無人機在交通領域應用之資通安全議題初探

Preliminary discussion on Cybersecurity Issues of Unmanned Aircraft Systems in the Transportation Sector

運輸科技及資訊組 黃于哲 童志浩 吳東凌 張益城

研究期間：民國112年4月至113年11月

摘　要

無人機具有高機動性、高自動化、操作簡易等優勢，可搭載各類感測儀器，提供三維空間環境資訊，已被廣泛用於交通運輸領域之設施巡檢、空拍監測、安全管理及物流運送等項目，惟其優勢如遭有心人士利用，亦可能造成資通安全之隱患。有心人士可利用無人機漏洞竊取敏感資訊、挾持運用於非法或惡意用途，或以干擾欺騙等方式影響正常無人機運作，進而影響業務執行與公眾安全，因此有必要進行相關探討研究。本研究透過蒐集相關文獻，首先探討無人機之資通安全特性、弱點威脅樣態，接續研析交通領域應用案例之攻擊情境，並彙整風險緩解策略，做為無人機應用單位及後續研究參據。

關鍵詞：

無人機、資通安全、風險管理。

無人機在交通領域應用之資通安全議題初探

一、 研究背景

隨著無人機技術日益進步，無人機不再僅限於空拍等個人娛樂用途，已廣泛被用於民間及軍事的各個領域，而無人機日益增長的應用案例與使用環境亦代表其攻擊面（Attack surface）的擴大，攻擊面係指網路或系統可能被攻擊者利用滲入之進入點和漏洞[9]。無人機的軟硬體運作特性，使得有心人士可能利用漏洞進行獲得不法利益、竊取隱私資料或惡意破壞等行為，加以威脅形式與攻擊技術不斷發展，因此有必要探討無人機之資通安全風險，並導入風險管理策略，以下說明維護無人機資通安全之重要性。

（一）維護公眾安全：無人機可能在人口密集地區執行任務或與有人機共享空域，攻擊者可能蓄意造成無人機失控，或奪取控制權將無人機武器化(Weaponize)做為實體攻擊工具，危及地面與空中之人員及資產安全。

（二）保障隱私：無人機經常收集、傳輸敏感數據，例如影像、感測器數據與位置資訊，安全漏洞可能導致未經授權的存取、操縱甚至外洩，從而危及隱私並可能造成財產損失。

（三）維持業務運作：無人機用於空拍、基礎設施巡檢、包裹投遞等商業用途日趨普及與成熟，無人機之資通安全漏洞可能導致企業財務損失、敏感資訊外流或業務運作中斷。

（四）建立公眾信任：無人機為新興科技，加強無人機資通安全，有助於維護公眾對此類技術的信任，對推動無人機科技之發展相當重要。

二、 無人機系統概述

(一)無人機系統構造與元件

無人機系統(Unmanned Aerial System, UAS)，包括無人機載具、遙控設備、通訊及控制信號鏈路、酬載設備及地面站等組成可執行任務之完整系統，各項系統簡要說明如下。[8][11][13][16]

1. 無人機：包括機體本身、動力系統及飛控系統，無人機機體之構造可分為固定翼、多旋翼，以及結合兩者特性之垂直起降定翼型等，動力系統包括馬達、螺旋槳等相關組件。

2. 通訊鏈路：一般指無人機與地面站之雙向數據傳輸，包括通訊(Communication)、控制(Control)(簡稱C2 Link)鏈路，無人機並可透過下行鏈路傳輸機載數據(如:感測器數據、監控數據、影像等)至地面站。此外,在群飛(Swarm)等特殊任務則有無人機間通訊需求,如。商用無人機通常使用無線射頻(Radio Frequency, RF)、Wi-Fi、藍牙或行動通訊網路 (Cellular network)等通訊方式。

3. 感測器：無人機上通常具有多種感測器，為飛控系統提供位置、姿態及外界環境等資訊，包括衛星導航系統接收器(Global Navigation Satellite System, GNSS)(以下以GPS代稱)、慣性測量單元(Inertial Measurement Unit, IMU)、氣壓計等，部分無人機裝備有視覺鏡頭、紅外線、光達LiDAR等裝置。

4. 飛控系統:飛行控制系統(flight controller)包括飛控電腦及韌體,其功能為整合感測器資訊及任務電腦,協調飛行控制面、動力系統,控制飛行姿態及速度。

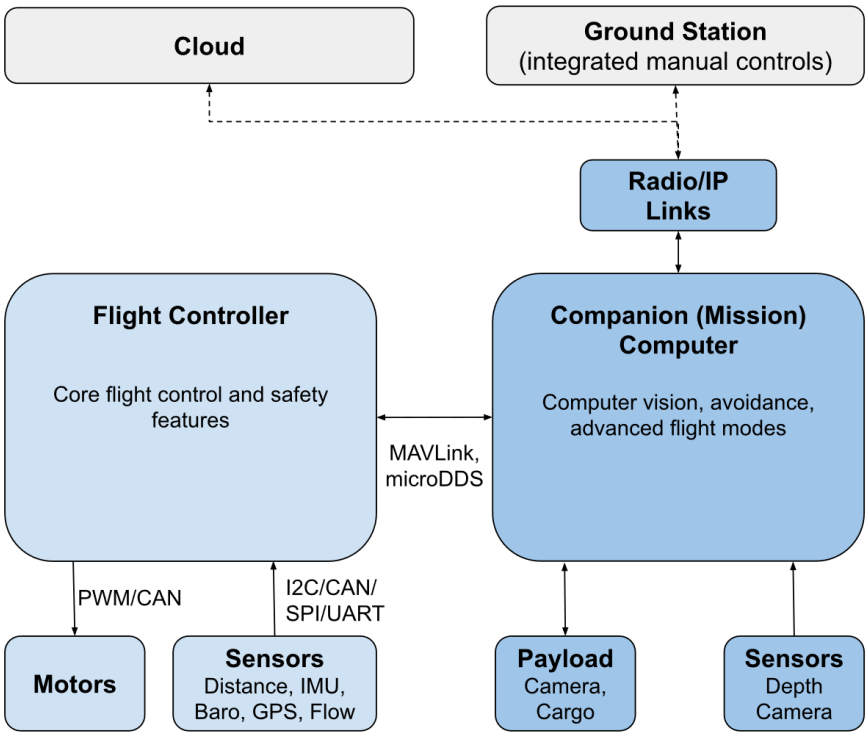
5. 任務電腦：機載任務電腦(mission computer)不直接操縱無人機飛行姿態及動力,其主要功能為提供機載運算能力,接收地面站指令,協助飛控系統執行飛行任務。

