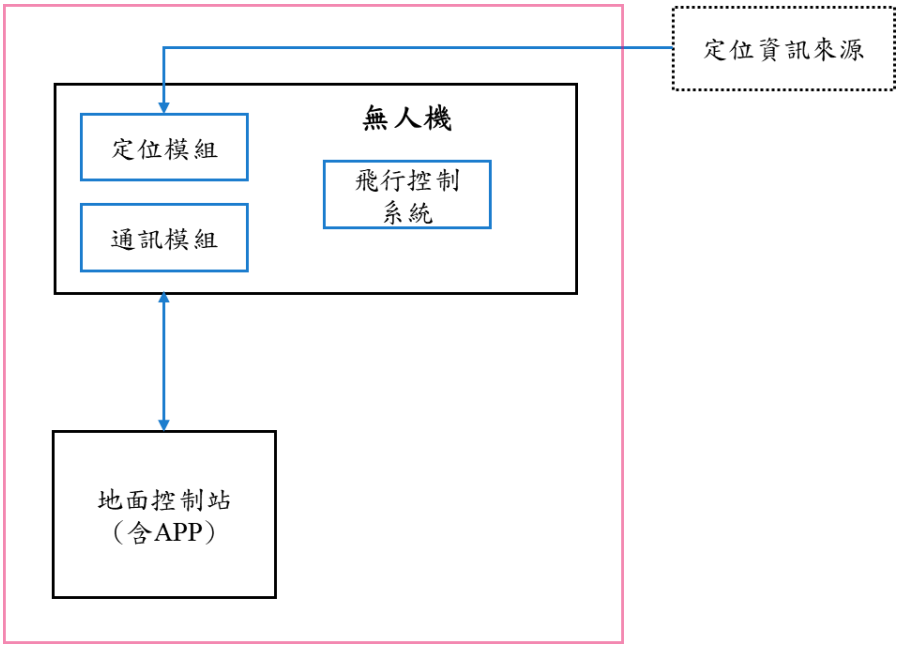

圖 1、本規範適用範圍

無人機酬載係無人機為執行任務外加裝備，其產生之資料不會輸出至飛行控制系統，亦不影響無人機飛行，根據任務的需求而有不同的設備。本規範未包含酬載之資安測試項目，建議具連網功能之酬載設備可參考業界常用之相關資安標準，亦可透過資安實驗室執行測試，取得測試報告或檢測通過證明，以強化無人機資安防護作為，詳見表 1。

表 1、酬載設備資安測試建議參考標準

具連網功能酬載類型	資安標準
網路攝影機	「影像監控系統安全－第1部：一般要求事項」(標準總號：CNS 16120-1)
無線寬頻設備	TAICS TS-0040 v1.0-無線寬頻分享器資安標準 TAICS TS-0041 v1.0-無線寬頻分享器資安測試規範
其他連網設備	TAICS TS-0045 v1.0-消費性物聯網產品資安標準 TAICS TS-0046 v1.0-消費性物聯網產品資安測試規範

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版（包括補充增修）。

國家科學及技術委員會科技辦公室	資訊供應商資安成熟度參考指引
行動應用資安聯盟	行動應用 App 基本資安規範
ANSI/CTA-2088-A	Baseline Cybersecurity Standard for Devices and Device Systems
ANSI/CTA -2088.1	Baseline Cybersecurity for Small Unmanned Aerial Systems
ANSI/CAN/UL 2900-1	Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
CNS 16120	影像監控系統安全－第 2 部：網路攝影機要求事項
NIST FIPS 140-3	Security Requirements for Cryptographic Modules
NIST FIPS 197	Advanced Encryption Standard (AES)
NIST SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-90A Rev. 1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
NIST SP 800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation
NIST SP 800-90C	Recommendation for Random Bit Generator (RBG) Constructions
NIST FIPS 180-4	Secure Hash Standard (SHS)
TAICS TR-0022 v2.0	物聯網場域資安防護評估指引 v2
TAICS TS-0015-2	影像監控系統資安測試規範-第二部_網路攝影機
U.S. Department of Homeland Security CISA,	Protecting against the threat of unmanned aircraft system (UAS)
U.S. Department of Homeland Security CISA,	Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS)

