Technical E-Paper

43

Introduzione Ai SISTEMI D'ANTENNA ANTI-DRONE C-UAS

Flaminio Bollini

In questi ultimi anni si è diffusa una tecnologia fino a non molto tempo fa impensabile: quella dei droni, ovvero di aeromobili telecomandati senza pilota a bordo.

Al 30 giugno 2024, gli operatori UAS (*Unmanned Aircraft System*) registrati in Italia erano 126.242, con un aumento del 27% rispetto ai 99.115 dell'anno precedente (Fonte: *Quadricottero*): questo dimostra un'adozione sempre più diffusa di droni per usi professionali e industriali.

L'incremento dell'uso dei droni ha anche sollevato nuove sfide legate alla sicurezza: l'uso improprio di questi dispositivi, sia su base involontaria che intenzionale, può rappresentare una minaccia per infrastrutture critiche, aeroporti, eventi pubblici e persino operazioni militari.

Per questo motivo, negli ultimi anni si è sviluppato il settore dei sistemi anti-drone, progettati per individuare, tracciare e neutralizzare droni potenzialmente pericolosi.

In questo articolo introduttivo ai sistemi anti-drone descriveremo questi dispositivi, soffermandoci sulle caratteristiche tecniche ed i requisiti che le antenne ad essi associate devono avere.

È indubbio come questo particolare settore di applicazione rappresenti lo stato dell'arte anche per quanto riguarda la definizione, la progettazione e la ingegnerizzazione di antenne con particolari requisiti elettrici, meccanici ed ambientali.