6. 酬載：無人機用於執行任務所需裝載之裝置，常見之酬載裝備包括

相機、科學儀器、遠端識別(ADS-B、Remote ID 等)、其他光電感測器以及用於運輸和釋放貨物之投遞機構。

除無人機本身與機載系統外，無人機系統尚包括地面控制站系統(Ground Control Station, GCS)部分，說明如下：

1. 遙控設備:提供地面人員監控或操控無人機之硬體設備,如遙控器、電腦及行動裝置等。
2. 應用軟體：無人機地面站應用軟體可安裝於筆記型電腦或行動裝置上，功能包括操作者與無人機互動、任務規劃、監控無人機狀態並存取數據，以及傳輸無人機資訊至伺服器或雲端。
3. 通訊與控制鏈路：地面站和無人機之間上下行通訊鏈路，以及地面站與伺服器或雲端之間通訊。
4. 伺服器及雲端:係指於異地儲存無人機本身及所蒐集相關資料之伺服器或雲端服務，如飛行紀錄、遙測及影像資料等。[8]



資料來源: [17]

圖一 飛控系統及任務電腦之架構示意圖

(二)無人機系統特性

以下說明無人機運作之資通訊特性，以及可能衍生之資安弱點：

1. 無線通訊：無人機主要依靠無線通訊技術進行命令與控制、數據傳輸以及與其他系統之互動，使其容易受到各種網路攻擊，包括干擾(Jamming)、欺騙(Spoofing)和攔截(Interception)。
2. 全球導航衛星系統:無人機依賴GPS等全球導航衛星系統進行導航，而商用無人機通常缺乏加密及驗證機制，使其易受干擾或欺騙攻擊的影響。
3. 資源限制：小型商用無人機受限於酬載重量及電源功耗，其機載運算能力有限，使其較不易實施強健之安全防護措施，且系統冗餘（Redundancy）程度較低，承受攻擊之韌性有限。[19]
4. 跨系統互動與整合:無人機之間、無人機與地面控制站、雲端平台，以及物聯網 （IoT） 中的其他設備，甚至其他空中無人機高度互動與整合，跨平台通訊安全與防護機制的複雜度更具有挑戰性。[11]
5. 作業環境與任務類型：無人機的作業環境多樣化且機動性高，跨越不同的位置、高度、地面障礙及空中避讓；此外，群飛(Swarm)及視距外飛行(Beyond Visual Line-of-Sight, BVLOS)等特殊任務型態，涉及無人機間通訊、長距離通訊等議題，亦可能增加資安風險。
6. 蒐集資料特性：無人機收集和傳輸敏感數據，如關鍵基礎設施、個人及資產之影像、感測數據和位置資訊，未經授權的存取、操縱，將可能導致重要資料外洩。
7. 開源軟硬體使用：自行組裝之無人機可能使用開源軟硬體，若未查證來源，並確認無安全性漏洞，可能形成資安威脅。

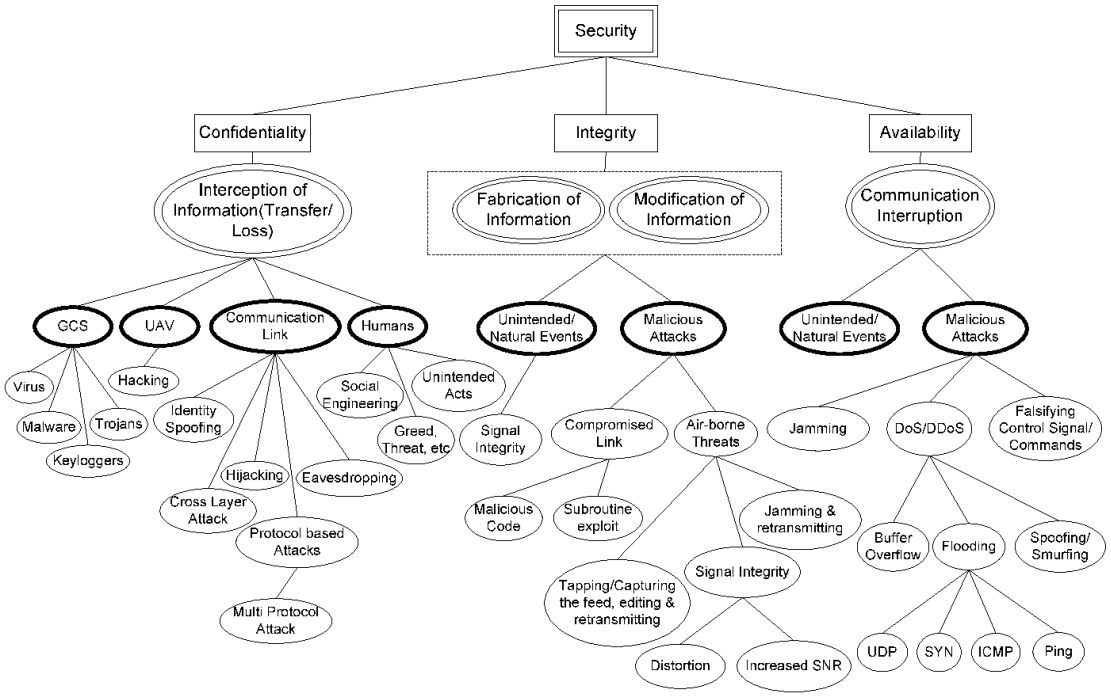
三、 無人機資通安全威脅情境

(一)資訊安全要素

C.I.A. 三要素在資訊安全領域分別代表機密性(Confidentiality)、完整性(Integrity)，以及可用性(Availability)，以下簡述三要素在無人機資通安全之意義。[13] [16][20]

1. 機密性：確保敏感資訊僅供授權人員或系統存取，保護數據免遭未經授權的存取、洩露或攔截。以無人機而言，確保敏感資訊（例如飛行計畫、感測器數據及蒐集影像）僅供授權的個人和實體存取，防止竊聽、數據洩露和未授權的存取企圖，以保護操作安全和隱私。
2. 完整性：防止資訊被不當修改或破壞，並確保資訊的不可否認性和真實性。在無人機資安方面，包括確保無人機飛控、感測器和通訊鏈路不被惡意者篡改，以防止劫持、竄改數據、變更飛行路徑或系統配置等潛在危險。
3. 可用性：確保及時且可靠的資訊存取和使用。確保無人機系統及其數據在需要時可供授權用戶存取，並防範阻斷服務攻擊(Denial-of-Service Attack, DoS attack)、通訊干擾及其他可能妨礙任務執行之攻擊。