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）

本規範之「無人機」即民用航空法之「遙控無人機」，指自遙控設備以信號鏈路進行飛航控制，或以自動駕駛操作，或其他經交通部民用航空局公告之無人航空器。

3.2 飛行控制系統（flight control system）

飛行控制系統為遙控無人機運作之核心，其主要功能包括執行起飛、航行及降落等動作。

3.3 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。此處地面控制站係指與無人機之間建立命令與控制連結（Command & Control Link, C2 Link），且具上行與下行鏈路之地面控制站，並可預先設定無人機飛行路徑以執行飛行任務。地面控制站應用程式亦可採行動應用 App 之形式，惟其通訊架構需符合上述條件。如行動應用 App 未具上述形式或無法設定執行任務飛行模式，而僅做影像傳輸之用，則非屬本項定義之地面控制站應用程式。

3.4 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。

3.5 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。

3.6 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。

3.7 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。

3.8 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。

備註：

用語定義參考來源：

無人機	https://www.cisa.gov/topics/physical-security/unmanned-aircraft-systems/law-enforcement (美國 Cybersecurity and Infrastructure Security Agency, CISA）
飛行控制系統	https://www.caa.gov.tw/Article.aspx?a=3718&lang=1（交通部民用航空局）
地面控制站	https://www.faa.gov/documentlibrary/media/notice/n_8900.227.pdf (美國聯邦航空總署, FAA)
無人機系統	https://www.faa.gov/faq/what-unmanned-aircraft-system-uas（美國聯邦航空總署, FAA）
資安成熟度	（cybersecurity maturity）https://www.nccoe.nist.gov/news-insights/cybersecurity-capability-maturity-model-nist-cybersecurity-framework-mapping（美國國家標準暨技術研究院, NIST)
安全軟體開發生命週期	https://csrc.nist.gov/Projects/ssdf（美國國家標準暨技術研究院, NIST）
通用漏洞評分系統	https://nvd.nist.gov/vuln-metrics/cvss（美國國家標準暨技術研究院, NIST）
受測物	https://www.3gpp.org/（3GPP, 第 3 代合作夥伴計劃）

4. 第一部分：製造商資安成熟度查驗

本查驗項目引用國家科學及技術委員會科技辦公室「資訊供應商資安成熟度參考指引」，受查驗廠商應符合 4.1 資安成熟度與 4.2 安全產品開發等要求。

4.1 資安成熟度

受查驗廠商之無人機開發環境須符合以下要求，包含資訊資產管理、存取控制、人員培訓、技術脆弱性、日常維運及事件管理等面向。

4.1.1 處理未經授權的資產

4.1.1.1 資安要求

廠商至少每周須處理未授權資產，如移除未授權資產連網、拒絕遠端連接到廠商網路或隔離資產。

4.1.1.2 預期結果

(1) 廠商應訂定發現未授權資產連線的處理紀錄。

(2) 廠商若有遠端連接到廠商網路的功能，應有適當的權限管理機制。

4.1.2 設定資料存取權限

4.1.2.1 資安要求

廠商針對檔案系統、資料庫等應用程式，依據使用者的僅知原則（僅開放職務所需的系統功能）配置資料的存取控制權限。

4.1.2.2 預期結果

(1) 廠商應有敏感資料盤點紀錄。

(2) 廠商應有敏感資料的權限清單。

4.1.3 實施和管理主機防火牆

4.1.3.1 資安要求

在終端設備上部署主機式防火牆或通訊埠過濾工具，以預設禁止、例外開放之原則設定存取規則，只允許開放需要之服務與通訊埠。

4.1.3.2 預期結果

(1) 廠商應有設備盤點清單。

(2) 設備上應部署主機式防火牆或通訊埠過濾工具。

4.1.4 建立使用者撤銷流程

4.1.4.1 資安要求

建立並遵循系統用戶撤銷流程，包含用戶中止、權限撤銷、角色改變等情況，帳號撤銷不應刪除帳號，以保留稽核確認使用。

4.1.4.2 預期結果

(1) 廠商應對重要系統盤點使用者紀錄。

(2) 使用者工作異動應該調整或撤銷權限。

4.1.5 培訓員工資料處理作業

4.1.5.1 資安要求

提供員工保護敏感資料的教育訓練，包含如何識別、儲存、傳輸、歸檔及銷毀敏感資料，教育訓練中應該透過案例來說明，如在離開座位時鎖定系統、在會議結束後應擦除白板上的討論資料等。

