

# Estudio de integración de drones con la aviación comercial en el ámbito de los sistemas de comunicación

**Manuel Santiago Sánchez Hernández**

Máster Universitario en Ingeniería de Telecomunicación UOC-URL  
Sistemas de comunicación

**Profesor responsable:** Carlos Monzo Sánchez

**Profesor colaborador:** Raúl Parada Medina

23/06/2019



Esta obra está sujeta a una licencia de Reconocimiento-  
NoComercial SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

## FICHA DEL TRABAJO FINAL

<b>Título del trabajo:</b>	<i>Estudio de integración de drones con la aviación comercial en el ámbito de los sistemas de comunicación</i>
<b>Nombre del autor:</b>	<i>Manuel Santiago Sánchez Hernández</i>
<b>Nombre del consultor:</b>	<i>Raúl Parada Medina</i>
<b>Nombre del PRA:</b>	<i>Carlos Monzo Sánchez</i>
<b>Fecha de entrega:</b>	<i>23/06/2019</i>
<b>Titulación:</b>	<i>Máster Universitario en Ingeniería de Telecomunicación UOC-URL</i>
<b>Área del Trabajo Final:</b>	<i>Sistemas de Comunicación</i>
<b>Idioma del trabajo:</b>	<i>Castellano</i>
<b>Palabras clave</b>	<i>Integración, Drones, Aviación comercial, Sistemas de comunicación</i>

### Resumen del Trabajo

El espacio aéreo ha sufrido una gran transformación debido a la presencia y uso crecientes de los drones y, con ello, ha aumentado el número de incidentes registrados entre estos aparatos dirigidos por control remoto y los aviones de pasajeros en aeropuertos de todo el mundo, poniendo en grave riesgo la seguridad aérea y de las personas.

En nuestro país, aún no se ha reportado ningún incidente de consideración. Sin embargo, se ha establecido una normativa que regula el diseño y fabricación de este tipo de aeronaves, así como las limitaciones de uso y espacios restringidos para evitar situaciones de riesgo. No obstante, existe cierta preocupación por el uso imprudente o malintencionado de estos artefactos, como ocurrió recientemente en el aeropuerto londinense de Gatwick.

Por este motivo, surge la necesidad de encontrar la forma de integrar y compatibilizar de forma segura el uso de drones con la aviación comercial mediante el análisis y estudio de las diferentes técnicas y sistemas de comunicaciones que existen para identificar, detectar y limitar la presencia de drones en el entorno aeroportuario español e integrarlos dentro de los sistemas de control de tránsito aéreo.

Para ello, se realizará la recolección de información relacionada con los distintos tipos de drones, así como sus características y se analizarán las diferentes normativas y regulaciones a nivel nacional e internacional para encontrar una o varias soluciones viables técnicamente que encajen dentro del marco normativo y que permita hacer un uso eficiente y seguro del espacio aéreo en el entorno aeroportuario español.

### **Abstract**

The airspace has undergone a great transformation due to the increasing presence and use of drones and, with this, the number of recorded incidents between these remote-controlled aircraft and passenger aircraft in airports around the world has increased, putting in serious risk the aviation security and of the people.

In our country, no significant incident has been reported yet. However, a regulation has been established that regulates the design and manufacture of this type of aircraft, as well as the limitations of use and restricted spaces to avoid situations of risk. However, there is some concern about the reckless or malicious use of these devices, as was recently the case at London's Gatwick airport.

For this reason, the need arises to find a way to integrate and securely combine the use of drones with commercial aviation through the analysis and study of the different techniques and communication systems that exist to identify, detect and limit the presence of drones in the Spanish airport environment and integrate them into air traffic control systems.

For this purpose, the collection of information related to the different types of drones will be carried out, as well as their characteristics, and the different regulations will be analyzed at a national and international level to find one or several technically feasible solutions that fit within the regulatory framework and that allow make an efficient and safe use of the airspace in the Spanish airport environment.

## Índice

<b>1. Introducción</b>	<b>1</b>
1.1 Contexto y justificación del Trabajo	1
1.2 Objetivos del Trabajo	1
1.3 Enfoque y método seguido	2
1.4 Planificación del Trabajo	3
1.5 Breve resumen de productos obtenidos	5
1.6 Breve descripción de los otros capítulos de la memoria	5
<b>2. Estado del arte</b>	<b>6</b>
2.1 Breve repaso de los sistemas de comunicación de los drones	6
2.3 Sistemas de comunicación y posicionamiento de drones basados en redes de telecomunicaciones	7
2.4 Proyectos de integración de sistemas de comunicación de drones en los sistemas de control de tráfico aéreo	8
2.5 Proyectos para detectar y neutralizar amenazas que en el espacio aéreo controlado y no controlado	11
<b>3. Origen y evolución de los drones</b>	<b>13</b>
3.1 Historia y evolución de los drones	13
3.2 El dron en la actualidad	14
3.2.1 Clasificación	15
3.2.2 Aplicaciones más comunes	16
<b>4. Problemática de los drones</b>	<b>19</b>
4.1. Incidentes con aeronaves comerciales	19
4.2. Daños producidos a las aeronaves	20
<b>5. Marco normativo de drones y aviones comerciales</b>	<b>24</b>
5.1. Marco regulatorio internacional	25
5.2 Régimen de regulación de los drones	26
5.3 Aspectos normativos en las comunicaciones de drones con ATC	27
5.3.1 Descripciones generales del sistema y terminología	27
5.3.2 Radioenlaces y arquitecturas necesarias para operaciones con drones	28
5.3.3 Enlace C2	31
5.3.3.1 Arquitecturas del enlace	31
5.3.3.2 Bandas frecuenciales	33
5.3.3.3 Pérdida y protección del enlace	34
5.3.4 Función S&A/ DAA (Detectar y evitar)	35
5.4 Flujos de información	36
5.5 Comunicaciones aeronáuticas de drones con ATC	37
5.6 Requisitos de espectro de frecuencias para las comunicaciones con drones	38
5.7 Normativa y restricciones en el espacio aéreo español	40
<b>6. Tecnologías y sistemas de integración de drones en el espacio aéreo</b>	<b>42</b>
6.1 Sistemas de detección, identificación y geolocalización de drones	42
6.1.1 Sistema S&A/ DAA (Detectar y Evitar)	42
6.1.2 Sistema ACAS-sXu	45
6.1.3 Geofencing	46
6.1.4 Identificación de drones	48
6.1.4.1 Identificación mediante etiquetas OID	48
6.1.4.2 Identificación mediante SIM integrada	49
6.1.5 Técnicas de posicionamiento basado en redes móviles	49
6.1.5.1 OTDOA (Observed Time Difference Of Arrival)	50
6.1.5.2 E-CID (Enhanced Cell ID)	50
6.2 Tecnologías de comunicación de los drones	52
6.2.1 WiFi	52
6.2.2 Redes LTE	54
6.2.3 Redes 5G	58

<b>7. Soluciones de integración de drones en el entorno aeroportuario.....</b>	<b>60</b>
7.1 Situación actual de la integración de drones en el espacio aéreo.....	60
7.1.1. Solución propuesta por Ericsson .....	62
7.1.1.1 Sistema de identificación .....	63
7.1.1.2 Sistema de geolocalización .....	63
7.1.1.3 Detección de uso no certificado de dispositivos móviles.....	63
7.1.2 Solución propuesta por Embention.....	64
7.1.3 Solución propuesta por INDRA.....	65
7.1.4 Solución propuesta por la NASA .....	66
7.1.4.1 Programa Piloto UTM .....	66
7.1.4.2 ECOsystem UTM de Thales .....	68
7.1.5 Solución propuesta por Airmap y Skyguide.....	69
7.2 Soluciones para neutralizar drones en casos de interferencia ilícita .....	71
7.2.1 Solución propuesta por Quantum Aviation .....	71
7.2.2 Solución propuesta por Thales Group .....	72
7.2.3 Solución propuesta por INDRA.....	73
<b>8. Conclusiones .....</b>	<b>76</b>
<b>9. Glosario de términos .....</b>	<b>77</b>
<b>10. Bibliografía .....</b>	<b>79</b>

## Listado de figuras

Figura 1: Diagrama de Gantt.....	4
Figura 2: Elementos para controlar y dirigir un dron. ....	14
Figura 3: Tipos de drones. ....	15
Figura 4: Daños producidos por un dron al colisionar con un ala de avión. ....	20
Figura 5: Niveles de daños producidos por un dron de 1,2 kg y 1,8 kg.....	21
Figura 6: Cinemática de la ingesta de un dron de ala fija durante el despegue. ....	22
Figura 7: Detalle de los daños producidos a los álabes en el impacto. ....	22
Figura 8: Radioenlace LOS en un UAS. ....	30
Figura 9: Radioenlace BLOS en un UAS. ....	30
Figura 10: Arquitectura RLOS. ....	31
Figura 11: Arquitectura BRLOS.....	31
Figura 12: Arquitectura de retransmisión mediante el RPA. ....	32
Figura 13: Arquitectura de retransmisión BRLOS – RPA. ....	32
Figura 14: Arquitectura sin retransmisión a través del RPA. ....	33
Figura 15: Arquitectura con enlace Tierra – Tierra. ....	33
Figura 16: Nivel de señal recibida en función del tiempo. ....	34
Figura 17: Flujo de información entre el UA y el UACS. ....	36
Figura 18: Flujo de información entre el UA, el UACS y el control ATC: .....	37
Figura 19: Interfaces del sistema. ....	38
Figura 20: Interferencias en función del tipo de usuario asignado. ....	39
Figura 21: Sistema S&A/DAA (Detectar y Evitar). ....	42
Figura 22: Componentes de un sistema S&A basado en visión computarizada. ....	43
Figura 23: Arquitectura base del sistema S&A del dron. ....	43
Figura 24: Sistema activo anticollision S&A/ DAA basado en redes móviles. ....	44
Figura 25: Funcionamiento del sistema ACAS-X.....	45
Figura 26: Delimitación de zonas de riesgo en un aeropuerto. ....	47
Figura 27: Captura de la aplicación GEOMap de DJI. ....	48
Figura 28: Medición TDOA basada en hipérbolas. ....	50
Figura 29: Métodos de Identificación Celular Mejorada (E-CID). ....	51
Figura 30: Dron de DJI I que usa la banda de 2,4 GHZ en su enlace de comunicaciones. ....	53
Figura 31: Esquema de modulación FHSS. ....	53
Figura 32: Posibles formas de conectividad. ....	55
Figura 33: Diagrama de antena de cada estación base. ....	55
Figura 34: Ganancia de acoplamiento de enlace descendente (Ganancia de antena + canal). ....	56
Figura 35: Ganancia de acoplamiento de enlace descendente (SINR).....	56
Figura 36: Patrones de asociación de células a diferentes altitudes. ....	57
Figura 37: Conectividad para drones pequeños a baja altitud con redes móviles. ....	64
Figura 38: Futuras aplicaciones tecnológicos de la red 5G. ....	58
Figura 39: Concepto del sistema de integración U-Space.....	61
Figura 40: Elementos de un sistema UTM con identificación de drones. ....	62
Figura 41: División de espacio aéreo en función de la aeronave. ....	64
Figura 42: Sistema Veronte Autopilot. ....	65
Figura 43: Concepto del Programa UPP.....	67
Figura 44: Ecosistema UPP. ....	67
Figura 45: Proyecto la NASA de integración de drones en el espacio aéreo norteamericano... ..	68
Figura 46: Funcionamiento del sistema LAANC. ....	69
Figura 47: Esquema de funcionamiento del proyecto Swiss U-Space. ....	70
Figura 48: Componentes de TITANIUM: a) Radar; b) Cámara EO/IR; c) Detector de RF. ....	72
Figura 49: Sistema anti-drones C-UAS de Thales. ....	73
Figura 50: Escudo anti-drones ARMS de Indra. ....	74
Figura 51: Cúpula de protección del escudo ARMS de INDRA. ....	74

## **Listado de tablas**

Tabla 1: Clasificación de los drones.....	16
Tabla 2: Evolución prevista de los drones en el espacio aéreo .....	24
Tabla 3: Tabla resumen de uso de drones según la normativa española.....	41
Tabla 4: Comparativa de tecnologías de comunicación de drones.....	59
Tabla 5: Descripción de las etapas U-Space y año previsto de implantación.....	62
Tabla 6: Resumen de soluciones de sistemas de gestión de drones UTM.....	71
Tabla 7: Resumen de soluciones para neutralizar drones en el espacio aéreo .....	75

# 1. Introducción

Este primer capítulo pretende realizar un primer acercamiento del lector al tema del trabajo. Para ello, se presentará el contexto y problemática en la que se centra el proyecto. Posteriormente, se abordarán una o varias soluciones viables en base a la definición de objetivos del trabajo. Por último, se mostrarán la metodología y enfoque seguidos para el diseño del sistema, así como una planificación temporal desde el punto de vista de la gestión de proyectos.

## 1.1 Contexto y justificación del Trabajo

Durante los últimos años, el espacio aéreo ha experimentado un gran cambio debido a la aparición de las aeronaves pilotadas por control remoto, los RPA o también llamados drones. La venta y el uso de estos aparatos ha crecido considerablemente y, con ello, la cantidad de incidentes que se están produciendo con los aviones de pasajeros en aeropuertos de todo el mundo, poniendo en grave riesgo la seguridad aérea y de las personas. Recientemente, el aeropuerto de Gatwick, el segundo más importante de Reino Unido, cerró durante más de 24 horas por la presencia de Drones sobrevolando su espacio aéreo [1]. Pero no es el único país que ha sufrido las consecuencias de estas imprevisibles situaciones. En Estados Unidos, en solo cinco meses se han reportado casi 600 situaciones de riesgo en maniobras de aterrizaje y despegue de aeronaves tripuladas. También, en menor medida, se han registrado incidentes en Gran Bretaña, Francia y Polonia [2].

En España, de momento no se ha reportado ningún incidente de consideración. No obstante, ha surgido la necesidad de establecer una regulación a través de la Agencia Estatal de Seguridad Aérea (AESA) que permita un mayor desarrollo en condiciones de seguridad de este nuevo sector, tecnológicamente puntero y emergente. Tras años de normativa transitoria, se ha aprobado una nueva regulación para las operaciones con drones que abre nuevos escenarios operativos, establece las condiciones que deben cumplir las organizaciones en el diseño, fabricación y mantenimiento de este tipo de aeronaves, así como los requisitos de formación para su pilotaje y obtención de la correspondiente licencia [3].

Aun así, aunque hay una normativa específica para el uso de estos dispositivos, existe cierta preocupación porque pueden resultar potencialmente muy peligrosos para la aviación comercial si se usan de forma imprudente o malintencionada, como ocurrió en el aeropuerto londinense.

Por este motivo, surge la necesidad de encontrar la forma de integrar y compatibilizar de forma segura el uso de drones con la aviación comercial. Para ello, se realizará el análisis y estudio de las diferentes técnicas y sistemas de comunicaciones que existen actualmente para identificar, detectar, comunicar y limitar la presencia de drones en el entorno aeroportuario o incluso neutralizarlos si suponen un grave riesgo para la seguridad aérea y de las personas.

## 1.2 Objetivos del Trabajo

Los objetivos del presente proyecto son los siguientes:

- Sintetizar las competencias adquiridas durante el máster y evidenciar el grado de madurez del autor para afrontar un proyecto de manera autónoma en el campo de la ingeniería de telecomunicación.

- Organizar y planificar las actividades del proyecto.
- Analizar la problemática existente actual entre las aeronaves no tripuladas y la aviación comercial desde el punto de vista de la seguridad aérea y de las comunicaciones.
- Establecer un marco conceptual y normativo que incluye la definición de los tipos de drones que existen actualmente y su normativa de uso aplicable en distintos países.
- Realizar el análisis y estudio de las diferentes técnicas y sistemas de comunicaciones que existen actualmente para identificar, detectar, comunicar y limitar la presencia de drones en el espacio aéreo.
- Proponer soluciones viables y adaptadas al ámbito aeroportuario.

### **1.3 Enfoque y método seguido**

El desarrollo de este trabajo se realizará desde la perspectiva de la gestión de proyectos en el marco de PMBOK, donde la planificación del tiempo, esfuerzo y alcance son dimensiones interrelacionadas que aseguran la correcta elaboración de los distintos entregables.

El enfoque del proyecto será el de realizar tareas de investigación mediante la recopilación de artículos científicos, industriales y/o académicos que traten sobre los distintos sistemas de comunicaciones que existen actualmente para integrar de forma segura el uso de drones con la aviación comercial en el espacio aéreo.

La metodología a seguir consistirá en la recolección de información relacionada con los distintos tipos de drones que hay en el mercado, así como las bandas de frecuencias y potencias de trabajo de sus sistemas de comunicación, con el fin de asimilar conocimientos complementarios a los adquiridos en los estudios y tener una visión global del funcionamiento y potencial de estos aparatos.

Seguidamente, se analizarán las distintas normativas y regulaciones a nivel de espectro frecuencial y limitaciones de potencias de uso que existen actualmente en distintos países y realizar una comparativa con la existente en nuestro país para establecer un marco normativo y conceptual adecuado para su integración.

Posteriormente, se analizarán en profundidad las diferentes técnicas y sistemas de comunicaciones que existen actualmente para identificar y detectar la presencia de drones y comunicar su situación a los gestores aeroportuarios, en concreto, al Control de Tránsito Aéreo, para que determinen las actuaciones oportunas para gestionar el espacio aéreo de forma segura. También se investigará sobre las posibles opciones que existen para neutralizar estas amenazas si suponen un grave riesgo para la seguridad aérea y de las personas.

Tras abordar dichos recursos, se identificarán todos los aspectos relevantes del problema a resolver y se obtendrá una visión holística de la sección en cuestión, que permitirá hallar una o varias soluciones viables que encajen dentro del ámbito aeroportuario español.

Finalmente, se procederá a la redacción de las conclusiones y de las tendencias futuras. Aplicando este enfoque y metodología se podrán cumplir los objetivos en los plazos determinados por las dimensiones del proyecto.

#### **1.4 Planificación del Trabajo**

El proyecto consiste en la realización de unas tareas de investigación y un estudio de mercado de diferentes soluciones a la problemática presentada, así como la realización de una memoria y una presentación. Para la elaboración de dichos entregables se emplearán fuentes de conocimiento al alcance del autor como son la web, los recursos electrónicos especializados, artículos científicos, industriales y/o académicos y libros. Al tratarse de un proyecto eminentemente teórico, estos elementos permitirán recolectar los datos necesarios para disponer de una bibliografía en la que basar el trabajo final.

El proyecto se divide en cinco entregables, los cuáles coinciden con las PEC de la asignatura. Estos entregables son los siguientes:

- **PEC 1:** Esta primera fase se basa en la definición de los aspectos fundamentales del proyecto. En ella se describió el alcance, la motivación, los objetivos y la metodología a emplear durante el trabajo final. Además, se ha de elaborar una planificación temporal del semestre que identifique la duración y las relaciones de dependencia entre las diferentes tareas del programa.
- **PEC 2:** Esta segunda fase trata de la redacción del estado del arte del proyecto. Para ello se deberá buscar y analizar diferentes artículos científicos, académicos o industriales que estén relacionados con la innovación en los sistemas de comunicación empleados para detectar e identificar la presencia de drones y su integración en los sistemas de control aéreo. Esta parte se empleará como un análisis previo del tema a tratar con el fin de recopilar bibliografía, definir un marco conceptual y normativo de la disciplina y describir las aportaciones previas a dicha área de conocimiento.
- **PEC 3:** La tercera fase del proyecto corresponde a la presentación de los distintos sistemas que encajen con la solución a la problemática expuesta. También se presentarán los recursos digitales que presenten toda la información relacionada y se redactarán las diferentes soluciones propuestas que sean técnicamente posibles y viables.
- **PEC 4:** La cuarta fase se basa en plasmar todo el trabajo previo realizado en una memoria. Este documento deberá recoger toda la información necesaria para llevar a cabo la presentación y ejecución de las propuestas.
- **PEC 5:** En esta última parte se realizará la defensa del proyecto por parte del autor.

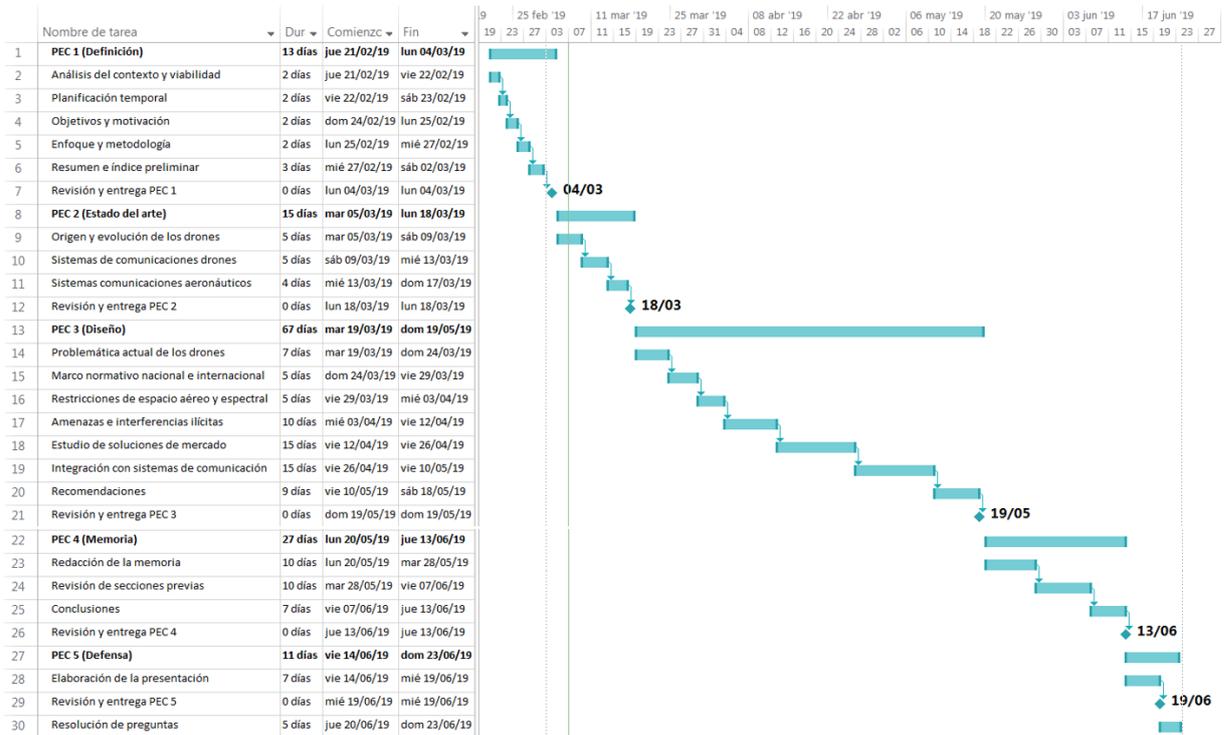


Figura 1: Diagrama de Gantt

## **1.5 Breve resumen de productos obtenidos**

El resultado de este estudio proporciona una amplia visión sobre las tecnologías y sistemas de comunicación que existen actualmente para integrar los drones y la aviación comercial en el espacio aéreo de forma segura y eficiente, teniendo en cuenta las normativas y regulaciones vigentes. Además, se proponen varias soluciones de integración diseñadas por empresas y organismos públicos que, en la actualidad ya están implantadas o se encuentran en fase de desarrollo.

## **1.6 Breve descripción de los otros capítulos de la memoria**

Para entrar en contexto, en el capítulo 2 se hace un breve repaso de los sistemas de comunicación que usan los drones para su control, navegación y posicionamiento, además de los proyectos que existen en la actualidad para integrar, detectar y neutralizar los drones en el espacio aéreo controlado y no controlado.

En el capítulo 3, se explica la evolución de los drones desde sus inicios hasta la actualidad, profundizando en los sistemas de comunicación, así como la clasificación y aplicaciones más comunes de estas aeronaves no tripuladas.

El capítulo 4 trata sobre la problemática que supone el cada vez mayor número de drones surcando el espacio aéreo y la amenaza que implica para el tráfico aéreo convencional, partiendo como base los recientes incidentes ocurridos en aeropuertos tan importantes como el de Gatwick. La finalidad de este capítulo es dar una idea de la importancia que supone encontrar una solución de integración efectiva que dé cabida a las aeronaves tripuladas y no tripuladas en el mismo espacio aéreo.

En el capítulo 5, como paso previo al estudio de integración, se analizan las normativas y regulaciones que existen actualmente sobre los sistemas que deben disponer los drones para comunicarse con el control de tráfico aéreo y para que puedan actuar de manera autónoma en caso de riesgo de colisión con objetos u otras aeronaves. También se repasan las normativas de uso de los drones en el espacio aéreo español.

El capítulo 6 ya entra en el estudio de las diferentes técnicas y tecnologías de comunicación que existen o que están en fase de desarrollo y que pueden formar parte de los sistemas de integración que se estudian el capítulo posterior.

El último capítulo de la memoria muestra el resultado de aunar todos los conocimientos que se han adquirido en los capítulos anteriores para encontrar soluciones que atajen el problema de la integración de los drones con la aviación comercial en distintos escenarios y entornos aeroportuarios. Se muestra además, la estrecha colaboración de organismos públicos y privados de distintos continentes para lograr una solución común a un problema que actualmente se considera global.

## 2. Estado del arte

En este capítulo se va a realizar un repaso de los diferentes proyectos industriales y académicos relacionados con el proyecto, así como una muestra de la situación actual en el ámbito de la investigación y el posicionamiento del trabajo en dicho marco de referencia.

Teniendo en cuenta que los sistemas de comunicaciones de los drones presentan un ámbito de estudio bastante amplio, se estudiarán los proyectos más relevantes relacionados con estos sistemas que ayuden a la integración de estos dispositivos con la aviación comercial en un espacio aéreo común.

### 2.1 Breve repaso de los sistemas de comunicación de los drones

Como una primera aproximación, podemos distinguir dos partes bien diferenciadas en los sistemas de comunicación de un dron que hacen posible su navegación y control: una parte aérea y otra terrestre. La parte aérea, está formada por tres sistemas: la plataforma aérea (el dron), con la carga útil y una parte del sistema de comunicaciones y la parte de tierra, que también incluye diversos sistemas como el de control de la aeronave y su carga útil, el equipo de comunicaciones y la estación de control terrestre, en ocasiones denominada GCS (*Ground Control Station*). En el caso de los drones comerciales, el lado de tierra sería el mando por control remoto que emplea el operador. La GCS permite mostrar la información de todos los sensores a los usuarios correspondientes de dos maneras: una directamente y otra a través de redes de comunicación. Ésta contiene los sistemas y equipos dedicados a la planificación y control de la misión (control del vuelo, carga útil...) y para la distribución de la información a los usuarios externos, comunicaciones con ATC (*Air Traffic Control*), etc. Además, la GCS contiene el sistema de comunicaciones y el enlace de datos en línea de vista LOS (*Line-Of-Sight*) o más allá de la línea de vista BLOS (*Beyond-Line-Of-Sight*), necesarios para acceder a la plataforma aérea o a los sistemas externos. Esta plataforma, por su parte, cuenta a bordo con los sistemas de posicionamiento, navegación, comunicación y enlace de datos. Se necesitan todos estos componentes para lograr el control de vuelo. La carga útil se define por los medios y equipos necesarios para la misión específica, tales como cámaras de video, carga transportable, etc. Respecto a los sistemas de comunicación requeridos para el control de vuelo, se agrupan en dos subsistemas: uno en la parte aérea y otro en la CGS o dispositivo de control del operador remoto. Este subsistema incluye los terminales de los enlaces de datos o el terminal para las comunicaciones por satélite en el caso de vehículos aéreos no tripulados de gran envergadura [4].

De todos los componentes que forman parte de un dron, uno de los más desde el punto de vista del desarrollo de este trabajo son los sistemas de comunicaciones. Sin estos sería imposible, además del control y la navegación del dron, la retransmisión de imágenes, voz y datos a las estaciones terrestres.

Generalmente, los sistemas de comunicaciones de los drones comerciales operan en las bandas de frecuencias de 2,4 GHz y 5,8 GHz. Se tratan de las bandas sin licencia de uso comercial más empleadas en los sistemas inalámbricos como WiFi, por lo que son más susceptibles a las interferencias con otros dispositivos cercanos o incluso entre las frecuencias próximas dentro de la misma banda, sobre todo la de 2,4 GHz. Como se detallará más adelante, un dron normalmente emplea dos enlaces de comunicaciones: un enlace para enviar los datos de control hacia el dron (*uplink*) y otro desde el dron hacia el operador o GCS (*downlink*). Para minimizar el problema de las interferencias en ambos enlaces, la mayoría de los drones comercializados utilizan técnicas

modulación de espectro ensanchado como FHSS (*Frequency Hopping Spread Spectrum*) o por secuencia directa DSSS (*Direct Sequence Spread Spectrum*). En el caso de drones de largo alcance, se emplean otras bandas frecuenciales y técnicas de comunicación distintas. Todos estos aspectos, se detallarán en capítulos posteriores.

### **2.3 Sistemas de comunicación y posicionamiento de drones basados en redes de telecomunicaciones**

Desde la perspectiva de los sistemas de comunicaciones, los actuales enlaces de datos vía radio en las bandas frecuenciales citadas anteriormente, tienen una capacidad de limitada y son vulnerables a interferencias. Para evitar estos inconvenientes, muchos drones utilizan las técnicas de modulación FHSS y DSSS, que permite que muchos operadores diferentes operen en la misma banda de 2,4 GHz sin conflictos. En el caso de FHSS, los receptores son virtualmente inmunes contra las interferencias ya que la frecuencia cambia varias veces por segundo dentro de la misma banda. En este proceso, el receptor reconoce los patrones de cambio de frecuencias que envía el transmisor y elige la frecuencia deseada. Respecto al empleo DSSS, el transmisor envía una señal original de banda estrecha a través de un generador de código de expansión que multiplica la señal por una frecuencia mucho más alta.

Sin embargo, investigadores de la Universidad Nacional de *Pukyong* y de *Tongmyongen*, en Corea del Sur, han estudiado y desarrollado recientemente una técnica de modulación en el enlace *downlink* (entre la aeronave y el GCS u operador de tierra) más eficiente y segura basada en la técnica de modulación SC-FDM (*Single Carrier Frequency Division Multiple Access*). Según el estudio, esta técnica permitiría aumentar el tiempo de vuelo, la velocidad de transmisión de datos y la fiabilidad del enlace de comunicación de los drones, especialmente en aquellos que se utilizan para operaciones de búsqueda y rescate o servicios de entrega de paquetería.

Debido a la cada vez mayor demanda de operaciones más largas y duraderas en el tiempo, las técnicas de modulación utilizadas actualmente tienen ciertas restricciones para satisfacerlas. La propuesta de estos investigadores basada en la modulación SC-FDM para controlar los drones ha sido ampliamente aceptada en las comunicaciones móviles. Se trata de un tipo de modulación híbrida que combina la flexibilidad de asignación de frecuencia y la resistencia multitrayecto de la técnica de multiplexación OFDM (*Orthogonal Frequency-Division Multiplexing*) y otras características importantes de un sistema de una sola portadora. Además, al analizar los resultados de su trabajo, han descubierto que las modulaciones BPSK y QPSK resultan óptimas para la técnica de modulación SC-FDM dentro de la banda de 2,4 GHz [5].

Otra línea de trabajo se centra en el aprovechamiento de la futura red 5G, que poseerá un mayor ancho de banda, una alta velocidad de transmisión de datos y una latencia mucho menor que las redes de telecomunicación actuales. Con la introducción del 5G, los drones poseerán un mayor alcance y una velocidad de respuesta mucho menor, lo que permitirá una mayor precisión en las maniobras, y una velocidad de transferencia de datos y cobertura mucho mayor, lo que hará que los drones permanezcan siempre conectados, incluso entre ellos, formando lo que se denomina *enjambres*. Una de las ventajas de esta tecnología sería, por ejemplo, que los drones de vigilancia para servicios de emergencia podrían volar con una fiabilidad mucho mayor sin necesidad de LOS y operarse con una mayor precisión [6]. En este sentido, el proveedor alemán de servicios de navegación aérea DFS y la operadora de telecomunicaciones Deutsche Telekom, han desarrollado conjuntamente un sistema para permitir la integración segura de los sistemas de aeronaves no tripuladas en el espacio aéreo más bajo (inferior a 150 metros). El Sistema de Gestión de Tráfico de Aeronaves no tripuladas UTM (*Unmanned Aerial System Traffic Management*) localiza los drones utilizando la red de

telecomunicaciones móviles y muestra en una pantalla su situación en el espacio aéreo. Los sistemas de comunicaciones de los drones transmiten los datos de su posición al sistema UTM a través de la red móvil. Estos están equipados con un módem LTE (aunque es previsible que en un futuro usen la red 5G), un módulo GPS y un transmisor móvil. El sistema puede detectar aviones no tripulados hasta una altura de 100 metros y a una gran distancia ya que depende de la cobertura de la red de telefonía móvil existente en la zona [7].

En la misma línea, la empresa española con sede en Valencia, *Embention*, ha desarrollado el sistema *Veronte Autopilot* [8]. Se trata de un sistema de aviónica de alta fiabilidad para el control avanzado de sistemas de aviones no tripulados. Este sistema de control incorpora un conjunto de sensores y procesadores junto con un radioenlace de datos que puede operarse en LOS y BLOS M2M (*BLOS Machine-2-Machine*), con un tamaño y peso reducidos. El sistema está diseñado para el control de cualquier vehículo no tripulado, ya sea multirrotores, helicópteros, de despegue y aterrizaje vertical VTOL (*Vertical Take-Off and Landing*) así como vehículos terrestres. El módulo M2M integrado en el dron se emplea para las comunicaciones 4G, permitiendo su control a través de internet, lo cual posibilita las operaciones BLOS.

#### **2.4 Proyectos de integración de sistemas de comunicación de drones en los sistemas de control de tráfico aéreo.**

En el apartado anterior, se comienza a prever cómo gracias al avance de las nuevas redes de telecomunicaciones y a la tecnología en los sistemas de comunicación de los drones y, por otro lado, al trabajo conjunto entre empresas del sector público y privado, como es el caso comentado antes, hace que se estén desarrollando sistemas para una integración segura entre el tráfico aéreo convencional y el cada vez mayor número de dispositivos aéreos no tripulados en el espacio aéreo.

El sistema de integración UTM que las entidades alemanas están desarrollando, dio sus primeros pasos en el año 2016. Está basado en el rastreador de sensores múltiples *Phoenix DFS*, ideado por la empresa, que se usa para mostrar datos radar para el control del tráfico aéreo. DFS adaptó el rastreador para mostrar correctamente los patrones de movimiento de los drones, que son significativamente diferentes a los de los aviones convencionales. El equipo se puede vincular a los Sistemas de Gestión de Tráfico Aéreo ATM (*Air Traffic Management*) existentes y advertir a los controladores en caso de conflictos o actos de interferencia ilícita. Sin embargo, las capacidades de este sistema van más allá de la simple localización de aviones no tripulados. También es posible integrar en el mismo panel visual, áreas prohibidas e información meteorológica, así como agregar datos de los sistemas de detección, lo que significa que el sistema podría usarse como base para contrarrestar la intrusión de drones en el espacio aéreo [7].