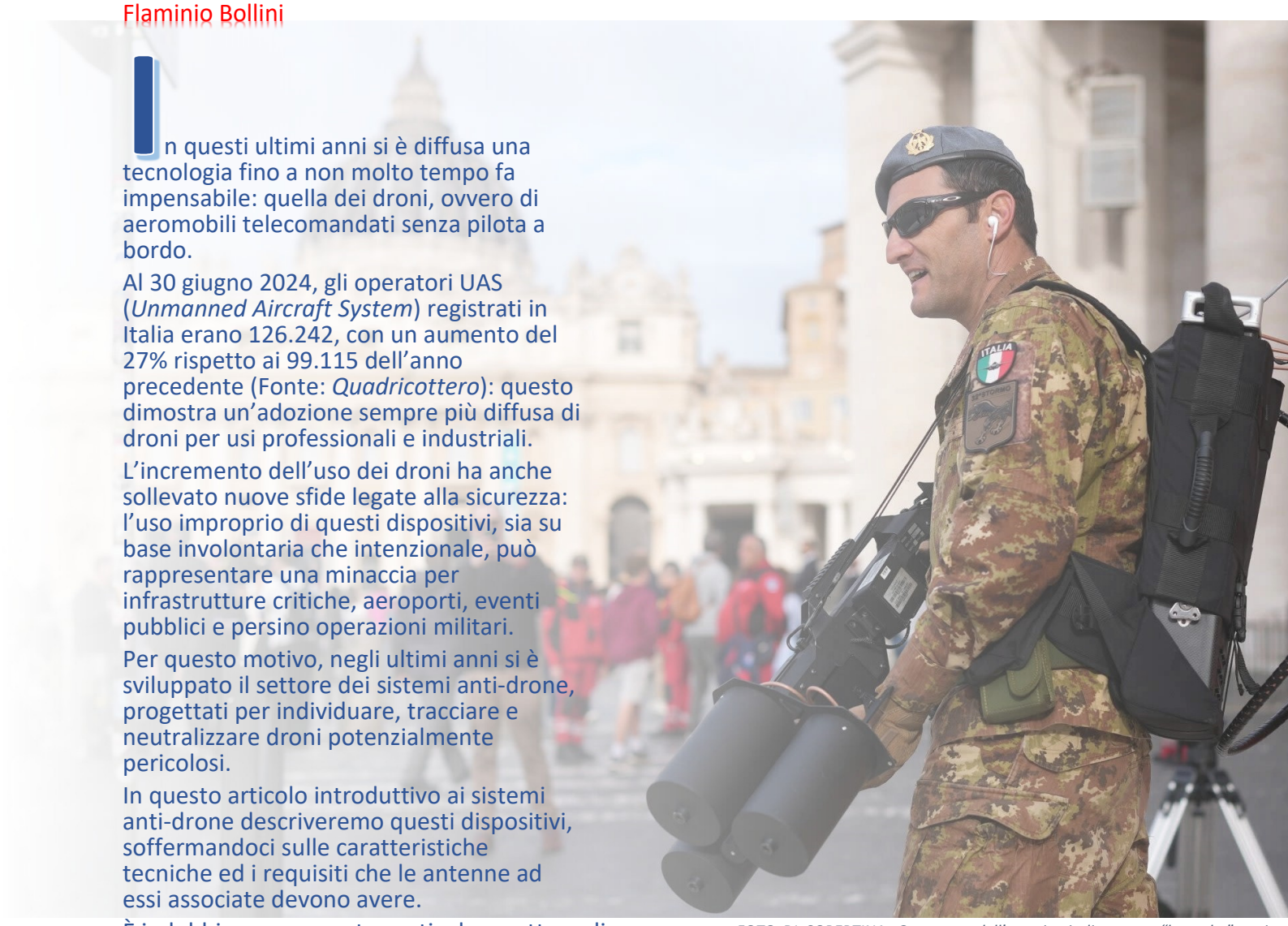

FOTO DI COPERTINA: Operatore dell'esercito italiano con "bazooka" anti-drone a presidio di piazza San Pietro, in occasione dei funerali di Papa Francesco.

ElettroMagnetic Services SRL

1. Introduzione.

Negli ultimi anni, l'impiego dei droni (*UAV – Unmanned Aerial Vehicles*) si è diffuso esponenzialmente, rendendoli strumenti imprescindibili in numerosi ambiti operativi, dall'agricoltura di precisione alla sorveglianza, fino alla logistica e alla gestione delle infrastrutture critiche. La loro capacità di fornire dati in tempo reale, supportare operazioni complesse e ridurre i costi operativi ha reso queste tecnologie una risorsa strategica.

Figura 1

L'impiego di droni a basso costo, consistenti in prodotti commerciali modificati con batterie supplementari e payload esplosivi, hanno definito nuovi, terrificanti scenari nella guerra in Ucraina.

Tuttavia, l'evoluzione del settore ha sollevato nuove criticità legate alla sicurezza e alla protezione delle informazioni. L'uso non autorizzato o malevolo dei droni rappresenta una minaccia concreta per la privacy, la difesa di aree sensibili e la prevenzione di attività illecite, come la sorveglianza clandestina o il trasporto illegale di materiali. Per questo motivo, la necessità di implementare sistemi di contrasto efficaci è diventata una priorità per enti governativi, aziende e infrastrutture ad alto rischio.

Le tecnologie di difesa contro i droni, note come ***Counter-Unmanned Aircraft Systems (C-UAS)***, comprendono diverse strategie di neutralizzazione, tra cui ***misure cinetiche*** (proiettili, reti, armi laser) e soluzioni elettroniche basate su interferenze RF. In particolare, il ***jamming*** – ovvero l'emissione controllata di segnali elettromagnetici per disturbare le comunicazioni tra il drone e il suo operatore – rappresenta una delle soluzioni più efficaci e versatili per la protezione di infrastrutture strategiche.

In questo articolo approfondiremo il funzionamento dei sistemi anti-drone, analizzando le loro applicazioni e le specifiche tecniche che devono caratterizzare le antenne impiegate in questi dispositivi. Infine, illustreremo i vantaggi offerti da un design su misura, essenziale per garantire le massime prestazioni in scenari operativi complessi.

2. I campi di applicazione.

I sistemi anti-drone trovano impiego in diversi contesti, sia civili che militari, per contrastare minacce legate all'uso improprio o malevolo di questi dispositivi.

Settore civile:

- Protezione di aeroporti e spazi aerei da incursioni non autorizzate;
- Difesa di infrastrutture critiche (centrali elettriche, impianti industriali, data center);
- Messa in sicurezza di eventi di massa e aree sensibili;
- Prevenzione di attività illecite, come la sorveglianza non autorizzata e il traffico illecito di materiali;

Settore militare e difesa:

- Protezione di basi operative e installazioni strategiche;
- Sicurezza di convogli e unità tattiche;
- Neutralizzazione di droni impiegati per attacchi mirati;
- Supporto in operazioni di guerra elettronica.

3. I sistemi anti-drone elettronici.

I sistemi elettronici atti a salvaguardare la sicurezza di un determinato spazio aereo dall'intrusione di velivoli non autorizzati possono essere di tipo ***DF*** (*direction finding*) o di tipo ***jammer***. Nel primo caso vengono utilizzati per rilevare la presenza e la posizione del drone, nel secondo caso per renderlo inoffensivo. Riportiamo di seguito una breve disamina.

3.1. I sistemi *Direction Finding (DF)*.

La tecnica del *Direction Finding (DF)* consente di determinare con precisione la direzione da cui proviene il segnale del drone, permettendo sia l'identificazione del velivolo sia la sua posizione, così come altri parametri di volo quali direzione, altezza e velocità. Se necessario si interviene quindi con contromisure di tipo cinetico od elettronico per rendere inoffensivo il drone.

Questi sistemi elettronici possono basarsi su principi differenti che fanno capo a sensori di diverse tipologie (radar, ottici, acustici).

Molto utilizzati sono i sistemi DF che ricercano le trasmissioni radio in essere tra il drone ed il suo pilota a terra che, nel caso di UAV per impiego civile, avvengono generalmente nelle bande dei 2.4GHz (controllo di volo) e 5 GHz (segnale video). Tali sistemi sono essenzialmente di due tipologie:

Figura 2

Sistema DF multibanda custom che integra sia elementi multisettoriali sia antenne omnidirezionali integrati in una struttura realizzata ad hoc.

- **a)** Sistemi che decodificano le informazioni contenute nel segnale radio trasmesso dal drone, non criptato, e ne ricavano i dati di navigazione di quest'ultimo. In questo caso vengono utilizzate antenne di tipo omnidirezionale.
- **b)** Sistemi che rilevano la posizione del drone basandosi sulle caratteristiche elettromagnetiche del segnale ricevuto (direzione di provenienza, intensità, ecc.) e non necessariamente sull'informazione in esso contenuta. In questo caso vengono utilizzate antenne direttive o settoriali, con scansione meccanica od elettronica, che fungono da filtro spaziale.

I sistemi DF di tipo ***a*** sono apparati più compatti e spesso sono nel catalogo delle aziende produttrici dei droni stessi, come ad esempio la ben nota DJI. Non sempre tali sistemi sono in grado di decodificare il segnale proveniente da un drone, specialmente se quest'ultimo è impiegato intenzionalmente per scopi malevoli, e di conseguenza in questo caso possono risultare inefficaci.

Per questo motivo sono sempre più utilizzati i sistemi di tipo ***b***, in quanto sono potenzialmente in grado di rilevare qualsiasi *UAV* in volo nello spazio aereo controllato, indipendentemente dal protocollo di comunicazione utilizzato per le comunicazioni con il pilota a terra. L'utilizzo congiunto di più sistemi di questo tipo, opportunamente dislocati lungo il perimetro dell'area da proteggere, permette anche una triangolazione molto precisa per conoscere posizione e parametri di volo del drone stesso.

3.2. I sistemi di *jamming*.

La tecnica cosiddetta di *jamming* genera interferenze elettromagnetiche sia sulle frequenze di comunicazione del drone sia sui segnali di posizionamento GPS, inibendo sia la ricezione dei comandi di volo dal pilota a terra sia i dati GPS necessari allo *homing*, ovvero all'attivazione della modalità di rientro automatico al punto di partenza.

Una tecnologia più raffinata impiegata in campo militare consiste nello ***spoofing***, una tecnica che non interrompe direttamente le comunicazioni, ma le manipola, inviando segnali GPS contraffatti: in questo modo il drone viene ingannato sulla propria posizione, e viene indotto a deviare dalla rotta originale o ad atterrare in un'area controllata. Questa tecnica è particolarmente utile per scenari in cui è necessario deviare un drone ostile senza destare sospetti.

I sistemi elettronici anti-drone più sofisticati incorporano sia la modalità di rilevamento (*DF*) sia le contromisure elettroniche necessarie alla neutralizzazione del drone (*jamming, spoofing*).

4. Antenne per sistemi anti-drone.

L'implementazione pratica di queste tecnologie apre uno scenario molto vario, essendoci dispositivi assai diversi tra loro, come ad esempio sistemi fissi a protezione di luoghi sensibili, sistemi installati su mezzi terrestri o navali e addirittura apparati portatili, come ad esempio il "bazooka" anti-drone mostrato nella foto di copertina.

Ciò implica la necessità di realizzare ad hoc antenne assai diverse, con specifiche elettriche ben definite, e spesso integrate in un hardware con caratteristiche meccaniche ed ambientali stringenti. Infatti, le antenne impiegate nei sistemi anti-drone devono soddisfare requisiti tecnici estremamente rigorosi per garantire un'efficace neutralizzazione della minaccia, operando in condizioni ambientali e operative variabili. La progettazione di questi dispositivi richiede un equilibrio ottimale tra prestazioni elettriche e robustezza meccanica, adattandosi a specifiche esigenze applicative.

Se prendiamo a riferimento i sistemi anti-drone descritti nel paragrafo precedente, i criteri di progetto elettrico prendono le mosse da dei requisiti iniziali che, in questo caso specifico, possono essere:

- ***a)*** *Antenne omnidirezionali o settoriali/direttive;*
- ***b)*** *Antenne per il solo uso DF ed antenne per jammer;*
- ***c)*** *Bande di frequenza.*

A questi si aggiungono dei requisiti di tipo meccanico/ambientale che generalmente sono:

- ***d)*** *Presenza di vincoli meccanici ed ambientali sulle dimensioni del sistema;*
- ***e)*** *Integrazione in una struttura multi-antenna che contiene anche la parte elettronica.*

Figura 3

Apparato jammer multibanda che impiega numerose antenne omnidirezionali montate molto vicine tra loro: in questa configurazione è difficile garantire una perfetta omnidirezionalità per ogni sottobanda operativa, nonché un adattamento soddisfacente.

4.1. Caratteristiche elettriche.

a) *Antenne omnidirezionali o settoriali/direttive.*

La copertura ideale di un'antenna-anti drone è rappresentata dal semispazio-superiore, in modo da poter controllare efficacemente qualsiasi oggetto volante in avvicinamento. Nel caso di **antenne omnidirezionali**, particolare cura dev'essere posta nella definizione di un elemento radiante caratterizzato da una elevata simmetria rotazionale rispetto all'asse verticale (*asse z*). Nello stesso tempo è necessario tener conto della coesistenza di diverse antenne, operanti su più bande di frequenza, così da non distorcere i rispettivi diagrammi di radiazione nel piano azimutale.

Nei sistemi che fanno uso di più **antenne settoriali o direttive** per coprire tutte le direzioni e discriminare quindi la direzione del bersaglio, è necessario che i diagrammi di radiazione siano privi di lobi laterali, con un elevato rapporto avanti/indietro (**Figura 4**). L'integrazione di più settori su di un'unica struttura con simmetria rotazionale rispetto all'asse *z* deve altresì garantire un elevato isolamento tra due settori adiacenti, ovvero le antenne di ciascun settore non devono essere influenzate dalla prossimità con gli altri settori che fanno parte del sistema (**Figura 5**).

In entrambi i casi, il diagramma di radiazione nel piano verticale deve poter coprire quasi tutti gli angoli di elevazione: in questo caso è possibile prevedere un *up-tilt*, meccanico od elettrico, in modo da limitare la dispersione di energia verso il semispazio inferiore.

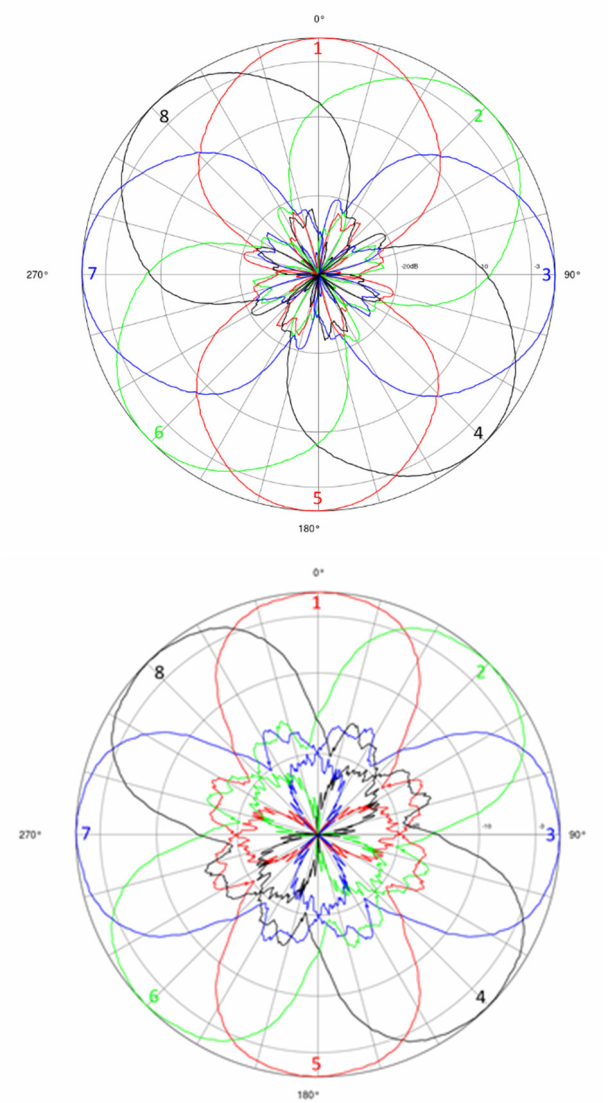

Figura 4

Diagrammi di radiazione nel piano azimutale del sistema DF multisettoriale di Figura 2, in banda 2.4 GHz e 5 GHz.

b) *Antenne per il solo uso DF ed antenne per jammer.*

La definizione ed il dimensionamento degli elementi radianti cambiano apprezzabilmente nel caso in cui si debba realizzare un sistema per il solo impiego come *DF* od un sistema che contempli anche la modalità *jammer*: infatti nel primo caso il sistema opera soltanto in ricezione, mentre nel secondo caso deve anche trasmettere un segnale di disturbo dell'ordine di qualche centinaio di watt.

c) *Bande di frequenza.*

In ambito civile, la maggior parte dei sistemi anti-drone è di tipo multibanda ed opera sui 2.4 GHz e 5 GHz, mentre nelle applicazioni militari le antenne devono essere concepite per poter operare a larga banda, con caratteristiche elettriche quali adattamento e larghezze di fascio il più possibile costanti nella porzione di spettro stabilita.

Nei sistemi a larga banda che operano su più ottave, come ad esempio da 700 MHz fino a 6 GHz, le antenne possono essere convenientemente suddivise in più sottobande così da garantire prestazioni elettriche uniformi.

4.2. Caratteristiche meccaniche ed ambientali.

d) *Presenza di vincoli meccanici ed ambientali sulle dimensioni del sistema.*

Le caratteristiche elettriche del paragrafo precedente devono essere implementate su antenne integrate in un sistema che soddisfa dei precisi vincoli meccanici ed ambientali, in particolare nel caso di installazioni veicolari o addirittura portatili. Non è raro infatti che la definizione elettrica degli elementi radianti utilizzabili nel progetto di un dato sistema anti-drone debba partire proprio da considerazioni su dimensioni, peso e resilienza a cicli termici e vibrazioni.

e) *Integrazione in una struttura multi-antenna che contiene anche la parte elettronica.*

Invece di utilizzare antenne separate e montate su di un unico supporto meccanico con i cablaggi a vista, il trend attuale consiste nel realizzare un sistema integrato in un unico radome, contenente sia le antenne, omnidirezionali o settoriali che siano, sia la parte elettronica RF e di controllo con i relativi cablaggi.

Oltre ad una maggiore affidabilità meccanica, la possibilità di integrare tutte le antenne del sistema in una struttura ad hoc permette un'ottimizzazione delle caratteristiche elettriche di queste ultime non ottenibile con un sistema costituito da elementi discreti. Risulta comunque evidente che un sistema anti-drone di questo tipo richiede anche una progettazione meccanica importante, oltre a quella elettrica.

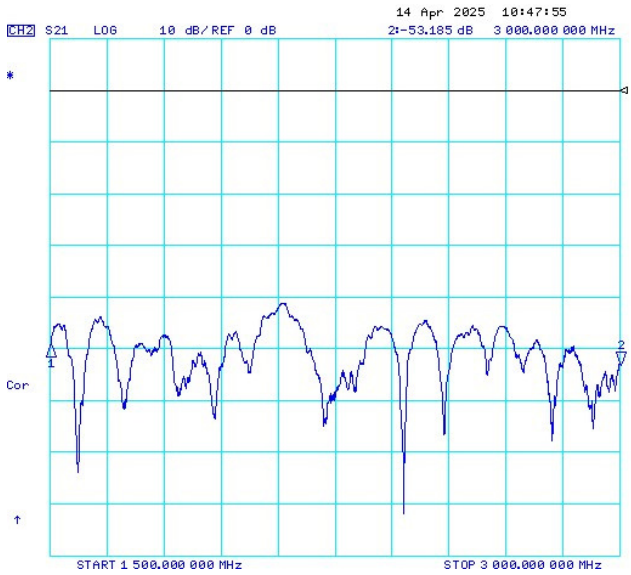

Figura 5

Isolamento tra due settori adiacenti di un sistema multisettoriale DF/jammer, nella sottobanda 1.5÷3 GHz: solo con una progettazione integrata ad hoc è possibile ottenere valori così elevati.

5. Vantaggi di una soluzione custom.

La progettazione di antenne per jammer anti-droni è un processo complesso, che non può essere affrontato con un approccio standardizzato. Non esiste una soluzione universale valida per ogni scenario operativo: ogni applicazione presenta variabili uniche che richiedono un design su misura per ottenere le massime prestazioni.

Come accade nello sviluppo di un qualsiasi prodotto industriale innovativo, anche la progettazione di antenne custom richiede la capacità di adattarsi ai requisiti del Cliente, sia a livello di specifiche di progetto iniziali sia nella previsione dei possibili inconvenienti che possono verificarsi durante tutta la vita operativa del prodotto.

Il progetto di sistemi d'antenna anti-drone è caratterizzato da una forte componente interdisciplinare: è infatti necessario tener conto sia delle specifiche elettriche che di quelle meccaniche, relative all'inserimento del sistema radiante in una struttura realizzata ad hoc.

Questi due aspetti risultano essere fortemente interdipendenti, e pertanto è doveroso considerare questi prodotti su misura come vere e proprie antenne integrate, come ad esempio le antenne montate nei dispositivi IoT. Rispetto a queste ultime però, le prestazioni elettriche dei sistemi anti-drone necessitano di essere molto più precise e performanti, e quindi la struttura meccanica che le ospita deve essere progettata su misura.

È infatti possibile affermare che ***nei sistemi IoT è l'apparato che ospita l'antenna***, mentre ***nei sistemi anti-drone è l'antenna che ospita l'apparato***.

Per tale motivo è fondamentale rivolgersi ad un'azienda in grado di farsi carico di entrambi gli aspetti, elettromagnetico e meccanico, del progetto, vantando una gestione dello sviluppo del prodotto centrale ed unificata, contrariamente a quanto avviene oggigiorno in molti progetti interdisciplinari (**Figura 6**).