在前述三項要素之外，可驗證性 (Authenticity)，指可辨別使用者身分、可歸責性(Accountability)，指使用者之行為可被追溯，以及不可否認性(Non-repudiation)，指使用者無法否認其行為，亦被列為重要原則;前述原則在執行面有對應之3A框架，亦即驗證(Authentication)、授權(Authorization)及記錄(Accounting)。



資料來源: [12]

圖二 應用 CIA 要素建立無人機資安風險模型

(二)STRIDE 威脅建模

STRIDE 是由微軟公司所提出，用於評估軟體開發生命週期之資安風險分類，將資安威脅分為六大類，其各字首所代表之資安威脅包括：欺騙(Spoofing)、竄改 (Tampering)、否認 (Repudiation)、資訊洩漏(Information disclosure)、阻斷服務 (Denial of Service)與權限提升 (Elevation of Privilege)。相關文獻運用 STRIDE 模型於分類無人機資安威脅樣態。[16][18][19][20][22]

1. 欺騙(Spoofing)：欺騙係指冒充身分或訊息，以獲得未經授權的存取權限或操縱系統。攻擊者可以假冒 GPS 訊號欺騙無人機，使其偏離預定航線甚至墜毀 。亦可能欺騙合法的通訊通道，向無人機發送虛假指令，遂行挾持等惡意行為。此類攻擊損害了 C.I.A.中的「機密性」原則。

2. 竄改 (Tampering)：篡改係指惡意修改數據或系統組件，藉以擾亂無人機操作。攻擊者可以篡改無人機感測器數據或狀態資訊，向控制系統或地面站提供錯誤資訊，或試圖修改無人機的韌體或軟體，

從而取得無人機控制權或導致故障。此類攻擊違背前述三要素之「完整性」及「可驗證性」。

3. 否認 (Repudiation)：否認係指使用者，包括惡意行為者，有能力否認其操作行為，例如無人機被劫持的情況下，攻擊者可以刪除或修改系統日誌以掩蓋其蹤跡，使攻擊行為難以證明與追蹤。此類攻擊有損前述之「完整性」及「不可否認性」。

4. 資訊洩漏 (Information disclosure)：資訊洩露指的是未經授權存取敏感數據，導致機敏資料及隱私洩露。例如攻擊者可以攔截無人機及其地面站之間未加密的通訊通道，監控無人機作業，並存取影片資訊、感測器讀數甚至控制指令。此類攻擊將損害無人機系統之「機密性」。

5. 阻斷服務 (Denial of Service, DoS)：DoS 目的係破壞系統或服務的可用性，妨礙或阻止合法的存取與操作。攻擊者可以干擾無人機使用的通訊頻率，中斷其與地面站的連接，導致其墜毀，或對地面站發動 DoS 攻擊，擾亂其控制或監視無人機能力。

6. 權限提升 (Elevation of Privilege)：提升權限係指攻擊者利用漏洞在系統中獲得比其授權更高的存取級別。攻擊者可以利用無人機軟體或韌體中的漏洞獲得對系統的超級使用者(Superuser)存取權限，使其獲得完全控制、存取或修改無人機系統之能力，攻擊違背系統的授權原則。

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

資料來源: [20]

圖三 STRIDE 威脅模型對應資安原則

Trend	Key UAS Feature	STRIDE Taxonomy Threat	Vulnerabilities and Attack Vectors
Simplified Control and Operation	Camera view-based flight; following target on camera	Repudiation and Information Disclosure	Third-party monitoring of user activities
	Gesture and speech-directed flight control	Elevation of Privilege and Tampering	Alteration of factory- installed configurations
Self-Operation and Vigilance	Location or sensor-based payload manipulation (e.g., crop spraying, medical supply delivery)	Elevation of Privilege	Intercept of payload usage or delivery
	Swarm drone maneuvers; multi-UAS operations	Elevation of Privilege and Tampering	Scaled-propagation of operational errors
	Preplanned hovering; patrol routines	Spoofing or Tampering	Override of authentic GPS signal or uploaded navigation files
Self-Maintenance and Protection	High-speed obstacle avoidance	Spoofing and Denial of Service	Sensor saturation or interference for obstruction of "view"
	Auto-docking; recharge; return to home	Repudiation and Information Disclosure or Spoofing and denial of service	Third-party monitoring of user activities and sensor interference for failure to register "home" state

資料來源: [18][22]

圖四 以 STRIDE 模型分析無人機之功能特性及資安威脅

(三)無人機資安攻擊樣態

以下主要摘錄由美國大學院校組成之 ASSURE 無人機研究聯盟所彙整無人機資安攻擊樣態，分為硬體、軟體、地面站、通訊鏈路及伺服器與雲端服務等五個面向。[8]

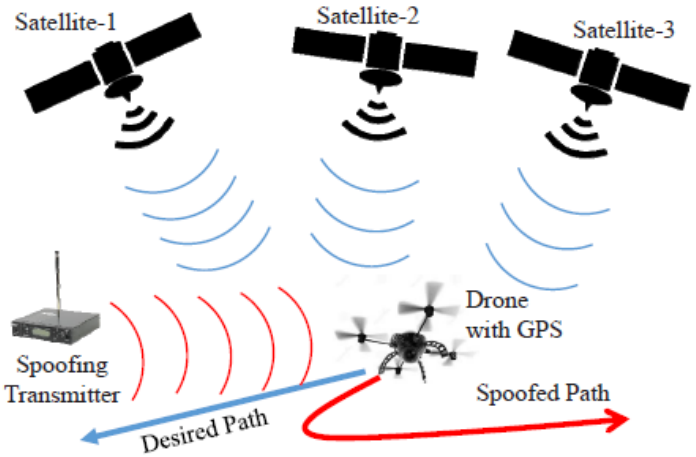
1. 硬體攻擊樣態

(1) 干擾(Jamming)：攻擊者將添加大量雜訊到無線電信號、聲音等傳播介質，使對應之機載接收或感測器可能無法區分正確信號和雜訊，導致無人機系統無法正常運作，達成阻斷服務(DoS)之攻擊目的。

(2) 欺騙(Spoofing)：欺騙攻擊係偽造相關訊號，使無人機對應之接收器依循假造訊號，從而誤判資訊，例如偽造 GPS 訊號，或以攔截與再傳播(Meaconing)方式，攔截正確 GPS 訊號後延遲送出，使無人機或地面站誤判位置、速率及時間。