4.1.5.2 預期結果

(1) 廠商應有定期資安培訓的規劃與紀錄。

(2) 廠商應該擁有適當的資安培訓教材。

4.1.6 建立存取授權流程

4.1.6.1 資安要求

制定廠商資產的存取授權流程，對於新進人員、系統授權、用戶角色變更等情境，皆遵循此流程。

4.1.6.2 預期結果

(1) 廠商應有重要系統的使用者存取權限盤點紀錄。

(2) 廠商應有使用者存取權限變更作業流程。

4.1.7 安全地銷毀資料

4.1.7.1 資安要求

制定資料敏感性定義與銷毀流程，對不同敏感性的資料有不同銷毀的方式。

4.1.7.2 預期結果

(1) 廠商應該擁有資料敏感性的定義說明。

(2) 廠商應該有針對不同敏感性等級資料的銷毀流程。

4.1.8 在伺服器上實施和管理防火牆

4.1.8.1 資安要求

在伺服器部署與管理防火牆機制，例如作業系統防火牆、虛擬防火牆或第三方的防火牆代理程式等。

4.1.8.2 預期結果

(1) 廠商應有設備盤點紀錄。

(2) 伺服器應有部署防火牆機制。

4.1.9 執行自動化作業系統更新管理

4.1.9.1 資安要求

廠商資產應自動化至少每月執行作業系統更新，或有更新風險管理機制。

4.1.9.2 預期結果

(1) 廠商應有設備盤點紀錄。

(2) 廠商應設定自動化的作業系統安全更新功能。

4.1.10 建立和維護弱點管理流程

4.1.10.1 資安要求

為廠商資產建立和維護弱點管理流程，每年或者在發生可能影響安全措施的重大廠商變更時，審查和更新文件。

4.1.10.2 預期結果

(1) 廠商應有應用程式盤點紀錄。

(2) 應用程式應有弱點管理機制。

4.1.11 執行自動化應用程序更新管理

4.1.11.1 資安要求

廠商資產應自動化至少每月執行應用程式更新，或有更新風險管理機制。

4.1.11.2 預期結果

(1) 廠商應有應用程式盤點紀錄。

(2) 廠商應有定期應用程式更新機制。

4.1.12部署和維護防毒軟體

4.1.12.1 資安要求

在所有可部署防毒軟體的廠商資產上皆應安裝防毒軟體。

4.1.12.2 預期結果

(1) 廠商應有資產盤點紀錄。

(2) 廠商的資產應有安裝防毒軟體。

4.1.13配置自動防毒軟體更新

4.1.13.1 資安要求

廠商使用的防毒軟體應設定病毒碼自動更新。

4.1.13.2 預期結果

廠商部署的防毒軟體應該開啟自動更新功能。

4.1.14建立和維護事故通報流程

4.1.14.1 資安要求

建立並維護資安事故通報流程，供員工報告資安事故，該流程包括報告時機、報告對象、方式及至少需要提供的訊息等，確保該流程對所有員工公開。每年或在發生可能影響此安全措施的重大廠商變化時，對此流程進行審查。

4.1.14.2 預期結果

(1) 廠商應有事故通報流程。

(2) 廠商應有事故處理紀錄。

4.2 安全產品開發

受查驗廠商之無人機產品開發流程須符合以下要求，包含資安專責人員、風險評估、系統更新、問題通報、事件應變等面向。

4.2.1 資安專責人員

4.2.1.1 資安要求

廠商之開發團隊中須有專責資安成員，以協助檢視安全開發各階段之資安作為是否符合安全性。

4.2.1.2 預期結果

(1) 資安成員擁有兩年以上的資安經歷。

(2) 資安成員於一年內須有安全開發相關的教育訓練紀錄。

4.2.2 資安風險評估

4.2.2.1 資安要求

廠商交付的成果應有風險評估分析，並擬定對應資安作為，以降低資安風險。

4.2.2.2 預期結果

廠商須提供資安風險評估分析報告，內含系統潛在的風險與對應的風險管控方法，並有資安成員與主管的審核紀錄。

4.2.3 系統更新功能

4.2.3.1 資安要求

開發環境之系統應有更新功能，並且在合理時間內提供更新檔案，以降低新弱點的威脅。

4.2.3.2 預期結果

廠商應提供相關系統的更新功能操作說明，內容包含當新弱點被揭露後，多久可以

提供更新檔案。

4.2.4 問題通報管道

4.2.4.1 資安要求

廠商應提供問題通報管道，讓開發團隊或資安專家可以向廠商通報問題。

4.2.4.2 預期結果

廠商提供通報管道及該通報管道正常運作的佐證資料。

4.2.5 資安事件應變

4.2.5.1 資安要求

廠商應提供資安事件的應變計畫，說明資安問題的處理流程（含重大事件的通報程序）與應變時間規劃。

4.2.5.2 預期結果

(1) 廠商提供資安事件的應變計畫說明文件，並有資安成員與主管的審核紀錄。

(2) 資安事件應變計畫內含有資安問題的處理流程與應變時間規劃。

5. 第二部分：產品資安測試

5.1 安全等級及安全要求

基於無人機應用情境多元，所面臨之資安風險不同，為利申請者得依其產品定位，驗測其具備之資安防護能量，爰將安全等級區分為初階、中階及高階等三級，相關等級說明及對應之測試項目，詳見表 2 至表 4。