Infatti l'analisi dei vincoli meccanici e dimensionali porta ad un primo abbozzo della struttura del sistema, con i presupposti per individuare la configurazione dell'elemento radiante più adatta a soddisfare i requisiti elettrici su tutto il range di frequenze operative. In particolare, la definizione accurata delle caratteristiche di radiazione (larghezze di fascio nei piani principali, attenuazione dei lobi laterali e ottimizzazione del rapporto A/I) è fondamentale per evitare interferenze indesiderate e garantire la massima precisione nel targeting del segnale di jamming.

Figura 6

Fase finale di assemblaggio di un sistema multisettoriale integrato a larga banda, progetto custom.

La progettazione meccanica dell'antenna gioca quindi un ruolo chiave nel miglioramento delle prestazioni complessive. Ad esempio, una struttura customizzata può essere progettata per minimizzare l'emissione di lobi di radiazione nelle direzioni indesiderate o per ottimizzare l'isolamento tra i diversi elementi radianti, riducendo così il rischio di segnali indesiderati e garantendo un funzionamento pulito ed efficace.

Dall'esperienza maturata nel contatto diretto con i nostri Clienti, emerge chiaramente che il tentativo di implementare sistemi jammer basati su antenne standard raramente produce risultati soddisfacenti. Sebbene possano rappresentare una soluzione temporanea o di compromesso, tali antenne difficilmente garantiscono il livello di prestazioni e affidabilità richiesto in applicazioni professionali. Solo un'antenna progettata ad hoc consente di ottimizzare ogni parametro tecnico e strutturale, assicurando il massimo controllo sulle prestazioni del sistema.

6. Conclusioni.

L'evoluzione tecnologica ha reso i droni strumenti sempre più diffusi e versatili, con applicazioni che spaziano dall'industria alla sicurezza. Tuttavia, il loro utilizzo improprio o malevolo rappresenta una minaccia concreta per la protezione di infrastrutture critiche, la sicurezza pubblica e la riservatezza delle informazioni. In questo scenario, l'adozione di misure di difesa efficaci è diventata una priorità.

I sistemi **jammer anti-drone** offrono una soluzione affidabile per neutralizzare le minacce UAV, interrompendo le comunicazioni tra il drone e il suo operatore attraverso tecniche di **jamming** e **spoofing**. Mentre il jamming degrada o elimina i segnali di controllo e navigazione, lo spoofing manipola le coordinate GPS, inducendo il drone a deviare dalla sua rotta.

L'efficacia di questi sistemi dipende in larga misura dalla qualità e dalla progettazione delle antenne impiegate. Un sistema jammer anti-drone richiede antenne con specifiche tecniche altamente precise, che devono essere ottimizzate in base alle condizioni operative, alle frequenze di utilizzo e agli obiettivi di mitigazione della minaccia. Fattori come la larghezza di fascio, l'attenuazione dei lobi laterali, l'isolamento tra gli elementi radianti e la gestione della potenza massima applicabile giocano un ruolo cruciale nella capacità del sistema di garantire prestazioni costanti ed efficaci.

Considerata la complessità di questi requisiti, l'utilizzo di **antenne custom** rappresenta la scelta strategica per ottenere soluzioni su misura, in grado di adattarsi perfettamente a ciascun scenario operativo. Solo attraverso una progettazione dedicata è possibile massimizzare l'efficienza del segnale di disturbo, ridurre al minimo le interferenze indesiderate e garantire un'integrazione ottimale con le piattaforme C-UAS.

♦

Tutte le informazioni e le esperienze riportate in questo articolo sono frutto dell'attività di **progettazione, sviluppo e realizzazione di antenne custom professionali** *svolta da* ***ElettroMagnetic Services Srl*** *con il metodo* ***AntennaSuMisura****.*

Per **domande, chiarimenti od approfondimenti** *in merito a questo o ad altri argomenti riguardanti* **le antenne professionali scrivi a** *bollini@elettromagneticservices.com*

Grazie per il tempo che hai dedicato alla lettura di questo articolo.

Trovi l'elenco completo delle nostre pubblicazioni tecniche cliccando qui:
https://www.elettromagneticservices.com/news

AntennaSuMisura

by

ElettroMagnetic Services SRL

Trasmettiamo la tua eccellenza!