(3) 韌體刷寫(Firmware Flashing)：攻擊者將無人機相關韌體替換為惡意版本，此類攻擊亦可能以遠端非實體方式遂行。

(4) 供應鏈攻擊(Supply chain attack)：此類攻擊者係指介入製造過程，蓄意提供具有缺陷之零件。



資料來源:[23]。

圖五 GPS 欺騙攻擊示意圖

表一 無人機硬體資安威脅

攻擊方式	攻擊面	敘述
干擾	GPS	傳輸雜訊淹沒正確訊號，阻礙 GPS 接收器運作。
	ADS-B/Remote-ID	以雜訊干擾機載位置回報裝置之接受或廣播功能。
	機載感測器	傳輸雜訊干擾機載感測裝置之量測訊號，使無人機無法獲得所處環境資訊。
	驅動裝置	以雜訊阻礙飛控系統與飛機控制面、馬達等驅動裝置之通訊。
欺騙	GPS	偽造並傳輸虛假的 GPS 訊號，以欺騙目標 GPS 接收機。
	ADS-B/Remote-ID	偽造位置回報裝置之無人機狀態訊息並廣播。
	機載感測器	偽造並傳輸虛假訊號或數據，覆蓋正確資料，以欺騙目標感測器。
	致動器	偽造無人機飛控系統指令，欺騙飛機控制面、馬達等實體動作機件。

韌體刷寫	韌體	以實體方式刷寫韌體，替換為經修改之惡意版本。
供應鏈攻擊	硬體組件	於供應鏈生產階段變造硬體組件。

資料來源:[8]、本研究整理。

2. 軟體攻擊樣態

(1) 注入攻擊(Injection):攻擊者輸入惡意程式碼或指令繞過系統限制或取得權限以進行惡意行為，或在資料庫中置入錯誤或偽裝的數據，在讀取和執行時觸發惡意行為。

(2) 緩衝區溢位(Buffer overflow):攻擊者惡意輸入超過實體記憶體之緩衝區容量之內容，使其溢位，覆蓋原有指令，並替換為攻擊者之指令，遂行惡意行為。

(3) 惡意程式(Malware):係指攻擊者以實體方式(如隨身碟)或無線網路連線等方式，於應用程式置入惡意程式，其目的可包括主動引起系統故障，或被動擴大感染及竊取資料。

(4) 韌體修改(Firmware modification):前述韌體刷寫，係以實體方式置換韌體內容；如使用者下載未驗證之更新檔案，並檢查檔案完整性，攻擊者亦可能透過網路更新方式，將變造之韌體版本置入無人機。

(5) 電池耗盡(Battery draining):此類攻擊係指攻擊者利用獲得之系統權限，執行大量耗費資源之工作程序或防止系統進入節能狀態，使電池耗盡。

(6) 供應鏈攻擊：攻擊者或惡意供應商透過介入供應鏈方式，在應用程式或韌體中置入後門、蠕蟲等惡意軟體。

表二 無人機軟體資安威脅

攻擊方式	攻擊面	敘述
注入攻擊	程式碼注入	輸入惡意的額外指令。
	資料庫注入	利用資料庫漏洞置入錯誤資料。
緩衝區溢位	作業系統、應用程式及韌體	覆寫應用程式記憶體，改變程式執行路徑。
惡意程式		利用系統漏洞感染惡意程式。
韌體修改	韌體	取得官方韌體更新的版本，進行分析、反組譯，並破解系統更新驗證機制。
電池耗盡	作業系統、應用程式及韌體	執行耗費系統資源之工作程序或使系統永不進入休眠狀態，使電池耗盡。
供應鏈攻擊		滲透應用程式或韌體供應鏈，植入惡意程式碼或漏洞。

資料來源: [8]、本研究整理。

3. 無人機地面控制站資安威脅

(1) 系統漏洞：攻擊者可能利用地面控制站之系統漏洞，提升權限，遂行惡意行為，包括阻礙作業執行、竊取資料等。文獻並指出，以手機為介面之地面操作平台可能帶來更高的資安風險，因新攻擊型態與修補更新之循環更加快速，使用者需即時執行安全性更新。[8]

(2) 人為因素：人為因素為無人機資安攻擊之重要面向，若無人機相關工作人員，如操作人員(飛手)、維修人員缺乏資安意識，可能成為攻擊者利用之弱點，在蓄意或非蓄意情況下損害系統安全，攻擊類型包括社交工程攻擊、竊取或破解密碼、植入惡意軟體等。[8][13][19]

表三 無人機地面控制站資安威脅

攻擊方式	攻擊面	敘述
遠端存取	地面站軟硬體/相關工作人員	將惡意軟體植入地面站，獲得遠端存取權限。
強制退出工作程序		造成地面站系統崩潰、破壞地面站與無人機連結。
資料外流		竊取地面站儲存之無人機系統及所蒐集資料。
密碼破解		破解系統帳號存取密碼。
逆向工程		對地面站應用程式進行逆向工程，尋找系統漏洞及敏感資訊。
社交工程		以詐騙、釣魚等方式誘使相關人員外流資料或取得系統權限。

資料來源: [8]、本研究整理。

4. 無人機通訊鏈路資安威脅

無人機作業仰賴無線通訊鏈路進行無人機之間，以及無人機與地面站之間上下行命令與控制以及資料傳輸。因此，無線通訊鏈路遭攻擊可能造成無人機失控、挾持，以及資料外流。以下彙整文獻中所提攻擊方式，因攻擊方式中文翻譯各有異同，表四列出文獻中所載原文，以便理解。[8]

(1) 路由攻擊(Routing)

攻擊者在放置一個或多個惡意節點，並偽裝成合法節點，以阻礙訊息正確傳遞，丟棄、延遲或重新導向封包，遂行阻斷或延遲服務等惡意行為。

(2) 干擾攻擊(Jamming)

干擾攻擊分為兩類，攻擊者可針對無線電頻率發送雜訊進

行干擾，或針對系統發送大量惡意訊息或請求(洪水攻擊，Flood attack)，使系統無法處理正確訊息，達成阻斷服務之目的。

(3) 解除認證攻擊 (De-authentication)

攻擊者可能利用未加密之地面站與無人機通訊，發送偽造訊息解除合法地面站認證，進而與無人機建立連線。

(4) 竊聽攻擊 (Eavesdropping)

攻擊者可監聽並記錄通訊內容，並運用分析通訊模式，取得或推斷加密之訊息。攻擊者並可利用擷取之訊息進行重送或轉送(重放攻擊或中繼攻擊)。

(5) 修改和偽造攻擊 (Modification and fabrication:)

攻擊者介入通訊者之間，誤導使用者正在進行合法通訊，藉以攔截、中繼、竊取並變造訊息，遂行惡意目的。

(6) 偽裝攻擊

攻擊者偽裝為合法節點或使用者，以建立連結，取得系統控制權或竊取資訊。

(7) 模糊測試

模糊測試攻擊之目的為尋找系統漏洞，攻擊者傳送大量隨機、無特定模式之訊息或語法，以測試系統之反應，前述訊息並可透過生成式人工智慧自動化生成[14]。模糊測試亦可做為資安防護手段，以發現系統缺陷，進行修復。