表2、安全等級說明

安全等級	說明
初階	為無人機基本安全要求，主要針對身分鑑別、異常流量、軟體弱點、惡意程式及通訊安全，提供強化無人機遭惡意使用或資料外洩的安全防護
中階	除須符合初階之所有安全要求外，並增加韌體已知漏洞及衛星定位系統等要求，提供強化無人機被惡意入侵或干擾的安全防護
高階	除須符合中階之所有安全要求外，並增加命令連結（Command Link）、工程除錯介面及未公開揭露應用程式，提供強化無人機被安裝後門的安全防護

備註：

安全等級初階可適用於各款無人機，惟無人機執行飛行任務涉及關鍵基礎設施或具有機敏性者，宜選用安全等級中階之測試項目，如為軍事用途宜選用安全等級高階之測試項目。

有關無人機群飛之資安防護宜從風險管理角度針對群飛系統包含無人機、地面控制設備及相關通訊設備等進行評估，涵括威脅建模、漏洞檢測、滲透測試及衝擊分析等步驟，其中漏洞檢測包含初始化安全及隱私設定、安全軟體及韌體更新機制、通行碼及加密機制、軟體及功能安全、授權機制、鑑別機制、安全的通訊方式、程序與文件要求等安全政策，以及軟/韌體更新機制測試、惡意程式測試、弱點掃描、資料傳輸加密檢測等測試項目，詳見台灣資通產業標準協會出版之「物聯網場域資安防護評估指引 v2」之 L1 要求。

表 3 至表 4 測試項目表說明：第 1 欄為安全構面，內容包含系統安全、軟體安全、通訊安全、韌體安全；第 2 欄為安全要求項目；第 3 欄為安全等級，依各安全等級對應必測(以符號 V 表示)或選測(以符號 O 表示)的安全要求項目。

表 3、UAV 不同等級測試項目表

安全構面	安全要求項目		安全等級		
			初階	中階	高階
5.2 系統安全	5.2.1	數據儲存安全			V
	5.2.2	無人機命令連結（command link）之認證機制			V
	5.2.3	工程除錯介面			V
	5.2.4	衛星定位系統強化能力		V	V
	5.2.5	衛星定位系統干擾處理能力		V	V
	5.2.6	身分鑑別			
	5.2.7	身分權限存取控制			
	5.2.8	網路服務埠檢測			
	5.2.9	系統異常流量	V	V	V
5.3 軟體安全	5.3.1	原始碼安全掃描			O
	5.3.2	未公開揭露應用程式			
	5.3.3	軟體更新安全			V
	5.3.4	取得行動應用 App 基本資安標章			
	5.3.5	惡意程式			
	5.3.6	弱點掃描			O
5.4 通訊安全	5.4.1	無線通訊安全	V	V	V
	5.4.2	無線通訊失效處理能力		V	V
5.5 韌體安全	5.5.1	韌體已知漏洞檢測		V	V
	5.5.2	韌體更新安全	V	V	V

註：本表以「V」標示表示必測項目，以「O」標示表示選測項目

表 4、GCS 不同等級測試項目表

安全構面	安全要求項目		安全等級		
			初階	中階	高階
5.2 系統安全	5.2.1	數據儲存安全			V
	5.2.2	無人機命令連結（command link）之認證機制			V
	5.2.3	工程除錯介面			
	5.2.4	衛星定位系統強化能力			
	5.2.5	衛星定位系統干擾處理能力			
	5.2.6	身分鑑別	V	V	V
	5.2.7	身分權限存取控制	V	V	V
	5.2.8	網路服務埠檢測	V	V	V
	5.2.9	系統異常流量	V	V	V
5.3 軟體安全	5.3.1	原始碼安全掃描			V
	5.3.2	未公開揭露應用程式			V
	5.3.3	軟體更新安全			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
	5.3.6	弱點掃描	V	V	V
5.4 通訊安全	5.4.1	無線通訊安全	V	V	V
	5.4.2	無線通訊失效處理能力		V	V
5.5 韌體安全	5.5.1	韌體已知漏洞檢測			
	5.5.2	韌體更新安全			