En la misma línea, la empresa *Embention*, está desarrollando el sistema *Veronte UTM* (basado en la tecnología en la nube o *Cloud*), por la que se pueden gestionar operaciones y misiones de drones desde cualquier parte del mundo. La gestión se realiza mediante conectividad 4G integrada en los drones, haciendo posible el control y monitorización de las operaciones desde la nube. También es capaz de habilitar una conexión a internet usando los sistemas en línea de vista de radio (RLOS) tradicionales con conexión a la red en la GCS. De este modo, se hace posible la recepción de información y telemetría en tiempo real de estos aparatos permitiendo monitorizar el vuelo desde un Centro de Control de Tránsito Aéreo.

Por otro lado, la base de datos de *Veronte Cloud* habilita un sistema de registro que permite la identificación del usuario de cada dron que esté dado de alta en su nube a

través de un número de serie, permitiendo a las autoridades acceder a un registro único de plataformas y operadores, así como de los datos de vuelos realizados previamente. Con este fin, los gestores del espacio aéreo controlado tendrán la capacidad de generar zonas de exclusión aérea, aprobar planes de vuelo, monitorizar operaciones y reorientar el tráfico aéreo. Los drones asociados a *Veronte UTM* pueden conocer fácilmente las áreas de exclusión aérea establecidas por las autoridades gracias al sistema de *geofencing*. En dichas áreas estará totalmente prohibido el vuelo, no permitiéndose ninguna operación que las sobrevuele en los períodos establecidos. Del mismo modo, es posible definir zonas de vuelo seguras en las que los operadores podrán realizar cualquier misión deseada siempre y cuando no sobrepase los límites definidos.

*Veronte UTM* está preparado para la integración con distintos operadores de drones a través de su *API*. Se trata de una herramienta en la que pueden intercambiar datos con *Veronte Cloud* para usarlo con cualquier sistema de control compatible. Además, se podrían validar automáticamente los planes de vuelo que cumpliesen las condiciones específicas y, en caso contrario, se les comunicaría a las autoridades para que éstas denegasen el permiso de vuelo en última instancia [8].

La NASA, por su parte, también está trabajando para crear la arquitectura de un sistema UTM que supervisará las operaciones de aviones tripulados y no tripulados en los Estados Unidos y que administre de manera segura el uso generalizado del espacio aéreo a baja altitud (hasta 120 m) y sus operaciones, independientemente del tipo de dron. Una de las principales características de este sistema es la no monitorización permanente por parte de operadores humanos.

El sistema podría proporcionar los datos necesarios para tomar decisiones estratégicas relacionadas con la iniciación, continuación y terminación de las operaciones en el espacio aéreo, de manera que garantizaría que solo los drones autenticados puedan operar dicho espacio. La NASA prevé dos tipos de sistemas UTM: uno portátil, el cual se podría trasladar entre áreas geográficas para, por ejemplo, operaciones de apoyo a la agricultura de precisión o emergencias en casos de desastre. Y un segundo tipo instalado permanentemente, que admitiría operaciones de baja altitud y ofrecería una cobertura fija para un área geográfica concreta. Cualquiera de estos dos sistemas requiere de la supervisión de los sistemas de Comunicación, Navegación y Vigilancia (*CNS, Communication, Navigation and Surveillance*) de los aeropuertos o Centros de Control para asegurar, monitorear y controlar el cumplimiento de los requisitos del sistema, por lo que sería necesario la colaboración estrecha entre los operadores aéreos y los organismos públicos de regulación [9].

En el ámbito internacional en cuanto a sistemas de integración, existe el proyecto JARUS. Se trata de un grupo de expertos de las Autoridades Nacionales de Aviación (ANA) y organizaciones regionales de seguridad de la aviación, cuyo propósito es recomendar un conjunto único de requisitos técnicos, de seguridad y operativos para la certificación y la integración segura de los sistemas de aviones no tripulados en el espacio aéreo y en los aeródromos. El objetivo de JARUS es proporcionar material de orientación con el objetivo de facilitar que cada autoridad defina sus propios requisitos y evitar esfuerzos duplicados [10].

En esta línea, Europa propone la creación del UTM *U-Space*, un espacio comunitario y automatizado de control del tráfico aéreo para drones que vuelen hasta los 150 metros de altura. La actual legislación comunitaria solo afecta a drones con un peso superior a los 150 kilos, mientras que los Estados miembros de la UE son responsables de la normativa para los dispositivos más ligeros. Ese nuevo espacio debería regirse por principios similares a los del control del tráfico aéreo tripulado y debería de funcionar de manera automatizada, con el objetivo de que esté operativo en los próximos años.

El plan se basa en tres pilares fundamentales: el registro obligatorio de los operadores de drones, la identificación electrónica de los aparatos y la dotación del aparato con un software que le impide traspasar las llamadas “geobarreras virtuales” (*geofencing*). Tras los preparativos iniciales y una vez iniciado el vuelo, el dron dispone de un sistema que le permite detectar y evitar posibles obstáculos, como esquivar una bandada de pájaros o una grúa que no estaba localizada en el programa de vuelo. En caso de que el dron invada el espacio aéreo controlado, el Centro de Control de Tránsito Aéreo recibe toda la información de manera automática y adaptaría las rutas de los aviones de pasajeros a estas nuevas circunstancias.

Para desarrollar el sistema UTM *U-Space*, se ha creado una red formada por varios países y organismos europeos para demostrar su utilidad en una amplia gama de actividades con drones y probar su integración en el espacio aéreo junto con la aviación comercial. De esta manera, se pretende reducir el riesgo de las implementaciones, acelerar el tiempo de espera para comercializar nuevos servicios y soluciones, y proporcionar una plataforma para reguladores y autoridades públicas, atrayendo negocios e inversiones adicionales de aviones no tripulados [11].

Para seguir la hoja de ruta de este proyecto se propone la creación de un ente o proveedor denominado UTM *AirMap*, el cual se divide en cuatro proyectos cuyos escenarios de prueba se sitúan en el mismo número de países: el *proyecto GOF USPACE* en Finlandia y Estonia, *DOMUS* en España, *VUTURA* en los Países Bajos y *GEOSAFE* en Francia.

En España, la empresa *AirMap* proporcionará servicios UTM al proyecto *DOMUS* en la provincia de Andalucía, la cual será el escenario para volar los drones en diversas circunstancias y entornos rurales, urbanos, marítimos y aeroportuarios. Para ello cuentan con la participación de la empresa pública Enaire, proveedora actual de servicios de navegación aérea en España y que, junto a varios operadores de drones, pondrán a prueba su capacidad para trabajar en este proyecto. Además, participarán las empresas Indra y la operadora Vodafone, que proporcionarán la tecnología necesaria para el desarrollo de las pruebas. Concretamente, Indra colaborará en el desarrollo de tecnologías bajo una arquitectura abierta que facilitará la integración de sistemas y aplicaciones de terceros y brindará la escalabilidad necesaria para adaptarse a las necesidades de cada cliente, ya sea a nivel municipal, dentro de una región o Provincia o a la autoridad responsable de controlar el tráfico de un país, Enaire en el caso de España [12].

Por su parte, Enaire está colaborando estrechamente junto a la empresa española *Everis Aeroespacial* para la realización de pruebas de integración de sistemas de gestión de drones y de control de tráfico aéreo convencional, en una de las demostraciones más avanzadas de *U-Space* que se han hecho hasta ahora en Europa. En el vuelo de los drones se han utilizado sistemas de *geofencing*, delimitadas con aplicaciones disponibles en el sistema *U-Space* desarrollado por *Airmap* y emitiendo avisos aeronáuticos (NOTAM) a través de Enaire al resto de usuarios del espacio aéreo. Otros ejercicios de simulación que se han realizado han consistido en conectar los sistemas de control de tráfico aéreo de Enaire y el sistema *U-Space* de gestión de los drones operados por Everis en tiempo real, en una misión tripulada de búsqueda y rescate, otra de vigilancia y una evacuación médica urgente por un helicóptero tripulado en la zona de operación. La exhibición ha contado con el apoyo de un pseudopiloto en el Centro Experimental de Demostración de Enaire para simular el vuelo del helicóptero y un controlador aéreo en una posición del sistema para el control de aeronaves (SACTA). El ente público trabaja en la integración segura de todos los usuarios del espacio aéreo bajo el compromiso de impulsar el desarrollo de UTM *U-Space* de prestación

automatizada de servicios de gestión de tráfico para drones operando a baja altitud en España [13].

## 2.5 Proyectos para detectar y neutralizar amenazas en el espacio aéreo controlado y no controlado

Como se ha visto, se está trabajando mucho a nivel nacional e internacional en la idea de integrar los drones en el espacio aéreo junto a la aviación comercial de forma segura mediante una serie de reglas y normativas que, al fin y al cabo, depende en gran medida de la voluntad de los operadores de drones cumplirlas o no. Pero ¿qué pasaría si un operador incumple dichas reglas de forma accidental o para provocar un daño de manera intencionada?

Todos los sistemas y dispositivos electrónicos de hoy en día son susceptibles de ser atacados o interferidos de forma ilícita por parte de terceros. El conocer sus vulnerabilidades es muy importante a la hora de desarrollar herramientas y mecanismos de seguridad para protegerlos, pero, en el caso que ocupa a este proyecto, se trataría de detectar las vulnerabilidades más comunes en los sistemas de comunicación de los drones para intentar neutralizarlos o desactivarlos.

En lo referente a los drones comerciales, sus sistemas de comunicación no están tan protegidos como en el caso de los militares y, en muchos casos, ni siquiera poseen medidas de seguridad, por lo que generalmente tienen un gran número de vulnerabilidades. Por este motivo, existen empresas y organismos que están centrando sus investigaciones en la manera de aprovecharlas para neutralizar los drones ante una posible amenaza. Una técnica muy conocida para interferir en cualquier sistema de comunicación es el *jamming*, cuyo objetivo es interrumpir el enlace de comunicaciones entre uno o más drones y sus operadores, evitando así que penetre en un espacio restringido por la normativa vigente.

En este sentido, la empresa iACiT, presenta un sistema bloqueador de señales de radiocomunicación con el nombre de *DRONEBlocker*. Para que el bloqueo de la señal radio sea efectivo, teniendo en cuenta la diversidad de modelos de drones que existente en el mercado, el bloqueador debe tener la capacidad y flexibilidad de transmitir diferentes señales realizando un barrido de frecuencias dentro de la banda de uso del enlace con distintos tipos de modulación. Además del tipo de modulación y rango de frecuencia, otra forma de interferir en el enlace de comunicación es la de reducir o anular la señal recibida por el dron actuando, por ejemplo, sobre el parámetro de señal a ruido (SNR) del enlace *uplink*.

La mayoría de las bandas de frecuencias para el control de drones comprenden las de WiFi o Bluetooth. Pero también hay modelos que emplean las bandas de HF y VHF para el envío de la telemetría al operador. Por otro lado, y aunque no se use para el control directo del dron, también se emplean las bandas de navegación GPS para que el dron vuele de forma autónoma. Esto es interesante tenerlo en cuenta para anular la capacidad que tienen los drones de ser programados para volar por una ruta prefijada por zonas no autorizadas [14].

Para evitar estas situaciones que potencialmente pueden ser peligrosas, la empresa española Indra ha diseñado un sistema inteligente denominado ARMS (*Anti RPAS Multisensor System*) para la detección e inhibición de señales de drones. Está diseñado para proteger espacios especialmente sensibles como edificios oficiales, plantas industriales o aeropuertos en los que la presencia de este tipo de aeronaves puede representar un problema de seguridad. El sistema de Indra detecta estos dispositivos mediante un radar que ofrece un alcance de varios kilómetros. Adicionalmente, una

cámara infrarroja puede confirmar la información del radar. En una siguiente fase y mediante el uso de un inhibidor de frecuencia en distintas bandas, el sistema ARMS procede a anular la señal de los equipos de geocalización del dron, así como su enlace de comunicaciones con la estación de control desde la que se maneja. Por otra parte, la empresa está implementando mejoras sobre su sistema para ofrecer la máxima precisión a la hora de que el sistema realice la clasificación y seguimiento del dron, combinando el empleo de imágenes térmicas y la escucha radioeléctrica. También está aplicando técnicas de suplantación de la señal de posicionamiento del dron (*spoofing*), para que el sistema pueda asumir el mando y dirigirlo a una zona sin riesgo. Asimismo, está dotando al algoritmo del sistema de capacidad de aprendizaje continuo, de modo que cuanto más se utilice mayor precisión ofrece [15].

Y he aquí un inconveniente. Las mismas técnicas que se emplean para bloquear o interferir en las señales de control de los drones, también pueden hacerlo con los sistemas de comunicación de las aeronaves comerciales y de los sistemas de navegación aérea. Los aeropuertos, torres y centros de control emplean en sus sistemas de comunicaciones, navegación, vigilancia, monitoreo y control frecuencias estandarizadas por organismos internacionales. Aun así, el bloqueador o inhibidor de señales tiene como objetivo provocar interferencias en un sistema concreto, entre otras maneras, realizando un barrido en frecuencia que puede afectar a los sistemas colindantes. Por esta razón, sería deseable que la solución sólo se activase durante un breve periodo de tiempo, el imprescindible para neutralizar la amenaza.

Cuando se trata de intervenir en la señal GPS de un dron como la L1 en 1.575,42 MHz o interferir en ella, cabe recordar que también puede afectar a un avión que la esté usando para posicionarse en el momento del bloqueo. Por lo que la utilización o no de esta técnica debe ser evaluada por el usuario teniendo en cuenta que su uso puede afectar la disponibilidad de la navegación basada en GPS en una región concreta del espacio aéreo. Por otra parte, hay que tener en cuenta que si no se actuase ante estas amenazas, las consecuencias podrían ser aún más catastróficas.

En este trabajo se intentará también dar respuesta a esta problemática mediante el estudio de las diferentes alternativas que pueden emplear los organismos de gestión del espacio aéreo español.

## 3. Origen y evolución de los drones

### 3.1 Historia y evolución de los drones

Para poner en contexto, en este apartado haremos un repaso de los sistemas de comunicaciones que se han estado empleando a lo largo de la historia de estas aeronaves no tripuladas.

En la Primera Guerra Mundial tuvo lugar el vuelo de la primera aeronave no tripulada. Desde el año 1917 hasta la actualidad, el desarrollo de estas aeronaves ha sido objeto de constantes mejoras, siendo hoy en día objeto de una expansión sin precedentes con cientos de dispositivos muy diferentes en peso, dimensiones y otras características, así como innumerables misiones y usos tanto a nivel civil como militar. Hasta el año 1927, el método de guiado de los aviones no tripulados era mediante un giróscopo y un barómetro aneroide disponible a bordo que, una vez conocidos el viento y la distancia al objetivo, calculaba la velocidad del motor requerida para alcanzarlo. En ese año, los británicos desarrollaron un avión monoplano bautizado como controlado por radio durante los primeros momentos del vuelo y después continuaba con un plan de vuelo específico. Entre 1934 y 1943 construyeron nuevos modelos radiocontrolados destinados a ser empleados por el Ejército Reino Unido en su entrenamiento como blancos móviles. Al mismo tiempo y con los mismos fines, EE. UU desarrolló un tipo de dron que supuso un banco de pruebas perfecto para desarrollar y mejorar la incipiente tecnología de control remoto por radio.

Por su parte, durante la Segunda Guerra Mundial, Alemania desarrolló un tipo de misil de crucero que era guiado por un sistema barométrico para regular la velocidad y la altura, y un anemómetro empleado para estimar la distancia. Durante la Guerra Fría, EE. UU, desarrolló una serie de objetivos aéreos no tripulados llamados equipados con cámaras para misiones de reconocimiento. Operaban a baja altitud donde era posible el control por radio bajo línea de visión LOS (*Line Of Sight*) desde una estación de control de tierra, o a altitudes superiores controladas desde otras aeronaves tripuladas. Posteriormente, durante los años 70, desarrolló una versión mejorada equipada con un piloto automático avanzado para operaciones más allá de la línea de vista BLOS (*Beyond Line Of Sight*).

Desde la década de los 70 a la actualidad, el desarrollo de estos dispositivos se iba volviendo cada más sofisticados tanto en los sistemas de comunicaciones de misión como en seguridad. Debido al incremento del riesgo y peligrosidad cada vez mayor de las misiones, empezaron a desarrollarse drones de reconocimiento como el "HALE" (*High Altitude Long Endurance*) de la Fuerza Aérea de EE. UU a finales de los años 60. Durante los años 80, varios países en todo el mundo buscaron extender las operaciones ISTAR (Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimiento) en tiempo real con drones sobre distancias más largas (del orden de 100 km), por lo que fue necesario mejorar la exactitud y fiabilidad de los sistemas de control de vuelo [4]. En la década de 1990, la agencia DARPA de EE. UU. desarrolló el famoso dron de reconocimiento Global Hawk, que tomó su primer vuelo en febrero de 1998 [16]. Su sistema de control y navegación principal consta de un sistema de navegación inercial (INS) y un GPS. En cuanto a los sistemas de comunicaciones, posee enlaces de datos satelitales de banda ancha y enlaces de datos de línea de vista LOS. En la superficie frontal superior del fuselaje, que le da al Global Hawk su apariencia distintiva, alberga la antena de comunicaciones satelitales de banda ancha de 1,2 metros en banda Ku (12 – 18 GHz [17]). Los datos se transfieren mediante comunicaciones satelitales en esta banda, enlaces de línea de vista en banda X y enlaces Satcom en la banda UHF [18].

### 3.2 El dron en la actualidad

Actualmente, un dron sigue siendo un vehículo aéreo sin un piloto en su interior que controle la aeronave, pero pueden ser manejados desde una estación remota por un operador humano situado en tierra o desde otra aeronave. A este tipo de dron se le denomina UAV (*Unmanned Aerial Vehicle*) o RPA (*Remotely Piloted Aircraft*). Además, existen UAV que tienen gran parte del control autónomo, es decir, siguen instrucciones preprogramadas de dónde tienen que dirigirse y qué tienen que hacer, pero no poseen un control en tiempo real como en los RPA, que normalmente los dirige un humano. Esto lleva a concluir que todos los RPA son UAV, pero no todos los UAV son RPA [19]. También se les denominan UAS (*Unmanned Aircraft System*) al conjunto formado por un UA (*Unmanned Aircraft*) controlado a distancia por un conjunto de sistemas formados por estaciones de control denominados UACS (*Unmanned Aerial Control System*) o RPAS (*Remotely Piloted Aircraft System*) en el caso de un RPA o dron.

Dentro de los UAV sin control remoto existen dos versiones, los UAV que han sido programados para que vuelen por una determinada zona recibiendo escasas órdenes del exterior y los UAV que reciben constantes indicaciones de a dónde tienen que dirigirse y qué hacer, pero que no pueden manejarse en tiempo real. Estos tipos de UAV se emplean sobre todo en el sector militar, aunque cada vez son más frecuentes en el sector privado y recreativo.

En el caso de los drones o RPA, su control reside en los mandos que usa un piloto humano que en ese momento maneja el vehículo, aunque también algunos incluyen sistemas de control autónomo, algo que difumina la línea que separa a los drones de los otros tipos de sistemas de aviones no tripulados más complejos. Por este motivo, es conveniente emplear otra clasificación más precisa, como la planteada en la Tabla 1. La manera de controlar estos vehículos se basa en la transmisión de órdenes e instrucciones a través de una antena emisora situada en una estación base remota. Dichas órdenes son recibidas e interpretadas por el dron para actuar en consecuencia. Adicionalmente, los drones más avanzados pueden transmitir al operador o la estación de control información de telemetría como la altitud, velocidad de crucero, situación, etc. También pueden incorporar pequeñas cámaras para ayudar a su navegación y controlar el entorno que lo rodea [20].

Por lo general, un dron posee los siguientes elementos para poder volar y ser controlado de forma remota:



Figura 2: Elementos para controlar y dirigir un dron. Fuente: elaboración propia

A lo largo de este trabajo se usarán diferentes terminologías para definirlos, pero en esencia siempre se estará refiriendo a un vehículo aéreo no tripulado controlado remotamente por un operador humano o por un conjunto de sistemas remotos situados en tierra o en el espacio.

### 3.3 Tipos y aplicaciones de los drones

Como se ha visto en el apartado anterior, bajo el término dron se engloban todas las aeronaves sin piloto a bordo, aunque se pueden clasificar de forma específica en función de su diseño y arquitecturas, distinguiéndose así dos grandes grupos: los de ala fija y los que consiguen la sustentación mediante el empleo de palas rotatorias (de uno o varios rotores), aunque existen algunos modelos denominados híbridos que conjugan ambas soluciones técnicas.

#### 3.2.1 Clasificación

Además de la distinción anterior, los drones también se pueden clasificar según la forma y disposición de sus elementos de sustentación (alas) y de propulsión (rotores), tal y como se muestra en la siguiente comparativa:

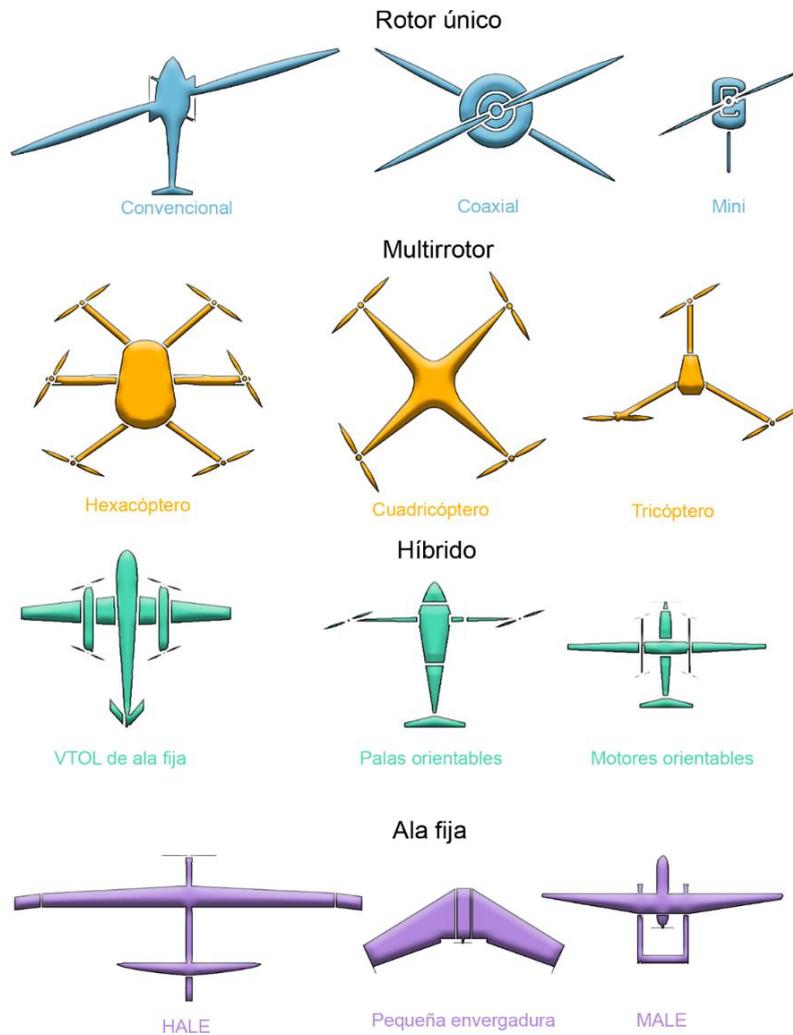


Figura 3: Tipos de drones. Fuente: elaboración propia

Asimismo, los drones también se pueden clasificar de acuerdo con la siguiente tabla:

	Categoría	Peso (kg)	Velocidad Crucero (km/h)	Altitud máxima (m)	Alcance Operativo (km)	Carga máx. Despegue (kg)	Autonomía (horas)
Micro/Mini	<b>Micro (MAV)</b>	< 2	< 111	250	< 10	0.10	1
	<b>Mini</b>	2 - 20		150 - 300	< 10	< 30	< 2
Tácticos	<b>Close Range (CR)</b>	20 - 150	< 111	3000	10 - 30	150	2 - 4
	<b>Short Range (SR)</b>			3000	30 - 70	200	3 - 6
	<b>Medium Range (MR)</b>			3000 - 5000	70 - 200	150 - 500	6 - 10
	<b>Long Range (LR)</b>	150 - 2000	111 - 185	5000	200 - 500	-	6 - 13
	<b>Endurance (EN)</b>			5000 - 8000	> 500	500 - 1500	12 - 24
	<b>Medium Altitude Long Endurance (MALE)</b>			5000 - 8000	> 500	1000 - 1500	24 - 48
Estratégicos	<b>High Altitude, Long Endurance (HALE)</b>	> 2000	> 185	15000-20000	> 2000	2500 - 12500	24 - 48
Misiones Especiales	<b>Lethal (LET)</b>			3000 - 4000	300	250	3 - 4
	<b>Decoys (DEC)</b>			50 - 5000	0 - 500	250	< 4
	<b>Stratospheric (Strato)</b>			20000- 30000	> 2000	Por definir	> 48
	<b>Exo-stratospheric (EXO)</b>			> 30000	Por definir	Por definir	Por definir

Tabla 1: Clasificación de los drones. Fuente: elaboración propia

### 3.2.2 Aplicaciones más comunes

La gran variedad de tipologías se traduce en un amplio rango de prestaciones que confieren a este tipo de aeronaves una gran flexibilidad. De esta forma, los drones se configuran como unas herramientas muy versátiles que pueden adaptarse para realizar numerosas tareas sin más que modificar o añadir algunos dispositivos al aparato denominados carga útil. Así, los drones suponen claras ventajas frente a las aeronaves tripuladas a la hora de afrontar la realización de tareas profesionales, entre las que cabe destacar:

- La disminución de costes tanto en lo referente al precio de la aeronave como a los costes operativos. El precio de los drones y los costes asociados a su operación (combustible, mantenimiento, personal, etc.) son muy inferiores a los incurridos por la operación de aeronaves tripuladas.
- La mejora de la seguridad en el ámbito laboral al poder realizar trabajos en entornos complejos sin exponer al piloto humano.
- La reducción del impacto ambiental de la operación respecto al producido por aeronaves tripuladas puesto que sus emisiones de gases son más reducidas y la contaminación acústica es menor, lo que contribuye a disminuir su afección al medioambiente.
- Mayor flexibilidad y velocidad de despliegue desde cualquier lugar, puesto que normalmente no requieren de unas infraestructuras específicas como aeródromos, durante las fases de despegue y aterrizaje.
- Ampliación del campo de aplicación de las aeronaves, al permitir la realización de nuevas tareas que hasta el momento no han podido ser asumidas por aeronaves convencionales como, por ejemplo, la inspección de estructuras.

Entre las tareas y propósitos relacionados con el uso de drones se encuentran los siguientes:

- **Mensajería:** los drones actuales son capaces de llevar cargas pesadas e incluso para realizar envíos y entregas de paquetería. Esto ayudará a la gente a obtener un servicio inmediato para sus pedidos.
- **Situaciones de emergencia:** los drones destacan por su efectividad en situaciones límites, especialmente en áreas azotadas por desastres naturales o de difícil acceso. Su velocidad de vuelo permite recorrer áreas enormes en muy poco tiempo, permitiendo realizar una evaluación previa de la zona del desastre y posteriormente enviar la ayuda necesaria en forma de víveres, medicamentos, bancos de sangre, etc.
- **Búsqueda y rescate:** La posibilidad de volar a poca altura junto con una cámara de alta calidad que transmite en tiempo real, permite el reconocimiento inmediato de personas perdidas en bosques o montañas, por ejemplo.
- **Control fiscal y de tráfico:** se pueden emplear para sobrevolar terrenos o propiedades y detectar cambios que pueden ser objetos de sanción si no poseen la correspondiente licencia de obra o construcción. Asimismo, se están empleando en carreteras para detectar y filmar comportamientos ilegales por parte de los conductores, ahorrando el coste que supone enviar un helicóptero tripulado para el mismo fin.
- **Vigilancia fronteriza:** el uso de drones junto a las Fuerzas de Seguridad del Estado, permiten vigilar en tiempo real el espacio fronterizo. Estos dispositivos, dotados de la tecnología necesaria en cada caso (cámaras térmicas, de movimiento, de visión nocturna...) envían los datos recopilados a un centro de control donde se reproducen para evaluar el posible despliegue de operativos, mejorar sus capacidades o encontrar puntos ciegos en la frontera.
- **Agricultura:** Los agricultores los pueden emplear para el control y vigilancia de los cultivos mediante imágenes multispectrales, control de la eficiencia del riego, identificación de las características del terreno o mejorar los trabajos de la maquinaria. También permiten la localización temprana de plagas o malezas o el control del rebaño.
- **Control de incendios forestales:** un dron puede supervisar una amplia zona boscosa desde el aire, sin riesgo de vidas humanas y reduciendo los costes comparado con los activos humanos o medios de transportes como helicópteros. Además, los drones pueden trabajar de forma individual o en colaboración (mediante técnicas de *swarm intelligence*) en la coordinación de retenes en caso de incendios, en la detección de focos activos y en el estudio aéreo de la evolución del fuego.
- **Geología:** permiten analizar la actividad volcánica tomando muestras del interior del volcán y de las cenizas que emite, permitiendo predecir erupciones logrando alertar con mayor anticipación a las poblaciones cercanas, sin riesgo para los vulcanólogos. Asimismo, se han utilizado drones para estudiar e intentar predecir la ruta de un huracán.
- **Biología:** Se han utilizado estos aviones teledirigidos para reproducir la ruta de aves en libertad. Se registra el vuelo con un GPS incorporado en el ave y luego

se reproduce con un dron. Los investigadores pueden determinar de esta manera la razón del recorrido animal al tener la posibilidad de registrar exactamente las características de la zona donde vuela.

- **Manipulación de residuos peligrosos:** Permiten la manipulación, limpieza y estudio de materiales nocivos para la salud de las personas. En Japón, se utilizaron para obtener una vista precisa del interior del reactor nuclear de Fukushima con el objetivo de elaborar un plan de limpieza y prevención de futuras fugas de radiación.
- **Expansión de internet:** Google planea el proyecto *SkyBender*, que investiga las posibilidades de propagar mundialmente internet con una red de drones no tripulados (*Solara 50*), cuyas alas alcanzan una envergadura de 50 metros y están impulsados con energía solar. En teoría, pueden volar ininterrumpidamente durante cinco años con la energía solar que recogen sus paneles que cubren por completo su fuselaje. Con este sistema se pretende alcanzar unas velocidades de datos unas 40 veces superior a las del actual 4G [21] [22] [23] [24].

## 4. Problemática de los drones

### 4.1. Incidentes con aeronaves comerciales

Desde los inicios de la aviación comercial, siempre ha existido la amenaza de que un pájaro u otro ave que esté volando en las inmediaciones aeroportuarias, impacte o colisione contra un avión durante la maniobra de despegue o aproximación al aeropuerto. En este sentido, se calcula que cada año tienen lugar más de 10.000 choques entre pájaros y aviones en todo el mundo. Además de resultar fatales para las aves, estos impactos, coloquialmente conocidos como *bird strikes*, generan pérdidas millonarias para las aerolíneas por los daños producidos a las aeronaves, las cancelaciones y los retrasos de vuelos [25] [26]. En ocasiones han llegado a causar víctimas mortales. El 90 % de las colisiones con aves se producen en las proximidades de los aeropuertos, por debajo de los 150 metros de altitud y durante el despegue o el aterrizaje, lo que ha obligado a las autoridades a adoptar diferentes medidas para ahuyentarlos como grabaciones de sonidos, destellos de luz, halcones entrenados o sensores para evitar golpes en los parabrisas de la cabina y, sobre todo, daños en los motores.

Pero, de un tiempo a esta parte, en el cielo planea una amenaza mayor que, potencialmente puede ser deliberada y más complicada de neutralizar: los drones.

Según la Administración Federal de Aviación de los EE.UU. (FAA), se prevé que la cantidad de drones de aficionados registrados en el país americano aumentarán de 1,1 millones de unidades en 2017 a 2,4 millones en 2022. Los registros de los drones comerciales totalizaron 110.604 en 2017 y se proyecta que aumentarán a 451.800 unidades en 2022 [27]. En 2017, la FAA exigió que los propietarios de drones aficionados y comerciales que pesen menos de 25 kg deben ser registrados y marcados con un número de registro y, los aviones más grandes, deben registrarse en la FAA como avión convencional.

En la Unión Europea (UE) se estima que existe un parque de entre 1 y 1,5 millones de drones de uso civil, que se ha alcanzado fundamentalmente por un fuerte crecimiento de los drones de uso recreativo, con incrementos superiores al 100% anual en los últimos años. De las cifras anteriores, se calcula que 10.000 unidades se corresponden con drones de uso profesional [28].

A la vista de estos datos, cabe prever que con el aumento de estos dispositivos aéreos no tripulados surcando el espacio aéreo, las probabilidades de que se produzcan un daño o colisión con un avión comercial aumentan en la misma proporción.

La incursión en el espacio aéreo controlado de un vehículo aéreo no tripulado, no suele ser por un despiste del operador, pero puede ser que ocurra de manera intencionada por su parte o por un fallo en los mecanismos de navegación y control del aparato. Si un dron, aunque sea de pequeño tamaño, colisiona con una aeronave a más de 200 km/h, las consecuencias pueden ser fatales, sobre todo si el impacto tiene lugar durante el despegue o aterrizaje, tal y como se demuestra en el siguiente apartado.

En España, es necesaria una autorización de la Agencia Estatal de Seguridad Aérea (AESA) para poder volar o hacer operaciones con este tipo de aparatos próximas a los aeropuertos. Pero hay gente inconsciente que se aproxima o incluso atraviesa zonas aeroportuarias restringidas para, por ejemplo, grabar aviones o, directamente, gente que lo hace de forma consciente para provocar el caos, como ocurrió en el aeropuerto de Londres. Para que esto no ocurra, hay fabricantes de drones que los dotan de la

capacidad para limitar por dónde pueden volar y las zonas críticas aeroportuarias suelen estar restringidas. Lo hacen con ayuda del GPS y con software específico aplicando una técnica denominada *geofencing*, que se explicará más adelante. Pero no todos los drones poseen esta capacidad, sobre todo los que están fabricados de forma casera o en países que carecen de legislación al respecto.

Aun así, si alguno de estos drones pretende usarse para causar daños de forma intencionada, existen sistemas para neutralizarlos empleando, por ejemplo, inhibidores de frecuencias, pero, si la aeronave sigue una ruta ya programada, habría que interferir en sus sistemas de control o en los de posicionamiento GPS con técnicas que se describen en el capítulo 7.

## 4.2. Daños producidos a las aeronaves

En octubre de 2017, un avión no tripulado chocó con un avión comercial en Canadá, golpeando una de las alas del avión. El avión sufrió daños menores, pero pudo aterrizar con seguridad [29].

En abril de 2018, un dron que estaba siendo pilotado desde una playa cercana al Aeropuerto de Alicante, impactó con un avión comercial sin producir, afortunadamente, daños personales a los pasajeros. [30].

Como se puede apreciar en estas noticias, los daños ocasionados a los aviones y al pasaje no han sido relevantes por las circunstancias en las que se produjeron los impactos o por el tamaño del dron, pero el riesgo está ahí e irá a peor. Aun así, ¿cuánto daño podría provocar realmente un dron a un avión comercial?

Para demostrarlo, el grupo de Física de Impacto del Instituto de Investigación de la Universidad de Dayton de los EE. UU, liderado por Kevin Poormon, ha realizado importantes investigaciones en este campo, analizando la capacidad de resistencia de los diferentes tipos de blindaje en aeronaves espaciales, así como el impacto provocado por la basura espacial viajando a más de 6 km/s. Además, están ayudando a las compañías aéreas a proteger sus aeronaves contra el impacto de objetos, desde aves hasta drones. En esta línea, los investigadores simularon una colisión en el aire entre un cuadricóptero DJI Phantom 2 (uno de los más vendidos y populares del mundo) de 1 kg de peso y una aeronave comercial que viajaba a unos 380 km/h [31]. Tras realizar la prueba descubrieron que el dron, no sólo se desintegró en el impacto, sino que rompió el borde de ataque del ala realizando un importante agujero, dañando y dejando el ala inservible, tal y como se muestra en la siguiente imagen:



Figura 4: Daños producidos por un dron al colisionar con un ala de avión. Fuente: [31]

Otra investigación realizada por la alianza para la seguridad ASSURE (*Alliance for System Safety of UAS through Research Excellence*) junto con la Autoridad Federal de Aviación de los EEUU (FAA) sugirió que los drones podrían causar más daño que una colisión con una ave ya que, además de daños estructurales, las baterías de litio que los alimentan no se rompen en el impacto, sino que se alojan en las estructuras del avión presentando un riesgo potencial de incendio [31].

Para demostrarlo, realizaron una serie de simulaciones que luego plasmaron en diferentes informes. En uno de ellos, se evaluaba la gravedad de la colisión de dos aeronaves no tripuladas, un cuadricóptero modelo Phantom 3 de DJI de 1,2 Kg y un dron de ala fija Lancaster Hawkeye III de 1,8 kg de peso chocando con un avión comercial Boeing 737 y un avión privado Learjet 31A. Los resultados de los posibles escenarios de impacto se analizaron y categorizaron en función de la gravedad del mismo en varios niveles:

- **Nivel 1:** cantidad mínima de daño localizado.
- **Nivel 2:** daño significativo visible en la superficie externa de la aeronave con algunos daños en los componentes internos, pero sin una ruptura apreciable de la superficie.
- **Nivel 3:** la superficie exterior de la aeronave está comprometida de tal manera que se podrían introducir objetos extraños en la estructura del avión.
- **Nivel 4:** abarca todos los daños anteriores, así como comprometer parte de la estructura principal del avión.

En la Figura 5 se muestra los daños ocasionados por un cuadricóptero de 1,2 kg (izquierda) y los que produce un dron de ala fija de 1,8 kg (derecha), a un Boeing 737:

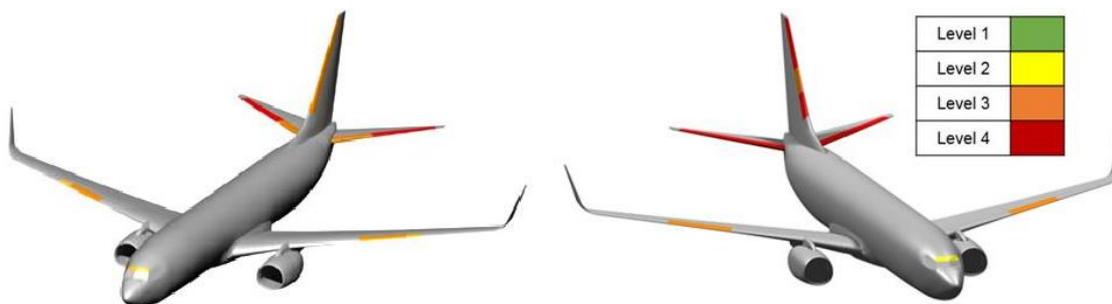


Figura 5: Niveles de daños producidos por un dron de 1,2 kg y 1,8 kg. Fuente: [31]

Según las simulaciones, el impacto producido con el avión volando a 250 nudos (unos 460 km/h) puede provocar un nivel de severidad de daño medio-alto (3-4) en el estabilizador horizontal y vertical, medio (2-3) en el borde delantero del ala y medio-bajo (2) en el parabrisas, según se revela en la Figura 5 que ilustra los niveles de gravedad del impacto en diferentes ubicaciones en el fuselaje de avión de transporte comercial analizado [32].

También se realizaron simulaciones respecto al daño producido si el dron se introduce en los motores del avión. En este caso, se usaron los mismos drones que en el caso anterior, pero, se comprobaron las consecuencias que tendría el impacto sobre 5 motores de distintos fabricantes y tamaños en diferentes condiciones de vuelo. Los resultados de la simulación en el caso del despegue se muestran en la siguiente imagen:

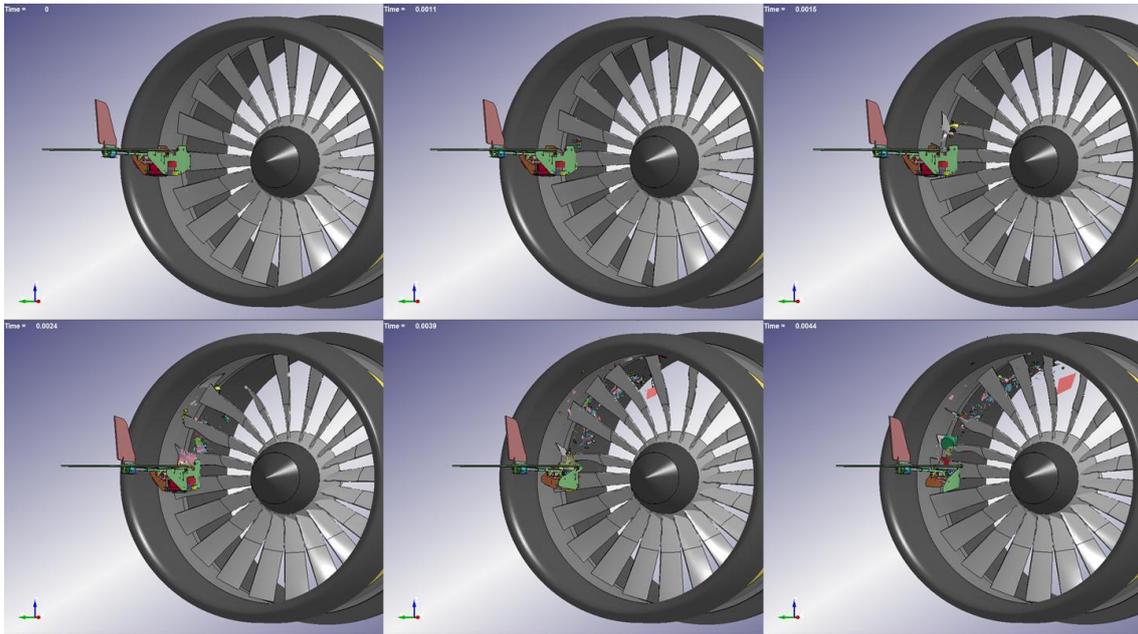


Figura 6: Cinemática de la ingesta de un dron de ala fija durante el despegue. Fuente: [33]

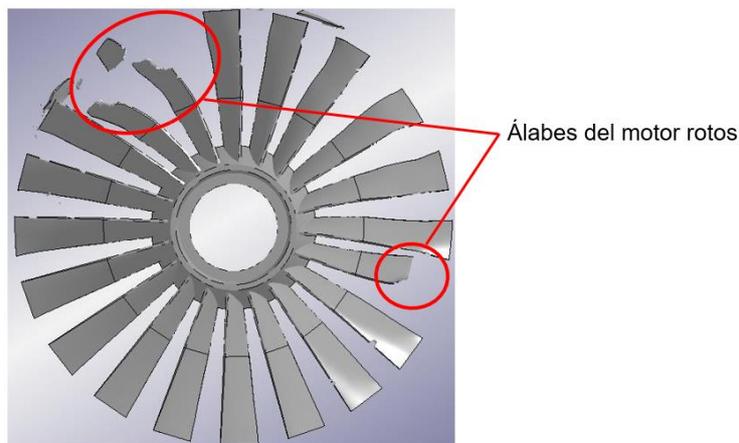


Figura 7: Detalle de los daños producidos a los álabes en el impacto. Fuente: [33]

Como era de esperar, las consecuencias de un impacto de este tipo en el motor del avión son catastróficas para la seguridad del vuelo. En este caso los daños oscilaron entre los niveles 1-3. Las pruebas de nivel de daño para los tres componentes principales de un dron (motor, cámara y batería) mostraron que el daño incurrido por estos depende en gran medida de la manera en que impacten en los álabes. Como se esperaba, el escenario de despegue es el peor de los casos, ya que es cuando los motores está a máxima potencia y por tanto cuando tienen mayor velocidad de giro.

Las conclusiones de este estudio son que, en los daños estructurales al fuselaje, la velocidad de impacto contribuyó a una mayor cantidad de daño que la masa de los drones, aunque al incrementar cualquiera de los parámetros se correlacionan con una mayor severidad y extensión del daño del fuselaje. Asimismo, se considera que las velocidades de los aviones por encima de las velocidades mínimas tanto en el despegue como en el aterrizaje se consideran críticas para drones con masas iguales o superiores a 1,2 kg.

En el caso de los daños al motor, depende de muchas variables como el tipo de rotor, la velocidad de rotación, los componentes del dron que impactan, la orientación del

impacto, la ubicación del motor, etc. Pero, como era de esperar, el daño del ala fija tiende a ser mayor que el del cuadricóptero debido a sus componentes centrales más pesados y grandes, particularmente el motor y la cámara [33].

En vista de las consecuencias catastróficas que el impacto de un dron puede tener sobre la seguridad en el vuelo de una aeronave comercial, en capítulos posteriores se resumirán las normativas y regulaciones que están adoptando las distintas autoridades a nivel nacional e internacional y las medidas que están llevando a cabo para intentar integrar de forma segura los drones y los aviones comerciales en el espacio aéreo controlado y no controlado.

## 5. Marco normativo de drones y aviones comerciales

En la actualidad, las operaciones civiles con drones se realizan en zonas del espacio aéreo separadas de las utilizadas por la aviación convencional (espacio segregado). Esto se traduce en la necesidad de una cierta coordinación entre ambos tipos de aeronaves a la hora de afrontar las operaciones con seguridad. Sin embargo, en el medio y largo plazo, la normativa y los distintos desarrollos tecnológicos que actualmente están en marcha, permitirán que los vuelos de los drones se extiendan a zonas del espacio aéreo transitadas por la aviación tradicional, a una altitud superior a los 4.000 m. Así, los drones deberán coexistir con el resto de usuarios y gestores del mismo, entre los que se encuentran las compañías aéreas, los proveedores de servicios de navegación aérea y los gestores aeroportuarios.

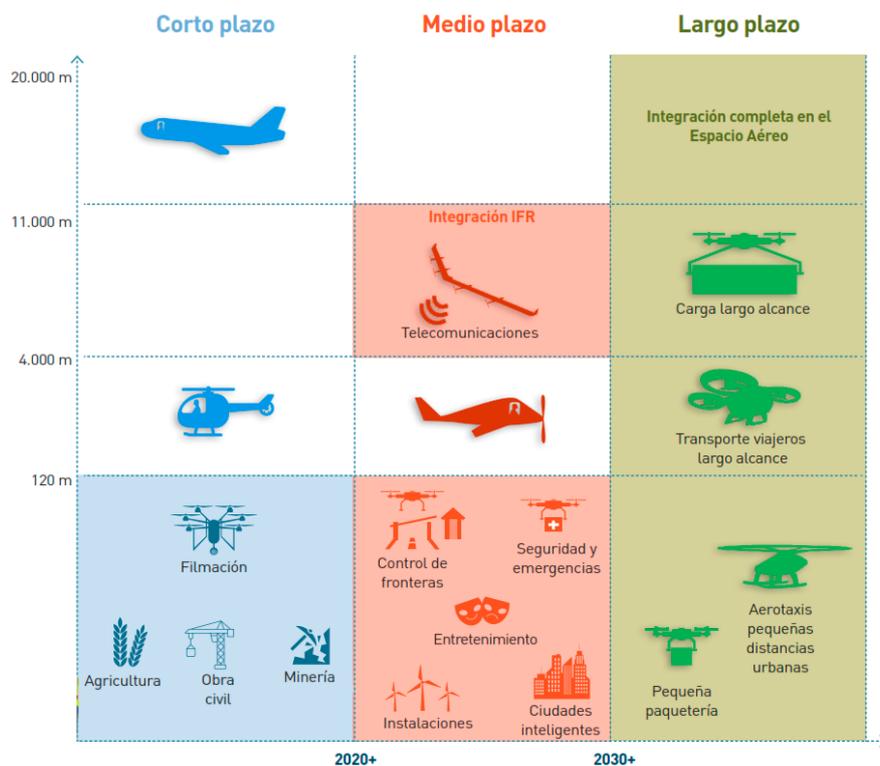


Tabla 2: Evolución prevista de los drones en el espacio aéreo. Fuente: elaboración propia

Desde el punto de vista de los sistemas de comunicaciones, la integración de los drones en el espacio aéreo controlado debe tener en cuenta una gestión eficiente del espectro radioeléctrico, permitiendo a los usuarios que dispongan de los canales de comunicación necesarios para llevar a cabo el control remoto de estas aeronaves, el intercambio de los datos capturados por sus sensores y la coordinación con los sistemas de gestión de tráfico aéreo actuales. En este sentido, el crecimiento previsto a medio plazo llevará a la operación simultánea de un número elevado de drones que requerirán una ordenación más estricta del uso de las comunicaciones de radio para permitir que, entre otros aspectos, puedan cumplirse los requisitos de estabilidad y seguridad de los enlaces de control y garantizarse que la actividad del sector sea compatible con la del resto de usuarios del espectro radioeléctrico.

## 5.1. Marco regulatorio internacional

En abril de 2005, dada la reciente preocupación por el auge de los dispositivos aéreos no tripulados, se realiza una consulta a los Estados y organizaciones internacionales sobre las actividades previstas con estos vehículos en el espacio aéreo civil, así como los procedimientos para evitar peligros a las aeronaves comerciales. Por este motivo, se plantean la expedición de autorizaciones especiales para los vuelos internacionales civiles con drones, entre otras medidas. Al año siguiente, la Organización de Aviación Civil Internacional (OACI) mantiene la primera reunión a alto nivel para tratar de determinar su papel en la futura reglamentación sobre los drones [34].

En 2007, este organismo internacional avanza sobre especificaciones técnicas para operaciones con aeronaves no tripuladas y se ahonda en la necesidad de garantizar la seguridad y la uniformidad con las operaciones de la aviación civil internacional. Finalmente, tras varias reuniones se concluye que este organismo debería coordinar la elaboración a nivel mundial de un concepto normativo sobre los drones a través de Normas y Métodos Recomendados (SARPS, *Standards and Recommended Practices*) y contribuir en la elaboración de especificaciones técnicas, así como identificar necesidades de comunicación para la actividad sobre las aeronaves no tripuladas. Además, se llega a la conclusión de que las aeronaves no tripuladas son, efectivamente, aeronaves y, por consiguiente, los SARPS existentes para la aviación convencional se les debería aplicar en gran medida [34]. La integración completa de los drones en los aeródromos y en las diversas clases de espacio aéreo exigirá, no obstante, la elaboración de SARPS específicos sobre drones para suplementar los ya existentes.

En 2011, la OACI desarrolla la Circular 328 AN/190 en la que se informa a los Estados sobre la perspectiva que tiene respecto de la integración de los drones en el espacio aéreo no segregado (aquel que deben compartir junto a la aviación comercial) y en los aeródromos. También se alienta a los Estados a que contribuyan a la elaboración de una política sobre drones proporcionando información sobre sus propias experiencias relacionadas con estas aeronaves.

En esa circular, se recuerda que, según el Artículo 8 del Convenio de Chicago del año 1944 sobre Aviación Civil Internacional “Ninguna aeronave capaz de volar sin piloto volará sin él sobre el territorio de un Estado contratante, a menos que se cuente con autorización especial de tal Estado y de conformidad con los términos de dicha autorización” [35, p. 22]. Por tanto, ya se asientan las bases para poder pilotar los drones con la correspondiente autorización. Además, se especifica que todas las aeronaves no tripuladas, ya sean pilotadas a distancia, autónomas o combinación de ambos, están sujetas a las disposiciones de dicho Artículo. Por tanto, la OACI ya prevé que los drones puedan integrarse en el futuro con los sistemas de la aviación civil convencional mediante algún sistema similar al actual de gestión del tráfico aéreo ATM (*Air Traffic Management*).

La OACI clasifica a los drones en dos categorías:

- **Sistema de aeronave pilotado a distancia (UAS):** conjunto de elementos configurables que consiste en una aeronave pilotada a distancia (UA, RPA o dron), su estación piloto asociada (UACS), los enlaces de comando y control requeridos y cualquier otro elemento del sistema según sea necesario, en cualquier punto durante la operación del vuelo.
- **Avión autónomo:** un avión no tripulado que no permite la intervención del piloto en la gestión del vuelo [34].

Este trabajo se centrará principalmente en la primera categoría, es decir, en todas aquellas aeronaves no tripuladas pilotadas a distancia (dron) ya sean controladas por un operador humano o un sistema de control remoto.

## 5.2 Régimen de regulación de los drones

El régimen de regulación que se describe a continuación está siendo estudiado por la OACI, pero también se basan en las regulaciones de la FAA de los EE. UU. y están en continuo cambio. El objetivo final del marco será lograr un entorno en el que la operación de los drones no requiera atención humana, en el sentido de que estos dispositivos son capaces de detectar la presencia de otros objetos voladores, ya sean aviones tripulados u otros drones, y tomar las medidas adecuadas para evitar cualquier colisión. En este documento regulatorio, se definen varias categorías para operar con drones:

- **Categoría abierta:** comprende la gran mayoría de los vehículos aéreos no tripulados. En un primer paso, la prevención de colisiones entre estos aviones no tripulados y aeronaves tripuladas se logrará mediante la segregación del espacio aéreo (separación física). Estos dispositivos, estarán diseñados para operar en altitudes bajas, por debajo de los sectores del espacio aéreo utilizados con fines de aviación civil y manteniendo una distancia segura en el espacio reservado para las operaciones del aeropuerto. Los vuelos dentro del alcance visual en línea de vista (VLOS) pueden respaldar la actividad de los drones cerca o incluso dentro de los sectores del espacio aéreo abiertos a la aviación civil.

En España, los vuelos VLOS pueden realizarse a una altitud máxima de 120 metros y fuera de las zonas específicas como aeropuertos, zonas protegidas por razones medioambientales o de seguridad, etc. También se prohíbe el sobrevuelo de aglomeraciones de personas (salvo los drones de menor peso) [36].

- **Categoría específica:** Hasta que los drones sean capaces de asegurar su propia separación con otras aeronaves, la segregación del espacio aéreo y las operaciones VLOS seguirán siendo el principal medio para asegurar la separación. Este método consiste en exigir que el piloto remoto mantenga contacto visual permanente con su aeronave y tome las medidas necesarias para evitar una colisión entre esta última y la aeronave convencional u otro dron.

En España, operar en esta categoría implica conocer un manual de operaciones obligatorio y debe ser aprobado por la autoridad aeronáutica basada en el riesgo específico de la operación.

- **Categoría certificada:** La categoría certificada comprende aquellos drones que se espera que operen de manera rutinaria dentro del espacio aéreo abierto a la navegación aérea civil. El entorno ATM actualmente es excesivamente complejo, tanto desde una perspectiva operativa como regulatoria, y el objetivo principal debe ser lograr la integración sin agregar otra capa de complejidad. En esta categoría se podrán realizar operaciones de vuelo más allá del alcance visual (BVLOS) basados en métodos que permitan a los drones volar dentro del espacio aéreo de la aviación civil sin la necesidad de que un operador humano mantenga un contacto visual permanente con el dron. El personal de los Servicios de Tránsito Aéreo (ATS) deberá proporcionar instrucciones a las aeronaves bajo su responsabilidad para evitar que ingresen en los límites restringidos del espacio aéreo.

Para operar en esta categoría en España, se debe contar con una licencia de piloto remoto, una certificación de drones, conocer el manual obligatorio de operación y operar bajo el régimen regulatorio similar al de la aviación convencional.

- **Gestión del tráfico UAS (UTM):** será necesario implementar algún tipo de infraestructura para garantizar la seguridad de las operaciones de los drones también fuera del espacio aéreo abierto a la aviación civil. El propósito de dicha infraestructura sería principalmente mantener a los drones separados unos de otros, pero también de los aviones, como los helicópteros que vuelan a baja altitud con los que pueden necesitar compartir el espacio aéreo. Esa infraestructura también debe integrar una función que evite que los drones ingresen en los sectores del espacio aéreo donde su operación está prohibida.

De aquí nace el concepto de UTM (*UAS Traffic Management*) que se tratará en el siguiente capítulo.

### 5.3 Aspectos normativos en las comunicaciones de drones con ATC

En 2009, el Sector de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-R, por sus siglas en inglés), en su informe M.2171, definió las características de los sistemas de aeronaves no tripuladas y los requisitos de espectro para respaldar su operación segura en el espacio aéreo no segregado desde el punto de vista de los sistemas de comunicación y de la cantidad de espectro radioeléctrico requerido para integrar de forma segura los procedimientos actuales de control de tráfico aéreo (ATC) y, al mismo tiempo, mantener los niveles de seguridad de los vuelos [37].

Para la ITU, el papel que juega las comunicaciones en los sistemas UAS son claves para la seguridad de las operaciones en el espacio aéreo y ello es debido a la naturaleza remota del operador humano. Por tanto, tal operación se basa en la seguridad y fiabilidad de las comunicaciones, para lo cual, resulta necesario definir el espectro radioeléctrico y los enlaces de comunicaciones necesarios para que ambos tipos de aeronaves operen en el espacio aéreo sin problemas. Con los años, la normativa ha ido sufriendo modificaciones adaptándose a los nuevos desafíos y retos tecnológicos que comportan el uso de drones en el espacio aéreo.

En los siguientes apartados se resumen los aspectos normativos fundamentales de las comunicaciones de los drones en el espacio aéreo controlado.

#### 5.3.1 Descripciones generales del sistema y terminología

Para entender esta normativa regulatoria, se definen a continuación los conceptos básicos y terminologías empleadas:

- **RPA, UA o dron:** Se refiere a todos los tipos de aeronaves no tripuladas controladas de forma remota.
- **UACS (Estación de Control de Aviones no tripulados):** instalaciones desde las que se controla un UA de forma remota. También puede hacer referencia al operador humano que controla el dron con un mando.
- **Enlace de comando y control (Enlace C2):** enlace de comunicaciones entre la UA y la UACS que llevan los telecomandos (desde el piloto a la UA) y la telemetría (desde la UA al piloto).

- **Comunicaciones de control y de carga no útil (CNPC):** enlaces de radio utilizados para intercambiar información entre la UA y la UACS, que garantizan una operación de vuelo segura, confiable y efectiva de la UA. Pueden llevar diferentes tipos de información como mensajes de comando y control, datos de telemetría de carga no útil (CNPC), soporte para ayudas a la navegación, retransmisión de voz de control de tráfico aéreo, retransmisión de datos de servicios ATC, seguimiento de objetivos, datos radar meteorológico, datos de enlace descendente de vídeo, etc.
- **S&A/ DAA (Sense & Avoid/ Detect And Avoidance):** son las siglas anglosajonas de “Detectar y Evitar”, es decir, aquella capacidad que debe poseer un dron de primero, detectar y después evitar obstáculos u otras aeronaves de forma automática o, proporcionar las correspondientes alertas al piloto remoto para evitar una colisión. S&A/DAA equivale a la capacidad de “Ver y evitar” que los pilotos humanos de aviones convencionales deben tener para asegurar la separación de las aeronaves con otros aviones en el aire, con el terreno u obstáculos cercanos.
- **UAS (Sistema de Aeronaves no tripulados):** es un sistema formado por el propio UA o dron, las estaciones de control de aeronaves no tripuladas (UACS), el subsistema de comunicaciones de control de tráfico aéreo (ATC), el subsistema S&A y la carga útil como, por ejemplo, una cámara de video.
- **RLOS (Línea de Visión de Radio):** es el radioenlace en línea de vista entre la UA y la UACS.
- **RBLOS (Más Allá de la Línea de Visión de Radio):** se define como el enlace de radiocomunicación indirecto (sin línea de visión directa) entre la UA y una UACS apoyado normalmente por los servicios de comunicación por satélite.
- **Traspaso de operaciones o hangover:** es la transferencia de un enlace de comunicación RLOS de un UACS a otro UACS o, de un enlace de comunicación de RLOS directo a otro indirecto RBLOS o viceversa.
- **Enlace ascendente (Uplink):** permite enviar telecomandos a la aeronave para el control del vuelo y la navegación del dron.
- **Enlace descendente (Downlink):** envía la información de telemetría, (como el estado de vuelo y del dron) hacia la UACS. También puede emplearse para enviar datos de video en *streaming* de una cámara integrada en el dron. Este enlace también puede llevar los datos del subsistema S&A por lo que tendría que soportar velocidades de datos del orden de Kb/s o Mb/s.

### 5.3.2 Radioenlaces y arquitecturas necesarias para operaciones con drones

Para las operaciones seguras de los drones en condiciones de VLOS y BVLOS, se requieren tres tipos de radiocomunicaciones entre el UA y UACS:

- Retransmisión de control de tráfico aéreo ATC
- Comando y control (Enlace C2)
- Apoyo a la función de S&A (Detectar y evitar)

En el espacio aéreo no segregado, se requerirá un enlace entre el control de tráfico aéreo ATC y el UACS a través del dron (denominado Retransmisión ATC) para transmitir las comunicaciones del ATC y las comunicaciones aire-aire recibidas y transmitidas por el dron.

Para comunicarse con ATC, el dron usaría el mismo equipo que un avión tripulado convencional. Esta normativa solo considera el enlace descendente que lleva la información ATC de la UA al UACS y el enlace ascendente de la UACS a la UA, lo que permite que la UACS se comunique con el ATC.

Como estas comunicaciones son críticas para una administración segura de los espacios aéreos controlados, especialmente en áreas de aproximación de aeropuertos con alta densidad de aeronaves, los futuros estándares de la OACI serán obligatorios para este tipo de comunicaciones.

Se espera que la velocidad de transmisión de datos para un solo UAS esté en función de los requisitos necesarios para:

- El intercambio de comunicaciones ATC-UAS que a su vez son una función directa de las categorías del espacio aéreo.
- El Enlace C2 (Comando y control) del UAS que a su vez son una función directa del diseño de los sistemas UAS y su grado de automatización y autonomía.
- El sistema S&A, que a su vez va en función de la categoría de espacio aéreo, el entorno del terreno (los UAS son responsables en todo momento de detectar y evitar el terreno cuando se opera a bajas altitudes) y el clima, ya que los UAS deberían ser capaces de detectar y evitar áreas con condiciones meteorológicas adversas.

En cuanto a los requisitos de espectro de frecuencias para la transmisión de estas señales, la ITU-R lo ha calculado teniendo en cuenta el número de drones que podrían desplegarse hasta el año 2030 a diferentes altitudes incluidas las inmediaciones aeroportuarias, los datos que se transmiten para el enlace C2 (comando y control), la retransmisión ATC, el S&A y el tipo de datos que se envían tanto de carga útil y no útil (video e información meteorológica). Una vez aplicadas diferentes metodologías, los requisitos de ancho de banda, así como los diferentes tipos de enlaces, son los que se muestran a continuación:

**Requisitos y enlaces involucrados para la línea de visión (LoS)**

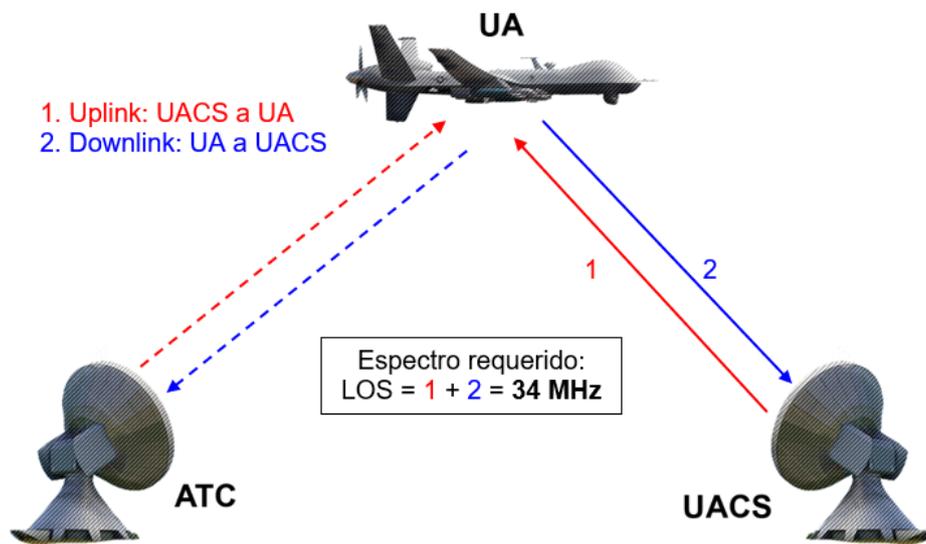


Figura 8: Radioenlace LOS en un UAS. Fuente: [37]

**Requisitos de espectro y enlaces implicados para más allá de la línea de visión (BLOS) vía satélite (con procesamiento a bordo)**

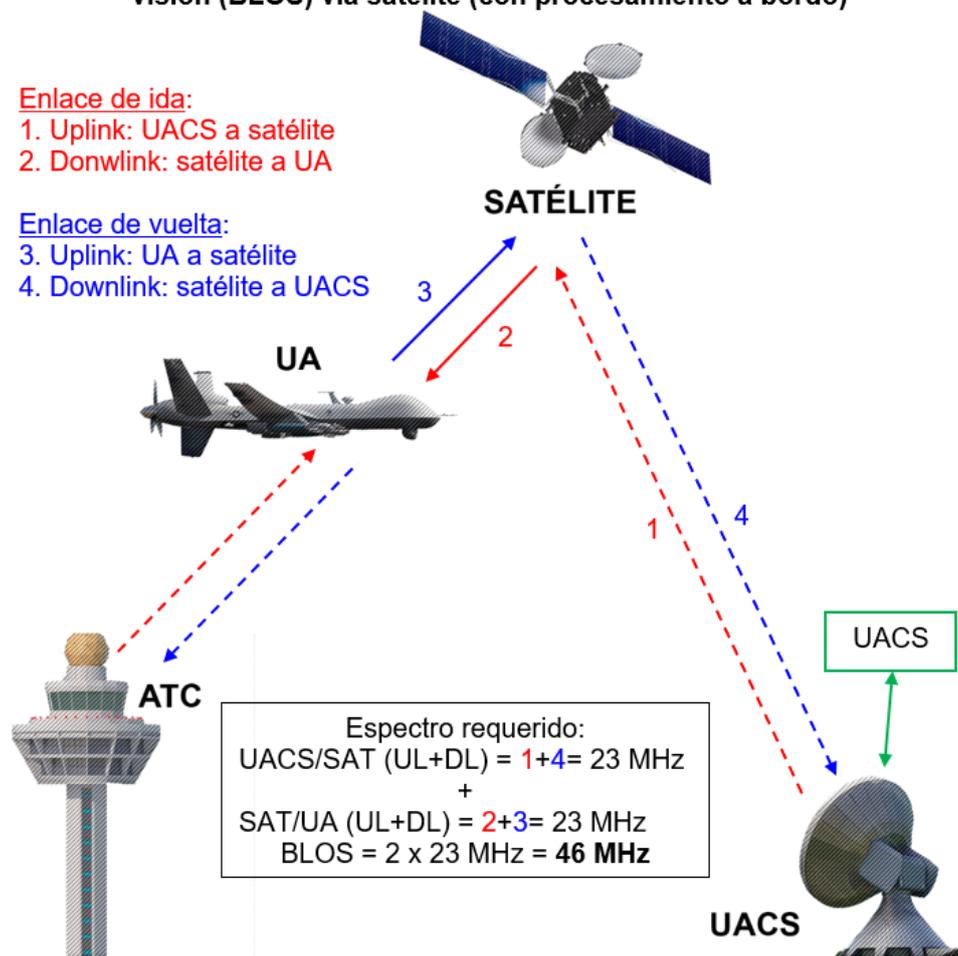


Figura 9: Radioenlace BLOS en un UAS. Fuente: [37]

### 5.3.3 Enlace C2

En 2015, la OACI presentó los avances que se han conseguido respecto al enlace de comando y control (C2) que, como se ha visto en el apartado anterior, es el enlace de datos entre el dron y la estación remota con el fin de gestionar el vuelo.

#### 5.3.3.1 Arquitecturas del enlace

Existe una variedad de posibles arquitecturas y consideraciones en el diseño, la seguridad y la administración del enlace C2 en función del modo de operación del dron y que se detallan a continuación:

- **RLOS:** es la operación en la que el RPA (dron) y la estación remota (RPS) están dentro de la cobertura del enlace de radio y, por lo tanto, pueden comunicarse directamente a través de la red existente. Las transmisiones deberían realizarse en un tiempo relativamente corto (retardo de la señal muy bajo):

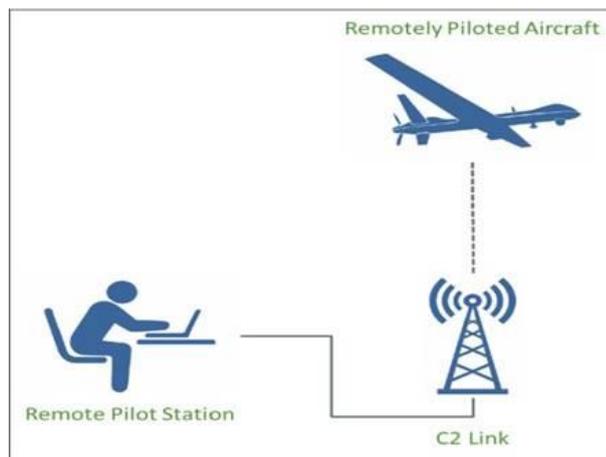


Figura 10: Arquitectura RLOS. Fuente: [38]

- **BRLOS:** es el caso en que el RPA y la RPS no pueden comunicarse directamente porque la distancia entre ellos es muy grande en comparación con la curvatura de la tierra. El retardo de la señal es significativamente mayor que para el caso RLOS. En este caso, la comunicación se puede apoyar en los satélites, así como utilizar una amplia red de radios terrestres RLOS para dar soporte al enlace C2:

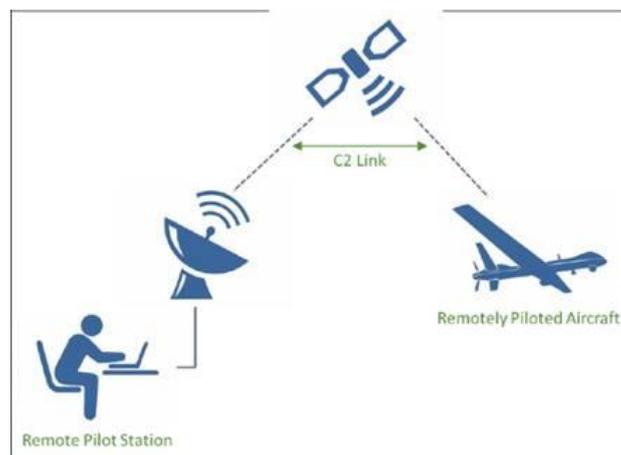


Figura 11: Arquitectura BRLOS. Fuente: [38]

- **Retransmisión a través del RPA:** en este caso, el dron se asemeja a un avión tripulado convencional de cara al establecimiento de las comunicaciones con el ATC. El dron está equipado con equipo VHF estándar y no habría ningún cambio en los procedimientos operativos o infraestructura de control ATC o de los servicios CNS. La retransmisión de la RPA puede degradar el rendimiento del enlace C2, aunque puede la degradación no llegue a ser significativa.

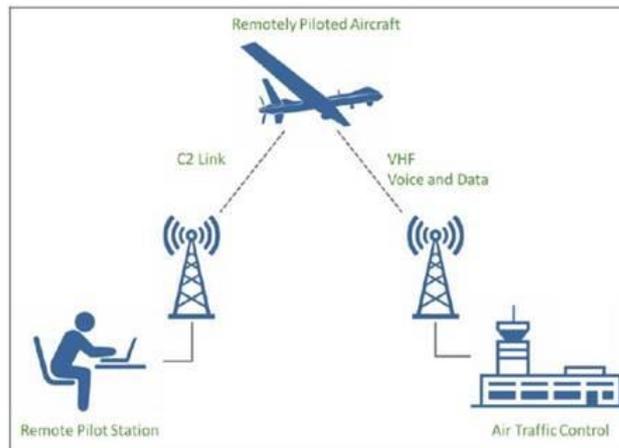


Figura 12: Arquitectura de retransmisión mediante el RPA. Fuente: [38]

- **Retransmisión BRLOS del RPA:** en esta arquitectura, la retransmisión se haría a través del satélite y el dron, lo cual podría añadir hasta 0,5 segundos de retardo en cada uno de los enlaces de comunicaciones *uplink* o *downlink*, por lo que la degradación en el rendimiento del enlace C2 podría ser significativa:

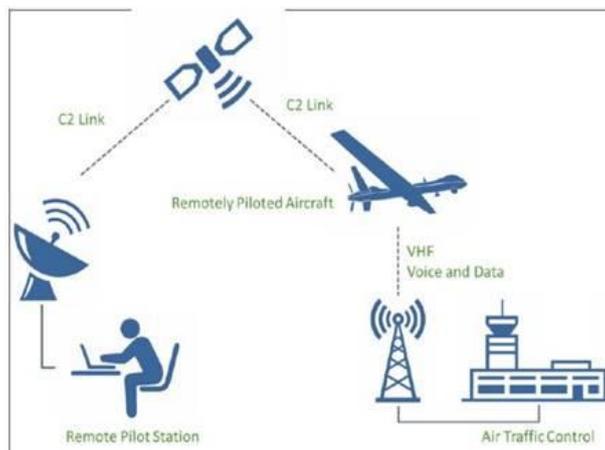


Figura 13: Arquitectura de retransmisión BRLOS - RPA. Fuente: [38]

- **Sin retransmisión a través del RPA:** como se muestra en la figura, en esta arquitectura no participan otros RPA en las comunicaciones. Se trataría de un enlace directo entre la RPS y el control de tráfico aéreo ATC para manejar un solo dron. Emplea un enlace radio VHF con un equipo VHF ATC estándar por lo que su uso tampoco implicaría cambios en la infraestructura o procedimientos ATC, aunque su cobertura es limitada.

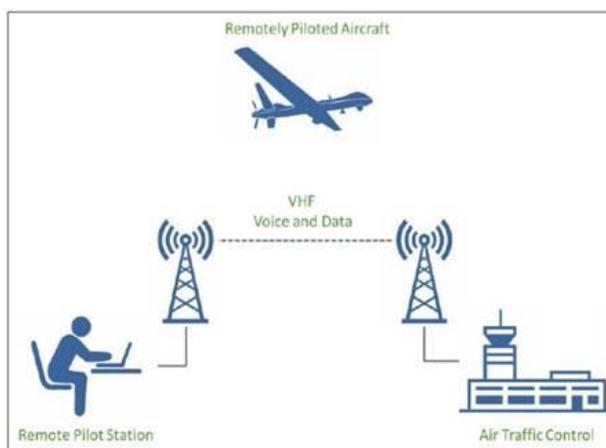


Figura 14: Arquitectura sin retransmisión a través del RPA. Fuente: [38]

- Enlace tierra – tierra:** esta arquitectura es un caso particular del anterior y se diferencia en que las comunicaciones se realizan a través de una red cableada que podría ser subterránea o aérea. Esto proporciona una latencia mucho menor y una confiabilidad y seguridad más alta que las comunicaciones basadas en que en la retransmisión BRLOS. Por el contrario, requiere de una nueva red para conectar las RPS con las estaciones ATC:

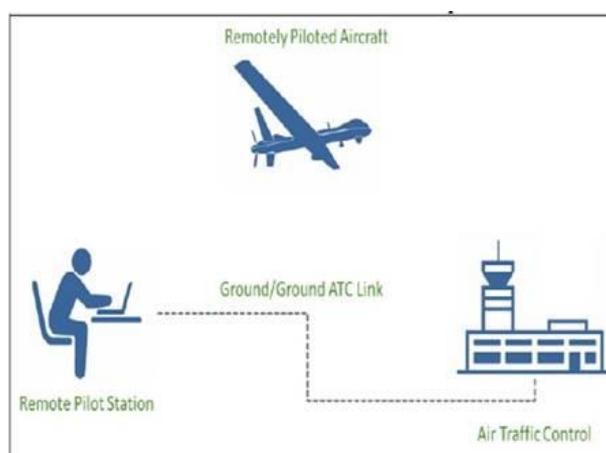


Figura 15: Arquitectura con enlace Tierra – Tierra. Fuente: [38]

### 5.3.3.2 Bandas frecuenciales

La Conferencia Mundial de Radiocomunicaciones de 2015 de la UIT (CMR-15) asigna, para el suministro tanto terrestre como satelital del Enlace C2, la banda frecuencial 5.030 – 5.091 MHz que antes estaba atribuida al servicio móvil aeronáutico por satélite (AMSS), aunque también se están considerando varias bandas de frecuencia del servicio fijo por satélite (SFS) para la provisión de este enlace de comunicaciones. Sin embargo, el uso de esta banda para el control de drones y las comunicaciones de carga no útil (CNPC) dependerían de unas condiciones específicas como las características técnicas de las estaciones terrenas y espaciales, del entorno de interferencias en el que deberá operar, así como el rendimiento requerido del enlace C2. La revisión de esta asignación estaría prevista para el año 2023 en la CMR-23.

Asimismo, el uso del espectro del enlace C2 deberá tener en cuenta las implicaciones de seguridad aeronáutica debido a posibles interrupciones o cortes del enlace, así como la latencia, integridad y seguridad de la transmisión de datos. Además, podría ser

necesario administrar las asignaciones de frecuencia para este enlace en áreas donde se espera que se realicen numerosas operaciones con drones.

### 5.3.3.3 Pérdida y protección del enlace

Durante la operación con un dron, se puede producir una pérdida del enlace C2 que puede ser causados por un fallo del equipamiento de a bordo o por la estación de control, por un error humano o por interferencias. Pero también pueden ser causadas por las condiciones de propagación de la señal RF tales como los desvanecimientos producidos por la atmósfera, reflexión de las señales en el terreno, los edificios y la estructura del avión (fuselaje), lo que hacen que el nivel de la señal de RF recibida varíe con el tiempo.

Para enlaces C2 terrestres y satelitales con una profundidad de desvanecimientos de hasta 30 dB y periodicidades de entre 10 ms y 100 s para cada uno, hay que tener en cuenta que la profundidad de desvanecimiento terrestre es mayor y, en el caso satelital, lo que aumenta es la duración de dicho desvanecimiento, tal y como se muestra en la siguiente figura:

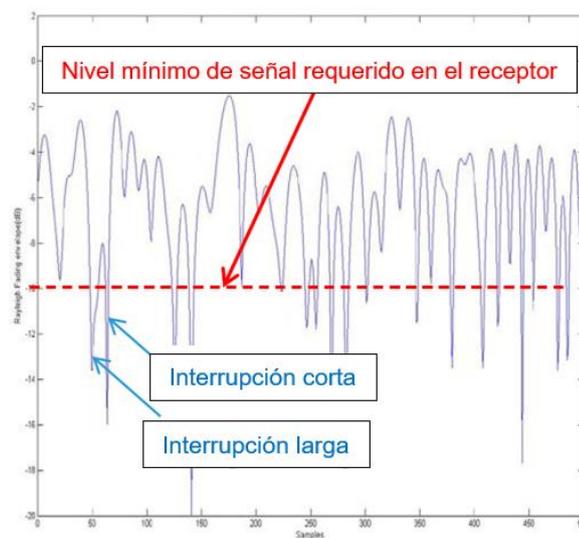


Figura 16: Nivel de señal recibida en función del tiempo. Fuente: [38]

La pérdida del enlace C2 puede causar situaciones de riesgo imprevisibles si no se implementan técnicas para mitigar las causas que lo producen. Teniendo en cuenta que el estado nominal del enlace C2 es aquel en el que el piloto remoto es capaz de gestionar activamente el vuelo del dron, se pueden dar otras situaciones en ocasiones no deseadas, como pueden ser:

- **Enlace C2 perdido y declarado:** el dron pierde el enlace y lo comunica rápidamente al piloto o estación remota por lo que este puede seguir realizando un plan de vuelo preestablecido siguiendo los procedimientos específicos de la OACI. El dron no resultaría una amenaza, por lo que podría continuar su vuelo, intentar recuperar el enlace o aterrizar en aeródromos alternativos.
- **Enlace C2 perdido y no declarado:** la aeronave pierde el enlace, pero aún no ha declarado su pérdida a la estación de control. El tiempo que transcurre desde que se pierde el enlace hasta que se comunica la pérdida, puede implicar una situación de inseguridad tanto en el operador remoto como en el control de tránsito aéreo, así como un riesgo para la seguridad de las personas y las cosas.

Para mitigar las pérdidas del enlace debido al desvanecimiento, se pueden implementar herramientas estadísticas que prevean dichas interrupciones, así como mecanismos de protección que establezcan la suficiente seguridad en el intercambio de datos entre el dron y la estación de control [39] [38].

Entre los mecanismos y soluciones para evitar o minimizar la probabilidad de pérdida del enlace se encuentran la utilización de múltiples antenas en el dron (MIMO) y la estación terrestre empleando diversidad espacial, emplear diversidad de frecuencias o usar múltiples enlaces C2 y que el receptor escoja el que tenga mejor calidad de señal.

### **5.3.4 Función S&A/ DAA (Detectar y evitar)**

Como se ha visto en el apartado 5.3.1, la función “Detectar y Evitar” (S&A o DAA) en un dron es análoga a la capacidad que deben tener los pilotos de aviones comerciales de “Ver y evitar” para detectar y evitar posibles colisiones con otros aeronaves u obstáculos. Esta función se considera clave para permitir la integración de los drones en el espacio aéreo controlado. Entre las capacidades de la función S&A/ DAA destacan:

- Mantener la vigilancia mientras se detectan y evitan conflictos en la aeronave y otros peligros como obstáculos, terrenos y clima severo.
- Determinar y ejecutar una maniobra de evitación efectiva y regresar de manera segura a la ruta de vuelo original o a su trayectoria segura hacia tierra.

Estas capacidades deben estar disponibles para el piloto remoto a fin de permitir las decisiones y acciones apropiadas para garantizar un vuelo seguro. Sin embargo, en caso de fallo, por ejemplo, como consecuencia de la pérdida del enlace C2, puede ser necesario que el sistema responda automáticamente para garantizar la seguridad del espacio aéreo.

Las tecnologías y procedimientos de la función DAA (tanto de la propia aeronave como de las estaciones terrestres) deberán desarrollarse y certificarse para garantizar no solo la seguridad del dron, sino también la interoperabilidad con otras aeronaves u otros sistemas para evitar colisiones como el sistema TCAS (*Traffic alert and Collision Avoidance System*) [40]. Es posible que se necesiten nuevos procedimientos para controladores y pilotos que garanticen que el uso de la función DAA se comprenda e integre en los procedimientos de operación normales y de contingencia. Además, la capacidad del sistema DAA debe ser compatible con las reglas del aire y con los servicios ATS que suministran la separación entre aeronaves. La solución DAA no debe degradar el nivel de seguridad del dron o del sistema de aviación en general.

En cuanto a los requisitos de espectro radioeléctrico necesarios para esta función, se deben considerar dos aspectos:

1. Todos los equipos de RF que recopilan los datos en bruto para la función S&A tendrán que ser compatibles con los servicios designados por la ITU-R en distintas tecnologías, es decir, si usa un sistema que evalúa la proximidad de un objeto, debe operar en las bandas frecuenciales del servicio de radiodeterminación (radar).
2. El funcionamiento correcto de la función S&A se verificará de forma permanente o regular en el UACS. Si es necesario, los parámetros del sistema S&A pueden ser modificados por este, dependiendo del área de vuelo, las condiciones climáticas o el nivel de autonomía asignado al dron.

Aquí, la ITU-R ya prevé el uso de sistemas de abordaje en las UA similares a los que emplean los aviones convencionales para detectar la proximidad de otros aviones y basados en sistemas radar como ACAS o ADS-B de a bordo. Además, recomienda que los datos derivados de los sensores pueden procesarse directamente dentro de la UA o transmitirse al UACS para su procesamiento. En cuanto a los flujos de datos bidireccionales entre la UA y la UACS de esta función, se deben considerar los siguientes:

- Enlace ascendente: permitirá al UACS controlar el funcionamiento de la función S&A de acuerdo con las condiciones del vuelo (similar al enlace C2) y la tasa de bits de datos no debe ser muy elevada.
- Enlace descendente: indicará que la función S&A funciona correctamente. Al igual que el requisito del enlace C2, se evitará que se solapen los datos de telemetría o de transmisión de video con los de la función S&A mediante los protocolos de transmisión adecuados.

De manera similar a las consideraciones del enlace C2, se espera que los requisitos de comunicación de RF de esta función tengan que cumplir con las futuras normas de la OACI para el vuelo seguro en áreas bajo la responsabilidad de las autoridades de aviación.

#### 5.4 Flujos de información

La figura 17 muestra los posibles flujos de información entre la estación de control UACS y el UA, así como los que proporcionan el control de tráfico aéreo y los sistemas de vigilancia de los proveedores de servicios de navegación aérea o ANSP, entre los que se incluyen:

- Los enlaces C2 de control UACS/ UA básicos.
- Datos de las *NavAids* (Ayudas a la navegación)
- Datos de vigilancia proporcionados por el sistema S&A de UAS.
- Otros datos de vigilancia, incluidos datos de radar meteorológico e imágenes de video.
- Mensajes de voz ATC que el UA debe retransmitir hacia y desde el UACS.
- Información ATS que la UA debe retransmitir desde y hacia el UACS.

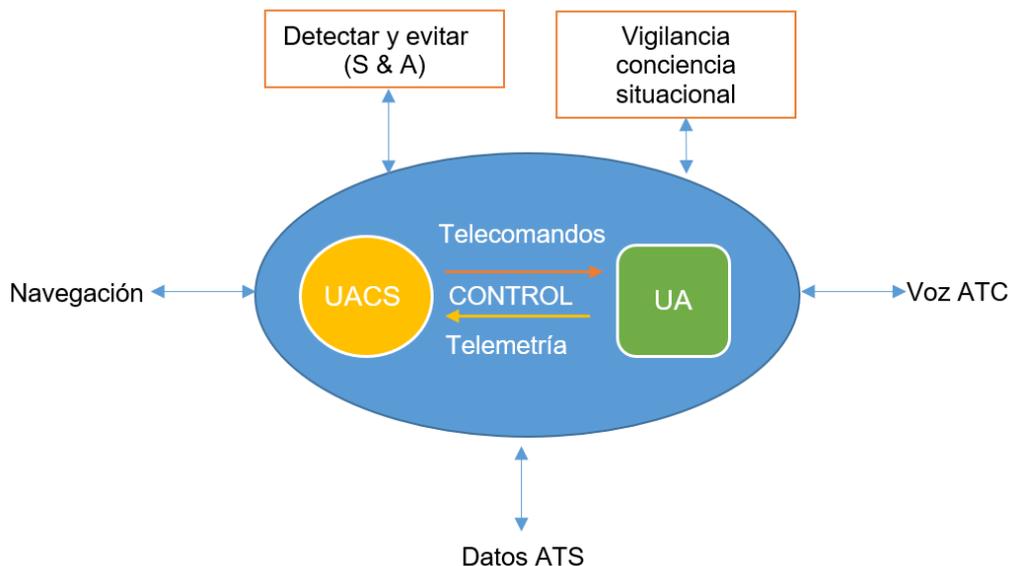


Figura 17: Flujo de información entre el UA y el UACS. Fuente: elaboración propia

En la Figura 18, se muestran los flujos de información de comando y control (enlace C2), S&A y ATC entre el UACS y el UA. Estos flujos incluyen no solo el intercambio de datos de control entre la UACS y el UA, sino también la retransmisión de los mensajes de voz ATC y de datos ATS que utilizan la UA en la retransmisión, así como el enlace descendente de los datos de navegación, pistas de destino, radar meteorológico e imágenes de video de la UA al UACS.

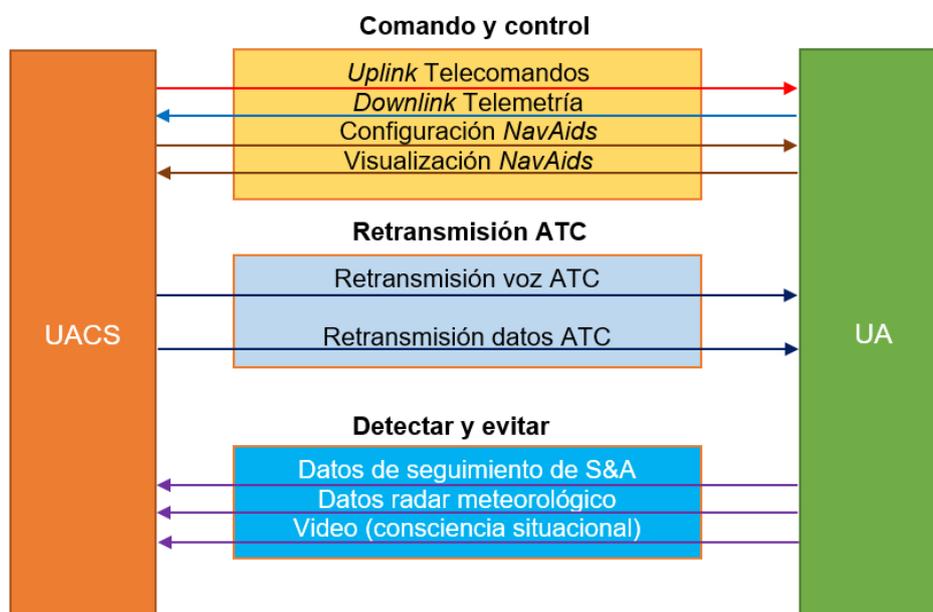


Figura 18: Flujo de información entre el UA, el UACS y el control ATC: Fuente:

## 5.5 Comunicaciones aeronáuticas de drones con ATC

Hasta la fecha, la mayoría de los vuelos realizados por los drones han tenido lugar en el espacio aéreo segregado, es decir, aquel en el que uso está restringido a ciertas áreas geográficas y a ciertas altitudes para evitar los peligros de colisión con las aeronaves convencionales. Las razones por las que los drones no pueden integrarse de forma segura y fluida con otros usuarios del espacio aéreo son: la incapacidad de cumplir los aspectos críticos del reglamento en el aire, las limitaciones tecnológicas y la falta de SARPS específicos para los drones y sus sistemas de apoyo.

Sin embargo, la OACI junto a otros organismos públicos y empresas tecnológicas privadas, están haciendo grandes esfuerzos para cambiar esta situación. En el reglamento de 2011, la OACI especifica que un factor fundamental en la integración segura de los drones en el espacio aéreo de aviación civil, será su capacidad de actuar y responder como hacen las aeronaves tripuladas a las instrucciones de los controladores del servicio ATS.

En este sentido, los drones deberán mantener una vigilancia continua en el canal de comunicación de voz con ATC, así como establecer una comunicación bidireccional con los controladores si fuese necesario y siempre que lo prescriba la autoridad ATS correspondiente. Los drones que realizan operaciones IFR (con reglas basadas en la instrumentación de a bordo) deben comunicarse con ATC mientras estén en el espacio aéreo controlado.

Los requisitos de los sistemas de comunicaciones deben estar en consonancia con el concepto de rendimiento de comunicación requeridos (RCP) y los SARP recomendados por la OACI.

En cuanto a las arquitecturas para transmitir información entre el dron y el ATC, los sistemas de navegación, los sistemas de vigilancia, el avión comercial, el dron y su estación de control pueden involucrar enlaces terrestres, satelitales y aéreos para transmitirla voz y datos del ATC a los pilotos remotos a través de sistemas de telecomunicaciones terrestres o mediante la transmisión a través del RPA, como se vio en el apartado 5.3.4. A su vez, las interfaces del sistema deben ser interoperables, en términos de rendimiento y funcionalidad, para garantizar intercambios de información confiables, disponibles, precisos y consistentes entre todos los usuarios del espacio aéreo controlado [39]. Estas interfaces y enlaces se observan en la Figura 19:

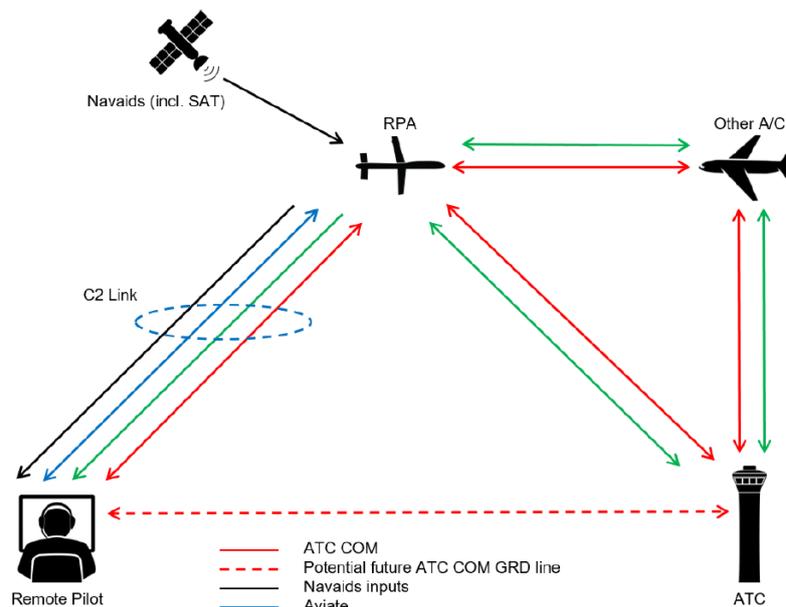


Figura 19: Interfaces del sistema. Fuente: [39]

Finalmente, cualquiera que sea la solución de comunicación con los servicios ATS, esta debe ser transparente a los controladores para mantener la consistencia de las comunicaciones con los aviones comerciales. Algunas de estas opciones de comunicación pueden implicar la intervención o contratación de proveedores de servicios de terceros, como se verá en el capítulo 7.

## 5.6 Requisitos de espectro de frecuencias para las comunicaciones con drones

La regulación internacional del uso del espectro de frecuencias se establece en el llamado Reglamento de Radiocomunicaciones (RR) que contiene los textos aprobados por las Conferencias Mundiales de Radiocomunicaciones (CMR), organizadas por la ITU [41]. Además de las regulaciones, contienen unas tablas que enumera todas las asignaciones de frecuencia tanto regionales como nacionales. Una asignación puede tener un estado primario o secundario, lo que significa que un usuario primario puede causar interferencias perjudiciales para un usuario secundario del espectro de frecuencias, pero no al revés. Varios países también disponen de una asignación terciaria que a menudo se desvía de la tabla de la ITU. Los usuarios terciarios no pueden causar ninguna interferencia a los usuarios primarios y secundarios y deben aceptar las interferencias de todos los demás. En la mayoría de los casos, el regulador nacional no

responde a los casos de interferencia a esos usuarios. Un ejemplo de este tipo de interferencias entre usuarios se ilustra en la siguiente figura:

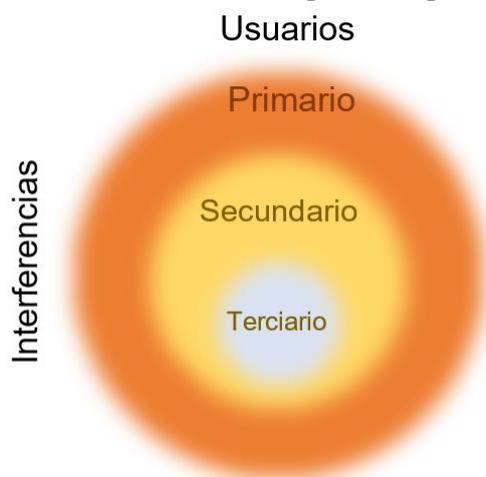


Figura 20: Interferencias en función del tipo de usuario asignado. Fuente: elaboración propia

Para las comunicaciones de los drones comerciales, a menudo se utilizan bandas sin licencia que pueden tener una asignación secundaria o terciaria, como se verá en este apartado.

Dentro de Europa, la CEPT (Conferencia Europea de Administraciones Postales y Telecomunicaciones) se encarga de la asignación detallada de frecuencias y de investigar la compatibilidad entre los sistemas de radio. En el apartado 5.3.3.2, se vio que la CMR-15 asignó, a título primario, la banda de frecuencias 5.030–5.091 MHz, que antes estaba atribuida al servicio móvil aeronáutico por satélite (AMSS), a las comunicaciones de comando y control y de carga no útil (CNPC) a los RPAS, pero solo para aquellos comerciales que pueden volar grandes distancias y en el espacio aéreo controlado. La OACI se ha encargado de establecer un plan para facilitar el uso internacional de esta banda frecuencial, sin embargo, aún no hay una coordinación clara en este aspecto.

Para drones pequeños, no se han realizado asignaciones de frecuencia específicas a nivel internacional para el enlace C2 (Comando y control) o de carga útil. Dados los principales desarrollos en esta área en los últimos años, la demanda de espectro de frecuencias está en aumento por lo que la falta de uno reservado para este fin implica que, en la mayoría de países, los drones solo pueden hacer uso de las bandas de frecuencias disponibles sin licencia. Dentro de Europa, se han asignado un gran número de bandas frecuenciales de este tipo y aparecen reflejados en la Recomendación ERC [42, pp. 70-03], en la que se da una lista de todas estas frecuencias junto con las limitaciones y requisitos técnicos. Las dos bandas sin licencia de uso común para los enlaces de comando y control y comunicaciones de carga útil de los drones son las de 2.4000–2.4835 MHz y 5.470–5.725 MHz (2,4 – 5,4 GHz) y deben cumplir con las regulaciones que se aplican a los sistemas de transmisión de datos de banda ancha como WiFi.

En Europa, la banda 5.725–5.875 MHz (5,8 GHz) está disponible para comunicaciones de corto alcance con una potencia de transmisión máxima de 25 mW de potencia isotrópica radiada efectiva. Debido a la popularidad de WiFi, especialmente en 2.4000–2.4835 MHz, existe una alta probabilidad de interferencia entre los sistemas de comunicaciones de los drones y otros dispositivos electrónicos usados en áreas pobladas, lo que puede llevar a la pérdida del enlace de control del dron. El receptor del dron podría captar un alto nivel de interferencias debido a la baja altura a la que operan,

por lo que junto a los bajos requisitos de potencia de transmisión, solo los drones que operen en VLOS pueden usar estas frecuencias.

Para vuelos de aviones no tripulados que operan a grandes distancias, se deben hacer arreglos especiales para que estos vuelos sean posibles, como por ejemplo, el uso compartido de bandas frecuenciales dedicados a otros servicios como los satelitales, como se vio en el apartado 5.3.4.2 o el uso de redes móviles. En la mayoría de los casos, se requiere una licencia para el uso de estas frecuencias, que es competencia de la Autoridad Reguladora Nacional (NRA).

En el futuro, el rango de frecuencia reservado internacionalmente entre 5.030- 5.091 MHz para CNPC (carga no útil) puede usarse para vuelos BVLOS [43]. Si durante un vuelo se requiere comunicación de carga útil, por ejemplo, en el caso de usar cámaras de vigilancia para el control de incendios o de fronteras, se necesitarían otras frecuencias adicionales.

Aun así, aunque exista regulación específica en el uso del espectro dentro de Europa, hay drones comprados fuera de la Unión Europea que podrían usar frecuencias destinadas a otros usos e interferir con ellos. El uso de una frecuencia particular requiere una licencia porque otros usuarios también pueden hacer uso de ellas. Además, la combinación de diferentes equipos transmisores a distintas frecuencias unido al uso de alta potencia de transmisión, puede causar graves interferencias e intermodulaciones que provoque el mal funcionamiento de los sistemas de comunicaciones de drones o dispositivos electrónicos cercanos.

Los casos de interferencia graves se pueden notificar a la ANR, la cual podría iniciar un procedimiento para intentar determinar su origen e incluso sancionar a los operadores que usen bandas de frecuencias prohibidas aunque, debido al tiempo de vuelo relativamente corto de los drones, la interferencia puede haber dejado de existir cuando el caso se investigue.

## **5.7 Normativa y restricciones en el espacio aéreo español**

En España, la nueva regulación en materia de drones entró en vigor en 2017 mediante el Real Decreto 1036/2017, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto.

Aunque el ámbito de aplicación afecta a todas las aeronaves en función de su masa máxima al despegue, las pequeñas aeronaves y los vuelos recreativos son una de las claves en los nuevos procedimientos de vuelos profesionales y de ocio. Tal y como expresa la nueva normativa, “el piloto remoto será, en todo momento, el responsable de detectar y evitar posibles colisiones y otros peligros” ello, sin perjuicio de las posibles tecnologías de que disponga el dron para evitar obstáculos de forma autónoma como las de S&A/ DAA, *geofencing*, etc., detalladas en el siguiente capítulo.

El sobrevuelo en zonas aéreas controladas, sobre aglomeraciones de personas al aire libre y sobre zonas urbanas sólo se permite para drones de peso no superior a 10 kg, dentro del alcance visual, a una distancia no superior a 100 metros y a una altura máxima de 120 metros. Además, se deben acotar las distancias de seguridad a 50 metros respecto de edificios, objetos o personas.

También está permitido realizar vuelos nocturnos siempre y cuando se obtenga la autorización expresa de la AESA mediante una solicitud por parte del operador junto a un estudio de seguridad específico. Además, el dron deberá estar adaptado a las

condiciones nocturnas debiendo incorporar luces, pintura u otros dispositivos que ayude a visualizarlo correctamente.

Para los casos de vuelos profesionales que se desarrollen sobre zonas aéreas controladas, será necesario que el piloto tenga conocimientos radiofónicos, debiendo estar acreditado para ello en la licencia de piloto según lo dispuesto en la normativa. Las distancias mínimas a respetar respecto aeródromos y aeropuertos serán de 8 kilómetros si está operando en condiciones de vuelo visual (VFR) y 15 kilómetros si se opera en condiciones de vuelo instrumental (IFR).

Para aquellos vehículos que no dispongan del correspondiente certificado de aeronavegabilidad, podrán realizar vuelos con fines recreativos, deportivos o de competición, bajo las siguientes condiciones:

- A una altura máxima sobre el terreno no mayor a 120 m, o sobre el obstáculo más alto situado dentro de un radio de 150 m desde la aeronave.
- A una distancia mínima de 8 km respecto a cualquier aeropuerto o aeródromo.
- Fuera del espacio aéreo controlado, de las zonas de información de vuelo (FIZ) o de cualquier zona de tránsito de aeródromo (ATZ).
- En vuelo diurno y bajo condiciones meteorológicas VLOS.
- Volar sobre edificios y aglomeraciones al aire libre si nuestro dron pesa menos de 250 gramos y nunca a más de 20 metros de altura.
- Volar sin sobrepasar edificios o aglomeraciones al aire libre siempre que nuestro dron pese menos de 2 kg y sin superar los 50 metros de altura, incluso en vuelos nocturnos.

Todo dron deberá llevar fijada a su estructura la correspondiente placa de identificación ignífuga, en la que deberá constar la identificación de la aeronave incluyendo el nombre del fabricante, el tipo, modelo, número de serie y los correspondientes datos del operador. Las aeronaves con un peso inferior a 25 kg quedan exentas del registro de matriculación. A continuación, se muestra una tabla resumen sobre las condiciones de uso de los drones en España:

Hobby/vuelos recreativos ¿Cómo volar tu dron?	Hobby/vuelos recreativos ¿Qué debes evitar con tu dron?	Prohibiciones uso profesional RPAS Si trabajas con un RPAS
 Siempre tenerlo a la vista, no volar a más de 120m del suelo	 NO volar sobre aglomeraciones de edificios	 Necesitas autorización para poder volar sobre edificios y personas
 Sólo volar de día, en condiciones meteorológicas adecuadas (sin niebla, sin lluvia y sin viento) y en zonas adecuadas para ello	 NO volar sobre personas	 No puedes volar de noche, sin autorización
 No hay que ser piloto, pero sí hay que volar con seguridad y bajo supervisión de un adulto	 NO volar de noche si tu dron pesa mas de 2Kg	 Necesitas autorización para volar a menor distancia de la que marca la ley en las proximidades de aeropuertos, aeródromos, etc..
 Eres responsable de los daños que pueda causar tu Dron. Es recomendable un seguro a terceros	 NO volar a un mínimo de 8 kilómetros de aeropuertos, aeródromos, etc.	 No puedes operar en espacio aéreo controlado, sin autorización
 La difusión de imágenes de personas o de espacios privados, necesitan de autorización de las mismas	 NO volar en espacio aéreo controlado ni donde se realicen otros vuelos a baja altura (zonas de parapente, paracaidismo, globos, ultraligeros, planeadores, etc.)	 No puedes poner en peligro o molestar a terceros (otras aeronaves, personas y bienes)
 No te olvides de cumplir la Ley de Protección de datos*, la del Derecho al Honor, Intimidad y propia imagen y las restricciones de toma de imágenes aéreas	 NO poner en peligro o molestar a terceros (otras aeronaves, personas y bienes en tierra)	

Tabla 3: Tabla resumen de uso de drones según la normativa española

## 6. Tecnologías y sistemas de integración de drones en el espacio aéreo

Como se ha visto en el capítulo anterior, para que un dron pueda volar en el espacio aéreo no segregado, deberá disponer, como mínimo, de un sistema aprobado de detección y evitación de colisiones. Además, debería contar con otras tecnologías basadas en sistemas de comunicaciones que permitan ser geolocalizadas e identificadas, bajo todas las reglas de vuelo. Las tecnologías que pueden dotar a los drones de estas capacidades se detallan en los siguientes apartados.

### 6.1 Sistemas de detección, identificación y geolocalización de drones

Según la normativa vista en el apartado 5.3, los aviones no tripulados deberían contar sistemas de detección y evitación de colisiones pero también podrían disponer de sistemas que permitan su localización, posicionamiento e identificación para que el operador y las autoridades de gestión del espacio aéreo sepan donde se encuentra el dron en cada momento y quién lo está pilotando. Algunas de estas tecnologías se describen a continuación.

#### 6.1.1 Sistema S&A/ DAA (Detectar y Evitar)

Según la normativa, para evitar colisiones en el aire, un dron puede contener un subsistema S&A/ DAA, con las siguientes funciones:

- Mantenimiento de la separación con otro tráfico al volar en VFR o IFR
- Detección y evitación de colisiones con el terreno u obstáculos en el suelo
- Detección y evitación de colisiones con aeronaves y obstáculos durante las operaciones cerca del aeródromo
- Detección y evitación de condiciones meteorológicas adversas
- Detección y evitación de aeronaves cercanas en el espacio aéreo controlado y no controlado en todas las condiciones de vuelo.

Para evitar colisiones, los drones pueden utilizar los mismos medios de detección, procesamiento, comunicación, actuación e incluso humanos que las aeronaves convencionales [34].

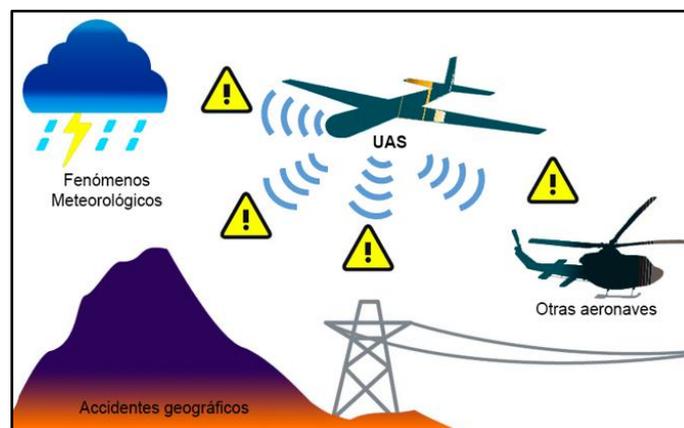


Figura 21: Sistema S&A/DAA (Detectar y Evitar). Fuente: elaboración propia

En este sentido, investigadores de la *Australian Research Center for Aeroespacial Automation* diseñaron en 2012, un sistema capaz de emular en un dron la capacidad que tiene un piloto de un avión convencional de “Ver y evitar” situaciones de conflictos

y colisiones en el aire. En aquel entonces ya sabían que los reguladores exigían que los drones debían demostrar un nivel de seguridad equivalente al de los aviones tripulados, antes de operar de manera rutinaria en el espacio aéreo civil. Así pues, propusieron técnicas, métodos e integraciones de hardware que describen un sistema de "Detección y evitación" o DAA, diseñado para abordar la falta de capacidad de "Ver y evitar" de las aeronaves no tripuladas.

Estas técnicas para evitar colisiones se basan en la detección de otras aeronaves utilizando sensores de imágenes integrados en los drones, así como un post-procesamiento basado en complejos algoritmos. Entre las dificultades que han tenido los diseñadores, destaca la diferenciación de amenazas de colisión dentro de un fondo saturado y las dificultades para estabilizar la imagen para facilitar la detección de objetivos mediante técnicas de procesamiento entre cuadros, así como la variabilidad y características únicas de propagación de la luz. A pesar de los desafíos, se ha conseguido realizar un procesamiento en tiempo real, mediante un sistema de captura de imágenes compuesto por una capturadora de video, un proceso de estabilización, un sistema de seguimiento del objetivo y un algoritmo de control o actuador que dirige el dron [44]. El diagrama de bloques del sistema se muestra en la siguiente imagen:

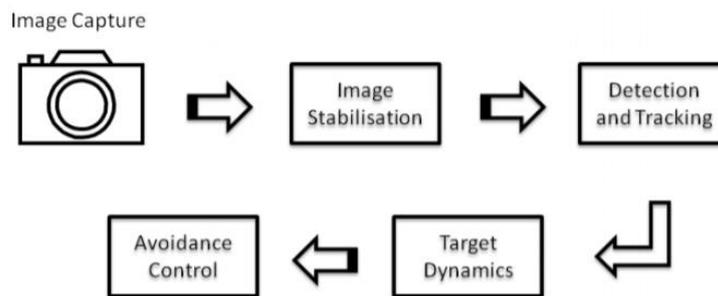


Figura 22: Componentes de un sistema S&A basado en visión computarizada. Fuente: [44]

Desde el punto de vista de los sistemas de comunicaciones, para controlar el dron de forma remota, se diseñó la arquitectura de un sistema de navegación y control basado en el piloto automático *MicroPilot 2128* y un conjunto de sensores a bordo. Los componentes del sistema se muestran en la siguiente figura:

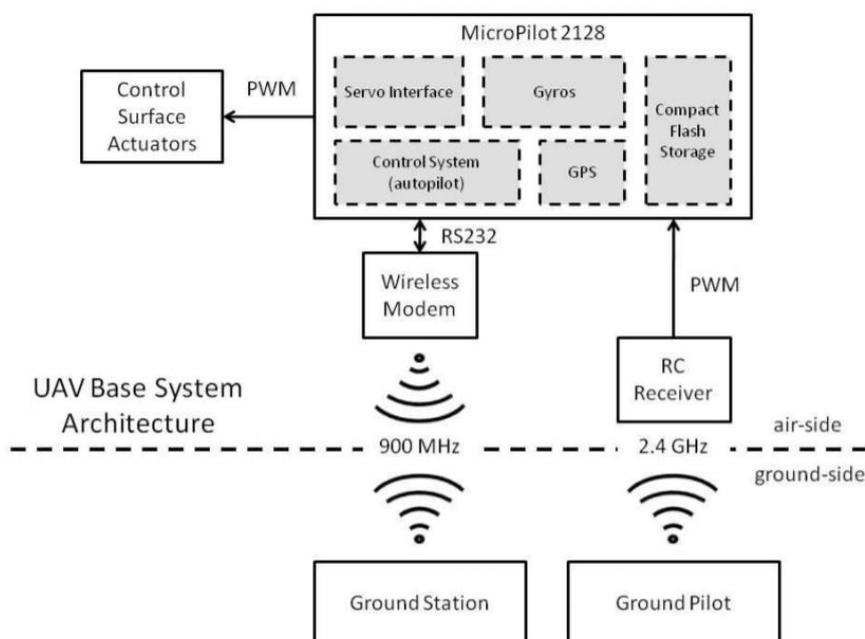


Figura 23: Arquitectura base del sistema S&A del dron. Fuente: [44]

Además del dron, se diseñó un sistema de detección que se instalaría en un avión ligero tipo Cessna 172, equipado con capacidades de procesamiento de imágenes en tiempo real y captura de datos a bordo para reproducir un sistema adecuado para las pruebas de detección y evitación en bucle cerrado, es decir, un sistema capaz de detectar automáticamente aviones intrusos, emitiendo y ejecutando comandos de control de evitación sin la interacción de un piloto remoto o de la estación terrestre.

Los resultados de las pruebas determinaron que el rango de detección usando una lente con un campo de visión (FOV) de 51° se obtuvieron unas distancias de detección de 400 a 900 m. Además, tomando el peor de los casos y aproximando el dron a una velocidad de 50 m/s, consiguió emitir una alerta de colisión 8 segundos antes del impacto. Este tiempo se acerca al tiempo de respuesta de 12,5 segundos que necesitan los pilotos humanos (después de detectar la amenaza) para evitar una colisión segura [44].

Sin embargo, el sistema S&A/ DAA descrito, aunque tiene la ventaja de ser un sistema autónomo instalado en el propio dron y ser independiente de los sistemas ATM instalados en tierra para el control de tráfico aéreo convencional, puede suponer un peligro si no funciona correctamente. A este respecto, el documento *Unmanned Aircraft Systems – ATM Collision Avoidance Requirements* de Eurocontrol [45], recomienda los siguientes aspectos para un sistema de prevención de colisiones:

- Debe estar diseñado para detectar cualquier peligro, no solo la colisión en el aire con otras aeronaves, sino con el terreno y obstáculos en el suelo, turbulencias generadas por la estela de otro avión o condiciones meteorológicas adversas. La degradación de su funcionalidad podría comprometer su capacidad de evitar colisiones y generar órdenes incompatibles con la seguridad aérea.
- Podría usarse como medio para proporcionar provisión de separación, especialmente en vuelos VFR. Esto compromete potencialmente la independencia de la capacidad de evitar colisiones (y, por lo tanto, su capacidad de actuar como una red de seguridad efectiva) en circunstancias donde la evitación de la colisión debido a la separación ha fallado.



Figura 24: Sistema activo anticolidión S&A/ DAA basado en redes móviles. Fuente: Elaboración propia

Así pues, debe encontrarse un sistema que, combinado con S&A proporcione un nivel adecuado de seguridad. Los sistemas que dependen de otros son susceptibles a las fallas comunes, pero aún se puede proporcionar un nivel adecuado de seguridad si se

garantiza que la integridad de los datos y la confiabilidad de los componentes comunes sea lo suficientemente alta. Por este motivo, en el mismo documento se contempla el diseño e implementación de un sistema activo de prevención de colisiones similar al TCAS (*Traffic alert and Collision Avoidance System*) que poseen los aviones comerciales y que funciona con independencia de los servicios de tránsito aéreo. Este sistema se estudia en el siguiente apartado.

### 6.1.2 Sistema ACAS-sXu

La Alianza de Investigación de Integración del Espacio Aéreo UAS del Noreste (NUAIR, por sus siglas en inglés) anunció recientemente un nuevo sistema de prevención de colisiones en el aire ACAS (*Airborne Collision Avoidance System*) para pequeños drones. Esta alianza, con sede en Nueva York, pone a prueba las investigaciones relacionadas con la aeronáutica, las operaciones de sistemas de aeronaves no tripuladas y la gestión de la seguridad.

El sistema es una versión más pequeña y compacta del ACAS X, esto es, un ACAS en desarrollo para grandes aviones de pasajeros y de carga. Según NUAIR, las pruebas demostraron que el sistema tiene la capacidad única de detectar y evitar otros aviones, tanto tripulados como no tripulados. El esquema de funcionamiento del ACAS X se muestra en la siguiente figura:

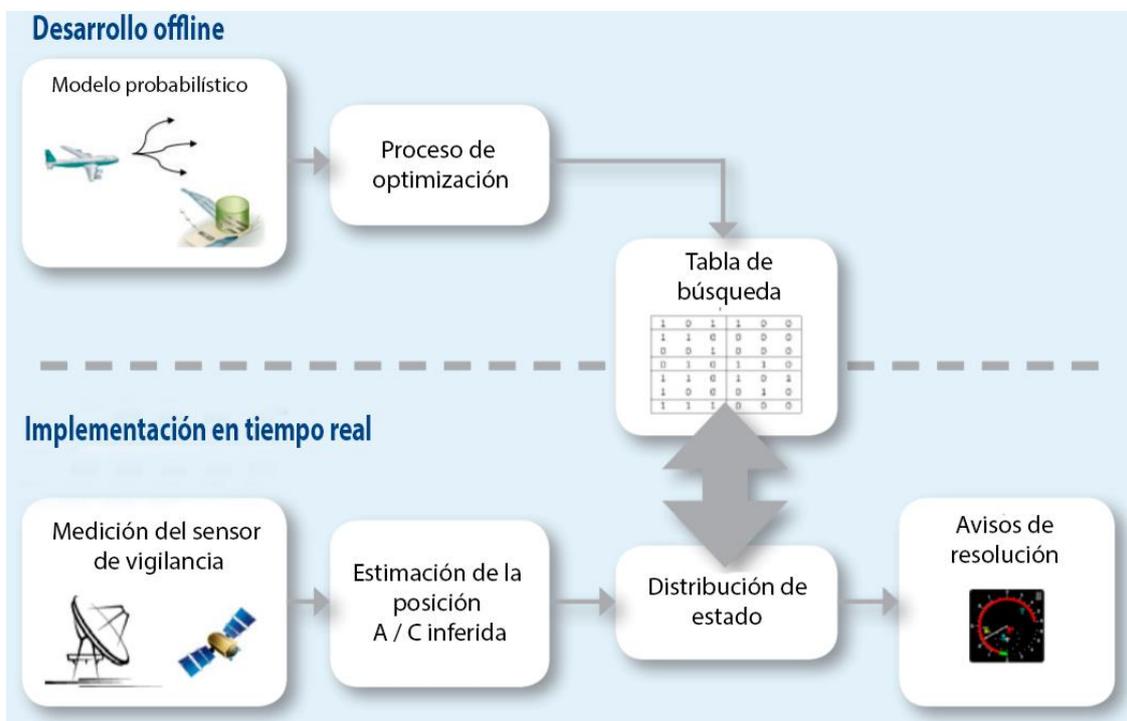


Figura 25: Funcionamiento del sistema ACAS-X. Fuente: [46]

En el **desarrollo offline**, ACAS X emplea un modelo probabilístico que proporciona una representación estadística de la posición de la aeronave en un instante futuro. También tiene en cuenta los objetivos operativos y de seguridad del sistema que permiten adaptar la lógica a procedimientos o configuraciones de espacio aéreo particulares. Esto alimenta a un proceso de optimización llamado "programación dinámica" para determinar la mejor ruta a seguir de acuerdo con el contexto del conflicto, tomando en cuenta un sistema de recompensas frente a costos para determinar qué acción generaría los mayores beneficios (considera rentable mantener una separación segura al implementar una maniobra de evitación). Las métricas clave para la idoneidad operacional y la aceptabilidad del piloto incluyen minimizar la frecuencia de las alertas

que resultan en los cruces intencionales de intrusos a cierta altitud o avisos en encuentros no críticos.

En la **implementación en tiempo real**, se utiliza la tabla de búsqueda a bordo del avión para resolver conflictos. ACAS X recopila mediciones de vigilancia de una variedad de fuentes una vez por segundo aproximadamente. Se utilizan varios modelos probabilísticos que tiene en cuenta las probabilidades de error de los sensores del avión, y estimar así una distribución de probabilidad estadística sobre las posiciones y velocidades actuales de la aeronave. La **distribución de estado** determina dónde buscar en la tabla para determinar la mejor acción a realizar. Si se considera necesario, se emiten avisos de resolución de conflictos a los pilotos [46].

Durante el vuelo, las capacidades de detección y evitación (S&A/ DAA) utilizan la información de los sensores de la aeronave y estaciones de control para que los pilotos conozcan el riesgo potencial de colisión y brinden orientación para garantizar un resultado seguro. El sistema ACAS-sXu está diseñado específicamente para hacer esto al proporcionar una capa adicional de seguridad para evitar colisiones más allá de los sistemas existentes de control de tráfico aéreo y los procedimientos de vuelo.

Según la alianza, estas características son clave para la comercialización de drones y la movilidad aérea urbana. Además, las pruebas de ACAS demostraron que el sistema podría integrarse en el dron y estar basado en la nube dentro de la arquitectura UTM de gestión de tráfico aéreo no tripulado, con las capacidades de S&A/ DAA que requiere la normativa.

"Esta prueba de colaboración de la industria marca otro hito: un radar DAA aerotransportado que proporciona datos de detección en el espacio aéreo en un ACAS-sXu a bordo y, además, genera avisos de resolución de conflictos para garantizar la prevención de una posible colisión aérea", dice Adam Robertson, cofundador de Fortem Technologies, empresa americana innovadora en el desarrollo de tecnologías radar de detección y evitación de intrusiones en aeronaves en tiempo real [47].

Finalmente, NUAIR señala que esta tecnología puede eliminar la necesidad de usar observadores visuales en operaciones BVLOS y llevar a cabo operaciones de mayor envergadura y más costosas [48].

### 6.1.3 Geofencing

La tecnología *geofencing* que, en español se podría traducir como *geocercado* o *geobarreras*, trata sobre la creación de cercos o *barreras virtuales* para mantener alejados a los drones de áreas críticas o restringidas. El *geofencing* emplea los sistemas de navegación por satélite GNSS (*Global Navigation Satellite System*), como el GPS, para ayudar a los drones a evitar de forma automática que vuelen cerca de lugares sensibles como aeropuertos, prisiones, centrales nucleares o eventos multitudinarios. En ciertos lugares, un dron no puede despegar o volar en un área *geocercada* sin una autorización especial. Algunos pilotos certificados pueden desbloquear estas áreas si consiguen la aprobación de las autoridades correspondientes, pero las áreas más críticas requieren, además, una autorización especial de algunos fabricantes de drones para desbloquearlas. Es el caso del fabricante chino DJI, que ha simplificado el proceso de aprobación para que los pilotos profesionales de drones con autorización para volar en lugares sensibles puedan recibir códigos de desbloqueo en menos de 30 minutos.

En este sentido, la empresa china líder mundial en drones civiles y tecnología de imágenes aéreas, está mejorando su tecnología *geofencing* para refinar las limitaciones del espacio aéreo para vuelos de aviones no tripulados cerca de los aeropuertos a fin

de proporcionar una protección más inteligente en áreas críticas. Esto supone un gran paso para la integración segura de aviones no tripulados en el espacio aéreo basado en una evaluación más precisa de los riesgos asociados con los aviones que se aproximan y salen de diferentes aeropuertos.

El nuevo sistema, denominado GEO II, permite crear zonas de seguridad tridimensionales detalladas en forma de "lazo de corbata" que rodean las trayectorias de vuelo sobre la pista, así como la creación de formas poligonales complejas alrededor de otras instalaciones sensibles, en lugar de usar simples círculos. Estas nuevas restricciones reflejan mejor el riesgo real que existe en esas áreas, al tiempo que permiten más vuelos cerca de las pistas donde el riesgo es sustancialmente menor [49]. Utilizando las recomendaciones del Anexo 14 de la OACI y los criterios de la FAA, la empresa china ha alineado su función de seguridad de *geofencing* con una comprensión más amplia del espacio aéreo y el riesgo en los aeropuertos, como se detalla en la Figura 26.

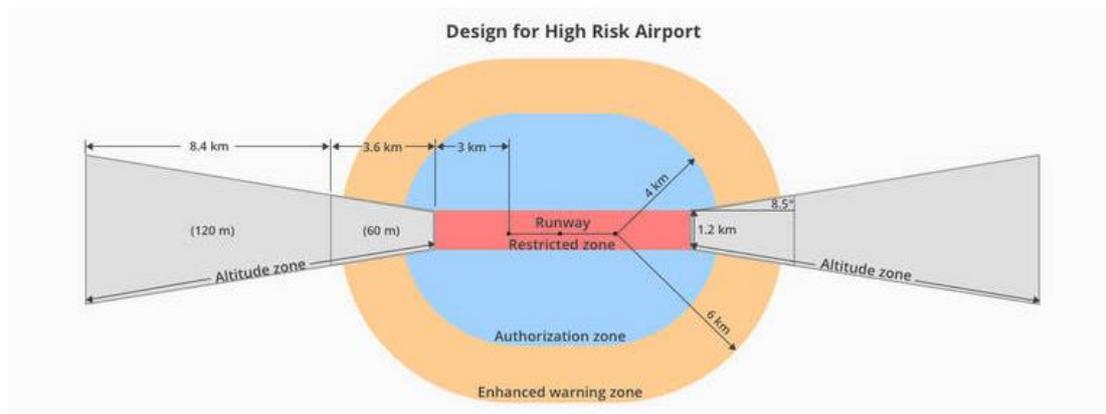


Figura 26: Delimitación de zonas de riesgo en un aeropuerto. Fuente: [50]

El sistema aplica las restricciones más fuertes a un rectángulo de 1,2 km de largo alrededor de cada pista (zona roja) y las rutas de vuelo en cada extremo, donde los aviones despegan y aterrizan. También se aplican restricciones, pero menos estrictas, a un área ovalada de unos 6 km de radio en cada pista (zona azul). La zona en forma de lazo de corbata (zona gris) abre más áreas a los lados de las pistas para otros usos con drones, en áreas de baja altitud a más de 3 km del final de una pista, al tiempo que aumenta la protección en los lugares donde realmente vuelan los aviones tripulados [50].

La información geoespacial la obtiene del proveedor de datos PrecisionHawk, que puede proporcionar detalles altamente precisos, como las ubicaciones exactas de las pistas de los aeropuertos y los límites de las instalaciones. Directivos de esta compañía aseguran que la tecnología puede desempeñar un papel fundamental en el desbloqueo de operaciones avanzadas BVLOS.

En la siguiente imagen se muestra una captura de las inmediaciones del Aeropuerto de Madrid-Adolfo Suárez, en la aplicación web del fabricante chino:

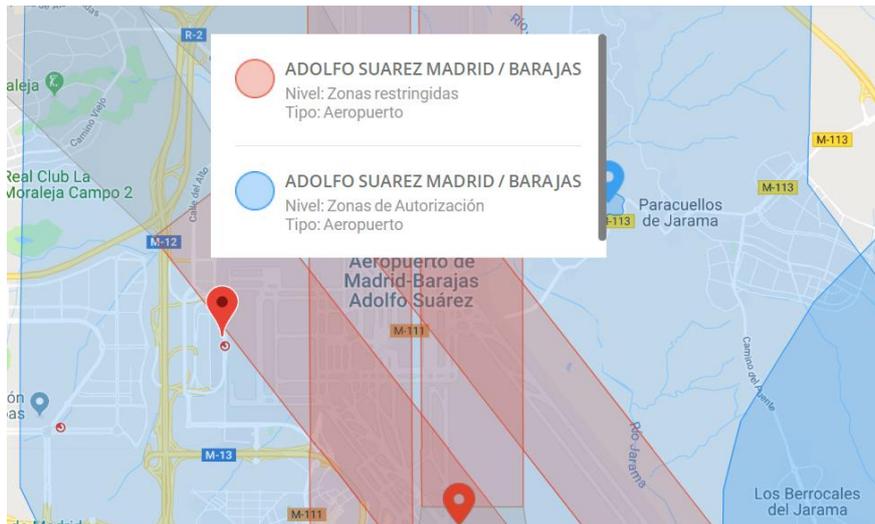


Figura 27: Captura de la aplicación GEOMap de DJI. Fuente: [www.dji.com](http://www.dji.com)

En Europa, la nueva normativa contemplará, además de un registro de operadores con el objetivo de cruzar datos con otros países, matrículas electrónicas para las aeronaves no tripuladas, así como sistemas de *geofencing* para evitar volar en zonas restringidas. Además, existirán categorías abiertas y específicas para operar y en el caso de operaciones de mayor riesgo, se establecerán unas categorías certificadas. Las tecnologías de identificación se detallan en el siguiente apartado.

#### 6.1.4 Identificación de drones

El concepto de integración de los drones en el espacio aéreo, requiere su identificación mediante un medio global, flexible y confiable que resuelva las etiquetas de identificación a través de un sistema de resolución basado en la red u otros mecanismos, como los que se detallan a continuación.

##### 6.1.4.1 Identificación mediante etiquetas OID

Una propuesta para la identificación de drones se basa en la plataforma de identificación basada en IoT (*Internet Of Things*) desarrollado por la UIT-T e ISO y que se están generalizando para identificar todo tipo de objetos. Se trata de los Identificadores de Objetos OID (*Object Identifiers*). En concreto, la recomendación UIT-T X.676 especifica un marco de resolución basado en OID para identificar varios servicios en entornos IoT. OID nombra un objeto con un espacio de nombres asignado jerárquicamente. En el ámbito IoT, se proporcionarán miles de servicios basados en recursos heterogéneos como combinaciones de diversos servicios. Para mayor eficiencia, se requerirán diversas tecnologías, como la vinculación de servicios dinámicos o servicios de conmutación, junto con la resolución e identificación de servicios agrupados. Esta Recomendación describe los conceptos de servicios agrupados de IoT, consideraciones, arquitecturas y procedimientos para un marco de resolución basado en OID para servicios agrupados de IoT [51].

Los OID son atractivos para identificar drones porque son completamente abiertos, tienen una estructura numérica simple, compacta y permite muchos tipos diferentes de implementaciones construidas alrededor de ellas. Estas estructuras pueden estar ordenadas por país, organización, sector del producto y todas pueden existir al mismo tiempo. El propietario de la estructura junto a los usuarios finales también puede controlar la disponibilidad de la información y los niveles de confianza. Por ejemplo, la

OACI usa identificadores bajo el OID 1.3.27 para su plataforma de pasaporte biométrico [52].

La adopción de una plataforma de identificación OID para drones civiles es solo un paso necesario para establecer un marco de identificación mundial común. Los próximos pasos requerirán especificaciones e implementaciones adicionales a través de múltiples organismos intergubernamentales, autoridades nacionales y proveedores [53].

#### 6.1.4.2 Identificación mediante SIM integrada

La compañía Ericsson, propone un sistema de identificación de drones basado en la Identidad Internacional de Equipos Móviles (IMEI) que se utiliza para identificar un teléfono o dispositivo móvil, y la Identidad Internacional del Abonado Móvil (IMSI) que se emplea para identificar a un usuario dentro de una red móvil. Los perfiles del suscriptor y del proveedor de conectividad móvil integrados en la tarjeta SIM, se suministran dinámicamente en la SIM integrada (eSIM) o en la Tarjeta de Circuito Integrado Universal Integrada (eUICC). Esto asegura una solución resistente a la manipulación indebida para la identificación de drones. Teniendo esto en cuenta, Ericsson propone usar el IMEI e IMSI como soluciones de identificación de drones y sus operadores, respectivamente, lo que proporciona una forma robusta y segura de obtener certificados de autenticidad para estos dispositivos. Existen dos categorías principales para la identificación de drones y que actualmente están soportadas por las redes móviles:

- **Difusión local:** puede utilizar las capacidades de comunicación LTE *sidelink* V2X e integrarse en los microchips de los móviles.
- **Publicación en red:** son inherentemente compatibles con la conectividad de datos proporcionada a los suscriptores móviles.

Uno de los principales beneficios de usar la tecnología móvil para ambos modos de identificación es que la comunicación está encriptada y utiliza un canal seguro tanto para la transmisión local como para los mecanismos de publicación en red. Además, las soluciones basadas en telefonía móvil, pueden usarse para acceder tanto a la información de publicación como a la red, por lo que no se requieren receptores especializados.

Con esta tecnología, además de identificar los drones, también se puede monitorear el dron a lo largo del tiempo. Esto es importante para garantizar que los sistemas de gestión de tráfico de drones UTM tengan información actualizada sobre las ubicaciones de cada dron, así como para poder localizarlos en el espacio aéreo [54].

#### 6.1.5 Técnicas de posicionamiento basado en redes móviles

La red de telefonía móvil es una infraestructura ampliamente distribuida que se puede usar para ubicar y respaldar las operaciones con drones.

Para proporcionar su ubicación, los drones podrían incorporar un chip LTE (4G) con un receptor de posicionamiento global GNSS integrado (GPS, por ejemplo) y así podría informar de su ubicación al sistema UTM u otros sistemas de tierra a través de la red. De manera similar a la identificación, la información de ubicación puede ser almacenada por un servidor para ser consultados en cualquier momento y, además, ser utilizados por el sistema UTM para verificar que el dron cumple con el plan de vuelo aprobado. Emplear este sistema de ubicación basado en la red móvil es muy interesante desde el

punto de vista de la seguridad del vuelo, ya que los sistemas GNSS son susceptibles de ser *hackeados*, pudiendo reportar una ubicación falsa o incorrecta [55]. Entre las soluciones de ubicaciones basadas en la red LTE se encuentran las técnicas que se detallan a continuación:

#### 6.1.5.1 OTDOA (*Observed Time Difference Of Arrival*)

La técnica OTDOA es una solución de posicionamiento que se puede emplear para orientar el dron en entornos urbanos e interiores, donde las señales GNSS no pueden usarse debido a la falta de línea de visión directa (LOS) con los satélites. Este método de estimación de la posición se basa en la medición de la diferencia de tiempo de llegada TDOA (*Time Difference Of Arrival*) de señales de referencia incrustadas en la señal de enlace *downlink* del dron recibidas en diferentes eNB (eNode B) de la red LTE. Cada una estas mediciones describen una hipérbola donde los puntos F1 y F2 son los dos eNB medidos. La medición debe tomarse al menos para tres pares de estaciones base. La posición del dispositivo sería la intersección de las tres hipérbolas para las tres estaciones base medidas (A-B, A-C, B-C), tal y como se muestra en la siguiente figura:

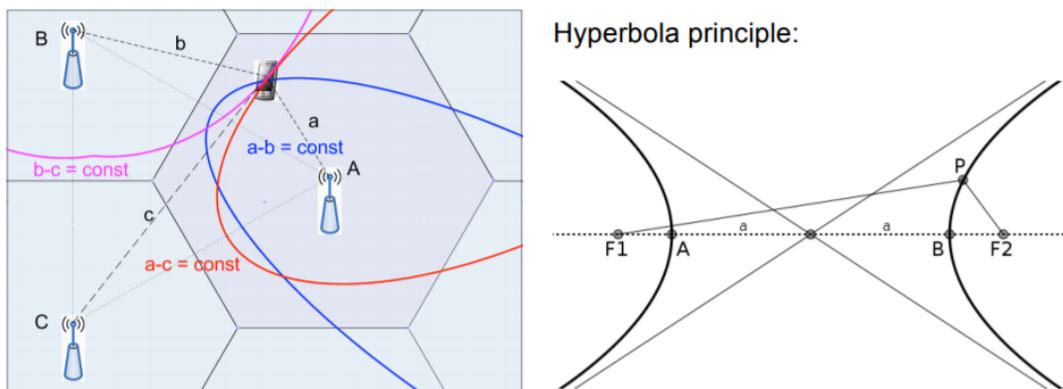


Figura 28: Medición TDOA basada en hipérbolas. Fuente: [55]

En el caso del modo de posicionamiento híbrido (aquel que emplea las redes móviles y GNSS para posicionarse), las mediciones de la señal de referencia se pueden combinar con las mediciones del receptor GNSS para calcular la posición del dispositivo con mayor precisión.

#### 6.1.5.2 E-CID (*Enhanced Cell ID*)

El método de Identificación de Celda Mejorada (E-CID) para la estimación de la posición basada en redes LTE, está basado en la técnica de posicionamiento móvil COO (*Cell Of Origin*) que se emplea para encontrar la ubicación de la celda desde la que llama un teléfono móvil [56]. Con COO, se estimaría la posición del dron utilizando las coordenadas geográficas del eNB de la red LTE a la que esté conectado. El conocimiento de la celda de servicio se puede obtener ejecutando una actualización del área de seguimiento o por paginación. La precisión de la posición está vinculada, en este caso, al tamaño de la celda, ya que el servidor de ubicación solo es consciente de que el dron está siendo atendido por esa estación base.

Este método de posicionamiento no es muy preciso por lo que se usa dentro de las redes LTE para dispositivos que no tienen un receptor GNSS integrado. Además de utilizar el conocimiento de las coordenadas geográficas de la estación base, la posición del dispositivo se estima con mayor precisión al realizar mediciones de señales de radio. El método E-CID se puede ejecutar de tres maneras, utilizando diferentes tipos de

mediciones en función de la distancia a la estación base, tal y como se muestra en la siguiente figura:

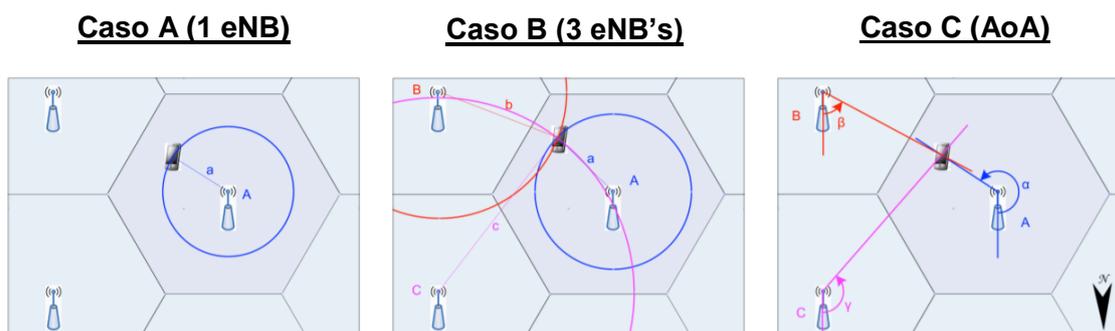


Figura 29: Métodos de Identificación Celular Mejorada (E-CID). Fuente: [55]

- **Caso A:** E-CID con la estimación de la distancia desde una estación base.
- **Caso B:** E-CID con la medición de la distancia desde 3 estaciones base.
- **Caso C:** E-CID midiendo el Ángulo de Llegada (AoA, *Angle Of Arrival*) de al menos 2 estaciones base (aunque mejor 3)

En cuanto a la precisión del posicionamiento de cada método, en el **caso A**, la precisión correspondería a la de encontrar el dron sobre una circunferencia. Los métodos de los **casos B** y **C** proporcionan la precisión de un punto sobre el plano, mientras se miden más fuentes. En los **casos A** y **B**, las mediciones son realizadas por el dispositivo móvil incorporado en el dron y, por lo tanto, son asistidas por el mismo. Para el **caso C**, las mediciones son tomadas por la estación base y, por lo tanto, son asistidas por las eNB.

En 2017, Vodafone demostró la capacidad de rastrear un dron utilizando su tecnología de posicionamiento por radio (RPS, *Radio Positioning System*), que es una variante de la técnica E-CID y, por lo tanto, independiente de los sistemas GNSS [57]. Aunque el uso de RPS no está ampliamente extendido, dada la ubicuidad de los receptores GNSS de los módems LTE, este ensayo demuestra que dichas técnicas pueden usarse para complementar y verificar cualquier información de ubicación de los drones basadas en GNSS.

Los métodos de posicionamiento expuestos anteriormente, han sido estandarizados por el 3GPP dentro de un marco común conocido como Arquitectura de Servicios de Ubicación (LCS) [58, p. 271]. A través de la Asociación GSM (GSMA), los operadores móviles están buscando la forma de desarrollar aún más estos servicios y trabajar conjuntamente con los fabricantes de drones para garantizar el cumplimiento de los requisitos de los sistemas UTM [59].

## Conclusiones

Si bien las soluciones propuestas para la identificación y el posicionamiento que utilizan la tecnología móvil se pueden aplicar a los drones con usos malintencionados, como se ha comentado al principio del trabajo, es posible que hayan drones que usen otro tipo de sistemas de comunicación o que no usen sistemas anticolidión basados en "Detectar y Evitar". Por ello, se están desarrollando diferentes tecnologías para detectar drones basados en emisiones de radio, radares de baja altitud, detección de video o audio combinados con triangulación y que se deben implementar en áreas próximas a las instalaciones críticas que se está protegiendo.

Por otro lado, la instalación de dispositivos móviles en los drones basados en IMEI y IMSI con tarjeta eSIM integrada, es una forma rentable y eficaz de implementar sistemas de detección e identificación de drones ya que se aprovechan de las tecnologías y las infraestructuras de las redes de telefonía móvil disponibles. Aun así, dado el riesgo de manipulación de estos dispositivos de identificación, deben implementarse soluciones para neutralizar drones que representen un riesgo para la seguridad aérea y para las personas. Estos dispositivos de defensa se mostrarán en el apartado 7.3.

## 6.2 Tecnologías de comunicación de los drones

En la actualidad, los drones emplean para el control y el envío de datos de telemetría o video en *streaming*, distintas tecnologías basadas en diferentes estándares, como los que se detallan en los siguientes apartados.

### 6.2.1 WiFi

La tecnología *Wifi* se rige bajo las especificaciones del estándar IEEE 802.11. Actualmente, es una de las tecnologías más usadas para la conexión a Internet de forma inalámbrica gracias a su eficiencia, versatilidad y, sobre todo, su expansión a nivel global. Pero también se emplea para la comunicación con los drones, usando las bandas de frecuencia de 2,4 y 5 GHz. En la banda de 2,4 GHz, ofrece hasta 14 canales de transmisión con un ancho de banda de 20 MHz (en la especificación se fija en 22 MHz), mientras que en la banda de 5 GHz posee hasta 24 canales sin solapamiento. Además, esta última posee menos interferencias, ya que aún no existen muchas tecnologías que operen a esta frecuencia y la mayoría de los dispositivos *Wifi* emplean la opción de los 2,4 GHz.

La comunicación entre la estación base (o mando de control) y el dron se suele producir gracias a que el propio dron genera su propia red *Wifi* en modo *ad-hoc* a la cual se conecta la estación base. Además, existen otras razones que han favorecido su implementación en este tipo de vehículos aéreos no tripulados [60]:

- En el caso de que se emplee la frecuencia de 2,4 GHz se logra un alcance medio de unos 100 metros en una superficie despejada, sin interferencias y sin el uso de repetidores. Si se emplea la frecuencia de 5 GHz el alcance es inferior en iguales condiciones de potencia de emisión. Esto se debe a que cuanto mayor sea la frecuencia empleada, mayor será la atenuación en espacio libre, lo cual afectaría a la cobertura. Por este motivo, se emplea en mayor medida la banda de 2,4 GHz.
- Gran ancho de banda y velocidad de transmisión, hasta 54 Mbps compartidos en la mayoría de las redes *Wifi* y hasta 1,3 Gbps en la tecnología más avanzada (802.11ac).
- Resulta muy sencillo y asequible el manejo de drones con este tipo de tecnología, debido a que en muchas ocasiones tan solo se necesita un *smartphone* o *tablet* para manejar y/o visualizar estos vehículos, omitiendo así la necesidad de usar un mando por control remoto con una pantalla adicional.

En cuanto a las desventajas que presenta esta tecnología para drones más profesionales:

- Mayor probabilidad de sufrir interferencias que podrían interrumpir el enlace de comunicaciones, ya que la banda de 2,4 GHz se usa en gran número dispositivos.

- Debido a su mayor uso, tiene una mayor posibilidad de ser interferidos mediante el método de *jamming* (interferencia intencionada) por parte de *hackers* perdiendo así el enlace de control vía Wifi.



Figura 30: Dron DJI 1 que usa la banda de 2,4 GHz en su enlace de comunicaciones. Fuente: [61]

En el caso del enlace de video, se suele utilizar la banda de frecuencia de 5,8 GHz, aunque también se usan las bandas de 1,2 y 2,4 GHz. Para el enlace de telemetría la banda más empleada en Europa es la de 433 MHz, aunque en Estados Unidos se emplea la banda de 900 MHz, ya que está libre de licencia [20].

En cuanto al alcance, depende de la longitud de onda, el tipo de modulación y la potencia de transmisión, así como de las características del entorno de propagación (meteorología, montañas, muros...). Si se consideran unas condiciones óptimas, el alcance máximo operativo que se puede alcanzar (sin el uso de satélites) con una señal en la banda de 900 MHz y en operaciones VLOS es hasta 64 km. En el caso de la banda de 2,4 GHz el rango máximo suele ser de 2 km, bastante inferior. Como inconvenientes mencionar la reducción del ancho de banda y el incremento de tamaño de la antena receptora cuanto menor sea la longitud de onda de la señal [20].

En cuanto a las técnicas de modulación, principalmente se emplean las de espectro ensanchado (*spread spectrum*) que se detallan a continuación:

- **FHSS (*Frequency Hopping Spread Spectrum*)**: la modulación de espectro ensanchado por salto de frecuencia se basa en la transmisión de la señal en distintas frecuencias pseudoaleatorias de acuerdo con un patrón de salto compartido entre los transmisores. El momento en el que ha de cambiar de frecuencia viene dado por cierto espacio de tiempo llamado *dwell time* (inferior a 400 ms) el cual ha de ser conocido. Las ventajas que este tipo de técnica ofrecen son sustanciales, como pueden ser la resistencia al ruido y a las interferencias, la dificultad a la hora de interceptarlas (debido al constante cambio de frecuencia) y la posibilidad de que varios dispositivos usen el mismo canal, ya que apenas se producen interferencias. A pesar de esto, esta técnica tiene una escasa eficiencia, lo que se traduce en un reducido ancho de banda [62]:

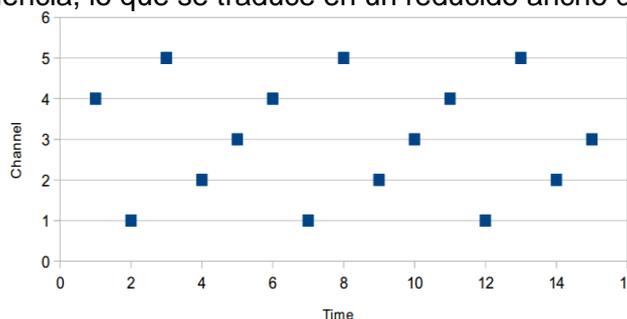


Figura 31: Esquema de modulación FHSS. Fuente: [62]

- **DSSS (*Direct Sequence Spread Spectrum*):** la modulación de espectro ensanchado por secuencia directa, genera una secuencia de bits pseudoaleatoria, redundante y compuesta por una secuencia de 1 y -1 (conocida como secuencia de *Barker*) que utiliza como pseudoruido para modular todos y cada uno de los bits de la señal de transmisión. De este modo solo quien recibe dicha secuencia podrá reconstruir la señal original. La principal ventaja de este método es la dificultad que presenta para la interceptación la señal, así como la gran resistencia al ataque por *jamming*. Otra característica es la posibilidad de que varios dispositivos compartan el mismo canal sin sufrir interferencias [62].
- **SC-FDM (*Single Carrier Frequency Division Multiple Access*):** esta técnica de modulación, desarrollada por los investigadores de la Universidad Nacional de *Pukyong* en Corea del Sur, mejora la eficiencia y seguridad del enlace *downlink* (entre el dron y el GCS u operador de tierra). La técnica permitiría aumentar el tiempo de vuelo, la velocidad de transmisión de datos y la fiabilidad del enlace de comunicación en los vuelos de los aviones no tripulados, especialmente en aquellos que se utilizan para operaciones de búsqueda y rescate o tareas de servicios de entrega de paquetería. La técnica se basa en un tipo de modulación híbrida que combina la flexibilidad de asignación de frecuencia y la resistencia multitrayecto de OFDM (*Orthogonal Frequency-Division Multiplexing*) y otras características importantes de un sistema de una sola portadora. Además, al analizar los resultados de su trabajo, han encontrado que BPSK y QPSK son esquemas de modulación óptimos para la técnica de modulación SC-FDM dentro de la banda de 2,4 GHz [5].

## 6.2.2 Redes LTE

En 2017, investigadores de la compañía Ericsson crearon un grupo de trabajo donde debatieron sobre los siguientes retos en cuanto a la conectividad con los drones mediante redes de telefonía móvil:

- **Cobertura:** las redes móviles existentes están optimizadas para comunicaciones de banda ancha terrestre. Las antenas de la estación base suelen estar inclinadas hacia abajo para reducir la interferencia entre las celdas y optimizar la cobertura terrestre. Esto significa que, los drones, al sobrevolar las estaciones base, estarían enfocados únicamente por los lóbulos laterales de las portadoras de la señal móvil, por lo que los investigadores se preguntan si la cobertura en el aire sería suficiente.
- **Interferencias:** en el espacio aéreo, la atenuación de propagación está más cercana a la propagación en el espacio libre. Por lo tanto, los drones generan más interferencias en las redes en el enlace *uplink* y sufren más interferencias en el enlace *downlink*, por lo que se requieren técnicas de mitigación de interferencias.
- **Soporte a la movilidad:** la asignación de celdas móviles en el espacio aéreo es bastante diferente a la asignación que se requiere en tierra por lo que se plantea cómo optimizar el soporte de movilidad para drones en el aire.

Tras estas cuestiones, deciden plantear varias métodos para agregar conectividad móvil a los drones, además de la forma tradicional y expuesta en el apartado anterior vía radio directamente mediante un enlace C2 (método 0):



Figura 32: Posibles formas de conectividad. Fuente: [63]

El método 1, consiste en dotar de conectividad móvil al control remoto conectando un teléfono móvil al controlador, pero se seguiría utilizando un enlace directo al dron para controlar su vuelo. De esta manera, el conocimiento del espacio aéreo del piloto se puede mejorar, ya que la información como las restricciones del espacio aéreo, las alarmas y las advertencias se pueden mostrar al durante toda la operación en tiempo real.

El método 2, trata de conectar el dron a la red móvil y usar la conectividad móvil para el comando y control. Esto mejora la seguridad porque toda la información en tiempo real del dron se puede enviar a través de la red móvil al sistema UTM. Además, ello permitiría realizar operaciones BVLOS ya que se puede emplear la amplia cobertura de la red para controlar el dron [63]. En las siguientes líneas se profundizará en este segundo método.

Para realizar las pruebas en el método 2, se consideró un escenario rural en el que se tiene un ancho de banda LTE de 10 MHz a una frecuencia de portadora de 700 MHz. Cada estación base tiene dos antenas con polarización cruzada a una altura de 35 m con 6° de inclinación hacia abajo. El diagrama de antenas de la estación base utilizado en la simulación se ilustra en la siguiente imagen:

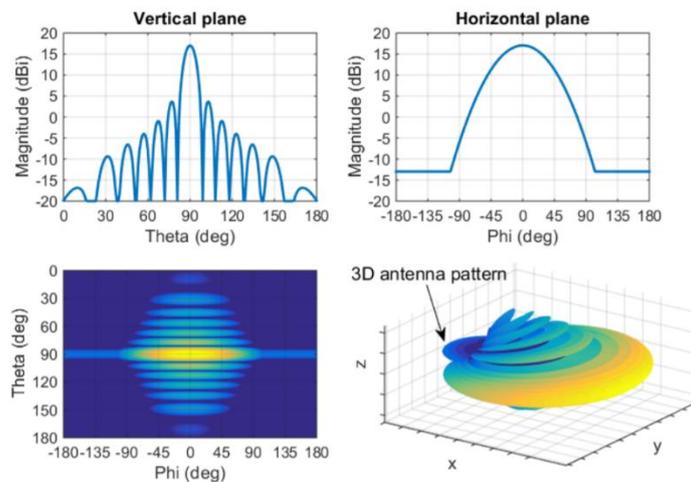


Figura 33: Diagrama de antena de cada estación base. Fuente: [64]

Tras la realización de las pruebas y simulaciones, los resultados fueron los siguientes:

En la Figura 34, se muestran las distribuciones de la ganancia de acoplamiento del enlace descendente en tres alturas diferentes. Uno está a 1,5 m, que es el nivel del suelo. El segundo está a 40 m, que es 5 m más alto que la altura de la antena de la estación base, y el último está a 120 m, que es el límite actual que impone la FAA para volar con drones en EE.UU. Por lo tanto, podemos ver que a 40 y 120 m, la ganancia de acoplamiento del enlace descendente es un 5% mayor que su contraparte en el nivel

del suelo. Esto significa que la propagación es más favorable en el aire, lo podría compensar la reducción de ganancia de la antena de la estación base.

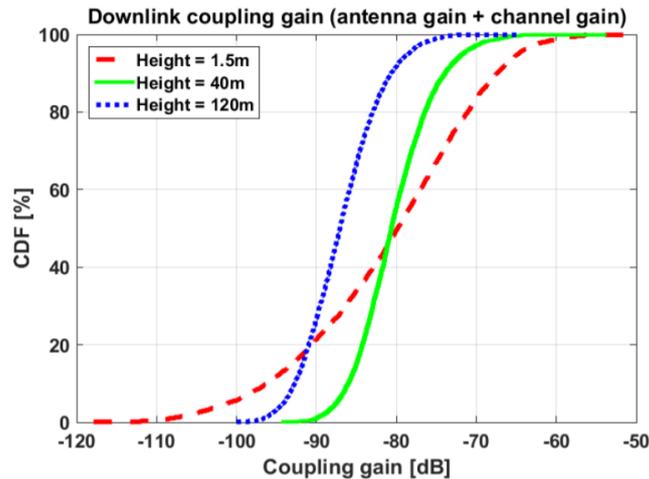


Figura 34: Ganancia de acoplamiento de enlace descendente (Ganancia de antena + canal). Fuente: [64]

En la Figura 35 se muestra la distribución SINR (Relación Señal a Ruido + Interferencia) del enlace descendente a tres alturas diferentes. En esta figura se puede ver que las distribuciones de SINR del enlace descendente tanto a 40 m como a 120 m son estadísticamente peores que sus contrapartes a nivel del suelo. Esto implica que la calidad de la señal es peor en el aire y, por este motivo, es posible que se necesiten algunas técnicas de mitigación de interferencias para operar los drones.

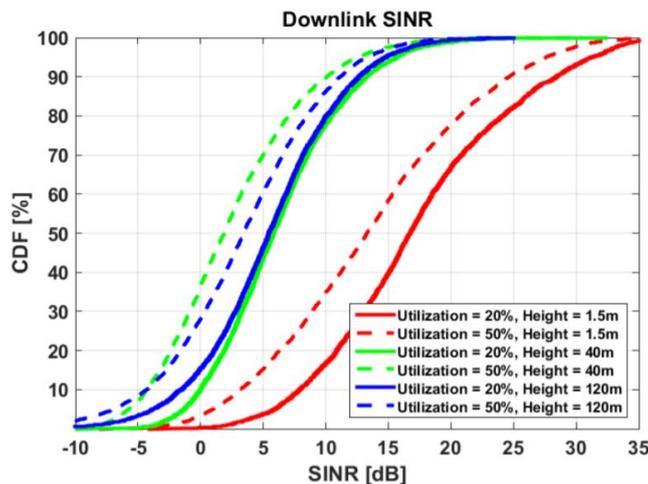


Figura 35: Ganancia de acoplamiento de enlace descendente (SINR). Fuente: [64]

En cuanto a la cobertura radio, las mediciones empíricas han demostrado que los canales de radio aéreos presentan diferentes características de propagación en comparación con los canales de radio terrestres. Una característica distintiva de los canales de radio aéreos es la mayor probabilidad de propagación en línea de visión directa debido a la ausencia de obstáculos en el cielo. En general, a medida que aumenta la altitud, la propagación se acerca más a la propagación en el espacio libre.

Como se ha dicho antes, las redes móviles en la actualidad están optimizadas para la comunicación terrestre de banda ancha ya que las antenas de las estaciones base están inclinadas hacia abajo para optimizar la cobertura en tierra y reducir la interferencia entre las celdas. Por este motivo, los drones que vuelan en el espacio aéreo pueden ser

alcanzados por los lóbulos laterales de las antenas, que tienen una menor ganancia. Sin embargo, la mayor probabilidad de propagación de la línea de visión puede compensar las reducciones de ganancia de la antena y, en algunos casos, puede dar lugar a intensidades de señal aún más fuertes.

En la Figura 34 se muestran los patrones de asociación de células basados en la potencia máxima recibida a nivel del suelo y a alturas de 50, 100 y 300 m en una macro red LTE rural simulada. Los dispositivos en las áreas marcadas con el mismo color están asociados con el mismo lugar. Se puede ver que los patrones de asociación de células cambian dramáticamente con la altura. A una altitud de 300 m, el patrón de los lóbulos laterales de la antena es claramente visible en el patrón de asociación de celdas:

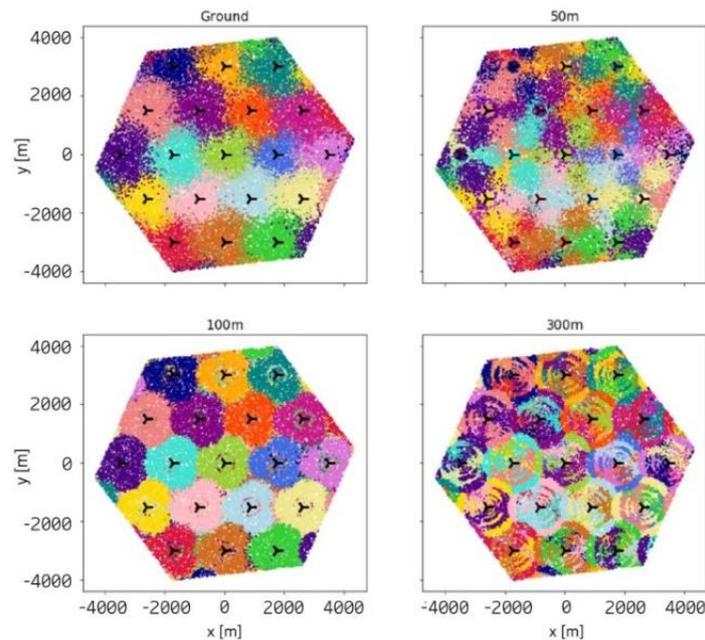


Figura 36: Patrones de asociación de celdas a diferentes altitudes. Fuente: [64]

Las redes LTE terrestres actuales pueden proporcionar un buen soporte de movilidad para el despliegue inicial de un pequeño número de drones, pero podrían surgir nuevos desafíos para la movilidad si la densidad de drones es muy alta o si vuelan en entornos de propagación radio más difíciles.

Tras los resultados de las pruebas anteriores, se identificaron dos problemas fundamentales:

- Cuando los drones se mueven a través de los nulos de los lóbulos laterales de las antenas de la estación base, el dron puede responder con lentitud a las órdenes que se envíen mediante los comandos de mando y control dentro de la red.
- Los drones pueden tener dificultades para establecer y mantener la conexión a la red si están en un entorno de propagación radio VLOS cerca de muchas celdas, ya que las celdas vecinas causan niveles de interferencia muy altos.

Estos resultados se pueden emplear para optimizar la conectividad móvil y proporcionar así un mejor rendimiento para los drones mientras se mantiene el de los dispositivos móviles en tierra. Sin embargo, los investigadores consideran que estos retos se resolverían con las futuras redes 5G, ya mejoraría el rendimiento de las redes lo que supone proporcionar una conectividad más rápida y eficiente para los drones que las actuales redes LTE [64].

### 6.2.3 Redes 5G

Tal y como se comenta al final del apartado anterior, los investigadores de la compañía Ericsson predicen que las redes 5G significarían un gran avance en la conectividad móvil de los drones. En el libro blanco sobre nuevos avances en este aspecto, la compañía reconoce que las redes móviles podrían estar bien adaptadas para soportar la comunicación de aviones no tripulados de baja altitud y para integrarse con los futuros Sistemas de Gestión de Tráfico de Aeronaves no tripuladas (UTM) para mejorar la seguridad de las operaciones.

En un capítulo anterior, se ha visto que los drones se utilizan ampliamente para fotografía y videografía, así como para usos industriales u otros fines. En este sentido, la compañía Qualcomm Technologies, Inc., también prevé que estas redes de nueva generación permitirán implementaciones a gran escala en el uso de drones en lugares críticos como en la gestión de tráfico aéreo UTM, usando la alta velocidad de conexión de Gb/s, con experiencia de usuario y anchos de banda mayores

La compañía destaca, entre otras, las mejoras que se representan en la siguiente imagen:

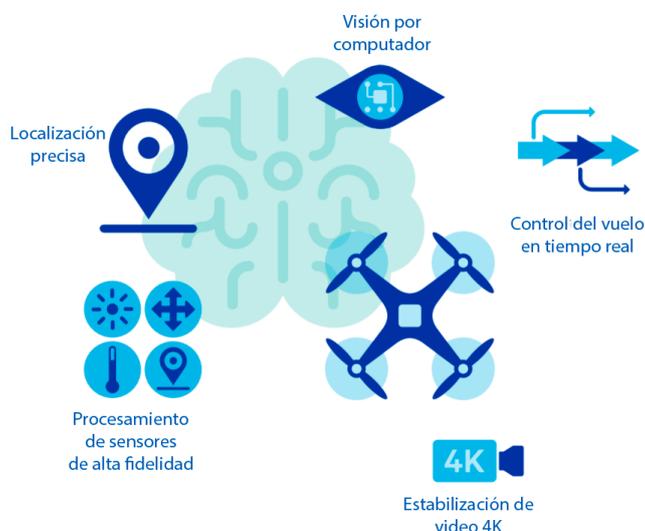


Figura 37: Futuras aplicaciones tecnológicas de la red 5G. Fuente: Qualcomm

Además, gracias a la alta capacidad y velocidad de la red 5G se podrían coordinar, controlar y manejar la ingente cantidad de información que enviarían miles de drones interconectados a la red y a los sistemas de control de tráfico aéreo, lo cual permitirá despliegues de aviones no tripulados más seguros, masivos y a mayor distancia en coordinación con el control de tráfico aéreo en entornos de espacio aéreo controlados y no controlados.

En este sentido, en 2016, Qualcomm junto a la operadora de telefonía AT&T comenzaron un estudio de cómo los drones podrían operar en las futuras redes 5G. El equipo pretendía analizar la cobertura, la potencia de señal y la movilidad a través de las células de la red y cómo responden en vuelo. El objetivo de los ensayos y la investigación era ayudar a habilitar futuras operaciones con drones, como BVLOS, a medida que las regulaciones evolucionan para permitirlos. La capacidad de volar más allá del alcance visual de un operador podría permitir la entrega exitosa de mercancías, la inspección remota y la exploración. La tecnología inalámbrica que proporcionan los futuros estándares, pueden aportar muchas ventajas a los drones, como la cobertura ubicua, el soporte móvil de alta velocidad, seguridad robusta, alta confiabilidad y calidad

de servicio (QoS, *Quality Of Service*). El vicepresidente ejecutivo y director de tecnología de Qualcomm Technologies Matt Grob, dijo que "La prueba con un operador con el alcance y la tecnología de AT&T es un paso importante en el desarrollo de tecnologías de conectividad para sistemas de aeronaves no tripuladas pequeñas, incluida la optimización de redes LTE y el avance de la tecnología 5G para drones" [65].

En conclusión, las redes móviles brindan conectividad inalámbrica segura en área muy extensa (tan amplia como la cobertura de la red móvil), utilizando tecnología probada basada en espectro móvil con licencia y estándares globales. Se han evaluado el rendimiento de las redes móviles para la comunicación de drones en el aire y se ha encontrado que actualmente, las redes LTE son capaces de soportar el despliegue inicial de aviones no tripulados de baja altitud aunque las capacidades significativamente mejoradas de las próximas redes 5G, proporcionarán una conectividad móvil nunca vistas hasta ahora, con unas elevadas tasas de transmisión de datos y unas latencias muy bajas (del orden de pocos milisegundos), lo cual permitirá, desde el punto de vista del dron, el envío de imágenes en ultra alta definición (4k) en *streaming*, aumentar la velocidad de respuesta de los sistemas de control de los drones a las órdenes del operador remoto y mejorar las respuesta de los sistemas S&A, ya que las señales que provienen del exterior serían procesadas con mayor rapidez.

Todo ello contribuirá a la integración y el desarrollo de un espacio aéreo más seguro.

En la siguiente tabla se muestra una comparativa de las diferentes tecnologías de comunicaciones que pueden emplearse actualmente para el comando, control, telemetría y envío de imágenes en los drones:

Especificación	WiFi	LTE 4G	5G
<b>Estándar/ versión</b>	802.11 b/g/n/ac	3GPP versión 10	3GPP versión 15
<b>Banda de frecuencias</b>	2,4 – 5,8 GHz	2 a 8 GHz	3 a 300 GHz
<b>Velocidad de datos</b>	54 Mbps – 1 Gbps	2 Mbps a 1 Gbps	> 10 Gbps
<b>Latencia</b>	Variable	20-100 ms	1-2 ms
<b>Alcance medio</b>	0,1 – 2 km	Depende de cobertura de la red	Depende de cobertura de la red
<b>Capacidad MIMO</b>	Sí	Sí	Sí
<b>Máx. nº drones conectados</b>	Depende del BW	Hasta 250/ sector	> 1000/ sector

Tabla 4: Comparativa de tecnologías de comunicación de drones.

## 7. Soluciones de integración de drones en el entorno aeroportuario

### 7.1 Situación actual de la integración de drones en el espacio aéreo.

En la actualidad, existen muchos desafíos para el desarrollo de un sistema de gestión de tráfico aéreo convencional que se pueda emplear para manejar las operaciones con drones de pequeño tamaño (inferior a 25 kg) operando a baja altura, es decir, a una altitud inferior a 150 metros. Sin embargo, a petición de la Comisión Europea, a través de la *Single European Sky ATM Research Joint Undertaking* (SJU) y la agencia Eurocontrol, se ha diseñado una hoja de ruta para conseguir la integración segura de los drones en el espacio aéreo civil.

La idea es desarrollar un sistema de gestión de tráfico aéreo para sistemas de aviación no tripulados, UTM (*UAS Traffic Management*), con funciones similares a las existentes para la gestión de tráfico aéreo de aviación comerciales (ATM), pero con infraestructuras y servicios adaptados a las especificidades de las operaciones con estas aeronaves. Pero no es tan sencillo. En la actualidad existen planos, documentos conceptuales e incluso tecnologías, pero no se sabe aún cómo aplicarlas técnica e institucionalmente a nivel europeo. "Tenemos que asegurarnos de que al integrar los aviones no tripulados más pequeños en los niveles más bajos del espacio aéreo no afectarán negativamente al lado tripulado (y en el futuro no tripulado) de la aviación civil", dice Mike Lissone, encargado de integración de UAS ATM para Eurocontrol. Este sistema de integración, al que han denominado U-Space, tiene como principal inconveniente la cantidad de organismos regulatorios, de certificación y de políticas de diferentes países involucrados a nivel europeo. A pesar de ello, la integración desde el punto de vista tecnológico puede resultar más sencilla debido a la cantidad de proveedores de sistemas UTM que existen en el continente y de empresas tecnológicas que pueden contribuir con su experiencia, conocimientos y tecnologías al desarrollo de este proyecto. No obstante, Mike Lissone es optimista dado que Eurocontrol ha desempeñado un papel fundamental durante muchos años en el desarrollo de conceptos y regulaciones europeos y globales para la integración de vehículos aéreos tripulados y no tripulados dada su experiencia en el desarrollo de normativas dentro de la OACI, como la Circular 328 de Sistemas de aeronaves no tripuladas (UAS) de 2011 [66] y cuyos puntos principales se han descrito en el capítulo 5 de este trabajo.

El sistema U-Space complementará al sistema de gestión de tráfico aéreo tradicional y se coordinará con él para garantizar la seguridad entre las operaciones de aeronaves tripuladas y no tripuladas. Entre las funciones más importantes se encuentran:

- Seguridad a niveles de baja altitud que será tan buena como la de la aviación tradicional.
- Sistema automatizado que proporcionará información a los drones para volar de forma segura y evitar obstáculos o colisiones, proporcionando un sistema de gestión de espacio aéreo y definiendo posibles limitaciones físicas de intrusión mediante *geofencing*.
- La separación de obstáculos y la previsión de meteorología adversa para la operación segura de los drones.
- El seguimiento continuo de los vuelos, identificando las operaciones no autorizadas.

El sistema está principalmente enfocado a la gestión de vuelos a muy baja cota, por debajo de los 120 o 150 m sobre el terreno, aunque dicha limitación dependerá de cada país. Su funcionamiento se basa en una gestión centralizada de planes de vuelo por lo que, previamente a la ejecución del vuelo, el operador habilitado deberá remitir el plan de vuelo que pretende realizar al sistema UTM, donde se analizará y se contrastará con otros planes de vuelos registrados. En caso de que proceda, se comparará con la información facilitada por los sistemas de gestión de tráfico ATM para su coordinación con el mismo. El propio sistema, como resultado del análisis, podrá proponer de forma automática cualquier modificación al plan de vuelo solicitado.

Durante el vuelo, la aeronave será monitorizada por la unidad de gestión de tráfico, con el fin de verificar el cumplimiento del plan de vuelo y proporcionar al piloto información en tiempo real sobre aspectos no planificados que puedan interferir en la operación. Una vez finalizado el vuelo, el sistema almacenará toda la información relativa al mismo que podrá ser remitida posteriormente al piloto y a las autoridades para una posible implementación de mejoras en su operativa.

El sistema U-Space permitirá ampliar las perspectivas de utilización de los drones, ya que facilitará la integración de vuelos de aeronaves autónomas, la realización de misiones más allá del alcance visual (BVLOS), la gestión de vuelos simultáneos de varios drones por un solo operador y la integración total en entornos urbanos.

En la siguiente infografía se muestra un boceto de lo que sería el sistema U-Space una vez implantado:



Figura 38: Concepto del sistema de integración U-Space. Fuente: [11]

La implantación del sistema U-Space consta de cuatro etapas que se irán desarrollando de forma progresiva en una ventana temporal que va desde el año 2019 hasta el 2035, en función del desarrollo de las tecnologías que se han estudiado en el capítulo anterior.

Las etapas y su descripción se muestran en la siguiente tabla:

Etapa U-Space	Descripción	Servicios UTM	Año implantación
U1	<b>Servicios Fundacionales:</b> serán la base del sistema de integración	<ul style="list-style-type: none"> <li>• Registro electrónico</li> <li>• Identificación electrónica</li> <li>• <i>Geofencing</i></li> </ul>	2019
U2	<b>Servicios iniciales:</b> proporcionarán soporte para la gestión de las operaciones de drones y las interfaces necesarias con las unidades de control de tráfico aéreo.	<ul style="list-style-type: none"> <li>• Planificación de vuelo</li> <li>• Aprobación de plan de vuelo</li> <li>• Seguimiento de información dinámica del espacio aéreo</li> <li>• Interfaz de procedimiento con ATC</li> </ul>	2022
U3	<b>Servicios avanzados:</b> proporcionarán soporte a las operaciones más complejas que se desarrollen en zonas de gran congestión de tráfico.	<ul style="list-style-type: none"> <li>• Gestión de capacidad</li> <li>• Asistencia para la detección de conflictos.</li> </ul>	2027/30
U4	<b>Servicios completos:</b> requerirán de un gran nivel de automatización, conectividad y digitalización del sistema para la integración completa de los drones dentro del espacio aéreo.	<ul style="list-style-type: none"> <li>• Nuevos servicios adicionales</li> <li>• Interfaces integradas con aviación tripulada</li> </ul>	2035

Tabla 5: Descripción de las etapas U-Space y año previsto de implantación

En la actualidad, la etapa que está más desarrollada es la U1 ya que se han desarrollado sistemas de comunicaciones y radiodetección que permiten proporcionar servicios de identificación de aeronaves, *geofencing*, S&A y otros sistemas que son de utilidad para identificar y neutralizar drones cuando suponen un peligro para la seguridad aérea [67]. Los avances en estas tecnologías, necesarios para la implantación total de la etapa U1, se han detallado en el capítulo 5.

## 7.2 Soluciones de integración propuestas por empresas y organismos internacionales

### 7.1.1. Solución propuesta por Ericsson

En un entorno de integración como U-Space, Ericsson plantea una arquitectura general para la gestión y operaciones del tráfico de aviones no tripulados como se muestra en la siguiente figura:

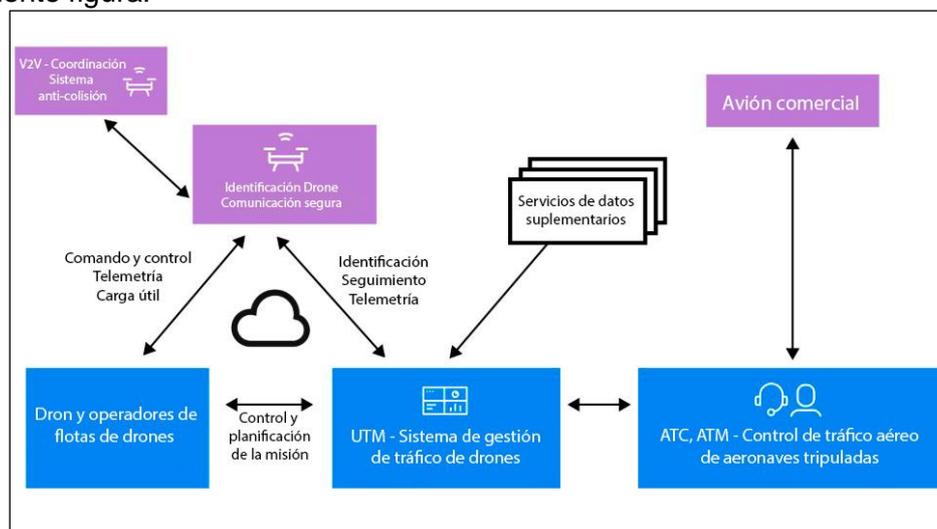


Figura 39: Elementos de un sistema UTM con identificación de drones. Fuente: Ericsson

El sistema UTM se encarga de las aprobaciones de los planes de vuelos de aviones no tripulados y de los drones no controlados. Además, también es responsable de la coordinación con la aviación tripulada y sus sistemas de control del tráfico aéreo, así como garantizar el cumplimiento de las restricciones del espacio aéreo de baja altitud. Los servicios de datos suplementarios tales como los servicios meteorológicos, por ejemplo, pueden proporcionar información al sistema UTM para ayudar a la toma de decisiones. Así mismo, los operadores de drones se conectarán al sistema para buscar la aprobación del plan de vuelo e informar periódicamente de su estado. Esto se puede conseguir, por ejemplo, proporcionando informes de telemetría para ayudar al sistema UTM a mantener un estado actualizado del espacio aéreo.

#### 7.1.1.1 Sistema de identificación

Como se vio en el apartado 7.1, las autoridades definen el requisito de identificación electrónica para la etapa U1 de U-Space, por lo que se requieren mecanismos para identificar de forma única a cada dron y también a sus operadores. Esta identificación debe ser segura y resistente a la manipulación. Más allá del etiquetado físico, se están considerando dos categorías principales para la identificación de drones. Por un lado, están las soluciones locales, que se basan en la transmisión de una señal de identificación por parte del avión no tripulado y que se puede leer en la zona donde está operando y, por otro lado, se prevén soluciones de publicación basadas en red y en el uso de conectividad móvil (ver apartado 6.1.4) en el que se publican los datos en un servidor remoto, probablemente ubicado en el sistema UTM [64].

Las redes móviles pueden ayudar con la identificación, autorización y *geofencing* de drones ya que están equipadas con una variedad de herramientas para identificar y autorizar a los usuarios y dispositivos que pueden acceder a las redes.

#### 7.1.1.2 Sistema de geolocalización

Un componente importante de las soluciones de rastreo de drones es el uso de sistemas GNSS. Los drones recuperan su información posicional de los receptores GNSS y, para su seguimiento, comunican esta información a un servidor central del sistema UTM. El inconveniente de esta solución es que los datos de telemetría proporcionados por un avión no tripulado pueden ser modificados fácilmente por un usuario malintencionado sin ser detectados por el sistema de gestión de tráfico de aviones no tripulados.

Los sistemas móviles también proporcionan un mecanismo de seguimiento de ubicación independiente. El sistema de posicionamiento móvil (MPS, *Mobile Positioning System*) se puede usar tanto para validar como para actuar como respaldo de la información de ubicación de los drones y, además, puede proporcionar una estimación de la ubicación con decenas de metros de precisión [68]. Esta precisión es suficiente para corroborar los datos de telemetría. Además, la información de posicionamiento MPS también se puede utilizar si el avión no envía la telemetría debido a un mal funcionamiento. En este caso, la información MPS puede usarse para continuar monitoreando si el dron infringe zonas de vuelo restringidas o, incluso, en caso de fallo del dron, localizar la zona del posible aterrizaje junto con una posición aproximada del incidente.

#### 7.1.1.3 Detección de uso no certificado de dispositivos móviles

Desde la perspectiva del operador de la red móvil, es importante detectar el uso no certificado de dispositivos móviles y suscripciones. Uno de estos usos es cuando un teléfono móvil normal se monta en un avión no tripulado y se usa, por ejemplo, para la transmisión de video. Este uso puede causar interferencias significativas en la red. Tan pronto como se detecte tal operación, se pueden iniciar técnicas de mitigación como,

por ejemplo, estrangular el tráfico de datos del suscriptor. La detección se puede realizar monitorizando las características del enlace de radio y los patrones de movilidad, aplicando técnicas de aprendizaje automático. Esto es posible ya que las características del enlace de radio y los patrones de movilidad son diferentes dependiendo de si el aparato se encuentra en el aire o en el suelo. Por ejemplo, se espera que un dron que opera a una gran altitud tendrá un entorno de propagación en línea de vista que implique una baja varianza de las RSRP (Potencias Recibidas de Señales de Referencia) de las células más fuertes. De manera similar, las estadísticas del RSSI (Indicador de Intensidad de Señal Recibida) de los móviles instalados en los drones, son diferentes de las de los móviles en tierra ya que un dispositivo móvil montado en un avión no tripulado puede recibir señales de varias celdas con fuerzas similares:

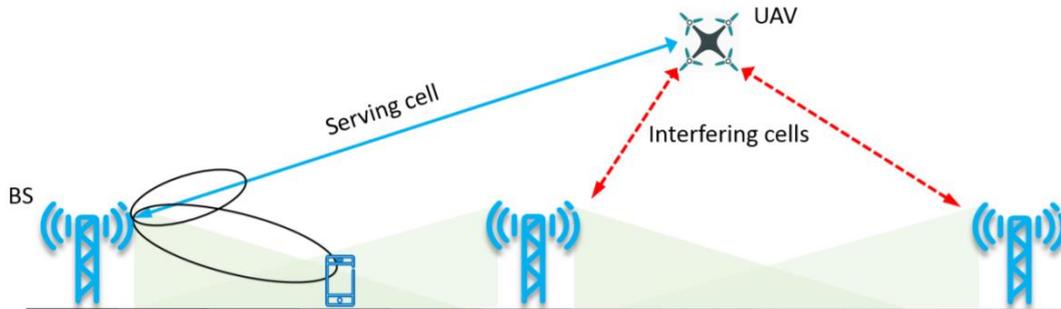


Figura 40: Conectividad para drones pequeños a baja altitud con redes móviles. Fuente: [64]

Básicamente, el sistema UTM que propone Ericsson es conceptual y se puede considerar la base tecnológica clave para el desarrollo de las futuras tecnologías necesarias para la identificación, autenticación, registro, geolocalización y neutralización de drones en el espacio aéreo. Su línea de trabajo gira en torno a la forma de aplicar estas técnicas empleando las redes móviles, siendo la base de los sistemas UTM que emplean algunas compañías aunque, otras, emplean técnicas basadas en la nube, cruzando datos procedentes de diferentes empresas privadas u organismos públicos para conseguir el mismo objetivo.

### 7.1.2 Solución propuesta por Embention

Según la empresa Embention, hoy en día no existe un estándar para la gestión del uso de los drones en el espacio de vuelo inferior (por debajo de los 150 m) y el sistema de gestión de tráfico aéreo ATM para la aviación convencional, no es compatible con los drones ya que se basa en la comunicación con los pilotos y en la detección por radar. Los drones no siempre tendrán un piloto y debido a su tamaño reducido y la altitud con la que operan no facilita que sean detectados por estos sistemas.

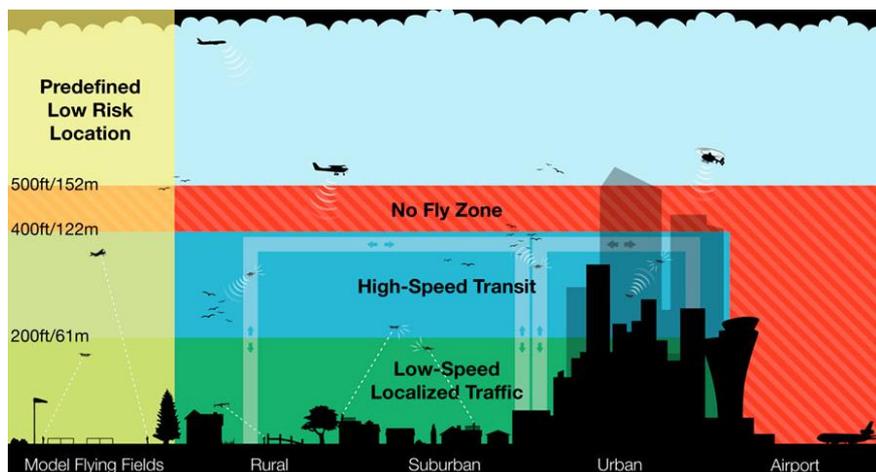


Figura 41: División de espacio aéreo en función de la aeronave. Fuente: <https://www.embention.com>

Por este motivo, la empresa define en líneas generales los requisitos esenciales que debería tener un sistema UTM:

- Seguimiento preciso y fiable de los drones
- Comunicación bidireccional sólida entre los drones y los sistemas UTM.
- Acceso a la información en tiempo real incluyendo la planificación del vuelo, la autorización del vuelo, la climatología, la posición, etc.
- Diseño rápido y simple del espacio aéreo en el que los controladores aéreos puedan crear zonas de exclusión aéreas o reorientar el tráfico aéreo.

La intervención de los operadores solo será necesaria ante emergencias, ya que las rutas estarán optimizadas para evitar colisiones mediante los sistemas Autopilot, diseñados por la misma empresa. Además, gracias a las comunicaciones LTE o 4G se pueden realizar operaciones BVLOS, como ya se ha detallado en el apartado 6.2.2 de este trabajo. En este sentido la empresa dispone del sistema Autopilot Veronte, que actualmente tiene la capacidad para cumplir los requisitos enumerados anteriormente gracias a las comunicaciones 4G integradas, su software de control Veronte Pipe y sus servicios en la nube Veronte Cloud.



Figura 42: Sistema Veronte Autopilot. Fuente: <https://www.embention.com>

El software Veronte Pipe puede mandar la autorización y el plan de vuelo, además de su posición a los controladores de tránsito aéreo ATC a través de Veronte Cloud, donde se accedería a los datos en tiempo real. Además, también se puede configurar zonas de exclusión aérea, obstáculos y evitar colisiones con su sistema “Sense and Avoid” [69].

### 7.1.3 Solución propuesta por INDRA

Las empresas Indra y AirMap han cerrado un acuerdo de colaboración con el que unen sus fuerzas para acelerar la introducción de las tecnologías de gestión de tráfico no tripulado (UTM) necesarias para facilitar la irrupción definitiva de los drones y que puedan prestar todo tipo de servicios a ciudadanos, empresas y administración. La alta complementariedad de las soluciones UTM de Indra y AirMap hace posible acortar los tiempos para que proveedores de servicios de navegación aérea, autoridades, reguladoras, fabricantes de drones y operadores dispongan de la infraestructura de última generación necesaria para poder volar estos aparatos de forma segura en zonas controladas y no controladas.

En esta alianza tecnológica, AirMap aporta su elevada especialización y experiencia internacional como líder en el desarrollo de plataformas UTM que ordenan el tráfico de drones a baja altura (por debajo de los 150 m). Mientras que Indra, por su parte, suma su solución UTM de última generación, su sistema de protección anti-drones ARMS y su gran experiencia en sistemas de gestión de tráfico aéreo en todo el mundo [70] [71].

#### 7.1.4 Solución propuesta por la NASA

En 2016, surge el Proyecto de Integración UAS en el Sistema Nacional del Espacio Aéreo de EE.UU. (Proyecto UAS-NAS) con el fin de identificar y desarrollar los procedimientos de acceso al espacio aéreo global de todas las clases de drones. El objetivo del proyecto es proporcionar resultados de la investigación, mediante la simulación y pruebas de vuelo, para respaldar el desarrollo y la validación de las tecnologías Detectar y Evitar (DAA) y Comando y Control (C2) necesarias para integrar los Sistemas de Aviones No Tripulados en el espacio aéreo norteamericano. Según la NASA, el proyecto se basa en dar respuesta a varios desafíos técnicos que presentan las principales tecnologías imprescindibles para una integración segura entre los drones y el espacio aéreo convencional como pueden ser:

- **Sistemas S&A/ DAA:** desarrollar estándares sobre el concepto “Detectar y evitar” que puedan implantarse en los drones con capacidad de dar soporte a los sistemas CNS y compatibles con operaciones IFR.
- **Enlace C2:** desarrollar los conceptos y tecnologías operacionales de Mando y control (C2) basados en satélites (Satcom) y terrestres compatibles con el espectro radioeléctrico protegido.

Todas estas actividades de investigación irían apoyadas por la FAA con pruebas y simulaciones para demostrar la correcta implantación del sistema de integración apoyados en los procedimientos operativos que ya se emplean en la aviación comercial [72].

##### 7.1.4.1 Programa Piloto UTM

En abril de 2017 y bajo la denominación *UTM Pilot Program* (Programa Piloto UTM o UPP) la NASA, junto a la FAA, comenzaron a desarrollar un modelo de gestión UTM el cual, se encuentra en una etapa bastante avanzada. Aun así, admiten que disponen de una infraestructura limitada para administrar la enorme expansión de las operaciones de aviones y drones dentro su Sistema Nacional de Espacio Aéreo en un futuro. Son conscientes de que necesitan un sistema UTM para garantizar que los drones se integren de manera segura y eficiente en su espacio aéreo.

A medida que la FAA, la NASA y sus socios tecnológicos avanzan, el objetivo principal del UPP es desarrollar, demostrar y proporcionar estos servicios utilizando una infraestructura en la nube, que apoyarán la implementación de las operaciones UTM, así como el intercambio de información que promueva la separación cooperativa entre aeronaves y la situación de los drones en cada punto del espacio aéreo. Las nuevas capacidades y servicios UTM evolucionarán a medida que los conceptos operativos de UTM y de intercambio de datos maduren.

El concepto UTM que presenta la NASA se muestra en la siguiente figura:

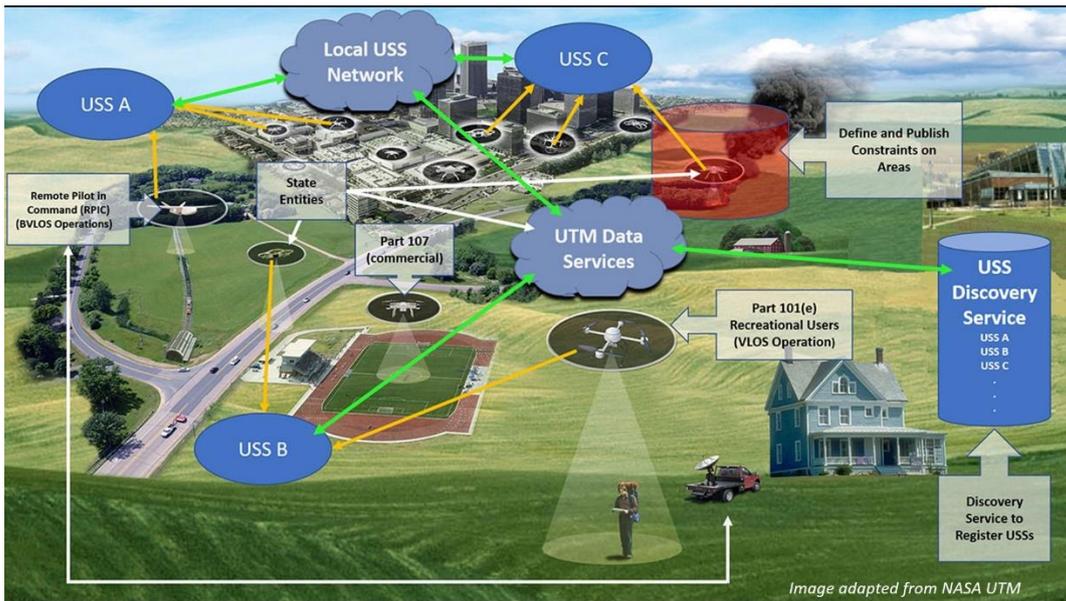


Figura 43: Concepto del Programa UPP. Fuente: [73]

Como se muestra en la figura, los servicios UTM de este programa incluyen compartir el plan de vuelo entre operadores de drones, la capacidad de un Proveedor de Servicios UAS (USS) para generar una Reserva de Volumen UAS (UVR), capacidad que se otorgaría a los USS autorizados para poder emitir notificaciones a los drones o aviones no tripulados. Estas notificaciones están relacionadas con las actividades aéreas o terrestres relevantes para su operación segura y se comparten con las partes interesadas, como pueden ser otros USS u operadores de drones [73].

El ecosistema UTM que propone la NASA en su conjunto se representa en la siguiente imagen:

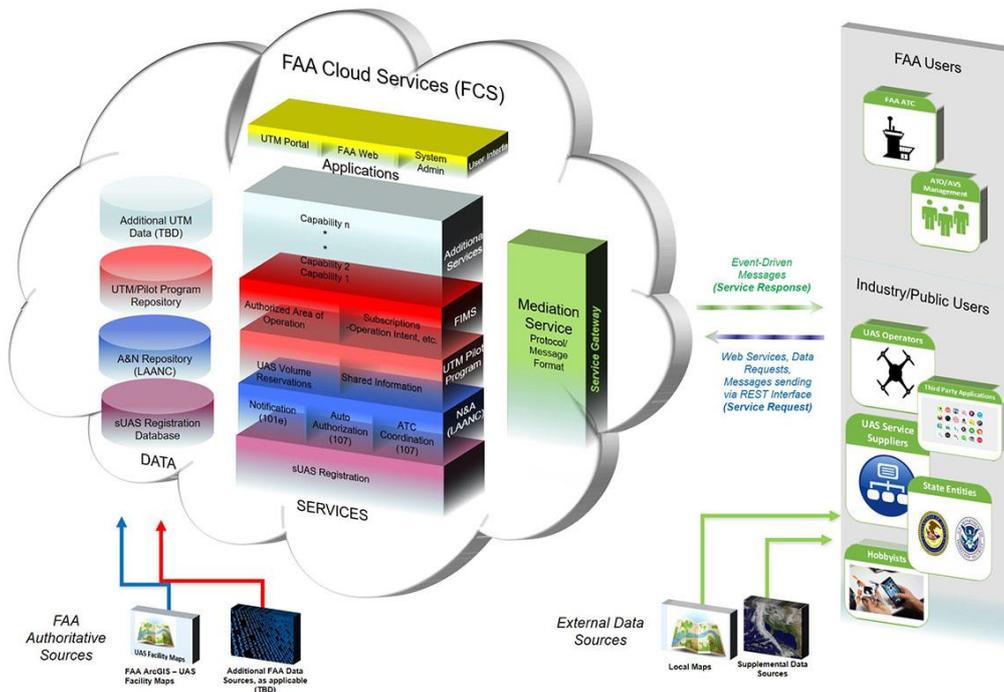


Figura 44: Ecosistema UPP. Fuente: [73]

### 7.1.4.2 ECOsystem UTM de Thales

Tras definir el ecosistema UTM, en 2018 la NASA alcanza un acuerdo con el Grupo Thales para continuar estableciendo este concepto de sistema de gestión de drones, aprovechando la amplia experiencia de este grupo en el desarrollo del concepto UTM. La NASA prevé completar la primera etapa del ECOsystem UTM en el Sistema Nacional de Espacio Aéreo (NAS) para finales de 2019.

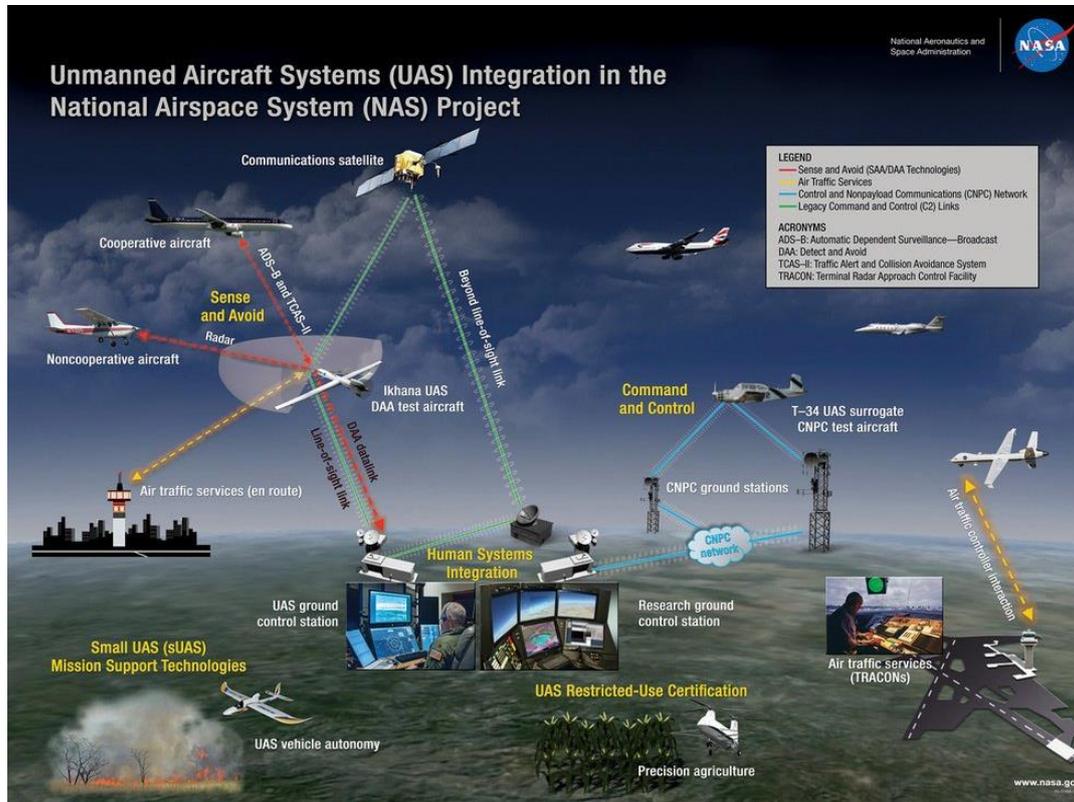


Figura 45: Proyecto la NASA de integración de drones en el espacio aéreo norteamericano

La misión de Thales es la investigación, desarrollo, pruebas y evaluación del sistema de gestión de tráfico de drones que operan a baja altitud (hasta 120 m) y que permitirá la autorización automática de vuelos de drones e integración de sus operaciones de manera segura en el NAS norteamericano [74].

La aplicación ECOsystem UTM está basada en la nube y aplica las reglas y flujo de trabajo definidos por el programa de intercambio de datos de UAS de la FAA (LAANC) aplicados a los drones de forma individual.

LAANC (Capacidad de Notificación y Autorización de Baja Altitud) es un enfoque innovador y colaborativo entre el gobierno y la industria privada que facilita el intercambio de datos del espacio aéreo entre las dos partes. El programa facilita la integración de los drones en el espacio aéreo, ya que proporciona acceso al espacio aéreo controlado cerca de los aeropuertos y muestra en tiempo real las autorizaciones por debajo de las altitudes aprobadas en el espacio aéreo controlado.

El sistema automatiza el proceso de solicitud y aprobación de autorizaciones de los operadores de drones. Estas solicitudes se comparan con múltiples fuentes de datos referentes al espacio aéreo como las restricciones de vuelo temporales, los NOTAM y los mapas de las instalaciones de drones como las UACS o RPAS. Si se aprueba el

plan de vuelo, los pilotos reciben su autorización casi en tiempo real. En la siguiente figura se muestra un ejemplo de su funcionamiento:

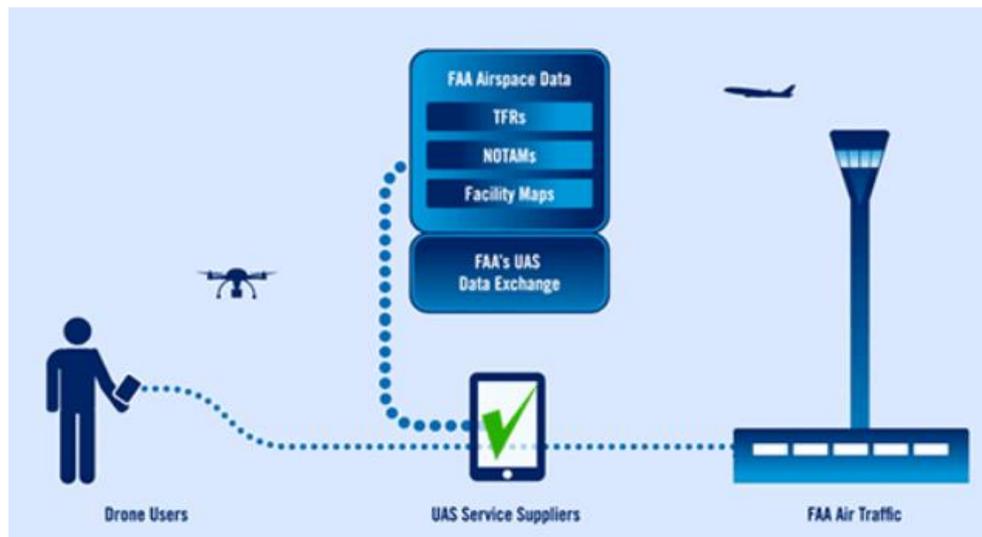


Figura 46: Funcionamiento del sistema LAANC. Fuente: [75]

La capacidad LAANC es compatible con los requisitos de autorización de control de tránsito aéreo para operaciones de drones realizadas bajo las reglas especiales para aeronaves y pequeños drones y, además, proporciona a los operadores de drones una solución optimizada para permitir la notificación y autorización automatizadas en tiempo real [75].

En 2019, la NASA alcanzará la etapa final del desarrollo del Sistema Nacional de Gestión de Tráfico para Drones (UTM), tras haber probado el sistema en un entorno urbano en el modo de operación BVLOS. Las pruebas consistieron en lanzar un dron desde una azotea a cinco pisos de altura, al tiempo que otros drones volaban más abajo. Equipados con GPS y mediante los sistemas DAA, consiguieron aterrizar en otros lugares sin chocar con ningún objeto u otra aeronave mediante la supervisión de un sistema situado en tierra fuera de la línea de visión de los drones [76] [77].

### 7.1.5 Solución propuesta por Airmap y Skyguide

Bajo el programa U-Space, Airmap y Skyguide se alían para desarrollar el primer sistema de gestión de tráfico de drones UTM en Europa. La plataforma suiza de U-Space es una infraestructura digital que permite a un avión no tripulado el intercambio de datos como su posición o las comunicaciones digitales con otros aviones no tripulados, aeronaves tripuladas, servicios de gestión del espacio aéreo como AirMap y otras partes interesadas, como los proveedores de servicios de navegación aérea (ANSP) y el control del tráfico aéreo (ATC).

Una de las fases piloto comenzó en junio de 2018, en la que planean integrar la plataforma AirMap UTM con la infraestructura de Skyguide e introducir la autorización de vuelo automatizada en un solo entorno de espacio aéreo [78].

En esencia, este proyecto se apoya en el concepto UTM de la NASA-FAA comentado antes. La plataforma Swiss U-Space incluirá características tales como:

- Registro basado en *blockchain* para usuarios y drones
- *Geofencing* dinámico y autorización de espacio aéreo digital instantánea
- Alertas de tráfico en tiempo real para pilotos de drones

- Telemetría de drones en vivo para administradores de espacio aéreo
- Conectividad y comunicación entre pilotos de aviones no tripulados y administradores del espacio aéreo
- Otros servicios para habilitar vuelos simultáneos en espacio aéreo compartido

El funcionamiento global del sistema propuesto por Swiss U-space se detalla en la siguiente figura:

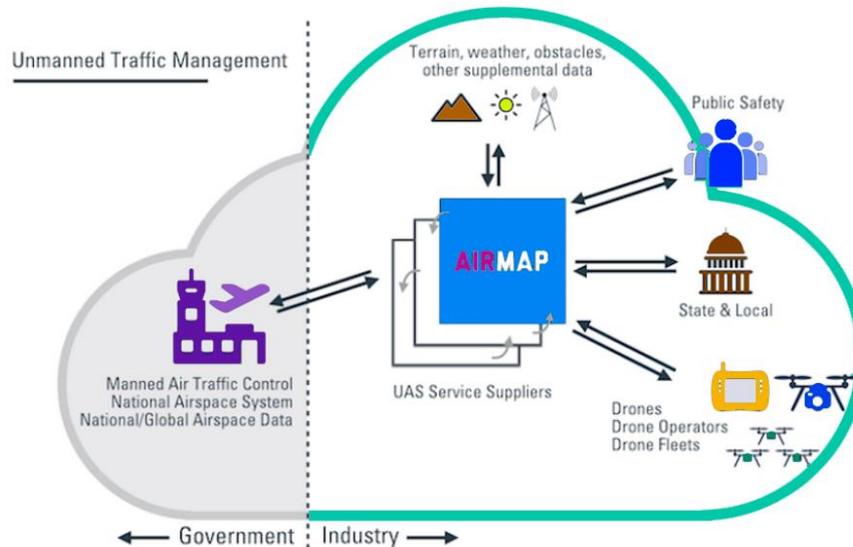


Figura 47: Esquema de funcionamiento del proyecto Swiss U-Space. Fuente: [79]

A través de la plataforma AirMap se proporcionan datos como los requisitos y reglas de navegación en el espacio aéreo, alertas sobre tráfico de aviones tripulados, climatología local, así como las ubicaciones de infraestructuras críticas y otros obstáculos a través del sistema D-NAS.

El sistema D-NAS (Sistema de Aviso y Reconocimiento Digital), facilita el contacto con los aeropuertos directamente desde una aplicación de AirMap al facilitar el envío de los planes de vuelo del operador del dron de forma digital y así recibir la autorización para volar. Una vez enviado y aprobado el plan de vuelo, aparece reflejado en un panel de control (basado en la web) situado en las consolas del centro de control del aeropuerto. Mediante este panel, se pueden visualizar en los mapas las operaciones de drones activas en tiempo real, definir zonas de vuelo restringidas alrededor del aeropuerto y comunicarse directamente con el operador del dron en caso de una emergencia, peligros o para cambiar la ruta de vuelo. D-NAS también ofrece información sobre la situación de los operadores de drones a los administradores de aeropuertos dentro de un radio de 8 km del entorno aeroportuario.

Planean tener operativas las primeras etapas de este sistema UTM en 2019 [79].

En la siguiente tabla, se muestra una comparativa de los diferentes sistemas que se han propuesto como solución para integrar los drones en el espacio aéreo con la aviación convencional:

Entidad	Ericsson	Embention	Indra	NASA	Airmap/Skyguide
Referencias	[64] [68]	[69]	[70] [71]	[72] [73] [74] [75] [76] [77]	[78] [79]
Identificación	<ul style="list-style-type: none"> <li>Tarjeta SIM</li> <li>Publicación en servidor remoto</li> </ul>	Veronte Cloud	Mediante plataforma UTM Hub y UTM Connect	Servidor en la nube FCS ( <i>FAA Cloud Services</i> )	Mediante plataforma AirMap
Registro electrónico	Basado en red	Mediante LTE	Basado en registros nacionales (red)	USS (Proveedor servicios UAS)	Basado en <i>blockchain</i>
Autenticación	IMEI e IMSI	Veronte Cloud	UTM Hub	USS (Proveedor servicios UAS)	Mediante AirMap
<i>Geofencing</i>	Basada en red móvil	Mediante red LTE	Mediante UTM Hub	Basado en red	Dinámico (D-NAS)
Geoposicionamiento	<ul style="list-style-type: none"> <li>Envío datos del sistema GNSS a servidor UTM</li> <li>MPS</li> </ul>	Veronte Pipe (software propietario)	Seguimiento en tiempo real (UTM Connect)	Basado en sistemas GNSS	<u>D-NAS:</u> <ul style="list-style-type: none"> <li>Visualizar operaciones activas</li> </ul>
Soporte a sistemas anticolidión	Sí	Autopilot Veronte (propietario)	Integrado en UTM Connect	A través de servicios web que se envían a la nube FCS	<u>D-NAS:</u> <ul style="list-style-type: none"> <li>Emite alertas anticolidión</li> </ul>
Integración con ATC	Sí	Sí	Mediante UTM Hub	Sí	Sí
Soporte a planes de vuelo	Sí	Sí	Sí	Sí	Sí
Altitud operativa del sistema	Hasta 150 m	Hasta 150 m	Hasta 150 m	Hasta 120 m	Hasta 150 m

Tabla 6: Resumen de soluciones de sistemas de gestión de drones UTM

## 7.2 Soluciones para neutralizar drones en casos de interferencia ilícita

Como se ha visto en el apartado 2.4, integrar los drones en el espacio aéreo junto a la aviación comercial de forma segura mediante una serie de reglas y normativas depende en gran medida de la voluntad de los operadores de drones para cumplirlas. Pero, hay casos recientes de uso malintencionado por parte de personas u organismos que usan estos dispositivos para provocar daño o generar caos en ciertos enclaves estratégicos, como ocurrió en el aeropuerto de Londres.

Para intentar atajar este problema, hay empresas y organismos que están centrando sus investigaciones en la manera de aprovechar éstas para detectar y neutralizar una posible amenaza con drones, mediante técnicas que tratan de interferir en los sistemas de comunicación de los drones. Una de esas técnicas es el *jamming*, que consiste en interferir en las bandas de frecuencias del enlace de comunicaciones de comando y control para que pierda que el operador pierda el control del dispositivo, y otra técnica es el *spoofing*, que trata de “engañar” al receptor GPS con el fin de desorientar al dron.

A continuación, se presentan algunas soluciones diseñadas por tres empresas.

### 7.2.1 Solución propuesta por Quantum Aviation

Quantum Aviation presenta su sistema TITANIUM, que permite detectar, alertar, identificar, rastrear y neutralizar las amenazas de aviones no tripulados desde pequeños multirrotores comerciales hasta grandes drones de ala fija.

El sistema está equipado de un radar 3D activo, con escaneado electrónico que opera en la banda S ya que en esta banda el sistema se comporta bien ante condiciones climáticas adversas. Es capaz de detectar aviones no tripulados de largo alcance

(HALE, MALE) hasta 100 km y drones más pequeños de la categoría nano, hasta 7 km. Además, posee una serie de sensores de panel plano, cada uno con un campo de visión de 90°, con elevación y acimut ajustables, que se combinan para ofrecer las capacidades de detección y seguimiento requeridas.

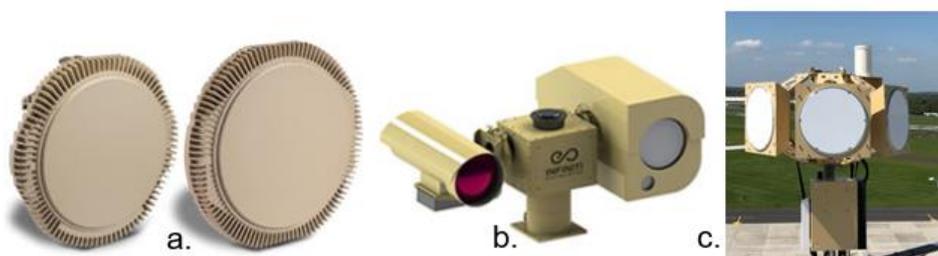


Figura 48: Componentes de TITANIUM: a) Radar; b) Cámara EO/IR; c) Detector de RF. Fuente: [80]

Para complementar este sistema, se pueden agregar más unidades para ampliar el área de vigilancia. Ofrecen una versión portátil de rápido despliegue que proporciona bajos tiempos de configuración y facilidad de uso. En cuanto a la cámara, posee capacidad infrarroja y un sensor de 2 MP que proporciona un buen equilibrio entre la sensibilidad a la luz y el zoom. Es capaz de detectar, reconocer e identificar un pequeño dron a 5 km, mientras que un objetivo de ala fija entre 3 m y 18 km. Además, dispone de la tecnología ZLID (*Zoom Laser IR Diode*) que sincroniza la intensidad de infrarrojos y la iluminación de área con la lente para aumentar el rendimiento, eliminando la sobreexposición y los puntos calientes para una identificación de largo alcance en la oscuridad total.

En cuanto a la detección de RF, emplea la tecnología probada de la compañía británica *Metis Aerospace*, la cual dispone de un aprendizaje inteligente del entorno de RF local que maximiza aún más las capacidades de detección. A través del análisis de telemetría, el sistema puede clasificar la amenaza con rangos de detección de más de 4 km para que el sistema pueda actuar a tiempo.

En el apartado de interferidores o *jammer*, el sistema TITATIUM emplea la tecnología proporcionada por la empresa Kirintec, especializada en proveer soluciones de defensa táctica provocando interferencias a los drones. La solución interfiere en el sistema de comunicaciones del dron realizando un barrido entre 20 MHz y 6 GHz en enlace C2, así como en las frecuencias de GPS y GLONASS. También permiten implementar soluciones omnidireccionales y direccionales para maximizar el rendimiento y la capacidad de neutralizar objetivos [80].

### 7.2.2 Solución propuesta por Thales Group

La solución C-UAS de Thales es capaz de detectar, identificar y neutralizar microdrones y nanodrones (entre 2 y 25 kg de peso) en entornos civiles, tanto urbanos como rurales y que ya ha sido implantado por las fuerzas armadas de un país del sudeste asiático.

La solución de Thales se compone de dos sistemas portátiles formados, por un lado, por un radar Squire y un radiogoniómetro capaz de detectar señales de los drones y sus estaciones de control a 4 km de distancia y, por otro lado, de una unidad optróica de alta calidad (denominada *Gecko*) dotada de cámaras térmicas que permite un dron a una distancia de 2 km y certificar si el dron transporta una carga que pueda suponer una amenaza para la seguridad, como puede ser una bomba o un explosivo.



Figura 49: Sistema anti-drones C-UAS de Thales. Fuente: [www.infodron.es](http://www.infodron.es)

Este sistema óptico, desarrollado en España, también permite detectar vehículos o pequeñas embarcaciones a una distancia de hasta 25 km. Debido a su simplicidad a la hora de utilizarlo y su portabilidad, el sistema C-UAS permite llevar a cabo tareas de vigilancia en eventos puntuales, detectando posibles amenazas de cualquier tipo de dron a gran distancia, de tal manera que se pueda proceder a su neutralización con tiempo suficiente mediante un inhibidor que corta el enlace de comunicaciones radio, haciendo que el dron aterrice en modo seguro o que regrese al punto de origen [81].

### 7.2.3 Solución propuesta por INDRA

La empresa española INDRA, ha diseñado el sistema inteligente denominado ARMS (*Anti RPAS Multisensor System*) de detección e inhibición de drones para proteger espacios especialmente sensibles como edificios oficiales, plantas industriales o aeropuertos en los que la presencia de este tipo de aeronaves puede representar un problema de seguridad. Indra detectó hace tiempo la preocupación que existe entre los operadores aeroportuarios y otras muchas infraestructuras sensibles como plantas industriales e incluso edificios oficiales por la amenaza creciente que supone el uso malintencionado de los drones. A partir de esta necesidad, desarrolló un escudo inteligente que se combina con las tecnologías de los sistemas de Gestión de Tráfico Aéreo de aeronaves tripuladas (ATM) y no tripuladas (UTM) propias de la firma española.

El sistema de Indra detecta a los drones mediante un radar a varios kilómetros de distancia. Adicionalmente, una cámara infrarroja puede confirmar la información del radar. En una siguiente fase de la neutralización y mediante el uso de un inhibidor de frecuencia en distintas bandas, el sistema procede a anular la señal de los equipos de geolocalización del dron, así como su enlace de comunicaciones C2. Desde la consola de control, se puede configurar las zonas de detección y las acciones a realizar por el operador. Además, la compañía está implementando mejoras dirigidas a ofrecer la máxima precisión a la hora de que el sistema realice la clasificación y seguimiento del dron, combinando el empleo de imágenes térmicas, la escucha radioeléctrica y la inteligencia artificial. El grado de inteligencia del sistema le permite incluso aplicar técnicas de *spoofing* avanzadas, en las que suplanta la señal de posicionamiento del dron, asume su mando y lo hace aterrizar en una zona determinada sin que cause daños. También está dotado de capacidad de aprendizaje continuo, incorporando avanzados algoritmos que hacen que el sistema gane precisión cuanto más se utiliza. El sistema anti-drones de Indra se muestra en la siguiente imagen:



Figura 50: Escudo anti-drones ARMS de Indra. Fuente: Indra

El sistema también radiodetecta y estudia cómo se está comunicando el dron, qué tipo de enlace de datos está utilizando, en qué frecuencia y cómo recibe información para orientarse, pudiendo incluso determinar desde dónde está siendo controlado y, por tanto, dónde se encuentra el piloto. La información de todos estos sensores se recibe en un centro de control, donde un operador visualiza y comprueba la información que le facilita el sistema. Esta información también se puede integrar con los sistemas UTM y ATM para realizar una gestión segura y fluida del espacio aéreo.

Además, el sistema de Indra puede utilizarse de forma dirigida para dejar fuera de servicio a un enjambre de drones, aplicando medidas más agresivas. En caso de que la invasión se produzca simultáneamente desde diferentes puntos, el sistema está preparado para activar una defensa completa, generando una especie de cúpula protectora en torno a la instalación crítica:



Figura 51: Cúpula de protección del escudo ARMS de INDRA. Fuente: Elaboración propia

Para la detección del blanco a abatir, el sistema ARMS posee un radar con las especificaciones siguientes:

- Banda Ku
- Barrido a 360°/s
- Baja potencia: seguro para personas
- Detección por técnicas de Doppler & Clutter Map

- Refresco real de trazas (posición, rumbo y velocidad)

Para el perturbador de señales o *jammer* cuenta con las siguientes características:

- Multibanda y alta potencia
- Perturbación inteligente
- Versiones directivas, sectoriales y omnidireccionales
- Perturbación por barrido de frecuencias en los enlaces de datos y control de 70 MHz a 6 GHz
- Capacidad de realizar *spoofing* en la señal GPS, Glonass, Beidou o Galileo
- Efectivo a más de 5 km

Para búsqueda, marcación y seguimiento del dron atacante, usa un sistema optrónico mejorado que se compone de:

- Cámaras IR y CCD de medio y largo alcance
- Plataforma de 360°
- Búsqueda y clasificación automática basada en IA
- Seguimiento y ubicación 3D

El sistema es adaptable a cada escenario según las necesidades, incluso en los sistemas UTM para generación de listas blancas con aquellos drones que tienen la licencia o certificación para volar en espacios permitidos y también generar informes de alertas para el Control de Tránsito Aéreo.

En la siguiente tabla, se muestra una comparativa de los diferentes sistemas para neutralizar los drones en caso de actos de interferencia ilícita en el espacio aéreo:

Empresa	Quantum Aviation	Thales Group	Indra
Referencias	[80]	[81]	[70] [71]
Capacidades	<ul style="list-style-type: none"> <li>• Detectar</li> <li>• Alertar</li> <li>• Rastrear</li> <li>• Neutralizar</li> </ul>	<ul style="list-style-type: none"> <li>• Detectar</li> <li>• Identificar</li> <li>• Neutralizar</li> </ul>	<ul style="list-style-type: none"> <li>• Detectar</li> <li>• Alertar</li> <li>• Rastrear</li> <li>• Neutralizar</li> </ul>
Tipos de drones	Nano drones hasta drones de largo alcance	Micro y nano drones (entre 2 y 25 kg)	Toda las clases
Radio de acción	<ul style="list-style-type: none"> <li>• Nano drones: 7 km</li> <li>• HALE: 100 km</li> </ul>	Entre 2 y 4 km	> 5 km
Radiodetección	<u>Radar 3D activo:</u> <ul style="list-style-type: none"> <li>• Escaneado electrónico</li> <li>• Banda S</li> </ul>	Radar <i>Squire</i> + Radiogoniómetro	<u>Radar 3D activo:</u> <ul style="list-style-type: none"> <li>• Barrido 360°/s</li> <li>• Banda Ku</li> <li>• <i>Doppler</i> y <i>Clutter Map</i></li> </ul>
Cámara de visión	<ul style="list-style-type: none"> <li>• Infrarrojos</li> <li>• Alta sensibilidad</li> <li>• Tecnología ZLID</li> <li>• MPS</li> </ul>	<u>Unidad Optrónica:</u> <ul style="list-style-type: none"> <li>• Infrarrojos (detección de señal térmica)</li> </ul>	<u>Unidad Optrónica:</u> <ul style="list-style-type: none"> <li>• Cámaras IR y CCD</li> <li>• Búsqueda y clasificación automática</li> </ul>
Detección RF	• Aprendizaje inteligente huella electromagnética	Sí	Aprendizaje inteligente huella electromagnética
Interferidores ( <i>Jammer</i> )	<ul style="list-style-type: none"> <li>• Interferencias enlace C2</li> <li>• Barrido 20 MHz - 6 GHz</li> </ul>	• Interferencias en enlace C2	<ul style="list-style-type: none"> <li>• Multibanda</li> <li>• Perturbación inteligente</li> <li>• Barrido 20 MHz - 6 GHz</li> </ul>
<i>Spoofing</i>	Sí (en señal GPS y GLONASS)	No	Sí (GPS, Glonass, Beidou, Galileo)

Tabla 7: Resumen de soluciones para neutralizar drones en el espacio aéreo

## 8. Conclusiones

En este trabajo se ha intentado dar respuesta, desde el punto de vista de los sistemas de comunicación, a uno de los retos más importantes a los que se enfrenta el mundo de aviación hoy en día: cómo integrar de forma segura los drones y la aviación comercial en el espacio aéreo.

Pero la respuesta no es sencilla. Tras un repaso por la historia y evolución de las aeronaves no tripuladas, se ha realizado una ardua labor de investigación repasando las diferentes normativas existentes sobre la integración de drones en el espacio aéreo no segregado hasta las distintas tecnologías que existen para controlar, manejar, detectar, identificar e incluso neutralizar este tipo de dispositivos que, potencialmente, pueden ocasionar graves incidencias en el normal funcionamiento del tráfico aéreo.

Tampoco ha sido sencillo buscar, clasificar y ordenar la ingente cantidad de documentación y reglamentación tanto nacional como internacional respecto a este asunto. Y es que, desde hace más de una década, distintos organismos públicos de distintos ámbitos y continentes como la OACI, la ITU, la NASA o Eurocontrol, han intentado armonizar y adaptar los conocimientos que han adquirido en sus respectivos dominios sobre la aviación tradicional al mundo de las pequeñas (y no tan pequeñas) aeronaves no tripuladas.

En cuanto a la integración, existen varias limitaciones y retos que hay que superar, tanto en materia tecnológica como regulatoria, para que llegue a buen puerto en torno al año 2035, al menos en las previsiones más optimistas de los organismos europeos.

Entre los retos a nivel regulatorio se encuentra la dificultad para poner de acuerdo a muchas instituciones internacionales. Ya dentro de Europa, no existe un consenso unánime en lo que a normativa se refiere, pero sí que se están llevando a cabo varias iniciativas como el proyecto U-Space. Es un primer paso y, su primera etapa, la U1, ya está en fase de pruebas. Al otro lado se encuentran los americanos, con la NASA y la FAA, encabezando un proyecto destinado al mismo fin que el de sus homólogos europeos. Pero hay algo en el que están todos de acuerdo: las limitaciones tecnológicas.

Aunque se han realizado muchos avances en el ámbito de los sistemas de comunicaciones, aún queda mucho por hacer, sobre todo para llevar a cabo las iniciativas tecnológicas que demandan las distintas regulaciones. Por ejemplo, requieren que los drones dispongan de sistemas que detecten, eviten y alerten de colisiones con objetos u otras aeronaves al modo como lo hacen actualmente los aviones tripulados. Aunque ya se han probado algunos de estos sistemas en drones, surge la dificultad de integrarlos en los sistemas de Control de Tránsito Aéreo junto con las retransmisiones de voz y datos para que los operadores de drones, pilotos y controladores puedan comunicarse. Igual ocurre con el *geofencing*, el etiquetado y la identificación de drones. En el apartado de *geofencing*, se ha avanzado bastante. Compañías como Airmap o DJI, han desarrollado sistemas de geobarreras virtuales apoyados en sistemas de navegación por satélite y cartografías muy detalladas que permiten la delimitación de zonas restringidas con mucha precisión. En cuanto a la identificación electrónica, la propuesta de Ericsson resulta bastante interesante, pues permite identificar un dron y su operador del mismo modo que se identifica y autentica un teléfono móvil y su propietario dentro de una red de telefonía móvil.

A pesar de todos estos retos, el desarrollo de las normativas y las tecnologías siguen evolucionando imparablemente hasta alcanzar la integración total que, se espera, se produzca en torno al año 2035.

## 9. Glosario de términos

<b>ACAS</b>	Airborne Collision Avoidance System
<b>AESA</b>	Agencia Estatal de Seguridad Aérea
<b>ANA</b>	National Aviation Authorities
<b>ANSP</b>	Air Navigation Service Provider
<b>API</b>	Application Programming Interface
<b>ARMS</b>	Anti RPAS Multisensor System
<b>ATC</b>	Air Traffic Control
<b>ATM</b>	Air Traffic Management
<b>ATS</b>	Air Traffic Services
<b>BLOS</b>	Beyond Line Of Sight
<b>BLOS M2M</b>	BLOS Machine-2-Machine
<b>BPSK</b>	Binary Phase-Shift Keying
<b>BVLOS</b>	Beyond Visual Line of Sight
<b>C2</b>	Mando y control
<b>C3</b>	Mando, control y comunicaciones
<b>CNS</b>	Communication, Navigation and Surveillance
<b>COO</b>	Cell Of Origin
<b>CW</b>	Continuous Wave
<b>DAA</b>	Detect And Avoidance
<b>DARPA</b>	Defense Advanced Research Projects Agency
<b>Donwlink</b>	Enlace descendente
<b>DSSS</b>	Direct Sequence Spread Spectrum
<b>eNB</b>	Evolved Node B
<b>FAA</b>	Federal Agency of Aviation
<b>FAA</b>	Federal Aviation Administration
<b>FHSS</b>	Frequency Hopping Spread Spectrum
<b>FIZ</b>	Flight Information Zone
<b>FOV</b>	Field Of View
<b>GCS</b>	Ground Control Station
<b>GNSS</b>	Global Navigation Satellite System
<b>GPS</b>	Global Positioning System
<b>HALE</b>	High Altitude Long Endurance
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IFR</b>	Instrumental Flight Rules
<b>IMEI</b>	International Mobile Equipment Identity
<b>IMSI</b>	International Mobile Subscriber Identity
<b>INS</b>	Inertial Navigation System
<b>IoT</b>	Internet of Things
<b>JARUS</b>	Joint Authorities for Rulemaking on Unmanned Systems
<b>L1</b>	Banda L1 de GPS
<b>LAANC</b>	Low Altitude Authorization and Notification Capability
<b>LOS</b>	Line Of Sight

<b>LTE</b>	Long Term Evolution
<b>MPS</b>	Mobile Positioning System
<b>NASA</b>	National Aeronautics and Space Administration
<b>NavAids</b>	Ayudas a la Navegación
<b>NOTAM</b>	Notice To AirMen
<b>NUAIR</b>	Northeast UAS Airspace Integration Research
<b>OACI</b>	Organización de Aviación Civil Internacional
<b>OFDM</b>	Orthogonal Frequency-Division Multiplexing
<b>OID</b>	Object Identifiers
<b>OTDOA</b>	Observed Time Difference Of Arrival
<b>PBN</b>	Performance Based Navigation
<b>QPSK</b>	Quadrature Phase-Shift Keying
<b>RCP</b>	Required Communication Performance
<b>RPA</b>	Remotely Piloted Aircraft
<b>RPAS</b>	Remotely Piloted Aircraft System
<b>SACTA</b>	Sistema Automático de Control de Tráfico Aéreo
<b>SARPS</b>	Standards And Recommended Practices
<b>SC-FDM</b>	Single Carrier Frequency Division Multiple Access
<b>SIM</b>	Subscriber Identity Module
<b>SINR</b>	Signal-to-Interference + Noise Ratio
<b>TCAS</b>	Traffic alert and Collision Avoidance System
<b>TDOA</b>	Time Difference Of Arrival
<b>UA</b>	Unmanned Aircraft
<b>UACS</b>	Unmanned Aerial Control System
<b>UAS</b>	Unmanned Aircraft System
<b>UAV</b>	Unmanned Aerial Vehicle
<b>UE</b>	Unión Europea
<b>UHF</b>	Ultra High Frequency
<b>UICC</b>	Universal Integrated Circuit Card
<b>Uplink</b>	Enlace ascendente
<b>UTM</b>	Unmanned Aerial System Traffic Management
<b>VFR</b>	Visual Flight Rules
<b>VLOS</b>	Visual Line Of Sight
<b>VTOL</b>	Vertical Take-Off and Landing
<b>WiFi</b>	Wireless Fidelity

## 10. Bibliografía

- [1] M. Jorge. 2018. «Cómo pueden unos drones generar tanto caos y cerrar más de 24 horas el segundo aeropuerto más grande de Reino Unido». Gizmodo en Español. <https://es.gizmodo.com/como-pueden-unos-drones-generar-tanto-caos-y-cerrar-mas-1831251705>
- [2] S. A. PILAR. 2016. «Drones, la amenaza creciente de los aviones de pasajeros». RTVE.es. <http://www.rtve.es/noticias/20160421/drones-amenaza-creciente-aviones-pasajeros/1341960.shtml>
- [3] AESA (Agencia Estatal de Seguridad Aérea). 2017. «Drones». Ministerio de Fomento. [https://www.seguridadaerea.gob.es/lang\\_castellano/cias\\_empresas/trabajos/rpas/default.aspx](https://www.seguridadaerea.gob.es/lang_castellano/cias_empresas/trabajos/rpas/default.aspx)
- [4] C. Cuerno Rejado, L. García Hernández, A. Sánchez Carmona, A. Carrio Fernández, J. L. Sánchez López, y P. Campoy Cervera. 2016. «Evolución histórica de los vehículos aéreos no tripulados hasta la actualidad». vol. 91, n.º 1, pp. 282-288. DYNA INGENIERIA E INDUSTRIA.
- [5] Atoev, Sukhrob; Kwon, Oh-Heum; Lee, Suk-Hwan; Kwon, Ki-Ryong. 2018. «An efficient SC-FDM modulation technique for a UAV communication link». ResearchGate. [https://www.researchgate.net/publication/329188093\\_An\\_efficient\\_SC-FDM\\_modulation\\_technique\\_for\\_a\\_UAV\\_communication\\_link](https://www.researchgate.net/publication/329188093_An_efficient_SC-FDM_modulation_technique_for_a_UAV_communication_link)
- [6] Netanel Malka. 2018. «Drones Leveraging 5G Technology». Sky Hopper by Mobilicom. <https://www.skyhopper.biz/drones-leveraging-5g-technology/>
- [7] DFS Deutsche Flugsicherung GmbH. 2019. «Drones connected: Safe and fair integration of drones via mobile network». [https://www.dfs.de/dfs\\_homepage/en/Press/Press%20releases/2018/05.03.2018.-%20Drones%20as%20flying%20smartphones/](https://www.dfs.de/dfs_homepage/en/Press/Press%20releases/2018/05.03.2018.-%20Drones%20as%20flying%20smartphones/)
- [8] Embention. 2018. «Autopilot Veronte para UAV, UAS y drones». <https://products.embention.com/veronte/autopiloto-uav>
- [9] V. D. L. S. 2019. «NASA UTM». NASA. <https://utm.arc.nasa.gov/index.shtml>
- [10] JARUS. 2019. «Proyecto JARUS ». <http://jarus-rpas.org/who-we-are>
- [11] RGSdron. 2017. «U-SPACE. Espacio aéreo europeo para drones hasta los 150 metros» RGSdron (Drones en Lugo y Ponferrada). <https://rgsdron.es/u-space-1917/>
- [12] AirCrew. 2018. «AirMap Named UTM Provider for 4 European Network of U-space Demonstrations». AirMap. <https://www.airmap.com/utm-provider-sesar-europe-u-space-gof-ospace-finland-estonia-vutura-netherlands-geosafe-france-domus-spain/>
- [13] ENAIRE. 2019. «Enaire y Everis realizan pruebas de integración de drones y de control de tráfico aéreo convencional». [https://www.enaire.es/es\\_ES/2018\\_06\\_06/ndp\\_enaire\\_everis\\_realizan\\_pruebas\\_integracion\\_sistemas\\_drones](https://www.enaire.es/es_ES/2018_06_06/ndp_enaire_everis_realizan_pruebas_integracion_sistemas_drones)
- [14] IACIT. 2019. «Uso de interferidores de drones en aeródromos». <http://www.iacit.com.br/es/news/uso-de-interferidores-de-drones-en-aerodromos>
- [15] Indra Company. 2017. «Indra presenta su solución inteligente para detectar y contrarrestar drones». <https://www.indracompany.com/es/noticia/indra-presenta-solucion-inteligente-detectar-contrarrestar-drones>
- [16] Wikipedia.org. 2019. «Northrop Grumman RQ-4 Global Hawk». [https://es.wikipedia.org/wiki/Northrop\\_Grumman\\_RQ-4\\_Global\\_Hawk](https://es.wikipedia.org/wiki/Northrop_Grumman_RQ-4_Global_Hawk)
- [17] Wikipedia.org. 2018. «Banda Ku». [https://es.wikipedia.org/wiki/Banda\\_Ku](https://es.wikipedia.org/wiki/Banda_Ku)
- [18] Airforce Technology. 2017. «RQ-4A/B Global Hawk HALE Reconnaissance UAV». <https://www.airforce-technology.com/projects/rq4-global-hawk-uav/>
- [19] Gradient. 2019. «DRON, RPA, RPAS, UAS y UAV: ¿Qué son y en qué se diferencian?». <https://www.gradient.org/blog/dron/>
- [20] Crespo Quirós, Guadalupe. 2015. «Sistema de enlace robusto para la teleoperación de un UAV (vehículo aéreo no tripulado) en la plataforma robótica ARGOS», <https://repositorio.uam.es/handle/10486/663682>
- [21] MuyInteresante. 2016. «Lo último de Google: internet ultrarrápido con drones». <https://www.muyinteresante.es/tecnologia/articulo/lo-ultimo-de-google-internet-ultrarrapido-con-drones-801454320785>
- [22] Wondershare. 2017. «Aplicaciones presentes y futuras de los drones». <https://filmora.wondershare.com/es/drones/drone-applications-and-uses-in-future.html>
- [23] Inteligencia DYNAMICS. 2013. «Aplicaciones y usos de los drones». [http://www.iuavs.com/pages/aplicaciones\\_y\\_usos](http://www.iuavs.com/pages/aplicaciones_y_usos)
- [24] eldiario.es. 2019. « Fronteras | Así funcionan los drones que el Gobierno planea usar para vigilar la frontera española». [https://www.eldiario.es/desalambre/Gobierno-utilizar-drones-vigilar-Ceuta\\_0\\_615588911.html](https://www.eldiario.es/desalambre/Gobierno-utilizar-drones-vigilar-Ceuta_0_615588911.html)
- [25] FAA. 2019. «FAA Wildlife Strike Database». <https://wildlife.faa.gov/>
- [26] ScareCrow Group. 2018. «Bird Strike Statistics- Lies, damned lies and bird strike statistics». <https://www.scarecrow.eu/bird-strike-statistics/>
- [27] Insurance Information Institute. 2017. «Facts + Statistics: Aviation and drones | III». <https://www.iii.org/fact-statistic/facts-statistics-aviation-and-drones>

- [28] SESAR – Joint Undertaking. 2016. «*European Drones Outlook Study*». [https://www.sesarju.eu/sites/default/files/documents/reports/European\\_Drones\\_Outlook\\_Study\\_2016.pdf](https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf)
- [29] D. L. Cellan-Jones Rory. 2017. «*Drone collides with commercial aeroplane*». BBC. <https://www.bbc.com/news/technology-41635518>
- [30] I. J. Iniesta. 2019. «Un avión choca contra un dron pilotado desde la costa de Elx». Levante-EMV. <https://www.levante-emv.com/comunitat-valenciana/2018/04/10/avion-choca-dron-pilotado-costa/1702185.html>
- [31] Pamela Gregg. 2018. «*Risk in the Sky?*» Dayton University (Ohio). <https://udayton.edu/blogs/udri/18-09-13-risk-in-the-sky.php>
- [32] ASSURE. 2017. «*Volume I - UAS Airborne Collision Severity Evaluation - Structural Evaluation*». FAA | U. S. Department of Administration. <http://www.assureuas.org/projects/deliverables/a3/Volume%20I%20-%20UAS%20Airborne%20Collision%20Severity%20Evaluation%20-%20Structural%20Evaluation.pdf>
- [33] ASSURE. 2017. «*Volume IV - UAS Airborne Collision Severity Evaluation - Engine Ingestion*». FAA | U. S. Department of Administration. <http://www.assureuas.org/projects/deliverables/a3/Volume%20IV%20-%20UAS%20Airborne%20Collision%20Severity%20Evaluation%20-%20Engine%20Ingestion.pdf>
- [34] OACI. 2011. Circular 328 AN/190, «Sistemas de aeronaves no tripuladas (UAS)»
- [35] OACI. 2006. Doc. 7300/9, «Convenio sobre Aviación Civil Internacional».
- [36] Aerial Insights. 2017. «Normativa sobre drones en España». <https://www.aerial-insights.co/blog/normativa-drones-espana/>
- [37] ITU-R. 2009. «*Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace*». <https://www.itu.int:443/es/publications/ITU-R/Pages/publications.aspx>
- [38] M. Neale y D. Colin. 2015. «*Technology Workshop ICAO RPAS MANUAL C2 Link and Communications*». Doc 10019 AN/507. OACI. <https://skybrary.aero/bookshelf/books/4053.pdf>
- [39] OACI. 2015. «*Remotely Piloted Aircraft System (RPAS) Concept of Operations (CONOPS) for International IFR operations*». 4th Edition. <https://eurocontrol.int/sites/default/files/publication/files/Brochure%20RPAS%20CONOPS.pdf>
- [40] Wikipedia.org. 2018. «*Traffic alert and Collision Avoidance System*». [https://es.wikipedia.org/wiki/Traffic\\_alert\\_and\\_Collision\\_Avoidance\\_System](https://es.wikipedia.org/wiki/Traffic_alert_and_Collision_Avoidance_System).
- [41] ITU. 2016. «*Reglamento de Radiocomunicaciones*». [En]. <https://www.itu.int/pub/R-REG-RR>
- [42] CEPT. 2018. «Recomendación ERC 70-03». <https://www.ecodocdb.dk/download/25c41779-cd6e/Rec7003e.pdf>
- [43] European Commission. 2016. «*Radio Equipment Directive (RED)*». Internal Market, Industry, Entrepreneurship and SMEs. [http://ec.europa.eu/growth/sectors/electrical-engineering/red-directive\\_en](http://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en)
- [44] J. S. Lai, J. J. Ford, L. Mejias, P. J. O'Shea, y R. A. Walker. 2012. «*See and avoid using on-board computer vision*». [https://www.researchgate.net/publication/258339148\\_Sense\\_and\\_Avoid\\_in\\_UAS\\_Research\\_and\\_Applications](https://www.researchgate.net/publication/258339148_Sense_and_Avoid_in_UAS_Research_and_Applications)
- [45] Koninklijke Brill NV. 2010. «*Unmanned Aircraft Systems – ATM Collision Avoidance Requirements*». Eurocontrol. [https://www.eurocontrol.int/sites/default/files/content/documents/nm/safety/ACAS/acas-unmannedaircraftsystemsatmcollisionavoidancerequirements-2010\\_.pdf](https://www.eurocontrol.int/sites/default/files/content/documents/nm/safety/ACAS/acas-unmannedaircraftsystemsatmcollisionavoidancerequirements-2010_.pdf)
- [46] Eurocontrol. 2013, «*ACAS X – The future of airborne collision avoidance*», pp. 29-36. Concise Encyclopedia of Traffic & Transportation Systems. Elsevier Editorial.
- [47] Fortem Technologies. 2018. «*Fortem Trueview Radar*». <https://fortemtech.com/products/trueview-radar/>
- [48] B. Lillian. 2018. «*Key UAS Detect-and-Avoid System Tested Successfully in N.Y.*». Unmanned Aerial. [https://unmanned-aerial.com/key-uas-detect-and-avoid-system-tested-successfully-in-n-y.](https://unmanned-aerial.com/key-uas-detect-and-avoid-system-tested-successfully-in-n-y/)
- [49] DJI. 2019. «*GEO ZONE MAP – Safety Flight*». DJI Official. <https://www.dji.com/es/flysafe/geo-map>
- [50] DJI. 2018. «*DJI Refines Geofencing To Enhance Airport Safety, Clarify Restrictions*». DJI Official. <https://www.dji.com/newsroom/news/dji-refines-geofencing-to-enhance-airport-safety-clarify-restrictions>
- [51] ITU-T. 2018. «Recomendaciones UIT-T OID». <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13712>
- [52] OACI. «*OID 1.3.27 ICAO Reference Info*». <http://oidref.com/1.3.27>
- [53] Anthony Rutkowski. 2019. «*ITU-T Takes Lead on Drone IoT Identification in 2019*». ITU-T. [http://www.circleid.com/posts/20190103\\_itu\\_t\\_takes\\_lead\\_on\\_drone\\_iiot\\_identification\\_in\\_2019/](http://www.circleid.com/posts/20190103_itu_t_takes_lead_on_drone_iiot_identification_in_2019/)
- [54] Ericsson. 2018. «*5G - Drones and networks: safe and secure operations*». <https://www.ericsson.com/en/white-papers/drones-and-networks-ensuring-safe-and-secure-operations>
- [55] Rohde & Schwarz. 2013. «*LTE Location Based Services Technology Introduction*». [http://www.rohde-schwarz-wireless.com/documents/LTE\\_LBSWhitePaper\\_RohdeSchwarz.pdf](http://www.rohde-schwarz-wireless.com/documents/LTE_LBSWhitePaper_RohdeSchwarz.pdf)
- [56] Wikipedia.org. 2018. «*Cell Of Origin (COO)*». [https://en.wikipedia.org/wiki/Cell\\_of\\_origin](https://en.wikipedia.org/wiki/Cell_of_origin)

- [57] Vodafone. 2017. «Vodafone utiliza la red móvil 4G como radar para controlar un dron en vuelo». [http://www.saladeprensa.vodafone.es/c/notas-prensa/hp\\_dron\\_utrera\\_2017/](http://www.saladeprensa.vodafone.es/c/notas-prensa/hp_dron_utrera_2017/)
- [58] 3GPP. 2017. «Locate Services Specification # 23.271». <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=834>
- [59] GSMA. 2018. «Mobile-Enabled Unmanned Aircraft. How mobile networks can support unmanned aircraft operations». <https://www.gsma.com/iot/wp-content/uploads/2018/02/Mobile-Enabled-Unmanned-Aircraft-web.pdf>
- [60] S. D. Luz. 2013. «Razones para usar la banda de 2.4GHz en Wi-Fi en lugar de 5GHz». Redes Zone. <https://www.redeszone.net/2013/01/06/razones-para-usar-la-banda-de-2-4ghz-en-wi-fi-en-lugar-de-5ghz/>
- [61] DJI. 2015. «DJI Phantom I Drone». DJI Official. <https://www.dji.com/es/phantom>
- [62] B. Wayne Tomasy. 2003. «Sistemas de Comunicaciones Electrónicas». 976 pág. 4ª Edición. Editorial Pearson Educación.
- [63] Xingqin Lin, Atila Takacs, y Heikki Mahkonen. 2017. «How mobile networks can support drone communication». <https://www.ericsson.com/en/blog/2017/11/how-mobile-networks-can-support-drone-communication>
- [64] X. Lin *et al.* 2018. «The Sky Is Not the Limit: LTE for Unmanned Aerial Vehicles», IEEE Communications Magazine, vol. 56, n.º 4, pp. 204-210. <https://ieeexplore.ieee.org/document/8337920>
- [65] Qualcomm Technologies, Inc. 2016. «Leading the world to 5G: Evolving cellular technologies for safer drone operation». <https://www.qualcomm.com/media/documents/files/leading-the-world-to-5g-evolving-cellular-technologies-for-safer-drone-operation.pdf>
- [66] Mike Lissone. 2018. «Eurocontrol sits at the heart of regulatory, research and operational drone integration work». Eurocontrol. <https://www.eurocontrol.int/sites/default/files/publication/Skyway/2018-skyway-68-cover-story-eurocontrol-drone-integration.pdf>
- [67] Eurocontrol. 2018. «Skyway No. 68 - Spring/Summer». <https://www.eurocontrol.int/publications/skyway-no-68-springsummer-2018>
- [68] Ericsson. 2018. «Mobile Positioning System». <https://www.ericsson.com/en/portfolio/digital-services/automated-network-operations/analytics-and-assurance/mobile-positioning-system>
- [69] Embention. 2017. «Sistemas UTM, Gestión del espacio aéreo con drones». <https://www.embention.com/es/news/sistemas-utm-gestion-espacio-aereo/>
- [70] Indra Company. 2019. «Indra y AirMap cierran un acuerdo de colaboración que refuerza su posición en el mercado de UTM». <https://www.indracompany.com/es/noticia/indra-airmap-cierran-acuerdo-colaboracion-refuerza-posicion-mercado-utm>
- [71] Indra Company. «UTM Connect». <https://www.indracompany.com/es/utm-connect>
- [72] L. Gipson. 2016. «UAS Integration in the NAS Project». NASA. <http://www.nasa.gov/aeroresearch/programs/iasp/uas/description>
- [73] NASA. 2019 (última modificación) «UTM Pilot Program». [https://www.faa.gov/uas/research\\_development/traffic\\_management/utm\\_pilot\\_program/](https://www.faa.gov/uas/research_development/traffic_management/utm_pilot_program/)
- [74] Thales Group. 2017. «Thales da a conocer Ecosystem UTM, autorización automática de vuelo de drones incorporando los conceptos de FAA LAANC». <https://www.thalesgroup.com/es/el-mundo/press-release/thales-da-conocer-ecosystem-utm-autorizacion-automatica-de-vuelo-de-drones>
- [75] FAA (Administración Federal de Aviación de los EEUU). 2019. «UAS Data Exchange (LAANC)». [https://www.faa.gov/uas/programs\\_partnerships/data\\_exchange/](https://www.faa.gov/uas/programs_partnerships/data_exchange/)
- [76] C. Miller. 2018. «Thales, NASA partner on UAS traffic management (UTM) system». 911 Security. <https://www.911security.com/news/thales-nasa-partner-on-uas-traffic-management-utm-system>
- [77] infodron.es. 2019. «La NASA despliega la etapa final de su UTM». Noticias Infodron.es. <http://www.infodron.es/id/2019/05/28/noticia-despliega-etapa-final.html>
- [78] C. Miller. 2018. «Airmap and Skyguide Team Up to Develop Europe's First Drone Traffic Management System». 911 Security. <https://www.911security.com/news/airmap-and-skyguide-team-up-to-develop-europes-first-drone-traffic-management-system>
- [79] AirCrew. 2017. «AirMap is UTM in Action». AirMap. <https://www.airmap.com/airmap-unmanned-traffic-management-utm-matt-koskela-product/>
- [80] Quantum Aviation, Ltd. 2018. «TITANIUM is a complete Counter-Unmanned Aerial Systems solution». <https://www.quantumaviation.co.uk/titanium-c-uas/>
- [81] infodron.es. 2019. «Thales ofrece al mercado europeo el antidrón que ha vendido en Asia». Noticias Infodron.es. <http://www.infodron.es/id/2019/05/25/noticia-thales-espana-presenta-solucion-inhibe-ataques-drones.html>