表四 無人機通訊鏈路資安威脅

攻擊方式	分類	敘述
黑洞/灰洞攻擊(Black Hole/Gray Hole)	路由攻擊	黑洞攻擊係指於網路中丟棄所有封包，灰洞攻擊則選擇性丟棄封包，藉以達成阻斷服務之目的。
蟲洞攻擊 (Wormhole)	路由攻擊	在兩個以上惡意或遭滲透節點之間建立隧道，直接轉送封包，以進行惡意行為。
女巫攻擊 (Sybil)	路由攻擊	攻擊者在網路中建立多個虛假使用者或節點，以取得控制權或擾亂系統。
沉洞攻擊 (Sinkhole)	路由攻擊	攻擊者利用惡意節點假冒為最佳路徑，吸引流量，進而遂行丟棄、延遲封包等惡意行為。
無線電頻率干擾(Radio Frequency (RF)-based Jamming)	干擾攻擊	針對無線電訊號進行實體干擾，需要靠近節點，使用足夠強的信號進行干擾。
通訊協定干擾 (Protocol-based Jamming (Message Flooding))	干擾攻擊	利用大量訊息淹沒網路，達成阻斷服務之目的。
解除認證(De-authentication)	解除認證攻擊	解除地面控制站之合法認證，切斷無人機與地面站間鏈接。
密碼破解(Password Breaking)	修改和偽造攻擊	竊取、推測、破解系統密碼。
中間人攻擊(Person-In-The-Middle)(Man-In-The-Middle)	修改和偽造攻擊	攻擊者於介入兩個端點間建立通訊，以進行竊聽、變造訊息等惡意行為。
指令注入(Command	修改和偽造	輸入惡意指令，遂行惡意行為。

Injection)	攻擊	
封包分析 (Packet Sniffing/Analysis)	竊聽攻擊	竊聽網路通訊，分析模式以判斷安全資訊。亦可做為資安防護手段。
重送攻擊 (Replay Attack)	竊聽攻擊	攻擊者觀察並記錄通訊內容，稍後重播以欺騙或遲延系統。
中繼攻擊(Relay Attack)	竊聽攻擊	攔截通訊內容，並轉送至一定距離外，遂行竊取資訊、存取系統權限等之目的。
偽裝 (Masquerading)	偽裝攻擊	偽裝為合法節點或使用者。
模糊測試 (Fuzzing)	模糊測試攻擊	攻擊者向目標傳送大量隨機、異常且不可預期之訊息，藉以尋找系統漏洞。

資料來源: [8]、本研究整理。

5. 伺服器及雲端資安威脅

無人機可能將飛行資訊,包括操作者資訊、飛行狀態、任務內容,以及所蒐集之影像、照片及感測數據儲存於伺服器及雲端空間,因此有必要探討其威脅樣態。

表五 無人機伺服器及雲端資安威脅

攻擊方式	攻擊面	敘述
資料外洩	伺服器及雲端	攻擊者竊取數據及敏感資訊。
操作者資訊外洩	伺服器及雲端	攻擊者竊取無人機操作者及所有者身分。
地點外洩	伺服器及雲端	攻擊者取得無人機及地面站位置資訊。

資料來源: [8]、本研究整理。

(四)無人機於交通領域應用之資安攻擊情境

1. 無人機作業階段

前一章節主要說明無人機軟硬體元件可能遭受之攻擊類型，本章節以無人機作業情境為主軸，說明執行任務過程可能遭受之資安威脅與情境，表六列出文獻所彙整無人機各階段工作內容。

表六 無人機作業階段及工作內容

無人機作業階段		敘述
任務規劃	飛行計畫	規劃航線、取得作業許可。
	設定自動飛行航線	建立地面站與無人機連線。
飛行前準備/系統檢查	地面控制站	完成飛航報告
	飛控系統	提供無人機手動操作或自動飛行能力
	資料鏈結	建立地面站與無人機連線。
	GPS	檢測 GPS 接收器。
	感測器	檢查感測器功能。
	動力源(電池/燃油)	確認動力源足夠並正確安裝。
起飛	系統檢查	確認無人機系統運作正常。
	高度確認	確認高度。
	飛行階段	無人機升空。
	手動控制起飛	起飛階段由操作員手動控制。
	自動飛行	無人機依設定航線自動飛行。
任務執行	飛行資料傳輸	飛行資訊傳輸。
	酬載影像傳輸	傳輸酬載影像裝置之數據。
	酬載感測資料傳輸	傳輸酬載感測裝置之數據。
降落	手動降落	操作員手動降落。
	自動降落	依設定航線自動降落。
飛行後作	地面控制站	完成飛航報告: 包括飛航時間、軌

業		跡、高度、任務概況及通訊頻率等。
	資料下載	自無人機下載資料。
其他	緊急程序	無人機緊急處理程序。

資料來源:[8]。

2. 無人機作業條件

(1) 操作方式:可分為手動控制及自動飛行兩類，手動控制由操作人員(飛手)，以遙控裝置於視距內或遙控範圍內透過機載感測裝置操控無人機。自動飛行係指由地面站預先設定飛行任務，包括航線、高度等，由無人機依據飛行計畫自動執行。無人機可自動完成起降、巡航、任務航線等階段，惟實務作業方面，如在天候不佳、地形限制或通訊條件不佳等特殊情境下，起降階段可由操作人員手動執行，巡航階段再交由無人機自動執行。

(2) 作業距離:視距內作業係指操作人員可目視無人機，並可透過設置目視觀察員方式，延伸視距範圍；視距外作業係指無人機已超出操作人員目視範圍之作業。視距外作業因操作人員無法直接獲得無人機環境狀態及飛行姿態，較難手動介入操作，故更為仰賴無線通訊、感測裝置及飛控電腦等計算單元之可靠度，作業風險亦較高。

(3) 作業環境:作業環境為評估無人機作業風險之重要因素，包括地面建築物、障礙物、活動人口、敏感設施，以及空域中航空器、其他無人機作業情況、是否鄰近航空站或飛行場等。