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 系統安全檢測

此節主要針對無人機與地面控制站之系統安全進行檢測，包含數據儲存安全、無人機命令連結（command link）之認證機制、工程除錯介面、衛星定位系統、身分鑑別與存取控制、網路服務埠檢測及系統異常流量等面向。

5.2.1 數據儲存安全

5.2.1.1 測試目的

查驗受測物之飛行紀錄等機敏資料，如有儲存至非揮發性記憶體儲存體應加密處理後儲存。機敏資料包括飛控紀錄，及廠商應提供機敏資料之定義說明。

5.2.1.2 測試方法

(1) 連接受測物，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。

5.2.1.3 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 FIPS 140-2 以上之版本所核可之加密處理機制進行加密。

5.2.2 無人機命令連結（command link）之認證機制

5.2.2.1 測試目的

測試對無人機之命令連結（command link）認證機制是否可被避開，讓攻擊者獲得無人機的控制與存取功能，或讓非法無人機完成認證。

5.2.2.2 測試方法

廠商宣告受測無人機所使用之認證辨識機制，檢測人員依廠商宣告之認證辨識機制進行測試，並確認是否可完成認證並讓無人機與地面控制站相互識別。

5.2.2.3 預期結果

驗證後與廠商宣告之認證方式相符且無人機與地面控制站相互識別。

5.2.3 工程除錯介面

5.2.3.1 測試目的

避免受測物之序列埠或任何存取介面存在未揭露或未受適當保護控制介面。

5.2.3.2 測試方法

(1) 依廠商提供說明文件及工具，與可連接之序列埠或存取介面進行連接。

(2) 分析是否存在工程除錯介面或未受適當保護之控制介面。

5.2.3.3 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，包含序列埠如 UART、JTAG、USB 等。

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，並非測試其定位精準度，而是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，使用衛星定位系統訊號產生工具產生離目前定位差距高於 100 公里之異常距離衛星定位訊號，並發送予無人機以進行定位欺騙。

(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 衛星定位系統干擾處理能力

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，或可啟動失效安全機制，以展現通訊韌性。

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等失效處理機制。

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 身分鑑別

5.2.6.1 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。

5.2.6.2 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（即須重置才能再次登入）。

(3) 受測物登入成功後閒置達 15 分鐘後，確認是否有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），前述通行碼亦可採用生物特徵。

5.2.6.3 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 分鐘應強制登出並要求重新登入。

(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。

5.2.7 身分權限存取控制

5.2.7.1 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。

5.2.7.2 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。

5.2.7.3 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。

5.2.8 網路服務埠檢測

5.2.8.1 測試目的

確保受測物沒有存在非預期之網路服務埠。

5.2.8.2 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 之 0～65535 埠之掃描。

(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。

5.2.8.3 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。

5.2.9 系統異常流量

5.2.9.1 測試目的

確保受測物無異常流量存在。

5.2.9.2 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。

5.2.9.3 預期結果

與廠商宣告之對外連線對象相符。

5.3 軟體安全檢測

此節主要針對地面控制站之軟體安全進行檢測，無人機如有適用項目亦參考可選測，包含原始碼安全掃描、未公開揭露應用程式、軟體更新安全、行動應用 App 基本資安標章、惡意程式、弱點掃描等面向。

5.3.1 原始碼安全掃描

5.3.1.1 測試目的

避免受測物存在資安漏洞或未揭露之程式。

5.3.1.2 測試方法

(1) 使用原始碼安全掃描工具，對受測物之原始碼進行掃描。

(2) 檢視該原始碼安全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。

5.3.1.3 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。

5.3.2 未公開揭露應用程式

5.3.2.1 測試目的

避免受測物存在資安漏洞或未揭露應用程式。

5.3.2.2 測試方法

依廠商提供說明文件及工具如軟體物料清單，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，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）。

5.3.2.3 預期結果

經檢驗受測物具備說明文件或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，且未檢出資安漏洞或未公開揭露應用程式。

5.3.3 軟體更新安全

5.3.3.1 測試目的

查驗地面控制站之軟體是否有經過加密保護，以及查驗模組之軟體更新採用安全通道，同時能鑑別安全通道所使用憑證之正確性及有效性。

5.3.3.2 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 FIPS 140-2 以上之版本所核可之安全功能、是否存在金鑰、是否存在所宣告之外的 email 資料、是否存在所宣告相連伺服器外之 IP 資料、是否存在所宣告相連伺服器外之 URL 資料。

(5) 使用安全通道掃描工具，對更新伺服器進行掃描。

(6) 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。

(7) 將測試電腦（或行動裝置）連接模組，並啟動更新。

(8) 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。

(9) 再次啟動更新。

(10) 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。

(11) 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。

(12) 如軟體更新採用非線上更新之方式，廠商可說明其軟體更新方式，檢測人員將依其方式確認是否可確保更新軟體受到適當保護以維持其正確性。

5.3.3.3 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 FIPS 140-2 以上之版本所核可之安全功能。

(3) 軟體之程式碼與安裝檔內其他檔案，無檢出通行碼資料、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、不存在非公開 email 資料、不存在所宣告相連伺服器外之 IP 資料、不存在所宣告相連伺服器外之 URL 資料。

(4) 軟體具備更新功能。

(5) 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。

(6) 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。

(7) 檢測人員依廠商提供之更新方式，確認軟體更新過程受到適當之保護。

5.3.4 取得行動應用 App 基本資安標章

5.3.4.1 測試目的

避免受測物用作地面控制站之行動應用 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 弱點掃描

5.3.6.1 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。

5.3.6.2 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，即含 7 分以上）之 CVE 漏洞。

5.3.6.3 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（或更新版本）評分時，以 CVSS v2 評分為依據。

5.4 通訊安全檢測

此節適用於檢測無人機與地面控制站間之通訊，包含無線通訊安全與無線通訊失效處理等測試項目。

5.4.1 無線通訊安全

5.4.1.1 測試目的

無人機與地面控制站之間使用之無線通訊傳輸應加密，且應使用符合國際或區域標準規範（例如：3GPP、ETSI、IEEE 等或其他相當標準規範）所採用之加密方式。

5.4.1.2 測試方法

(1) 審閱無線通訊使用符合國際或區域標準加密方式之規格文件。

(2) 若無線通訊使用 IEEE 802.11 協定，則使用安全通道檢測工具或網路封包檢測是否使用 WPA2 或以上版本之加密方式。

(3) 送測之無人機如進行初階之測試，倘若無法對其使用之無線通訊傳輸進行加密，將確認其使用手冊或包裝外盒是否有明確說明無線通訊傳輸未加密造成之資安風險。

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) 使用手冊或包裝外盒有明確說明無線通訊傳輸未加密造成之資安風險。

5.4.2 無線通訊失效處理能力

5.4.2.1 測試目的

確保受測無人機在無線通訊失效下仍可正常運行，或具有自我防護機制，展現通訊韌性。

5.4.2.2 測試方法

(1) 啟動受測無人機，待受測無人機升空穩定後將地面控制站關閉。

(2) 確認受測無人機是否在訊號喪失後，即啟動返航或迫降機制。

5.4.2.3 預期結果

受測無人機應持續維持正常運作。若無法達成，無人機應啟動自我防護進行迫降或返航模式。

5.5 韌體安全檢測

此節主要針對無人機之韌體進行檢測，地面控制站如有適用項目亦參考可選測，包含韌體已知漏洞檢測與韌體更新安全等測試項目。

5.5.1 韌體已知漏洞檢測

5.5.1.1 測試目的

測試受測物韌體是否存在高風險 CVE 漏洞。

5.5.1.2 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。

(3) 送測之無人機如進行中階測試，且採用開放原始碼之飛控模組，可提供尚未進行參數設定之韌體原始碼，或提供其韌體採用開放原始碼之版本資訊，再進行掃描。

5.5.1.3 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。

5.5.2 韌體更新安全

5.5.2.1 測試目的

查驗飛控模組之韌體是否有經過加密保護，以及查驗模組之韌體更新採用安全通道，同時能鑑別安全通道所使用憑證之正確性及有效性。

5.5.2.2 測試方法

初階

(1) 若具有線上下載韌體供使用者自主更新功能，應提供校驗碼 (Checksums)供使用者確認是否韌體遭植入惡意內容與確定來源。

中/高階

(1) 使用具韌體拆解功能之工具，對模組之韌體進行拆解。

(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 FIPS 140-2 以上之版本所核可之安全功能、是否存在金鑰、是否存在所宣告之外的 email 資料、是否存在所宣告相連伺服器外之 IP 資料、是否存在所宣告相連伺服器外之 URL 資料。