(4) 任務內容:可包括設施巡檢、監視、影像蒐集及投擲或噴灑物品等任務類型。

(5) 群飛作業:群飛作業常用於表演或軍事用途，因其仰賴多架無人機在同一空域中互相通訊、協調完成任務，其作業風險亦較高。

3. 無人機於交通領域應用案例及威脅情境

本章節聚焦無人機在交通領域之應用案例，以交通部運輸研究

所刻正推動之無人機於交通領域應用相關研究，包括港區設施巡檢、交通監測、橋梁巡檢及物流運送等 4 個應用項目為情境，分析各項作業之資安威脅情境。

(1) 港區設施巡檢:港區為交通領域重要基礎設施，因港區幅員廣大，岸上設施、設備種類眾多，作業人員及車輛密集，無人機可有效提升港區設施與安全管理效率。無人機港區巡檢係利用光學、熱像及光達等酬載設備，蒐集感測資訊，於後端運用人工智慧影像辨識等技術進行自動化巡檢管理。因港區面積可達數千公頃，且需進行多時期同物件影像之比較分析，故以自動化飛行為主，作業範圍可達視距外。此類應用案例之資安威脅情境包括惡意者透過干擾或挾持等手段使無人機墜毀於港區內，造成人員財產損失，或於傳輸及後端作業過程竊取機敏資料。

資料來源:[3]。

圖六 無人機港區設施巡檢案例

(2) 交通監測:無人機可於空中大範圍蒐集交通資訊，具有取代或輔助路側攝影機或車輛偵測器等設備進行交通監測之潛力。目前交通監測之應用案例包括高、快速道路車流監測及分析；以及於市區道路蒐集影像資料，於後端進行分析交通衝突等事件。由於此類應用案例於人車密集地區作業，須注意之資安威脅包括無人機遭干擾失控對地面人員及車輛造成損害，以及後端作業資料遭竊取等。

資料來源:[2]。

圖七 無人機港區設施巡檢案例

(3) 橋梁巡檢:傳統橋樑檢測工作以人力及目視檢查為主,應用無人機蒐集影像資料,並結合人工智慧影像辨識技術,可有效提升檢查效能。橋梁巡檢作業因需於近距離蒐集橋梁構造影像資料,以手動飛行對操作人員較具挑戰性且作業風險較高,又因橋梁遮蔽導致 GPS 訊號不佳,故需輔以超寬頻(Ultra-wide Band,UWB)、視覺感測器等定位方式,以進行自動飛行[5],此類感測器融合(Sensor Fusion)作法,可增加無人機定位之考靠度及冗餘,惟可能遭受攻擊之層面亦相對增加。可能之資安風險包括定位干擾或欺騙阻礙任務執行、失控造成橋梁構造及人車損害,而此類應用案例需大量後端分析作業,亦需留意資料外流風險。

資料來源:[5]。

圖八 無人機橋梁巡檢案例

(4) 物流運送:運用無人機酬載貨物進行商品、醫療器材運送，以及緊急災害運補等情境，被視為無人機現階段最具突破性應用之依，目前國內外已有多項先導測試案例。[4]我國之潛在應用場域，則以偏遠或交通不便之山區、離島為主，涉及視距外飛行作業、長距離通訊以及自動飛行，同時需考量山區地形遮蔽通訊，以及氣候變化等因素，加以物流無人機之尺寸及重量較大，需接近地面投擲或降落，如失控對地面損害程度較高，故此類案例屬於較高風險之作業型態。無人機物流因屬視距外作業，無人機採長距離自動飛行，惡意干擾可能使地面站失去與無人機鏈結，甚或遭欺騙或挾持降落偏離航線以盜取貨物。此外，為使地面人員掌握無人機資訊，無人機如裝有廣播式或網路式遠端識別裝置(Remote ID)，亦可能成為潛在攻擊面，惡意者可能攔截、變造或干擾裝置傳輸訊息，阻礙地面人員了解無人機相關飛行資訊。另國際間有案例採多架物流無人機於同一空域作業，涉及無人機間通訊，以及無人機飛航管理系統(UAS Traffic Management，UTM)等議題。

資料來源:[4]。

圖九 無人機物流運送案例

表七 無人機於交通領域應用案例之資安威脅情境

應用案例	作業條件	作業敘述	威脅情境
港區設施巡檢	1. 自動飛行為主 2. 視距內及視距外作業 3. 地面設備、作業船舶、人員及車輛密集 4. 單機作業為主	運用無人機酬載設備蒐集港區資訊，進行分析，輔助管理維護。	失控造成地面損害、挾持進行惡行為、竊取資料。
車流監測	1. 自動飛行為主 2. 視距內及視距外 3. 接近地面車輛或市區人車密集地區 4. 單機作業為主	運用無人機酬載設備監測車流、路徑及交通事件，並就所蒐集資料進行分析。	失控造成地面損害、挾持進行惡行為、竊取資料。
橋梁巡檢	1. 自動飛行為主 2. 視距內作業 3. 接近橋梁構造物 4. 融合多種感測裝置 5. 單機作業	運用酬載影像設備監測車流、路徑及交通事件，並就所蒐集資料進行分析。	定位干擾及欺騙影響作業、失控造成橋梁構造及地面損害、竊取資料。
物流運送	1. 自動飛行為主，部分手動 2. 常見視距外作業 3. 投遞或卸貨時地面風險較高。 4. 可能多機作業	無人機裝載貨品，飛行至目的地進行投擲或降落裝卸貨作業。	定位干擾及欺騙影響作業、失控造成地面損害、挾持盜取貨物。

資料來源:本研究整理。

四、 無人機資通安全風險緩解策略

(一)風險緩解技術發展趨勢

以下摘錄 ASSURE 研究聯盟彙整相關文獻就無人機軟硬體各層面提出風險緩解之技術與策略發展趨勢。[8]

1. 硬體風險緩解

(1) 入侵偵測系統(Intrusion Detection System, IDS):運用機器學習技術監測無人機硬體組件(如感測器與致動器)運作狀態,偵測系統異常行為,以防範攻擊行動。

(2) 飛控系統:偵測飛控系統異常行為、冗餘系統,以及防範入侵之韌體演算法等。

(3) 感測器融合:無人機裝載整合多個感測器數據,交叉驗證數據,以偵測針對單一感測器的攻擊,並避免感測器遭受攻擊使系統失效。

(4) 硬體檢驗:使用遠端驗證等技術檢查硬體配置,偵測未經授權的修改。

(5) 硬體設計:在硬體設計階段考慮安全需求,採用預防攻擊之安全設計方法,以及防範逆向工程的技術。

2. 軟體風險緩解

(1) 入侵偵測系統:軟體入侵偵測系統與硬體類似,但以偵測惡意程式、控制流程劫持等軟體層級攻擊為主。

(2) 遠端驗證:以遠端方式驗證無人機的軟體配置,確保未被惡意修改。

(3) 軟體隔離:將遭受入侵之軟體與無人機關鍵系統元件隔離,減少攻擊影響。

(4) 軟體設計: 於軟體開發過程中導入防止入侵之安全程式碼撰寫(Secure coding)原則,並進行弱點掃描、模糊測試,以發現漏洞。

3. 地面控制站風險緩解

(1) 軟體保護措施： 採用防火牆、入侵防禦系統和安全程式碼撰寫等措施，防止攻擊者進行逆向工程或利用漏洞，增強系統安全。

(2) 身份驗證與授權：使用強化的驗證機制（如多因子認證，Multi-factor Authentication)，確保僅有授權用戶可存取地面站。

4. 通訊鏈路風險緩解

(1) 入侵偵測系統：監控網路流量，偵測可疑活動及潛在攻擊。

(2) 加密與驗證通訊：加密網路流量以保護數據機密性與完整性，同時透過驗證確認通訊雙方身份。

(3) 安全路由協定：保護路由協定，防止操縱資料路徑的攻擊(如蟲洞攻擊、黑洞攻擊和女巫攻擊等)，維持網路可用性。

(4) 區塊鏈技術：利用區塊鏈不可篡改的特性，應用於無人機通訊鏈路之安全數據儲存與通訊加密。

(5) 信任模型：建立無人機網路行為之信任模型(Trust Model)，以評估網路節點狀態，識別入侵行為並隔離惡意節點。

(6) 網路服務設定：安全配置網路服務，包括強密碼、停用非必要服務及保持軟體更新。

5. 伺服器及雲端風險緩解

(1) 加密數據：在數據上傳或儲存至伺服器及雲端服務之前進行加密，確保機密性。

(2) 身份驗證與授權： 建立驗證與授權機制，防止未授權用戶存取資料。

6. 參考相關標準

參考相關標準及指引，例如美國商務部國家標準技術研究院（National Institute of Standards and Technology，NIST)、美國國家標準協會(American National Standards Institute，ANSI)資通

安全相關標準，以及美國網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency，CISA)相關指引。

(二)CISA 商用無人機系統資通安全作業指引

前述緩解策略主要針對技術層面，在無人機實務作業方面，以下摘錄美國網路安全暨基礎設施安全局(CISA)提出之「商用無人機系統資通安全作業指引(Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems)」，提供無人機使用單位做為參據，以降低可能衍生之資安風險。[10]

1. 軟體和韌體安全指引

本項指引係無人機軟體及韌體於安裝及使用過程之注意事項，以降低資安風險。

(1) 確認下載及安裝無人機軟體及韌體之裝置與企業內網隔離，並加強前述裝置，如筆記型電腦、智慧型手機之安全管理。

(2) 僅從可信賴的、經過驗證的無人機製造商或第三方網站、應用程式商店下載軟體。

(3) 確認下載檔案之完整性，未經過竄改，例如核對下載檔案之雜湊值(Hash value)或校驗碼(checksum)是否與來源一致。

(4) 使用更新至最新版本之防毒軟體掃描所有下載的檔案，並確保在整個安裝過程中保持防毒軟體啟用。

(5) 確認電腦或行動裝置上的防火牆已啟用，以檢查最近安裝的軟體可能導致的潛在惡意流量；並注意應用程式安裝過程所需外部網路連接可能潛藏的風險。

(6) 避免於安裝過程中使用系統預設值，並關閉自動更新，仔細研讀使用條款，並於必要時徵詢法務單位意見，避免於不知情狀況下授權應用程式進行不安全行為或資料外流。

2. 無人機操作安全指引

本項指引係避免無人機於操作過程中與地面通訊遭攔截，或遭惡意挾持之風險。

(1) 使用 WPA2-AES 或更高標準之加密技術保護無人機與遙控器之間的 Wi-Fi 連線。

(2) 避免（Service Set Identifier, SSID）名稱洩漏無人機資訊；關閉廣播 SSID；變更加密金鑰時應於安全地點進行，避免實體或網路之窺探或竊聽。

(3) 啟用傳輸層安全協定(Transport Layer Security, TLS)。

(4) 使用不同金鑰加密無人機控制、遙測、酬載、影像及音訊等各種傳輸鏈結，並確認無人機可加密其內部儲存的資料。

(5) 與無人機操作相關之行動裝置應使用獨立、無外部連線之裝置，或於操作期間關閉所有外部網際網路連線。並評估於操作期間進行無線網路流量分析，以了解和監控無人機通訊流量。

(6) 在安全的虛擬環境中執行行動應用程式。

3. 資料儲存與傳輸安全指引

本項指引係確保無人機數據在儲存或傳輸過程中之安全性與隱私性。

(1) 使用非聯網設備連接無人機或可移除儲存裝置。

(2) 確認連接無人機或可移除儲存裝置之電腦或行動裝置上的防火牆已啟用，並確保電腦已安裝最新的防毒軟體。

(3) 資料於儲存及傳輸過程中均應進行加密。

(4) 對於存取私密或機密資料的無人機，應實施適當的認證機制，並建議採用多因子驗證機制。

(5) 訂定並遵循靜止資料(Data at Rest)、傳輸中資料(Data in Transit)之資料管理政策。

(6) 每次使用後，應刪除無人機及可移除儲存裝置中所有數據。

4. 資訊分享及弱點通報

本項指引係鼓勵無人機使用單位參與資訊分享與漏洞通報相關計畫，以獲得即時資訊，並分享可能資安漏洞。

(1) 參與相關資訊分享計畫,與主管機關及相關公協學會組織交流,以即時獲知最新資安威脅，實施適當安全措施。

(2) 如發現無人機軟硬體漏洞,或發生無人機資安事件,應通報主管機關或相關組織。

(三)其他風險緩解措施

1. 實體安全措施:避免無人機系統遭破壞或竊取，使其功能失效、取得敏感資料或用於惡意用途，應加強無人機設備之實體安全，包括實體儲放空間之安全措施，並加強使用者管理及紀錄，避免未授權人士存取無人機系統。[19]

2. 人員資通安全意識:避免因人員有意或無意之疏失造成損害，應加強教育訓練,包括無人機操作者、維護人員、保管及經手資料之相關人員，並落實密碼管理、防範社交工程等措施。[19]

3. 供應鏈安全:使用單位應充分了解無人機系統之來源,以及原廠揭露資訊中涉及資安之說明及使用條款，並僅向可信任廠商或第三方購買或取得相關軟硬體。[16]

4. 新興科技:文獻指出，5G 行動通訊網路相較 4G/LTE 技術，具有更強的資訊安全防護能力，適合用於無人機命令控制及資料傳輸[18][22]。此外,區塊鏈(Blockchain)去中心化、分散式總帳及共識機制，使得資料難以竄改或刪除，目前已有相關研究將區塊鏈技術導入無人機之通訊加密及資料管理。[8][18]