(5) 使用安全通道掃描工具，對更新伺服器進行掃描。

(6) 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。

(7) 將測試電腦（或行動裝置）連接模組，並啟動更新。

(8) 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。

(9) 再次啟動更新。

(10) 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。

(11) 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。

(12) 如韌體更新採用非線上更新之方式，廠商可說明其韌體更新方式，檢測人員將依其方式確認是否可確保更新韌體受到適當保護以維持其正確性。

5.5.2.3 預期結果

初階

(1) 線上韌體更新來源應提供與下載韌體一致之校驗碼(Checksums)供查核。

中/高階

(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 FIPS 140-2 以上之版本所核可之安全功能。

(3) 韌體之程式碼與安裝檔內其他檔案，無檢出通行碼資料、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、不存在非公開 email 資料、不存在所宣告相連伺服器外之 IP 資料、不存在所宣告相連伺服器外之 URL 資料。

(4) 韌體具備更新功能。

(5) 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。

(6) 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。

(7) 檢測人員依廠商提供之更新方式，確認韌體更新過程受到適當之保護。

6. 第三部分：晶片安全測試

晶片安全為獨立測試項目且僅針對無人機使用之加解密晶片模組，與取得初階、中階或高階資安驗證無關。若送測廠商欲於報告或證書加註無人機通過晶片安全測試，其該加解密晶片模組須通過 FIPS 140-2 以上或 ISO 15408 或同等加密模組認證，於提交佐證資料經查驗後得免予測試。如果使用未經上述認證過的加密模組，則需進行表 5 所列之晶片安全測試項目檢測。

表 5、UAV 之加解密晶片模組安全測試項目表

安全構面	安全要求項目
6.1 晶片安全	6.1.1 密碼模組旁道洩漏防護
	6.1.2 錯誤注入攻擊
	6.1.3 AES 加密演算法
	6.1.4 RSA 2048 加密演算法
	6.1.5 確定性亂數產生器（DRBG）
	6.1.6 非確定性亂數產生器（NRBG）

6.1 晶片安全檢測

此節主要針對無人機使用之加解密晶片模組進行檢測，包含密碼模組旁道洩漏防護、錯誤注入攻擊、加密演算法、亂數產生器等面向。

6.1.1 密碼模組旁道洩漏防護

6.1.1.1 測試目的

確保受測物不會透過旁道分析而洩漏密鑰。

6.1.1.2 測試方法

(1) 廠商須配合偕同完成建立測試儀器與受測物之連線，及提供所需相關必要資訊。

(2) 完成軟硬體通訊介面定位並產生觸發訊號。

6.1.1.3 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。

6.1.2 錯誤注入攻擊

6.1.2.1 測試目的

確保受測物具備錯誤注入攻擊防護。

6.1.2.2 測試方法

(1) 廠商須配合偕同完成建立測試儀器與受測物之連線，及提供所需相關必要資訊。

(2) 完成軟硬體通訊介面定位並產生觸發訊號。

6.1.2.3 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。

6.1.3 AES 加密演算法

6.1.3.1 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。

6.1.3.2 測試方法

依 NIST SP 197 及 SP 800-38A 相關規範進行驗證。

6.1.3.3 預期結果

廠商所提交的結果符合實驗室實測結果。

6.1.4 RSA 2048 加密演算法

6.1.4.1 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。

6.1.4.2 測試方法

依 NIST PUB 180-4 進行驗證。

6.1.4.3 預期結果

廠商所提交的結果符合實驗室實測結果。

6.1.5 確定性亂數產生器（Deterministic Random Bit Generator, DRBG）

6.1.5.1 測試目的

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

6.1.5.2 測試方法

依據 NIST SP 800-90A 規範進行驗證。

6.1.5.3 預期結果

廠商所提交之結果符合實驗室依據 NIST SP 800-90A 規範實測之結果。

6.1.6 非確定性亂數產生器（Non-deterministic Random Bit Generators, NRBG）

6.1.6.1 測試目的

確認 NRBG 產生器亂度（Entropy）符合標準。

6.1.6.2 測試方法

依據 NIST SP 800-90B/C 規範進行驗證。

6.1.6.3 預期結果

廠商所提交之結果符合實驗室依據 NIST SP 800-90B/C 規範實測之結果。

版本修改紀錄

版本	日期	摘要
v1.0	2022/12/30	出版
v2.0	2023/6	1. 廣納各界專家學者意見後進行改版 2. 增列第一部分：製造商資安成熟度查驗之測試項目 3. 增列無人機群飛系統資安檢測說明 4. 將晶片檢測獨立為第三部分(第 6 章節)

附錄 A 安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

A.1 TLSv1.2

TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES256_SHA384
TLS_ECDHE_RSA_WITH_AES256_SHA384
TLS_ECDHE_ECDSA_WITH_AES128_SHA256
TLS_ECDHE_RSA_WITH_AES128_SHA256

A.2 TLSv1.3

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256

附錄 B 安全要求項目與引用標準表

安全構面	安全要求項目	引用標準
5.2 系統安全	5.2.1 數據儲存安全	U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) ANSI/CTA-2088-A
	5.2.2 無人機命令連結（command link）之認證機制	U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) ANSI/CTA-2088-A
	5.2.3 工程除錯介面	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements ANSI/CTA-2088-A
	5.2.4 衛星定位系統強化能力	U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS)
	5.2.5 衛星定位系統干擾處理能力	U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS)
	5.2.6 身分鑑別	U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) ANSI/CTA-2088-A
	5.2.7 身分權限存取控制	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements ANSI/CTA-2088-A
	5.2.8 網路服務埠檢測	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements ANSI/CTA-2088-A
	5.2.9 系統異常流量	TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引 ANSI/CTA-2088-A
5.3 軟體安全	5.3.1 原始碼安全掃描	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引
	5.3.2 未公開揭露應用程式	TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引

安全構面	安全要求項目	引用標準
		ANSI/CTA-2088-A
	5.3.3 軟體更新安全	ANSI/CTA-2088-A NIST SP 800-53 ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引
	5.3.4 取得行動應用 App 基本資安標章	行動應用資安聯盟 行動應用 App 基本資安規範 V1.4
	5.3.5 惡意程式	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements NIST SP 800-53 TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引
	5.3.6 弱點掃描	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements NIST SP 800-53 TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引
5.4 通訊安全	5.4.1 無線通訊安全	U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS) U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) ANSI/CTA-2088-A TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引
	5.4.2 無線通訊失效處理能力	U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS) U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS) ANSI/CTA-2088-A
5.5 韌體安全	5.5.1 韌體已知漏洞檢測	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
	5.5.2 韌體更新安全	ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

安全構面	安全要求項目	引用標準
		ANSI/CTA-2088-A NIST.SP.800-53r5
6.1 晶片安全	6.1.1 密碼模組旁道洩漏防護	ANSI/CTA-2088-A FIPS 140-3
	6.1.2 錯誤注入攻擊	FIPS 140-3
	6.1.3 AES 加密演算法	NIST SP 197、SP 800-38A FIPS 140-3
	6.1.4 RSA 2048 加密演算法	NIST PUB 180-4 FIPS 140-3
	6.1.5 確定性亂數產生器（DRBG）	NIST SP 800-90A FIPS 140-3
	6.1.6 非確定性亂數產生器（NRBG）	NIST SP 800-90B/C

附錄 C 原文縮寫對照

3GPP	Third Generation Partnership Project
AES	Advanced Encryption Standard
CBC	Cipher-block chaining
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DRBG	Deterministic Random Bit Generator
ECB	Electronic codebook
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
GCS	ground control station
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
JTAG	Joint Test Action Group
MAS	Mobile Application Basic Security
NIST	National Institute of Standards and Technology
NRBG	Non-deterministic Random Bit Generators
RSA	Rivest-Shamir-Adleman
SANS	SysAdmin, Audit, Network and Security
SigGen	Special Interest Group on Generation
SP	Special Publication
TCP	Transmission Control Protocol
UART	universal asynchronous receiver-transmitter
UAS	unmanned aerial system
UAV	unmanned aerial vehicle
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
UUT	unit under test
WPA2	Wi-Fi Protected Access 2

參考資料

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

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

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

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

[5] FIPS 140-3: “Security Requirements for Cryptographic Modules”.

[6] FAA 14 CFR Parts 89: “Remote Identification of Unmanned Aircraft”.

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

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

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

[10] IEC 62443-3-3 “System security requirements and security levels”.

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

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

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

[14] NIST SP 800-218 “Secure Software Development Framework (SSDF)”.

[15] NIST SP 800-53 “Security and Privacy Controls for Information Systems and Organizations”.

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

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

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

[19] NIST SP 800-90B “Recommendation for the Entropy Sources Used for Random Bit Generation”.

[20] NIST SP 800-90C “Recommendation for Random Bit 4 Generator (RBG) Constructions”.

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

[22] U.S. Department of Homeland Security CISA, Protecting against the threat of unmanned aircraft system (UAS)

[23] U.S. Department of Homeland Security CISA, Cybersecurity best practices for operating commercial unmanned aircraft systems(UASS)

[24] 台灣資通產業標準協會「TAICS TR-0022 v2.0:2023 物聯網場域資安防護評估指引」。

[25] 行動應用資安聯盟「行動應用 App 基本資安規範 V1.4」。