5G Security Aspect	UAS Component Benefiting
Subscriber identifier privacy (Subscription Concealed Identifier (SUCI))	UA and GCS cellular identifier protection
Updated key establishment procedures (Authentication and Key Agreement (AKA))	Strong authentication of UA and GCS to the network
Data integrity and confidentiality protection over the air interface	Security of the traffic exchanged between the UA and the radio and core network, and the GCS and the radio and core network
Increased home network control	Security of roaming UAs
Detection of false base stations	Security of the UA attaching to the network
Secondary and additional authentication to third-party providers	Authentication/authorization of UA to the UTM
Use of millimeter wave radio	UA communication jamming resistance (closer proximity is required)

資料來源:[22]

圖十 5G 科技於提升無人機資安之效益

五、 結論與建議

本研究已初步探討無人機之系統架構與特性，資通安全威脅類型與交通領域應用案例之風險情境，並彙整常見之風險緩解措施，以下綜整提出本研究結論，以及針對加強無人機資通安全之建議與後續討論事項。

(一)結論

1. 無人機系統之特性提升資安風險：無人機系統安全涉及硬體、軟體、通訊鏈路和操作人員等多個層面，加上系統資源及作業環境特性，增加了資通安全之脆弱性，任何一個漏洞遭利用都可能危及整個系統。

2. 低成本商用無人機之普及與隱憂：商用無人機系統具有成本低、易操作等好處，若缺乏強健的安全機制與軟硬體資源，容易成為惡意行為者的理想目標。

3. 攻擊情境與方法日益複雜：針對無人機系統的攻擊情境與方法日趨多樣化，攻擊者利用人工智慧等新興技術不斷演變策略，使得惡意行為更加難以防範及察覺。

4. 無人機應用之機會與風險：隨著無人機應用日趨廣泛，被應用在高價值或高機敏性之基礎設施或人口密集地區，而在設施巡檢、災害防救等情境，其遭受攻擊的動機提升，其後果嚴重性亦隨之增加。

(二)建議

1. 健全無人機資通安全防護機制：在無人機運作的每一個環節上都需具備完善安全措施，無人機系統自硬軟體採購、安裝設定、現場作業、內業分析及更新維護之生命週期，均應導入資安防護作為。

2. 導入資安意識於作業流程：除軟硬體安全防護機制，人為因素亦扮演重要角色，因此，應建構軟硬體、作業程序、實體安全、人員訓練之多層資通安全管理措施，並針對類各類型作業可能產生之資安

風險類型進行評估，據以擬定防護計畫與指引，並將標準化之防護作為納入無人機作業流程。

3. 發展業界公認之資安驗證基準與防護機制:建議國內產官學研單位，參考國際標準與發展趨勢，共同建立無人機資通安全之檢驗基準與防護機制，提供研發、製造與應用無人機之相關單位據以依循。

4. 探討新興科技於無人機資安防護之機會與風險：人工智慧等新興技術可被應用於偵測可能的入侵行為，進行防範或鑑識分析。區塊鏈可用於加密及驗證、5G 及邊緣運算技術可加強無人機的傳輸效率與機載運算能力，進而加強防護能力。然而，前述技術亦可能對無人機形成新型態的資安威脅，因此須一併評估其對於無人機資安防護之機會與風險。

參考文獻

[1] 交通部(2024)，遙控無人機管理規則

[2] 交通部運輸研究所(2022)，以無人機探勘人車流動資訊之應用情境規劃與先導測試(1/3) -建立分年測試計畫

[3] 交通部運輸研究所(2022)，無人機影像監測技術應用於臺中港區管理之研究

[4] 交通部運輸研究所(2024)，無人機偏鄉物流運送服務驗證計畫(1/2)-服務模式規劃與系統發展

[5] 交通部運輸研究所(2024)，無人機搭配 AI 影像辨識應用於橋梁檢測之研究. (2/2) : 無人機自動化檢測架構探討

[6] 財團法人電信技術中心(2023)，無人機資安保障規範 2.0 版

[7] 數位發展部、交通部(2024)，遙控無人機資安檢測規範(草案)簡報

[8] Alliance for System Safety of UAS through Research Excellence (ASSURE): Oregon State University, New Mexico State University and University of North Dakota. (2022). *UAS Cyber Security and Safety Literature Review.*

[9] Cloudflare (2024). *What is an attack surface?* Accessed October 18, 2024, https://www.cloudflare.com/learning/security/what-is-an-attack-surface/

[10] Cybersecurity and Infrastructure Security Agency (CISA) (2019), *Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems*.

[11] Cybersecurity and Infrastructure Security Agency (CISA)(January 27, 2023), *Secure Your Drone: Secure Your Drone: Privacy and Data Protection Guidance*.

[12] Javaid, A.Y., Sun, W., Devabhaktuni, V.K., & Alam, M. (2012). *Cyber security threat analysis and modeling of an unmanned aerial vehicle system.* 2012 IEEE Conference on Technologies for Homeland Security (HST), 585-590.

[13] Lattimore, G. L. (2019). *Unmanned Aerial System Cybersecurity Risk Management Decision Matrix for Tactical Operators*. Naval Postgraduate School.

[14] Naraine, R. (2023). *Google Brings AI Magic to Fuzz Testing With Eye-Opening Results.* SECURITY WEEK. Accessed November 23, 2024, https://www.securityweek.com/google-brings-ai-magic-to-fuzz-testing-with-eye-opening-results/

[15] National Institute of Standards and Technology (NIST) (n.d.). Accessed November 14, 2024, https://csrc.nist.gov/glossary/term/cybersecurity

[16] Pettit, D. M. (2020). *Cyber Risk Assessment and Scoring Model for Small Unmanned Aerial Vehicles*. Air Force Institute of Technology.
[17] PX4 Guide (n.d.). Accessed October 14, 2024, https://docs.px4.io/main/en/companion_computer/
[18] RAND Corporation (2020). *How to Analyze the Cyber Threat from Drones*
[19] Shafik, W., Matinkhah, S. M., and Shokoor, F. (2023). *Cybersecurity in unmanned aerial vehicles: A review*. International Journal on Smart Sensing and Intelligent Systems, 16(1).
[20] Shevchenko, N. (2018). *Threat Modeling: 12 Available Methods*. Carnegie Mellon University, Software Engineering Institute's Insights (blog). Accessed November 14, 2024, https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.
[21] Sihag, V., Choudhary, G., Choudhary, P., Dragoni, N. (2023). *Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones.* Drones.
[22] Vanderveen, M. (2023). *Overview of Security of Uncrewed Aircraft Systems (UAS)*, MITRE.
[23] Vattapparamban, E., Güvenç, İ., Yurekli, A. İ., Akkaya, K. and Uluağaç, S.(2016). *Drones for smart cities: Issues in cybersecurity, privacy, and public safety*, 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus