Universidad Zaragoza
1542

Trabajo Fin de Grado

ALTERNATIVAS AL GNSS COMO SISTEMA DE POSICIONAMIENTO DE RPAS

Autor: Glen Fermisson Ceinos

Director académico: Dra. María Teresa Lamelas Gracia

Director militar: Cap. D. Juan José Bermúdez Antona

Centro Universitario de la Defensa-Academia General Militar

2023

Agradecimientos

En primer lugar, agradecer a mi familia por el constante apoyo y paciencia a lo largo del desarrollo de este trabajo.

En segundo lugar, agradecer a mis tutores la excepcional paciencia y consideración que han tenido y su inmenso apoyo y ayuda. No podría haber podido terminar este trabajo sin sus consejos y aportaciones. Mención al Capitán D. Juan José Bermúdez Antona por haber cumplido los objetivos que nos habíamos planteado. Sobre todo, le agradezco que, aunque al principio no tuviese los conocimientos necesarios para la realización de este proyecto, me ha guiado e inculcado una serie de conceptos sin los cuales no podría haber realizado este trabajo.

En tercer lugar, agradecer a los expertos consultados, que con entusiasmo han respondido todas mis dudas y propuesto sus consideraciones que han conseguido que este trabajo sea una realidad.

No puedo olvidar mencionar al Teniente Coronel Ramón Becerra Rubio, que me ha mostrado todo su apoyo y confianza en la parte final de este trabajo.

Por último, agradecer a mis compañeros del CXXX Curso de Piloto de Helicópteros del Ejército de Tierra, que han sido un gran apoyo durante el curso y en la parte final de este trabajo.

RESUMEN

Los sistemas aéreos no tripulados (Unmanned Aerial System, UAS), incluyendo los sistemas aéreos remotamente pilotados (Remoted Piloted Aircraft, RPAS), suponen un gran avance tecnológico que ha propiciado la humanidad en su proceso evolutivo. No obstante, unido al gran escalón que estas tecnologías suponen para el mundo, se debe considerar el desarrollo de la tecnología inercial en combinación con Global Positioning System (GPS) en la navegación. Para que esta navegación sea efectiva, además, se debe contar con otros medios de refuerzo o alternativos. Esto se debe a que varios estudios han puesto en evidencia la vulnerabilidad de los sistemas GNSS, que actualmente pueden significar un riesgo para la seguridad internacional.

La creciente importancia del sector de los RPAS se debe a su capacidad industrial y estratégica, que se ha visto reflejada en su aumento constante en el ámbito de la Defensa y otras aplicaciones para la sociedad en general. Aplicaciones que van desde; la gestión de emergencias, el control de tráfico, el control de fronteras marítimas y terrestres, y en la construcción, entre otros. La revolución en los RPAS en el contexto de la estrategia de la guerra se ha visto en los recientes conflictos en Europa (Ucrania). Esto es debido a diversos factores como es la capacidad de aprovechar la dificultad de su detección (de los RPAS) por medios radares convencionales. Sin embargo, al mismo tiempo se ha evidenciado su dependencia a la tecnología Global Navigation Satelite System (GNSS). Estos sistemas obtienen, en gran parte, el posicionamiento, las comunicaciones y la designación de objetivos mediante el servicio GNSS. Esta dependencia hace vulnerable a los RPAS una vez que se interrumpen las señales del satélite, dejando al equipo a ciegas ante situaciones críticas. Las señales son proporcionadas a nivel global por cuatro constelaciones: GPS, GLONASS (servicio GNSS Ruso), GALILEO (sistema europeo de GNSS) y BEIDOU *(*sistema de navegación por satélite chino). Por lo tanto, en este trabajo se ha sido estudiado y evaluado las alternativas al GNSS como sistema de posicionamiento de lo RPAS para encontrar una respuesta clara a las necesidades identificadas.

Para llevar a cabo esta investigación se ha realizado una búsqueda exhaustiva de más de 300 archivos y referencias bibliográficas, de los cuales se han seleccionado 25 referencias específicas y se llevaron a cabo cuatro entrevistas a expertos en la materia. Esta información ha proporcionado un conocimiento preciso y útil sobre las nuevas tecnologías de geoespaciales y de geoposicionamiento. Además de entender como están causando una revolución en diversos países que quieren involucrarse en el valor estratégico, tecnológico, social y económico que representan estas tecnologías en continuo desarrollo. Estas tecnologías están siendo utilizadas en una amplia variedad de aplicaciones, incluso en los dispositivos móviles más novedosos para el usuario común.

Los resultados de la investigación han revelado que se están desarrollando tecnologías innovadoras para mejorar el funcionamiento de los RPAS, como microchips, la tecnología de detección y medición láser (LIDAR), las antenas (CRPA), así como proyectos como el GPS OCS y otras alternativas a considerar. Es importante tener en cuenta que estas tecnologías no pueden considerarse, por el momento, como un reemplazo completo de los sistemas GNSS, sino más bien como soluciones complementarias que pueden mejorar y reforzar el funcionamiento de los RPAS. Esto permitirá minimizar riesgos y amenazas, además de potenciar los beneficios y aplicaciones en el ámbito civil y militar.

PALABRAS CLAVE

UAVs, RPAS, GNSS, Seguridad Internacional, Operaciones militares, Ambiente denegado al GNSS.

ABSTRACT

Unmanned aerial systems (UAS), including remotely piloted aerial systems (Remoted Piloted Aircraft, RPAS), represent a great technological advance that humanity has fostered in its evolutionary process. However, together with the great step that these technologies represent for the world, the development of inertial technology in combination with the Global Positioning System (GPS) in navigation should be considered. For this navigation to be effective, in addition, other reinforcement or alternative means must be available. This is because several studies have highlighted the vulnerability of GNSS systems, which can currently pose a risk to international security.

The growing importance of the RPAS sector is due to its industrial and strategic capacity, which has been reflected in its constant increase in the field of Defense and other applications for society in general. Applications ranging from; emergency management, traffic control, maritime and land border control, and construction, among others. The revolution in RPAS in the context of war strategy has been seen in the recent conflicts in Europe (Ukraine). This is due to various factors such as the ability to take advantage of the difficulty of their detection (of RPAS) by conventional radar means. However, at the same time, its dependence on Global Navigation Satellite System (GNSS) technology has become evident. These systems obtain, to a large extent, the positioning, the communications, and the designation of objectives by means of the GNSS service. This dependency makes RPAS vulnerable once satellite signals are disrupted, leaving the team blindsided to critical situations. Signals are provided globally by four constellations: GPS, GLONASS (Russian GNSS service), GALILEO (European GNSS system) and BEIDOU (Chinese satellite navigation system). Therefore, in this work the alternatives to GNSS as a positioning system of RPAS have been studied and evaluated to find a clear answer to the identified needs.

To carry out this research, an exhaustive search of more than 300 files and bibliographical references has been carried out, of which 25 specific references have been selected and four interviews were carried out with experts in the field. This information has provided accurate and useful insight into new geospatial and geopositioning technologies. In addition to understanding how they are causing a revolution in various countries that want to get involved in the strategic, technological, social, and economic value that these technologies in continuous development represent. These technologies are being used in a wide variety of applications, including the latest mobile devices for the common user.

The research results have revealed that innovative technologies are being developed to improve the performance of RPAS, such as microchips, laser detection and measurement technology (LIDAR), antennas (CRPA), as well as projects such as GPS OCS and other alternatives to consider. It is important to note that these technologies cannot be considered, for the moment, as a complete replacement for GNSS systems, but rather as complementary solutions that can improve and strengthen the performance of RPAS. This will make it possible to minimize risks and threats, in addition to enhancing the benefits and applications in the civil and military spheres.

KEYWORDS

UAVs, RPAS, GNSS, International Security, Military Operations, GNSS-denied environment.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

A2/AD: sistema anti-acceso y denegación de área (interrupción comunicaciones satelite).
ABAS: Airborne Based Augmentation System / Sistema de aumentación basado en la aeronave.
ACAVIET: Academia de Aviación del Ejército de Tierra.
AGL: Above Ground Level / Sobre el nivel del suelo.
AP: Automatic Pilot/ Piloto automático.
BEIDOU: *Běidǒu Wèixīng Dǎoháng Xìtǒng (sistema de navegación por satélite chino).*
BD: Base de Datos.
BLOS: Beyond Line of Sight / Más allá de la línea de visión.
BVLOS: Beyond VLOS Operations / Más allá de las operaciones VLOS.
C/A: Coarse/Acquisition/ Código de adquisición grosera.
CNSA: Consejo Nacional de Seguridad Aeroespacial.
CRPA: Controlled Reception Pattern Antenna.
dBi: Ganancia de antena en dB por encima de un radiador isotópico.
dBm: decibel-milliwatts/ Relación de potencia en decibeles(dB) referidos a un mili watt.
dBW: decibel-watt/ relación de potencia en decibeles(dB) referidos a un watt(W).
DARPA: Defense Advances Research Projects Agency.
DGAM: Dirección General de Armamento y Material.
DME: Distance Measuring Equipment/ Equipo Medidor de Distancia (telémetro).
DRN: Dead Reckoning Navigation/ Cálculo de posición por sensores y posición inicial.
EECTI: Estrategia Española de Ciencia, Tecnología e Innovación.
ETID: Estrategia de Tecnología e Innovación para la Defensa.
EE. UU.: Estados Unidos de América.
EGNOS: European Geostationary Navigation Overlay Service/ Sistema Europeo para el aumento del capacidad GNSS.
ET: Ejército de Tierra.
EW: Electronic Warfare/ Guerra Electrónica.
FAMET: Fuerzas Aeromóviles del Ejército de Tierra.
FAS: Fuerzas Armadas.
FCS: Flight Control System/ Sistema del Control de Vuelo.
GBAS: Ground Based Augmentation System / Sistema de aumentación basado en tierra.
GCS: Ground Control System/ Sistema de control en tierra.
GIS: Sistema de información geográfica.
GLONASS: Global'naya Navigatsionnaya Sputnikovaya Sistema (GNSS).
GNSS: Global Navigation Satellite System/ Sistema global de navegación por satélite.
IDM: Interference, Detection and Mitigation/ Interferencia, Detección y Mitigación.
IFR: Instrumental Flight Rules/ Reglas de Vuelo Instrumental.
IMU: Inertial Measurement Unit/ Unidad de Medición Inercial.
INS: Inertial Navigation System/ Sistema de Navegación Inercial.
INTA: Instituto Nacional de Técnica Aeroespacial.
ISR: Intelligence, Surveillance and Reconnaissance/Reconocimiento, Vigilancia e Inteligencia.
LOS: Line of Sight / Línea de Visión.
LIDAR: Light Detection and Ranging.
MDE: Modelo Digital de Elevación del terreno.
OFEN: Oficial de Enlace/ Oficial encargado de mantener la comunicación con otro ejército.
PBN: Performance- Based Navigation / Navegación basada en el Rendimiento.

PI: Petición de información.
PinS: Punto en el espacio.
PNT: Positioning, Navigation and Timing/ Posicionamiento, Navegación y Sincronización.
PPS: Servicio de Posicionamiento Preciso.
PPP: Posicionamiento de Punto Preciso, es un servicio de posicionamiento mundial preciso.
PRS: Servicio de Navegación Cifrado Resistente a las Interferencias.
RNAV: Area Navigation/ Navegación de Área.
RPA: Remoted Piloted Aircraft. Aeronave Pilotada Remotamente.
RPAS: Remoted Piloted Aircraft System/ Sistema de vuelo pilotado de manera remota.
SBAS: Satellite Based Augmentation System/ Sistema de aumentación basado en satélites.
SHORAD: Short Range Air Defense/ Defensa antiaérea cercana.
SLAM: Simultaneous Localization and Mapping.
SOPT: Sistema de Observación y Prospectiva Tecnológica.
SPS: Servicio Estándar de Posicionamiento, en L1 con el código C/A.
TIMU: Timing and Inertial Measurement Unit
TO: Teatro de Operaciones.
TTP: Técnicas, Tácticas y Procedimientos.
UE: Unión Europea.
UAS: Unmanned Aerial System.
UAV: Unmanned Aerial Vehicle.
UCAV: Unmanned Combat Aerial Vehicle.
VFR: Visual Flight Rules/ Reglas de Vuelo Visual.
VLOS: Visual Line of Sight Operations / Operaciones de línea de visión.
VNS: Visual Navigation System/ Sistema de Navegación Visual.
VOR: Very High Frequency Omni-Directional Range/ Baliza omnidireccional de alta frecuencia.

1. INTRODUCCIÓN

En la actualidad, para entender la navegación mediante GNSS, es necesario comprender qué supone procesar un gran flujo de información, qué a su vez, tiene una gran limitación. Esta limitación se debe a la dependencia de los sistemas que basan su operación en los satélites y el flujo de información que les proporciona. Por ejemplo, los RPAS dependen del GNSS para la adquisición, sincronización, procesamiento, integración y transformación de las medidas de los datos de todos los subsistemas (sistemas que proporcionan datos de navegación con apoyo de satélites, los Sistemas de Navegación Inercial -INS-, que actualizan su posición en tiempo real con la información del satélite, el Air Data Computer -ADC-, antenas GNSS por donde recibe y responde a las señales satélite…) en parámetros como el de posicionamiento global y otros necesarios para la operación, como es la trayectoria aérea, entre otros.

Si consideramos el significativo progreso de las tecnologías de posicionamiento han supuesto para el mundo y aumento de la dependencia tecnológica del GNSS en la navegación de los diferentes sistemas aéreos o terrestres, podemos encontramos en varios estudios, que su vulnerabilidad también ha quedado en evidencia. De hecho, estas vulnerabilidades de los sistemas GNSS pueden representar actualmente un riesgo para la seguridad internacional.

Ahora bien, el término GNSS, que engloba los Sistemas de Navegación por Satélite, constituye una infraestructura espacial de satélites generadores de señales, y comprende aquellos subsistemas que están en capacidad de proporcionar posicionamiento y navegación, así como un óptimo sistema de definición de velocidad y tiempos. Dichas señales son a nivel global proporcionadas por cuatro constelaciones: GPS-NAVSTAR, GLONASS, GALILEO y BeiDou. (Berné Valero, 2019).

El mercado de GNSS, junto con las nuevas tecnologías geoespaciales y de geoposicionamiento, está revolucionando diversos países, al hacerles comprender su valor estratégico, tecnológico, social y económico. Además, estas tecnologías pueden tener aplicaciones en una amplia gama de áreas, incluyendo dispositivos móviles de uso común. Según el presidente de Hexagon Geospatial, Mladen Stojic, el impacto de GNSS radica en su capacidad para determinar con precisión la ubicación, lo que permite a los usuarios tomar decisiones informadas. (Berné Valero, 2019). Otros autores afirman, además, que la navegación por satélite es uno de los sectores de mayor crecimiento actualmente en términos de desarrollo de sistemas y aplicaciones. (Ventura, 2015).

Por otra parte, el estudio llevado a cabo por el Sistema de Observación y Prospectiva Tecnológica (SOPT) y el Instituto Nacional de Técnica Aeroespacial (INTA), (Ministerio de Defensa, 2016), ha señalado la importancia de la prospectiva tecnológica de la navegación en condiciones de denegación de GNSS, lo que supone la pérdida de comunicación con satélites de posicionamiento. En este sentido, se recomienda el análisis de los sistemas de navegación, especialmente cuando se utilizan en UAS, como los RPAS, en colaboración con las Fuerzas Armadas (FAS). Esta colaboración se justifica por los problemas que las FAS han experimentado al operar estos equipos, debido a diversos fallos en la señal GNSS.

Además, los resultados del estudio han destacado una serie de aspectos tecnológicos que necesitan ser investigados de forma exhaustiva en un momento de conflictos internacionales en la que la navegación con GNSS tal como hoy se conoce, está siendo afectada significativamente por interferencias intencionadas o no, y denegación.

Teniendo esto en consideración, el propósito de este trabajo es realizar una revisión crítica de las alternativas de posicionamiento de RPAS distintas al GNSS. También se busca evaluar el impacto que supone la vulnerabilidad de este sistema en medio de situaciones de crisis y conflicto internacional. Para esto, se enfoca este estudio en los métodos actuales de navegación que pueden ser afectados por interferencias, así como en el uso de nuevas tecnologías en desarrollo y las alternativas al GNSS para el posicionamiento de RPAS en el ámbito de la Defensa y Seguridad.

1.1. Consideraciones preliminares

En el marco del tema abordado: Alternativas al GNSS como sistema de posicionamiento de RPAS, deben tenerse en cuenta una serie de consideraciones preliminares al estudio en cuestión:

1. Se están desarrollando actualmente diversos sistemas adaptables a los requisitos de las FAS para mejorar las capacidades de navegación, comunicación, entre otros, de los RPAS y responder de manera efectiva ante los nuevos retos de un mundo cada vez más globalizado y en conflicto (Dirección General de Armamento y Material, DGAM, 2020).
2. El avance tecnológico y el incremento del uso de sistemas de interferencia a la señal del GNSS, que por ende irrumpen el óptimo funcionamiento de los RPAS del Ejército de Tierra (ET), parece una constante a la que las FAS se tiene que adaptar (García, 2022).
3. Las capacidades en materia de operatividad, coordinación e integración de los sistemas RPAS, debido a las vulnerabilidades que motivan este trabajo, tienen como resultado bajos niveles de eficacia. Sin embargo, esta eficacia es un requisito indispensable para el cumplimiento de la misión en determinados entornos. (Martínez, 2020).
4. El desarrollo de nuevas tecnologías, así como el descenso de los costes de estos sistemas en la actualidad, han hecho más factible su adquisición en el mercado internacional. Esta facilidad de adquisición supone, sin embargo, un riesgo evidente, al poner en manos de diversos actores estatales o particulares, la voluntad y oportunidad de interferir en las operaciones de los RPAS, amenazando así la seguridad mundial (Consejo Nacional de Seguridad Aeroespacial, CNSA, 2022).
5. El impacto de la vulnerabilidad del GNSS en los RPAS radica principalmente en la emergencia que supone la pérdida se señal del satélite, ya sea por interferencia o falta de cobertura, conllevando a un vuelo degradado, no operativo o no óptimo, ante las funciones para las que fue desarrollado (comunicación personal Cruz Hernández, 2022).
6. La adaptación de las nuevas tecnologías que ya están disponibles en el mercado global, como las antenas contra interferencia intencionada (Controlled Reception Pattern Antenna, CRPA), que garantizan una muy alta resistencia y seguridad al funcionamiento de todo el sistema, manteniendo un enlace seguro entre RPAS y satelite. Por otro lado, los sistemas de Navegación Visual (VNS) que mejoran la navegación en entornos con señal GNSS denegada a través de técnicas de odometría visual, pueden aportar grandes beneficios a las FAS. Si tenemos en cuenta el plan estratégico del ministerio de Fomento para el desarrollo del sector civil de los drones en España, junto con las necesidades de las FAS identificadas a través de las monografías del SOPT, podemos esperar una sinergia positiva entre industria y las FAS. Esta sinergia, se encuentra destacada en el Plan Director de RPAS del Ministerio de Defensa, para el desarrollo conjunto con la industria nacional de las nuevas tecnologías de RPAS, encaminadas a mejorar sus sistemas de navegación.

7. Es evidente que, actualmente, hay muchas aplicaciones en las que una correcta navegación es crítica y, por ello, los factores relativos a su fiabilidad están ganando importancia. Dado que la fiabilidad está estrechamente relacionada con la redundancia de sensores, se detecta la necesidad de complementar la navegación basada en GNSS con otros sistemas de navegación colaborativos (SOPT, 2013).
8. El proceso de implementación de los sistemas necesarios para mejorar las capacidades de los RPAS del Ejército de Tierra (ET) en operaciones en zonas de GNSS denegados, podría suponer: la optimización de medios y la innovación aeronáutica liderada por el ejército.

2. OBJETIVOS Y METODOLOGÍA

2.1. Objetivos y alcance

2.1.1. Objetivo general

El objetivo general de la presente investigación es evaluar las alternativas al GNSS para el posicionamiento de los RPAS y el impacto que supone la vulnerabilidad del sistema, que es utilizado en gran medida en la navegación de las FAS, en España y en el mundo en general, especialmente en situaciones controversiales y de conflicto internacional, como es la guerra.

2.1.1.1. Objetivos específicos

Por su parte, los objetivos secundarios y específicos que se han planificado en función del cumplimiento del anterior se resumen a continuación:

1. Analizar el estado de la cuestión de los RPAS en dotación del ET, sus características de navegación, beneficios, vulnerabilidades, dependencia de GNSS y su comportamiento en un ambiente de denegación.
2. Identificar las necesidades actuales en zona de operaciones en misiones en las que se utilizan los RPAS, operando bajo condiciones GNSS degradadas.
3. Estudiar la implementación de nuevas tecnologías o modelos en desarrollo de RPAS en el refuerzo del enlace GNSS o en la navegación sin enlace satélite, frente a las necesidades identificadas.

2.1.2. Alcance de la investigación

El alcance de la investigación se resume en cómo se han empleado todos los recursos a los que se ha logrado acceder, en función del cumplimiento de los objetivos planteados, siguiendo además una planificación estructurada.

En este sentido se pretende, en general, evaluar las alternativas al GNSS de RPAS y el impacto que supone la vulnerabilidad de dicho sistema en medio de situaciones controversiales y de conflicto internacional, como la guerra. Por lo tanto, en el marco de los recursos disponibles se aplican una serie de entrevistas, así como una exhaustiva revisión bibliográfica.

Por un lado, la navegación por imagen parece ser una de las soluciones alternativas en función de la compensación de las vulnerabilidades evidenciadas en la tecnología GNSS, apoyándose en el desarrollo de sensores de refuerzo a los inerciales para aumentar la seguridad en la navegación, y contribuir al cumplimiento eficiente de las misiones y operaciones en cuestión. Sin embargo, no se centra esta investigación en profundidad en las nuevas tecnologías o en la determinación de soluciones a corto plazo, sino más bien en el planteamiento y evaluación crítica de las diversas alternativas sobre las tecnologías existentes y en desarrollo, respecto a la vulnerabilidad de estas, y lo que eso significa en la perspectiva global en la actualidad.

En consecuencia, se ha realizado un estudio de la normativa vigente en referencia a los sistemas RPA, analizando cómo los avances en la materia han llevado al desarrollo de un nuevo reglamento europeo cuya aplicación en España ha sido progresiva desde el 2021 y espera finalizar en 2023, así como el hecho de que pese a las mejoras en las capacidades actuales de los RPAS, estos mantienen aún una dependencia significativa sobre el GNSS, por lo que se hace más que evidente la necesidad de crear una navegación con mayor fiabilidad que deja dos principales alternativas a la vista: el incremento en la seguridad del enlace con los satélites en cuestión, o la dependencia en menor medida de éstos.

Con esto en cuenta, el alcance de la investigación está limitado a los contactos que se han podido entrevistar en el ET y a la información bibliográfica limitada sobre ejercicios, características, proyectos de mejora de capacidades y evaluaciones, hallada en medios digitales e impresos que además ha debido filtrarse según determinados criterios de inclusión y exclusión definidos en el siguiente apartado. No se pretende entonces, desde una perspectiva realista y lógica, determinar las alternativas más eficientes a las necesidades identificadas en el estudio o aportar soluciones lógicas a corto plazo porque no se disponen de los recursos necesarios para lograrlo.

Se tienen en cuenta también, en medio de esta investigación, las necesidades actuales y futuras de las FAS, expuestas en el Plan Director de RPAS cuya visión aporta una referencia clara al sector industrial español en la materia con intención de que éste pueda competir en igualdad de condiciones con otras empresas extranjeras, desplegando sistemas e incrementando las capacidades nacionales en desarrollo sobre Defensa.

Así, esta memoria resume, en el marco del grado de Organización Industrial impartido por el Centro Universitario de la Defensa en la Academia General Militar (Zaragoza), los resultados de un estudio producto de las necesidades identificadas principalmente en la zona de operaciones en misiones de RPAS. Siendo valoradas sobre la operación bajo condiciones GNSS degradadas, que han llevado a contemplar tecnologías alternativas que éstos puedan adoptar en los nuevos modelos en desarrollo. Además, teniendo en cuenta que deben hacer frente a las nuevas exigencias de las operaciones militares y de seguridad internacional. La misma considera en un análisis crítico, la revolución interna que llevó a las FAS a modificar y perfeccionar los métodos de planeamiento y ejecución de despliegue con el objetivo de reducir el número de bajas a cero. Para ello acabo integrando los RPAS que cumplen un papel fundamental en las operaciones militares para labores de reconocimiento y prevención de riesgos para las tripulaciones. Sin embargo, el enfoque principal radica no sólo en la evolución de los RPAS, sino también en la de aquellos sistemas que interfieren significativamente con su labor. Consiguiendo que estos sean vulnerables en la zona de operaciones, ante el jamming o el spoofing (interferencias o manipulación de las señales de satélite) que actúan con eficacia en contra de los primeros.

2.2. Metodología

La metodología aplicada en el desarrollo de la presente investigación ha sido de tipo mixta: cualitativa y cuantitativa.

En el marco de los modelos de análisis empleados en el estudio de los requisitos y necesidades que demandan principalmente los operadores de RPAS, y en función del cumplimiento de los objetivos planteados, teniendo claro además el alcance al que puede llegar esta investigación, se han empleado dos técnicas principales para la obtención y análisis de la información: la revisión documental y bibliográfica por un lado y las entrevistas a expertos para fundamentar los resultados.

En la primera fase, de revisión documental y bibliográfica, se ha recopilado información relativa a la problemática planteada, identificando las principales vulnerabilidades de los RPAS en ambiente de denegación de GNSS, así como definiendo numerosos conceptos y antecedentes propios a la investigación. Para ello se ha realizado una búsqueda exhaustiva en medios digitales e impresos, en bibliotecas, libros, trabajos académicos previos, artículos de investigación, publicaciones académicas. Utilizando también repositorios de información como Dialnet, Google Scholar, la biblioteca Unizar, publicaciones de prensa o de contenido digital en la página web de US Army y otros sitios web en línea, encontrando un número limitado de 325

archivos relacionados de los cuales se han seleccionado 37 referentes para incluir en este documento.

Los criterios de inclusión y exclusión se han resumido por su parte, de la siguiente manera:

Criterios de inclusión:

1. Artículos de investigación disponibles gratuitamente a los que pueda acceder cualquier lector o estudiante de esta propuesta, con fines de verificar la información suministrada.
2. Artículos con una antigüedad no mayor a 15 años (2007-2022) a no ser que sean relevantes para la investigación.
3. Artículos en inglés o español. Se incluye el inglés debido a su importancia internacional en general y en el mundo aeronáutico en particular. Y para poder utilizar los estudios internacionales más relevantes y del US Army que se realizan en inglés sobre el tema en estudio.
4. Libros, trabajos académicos previos, artículos académicos, artículos de prensa o de contenido web con información contrastada o con autores de reconocida reputación, y otros documentos de calidad académica, técnica y científica.
5. Artículos relacionados con las palabras clave y el tema de estudio abordado.

Criterios de exclusión:

1. Artículos que sólo están disponibles bajo licencia de pago.
2. Artículos del año 2006 o de años anteriores (a no ser que sean relevantes para el estudio).
3. Artículos de blog sin ninguna referencia bibliográfica y científica verificable.
4. Artículos de temáticas irrelevantes a la investigación.
5. Artículos redundantes y de poca claridad científica.

En la tabla 1, pueden observarse específicamente las muestras de los resultados obtenidos en la búsqueda bibliográfica, así como el total de referencias incluidas en la presente investigación.

Tabla 1 Resultados de búsqueda documental y bibliográfica.

Términos y combinaciones de búsqueda	**Resultados**	**Excluidos**	**Incluidos**
UAVs AND RPAS	125	120	5
GNSS como sistema de posicionamiento de RPAS	25	20	5
Alternativas al GNSS	15	11	4
Conjunto de GNSS	30	27	3
Beneficios y debilidades de los RPAS	40	34	6
Normativa vigente sobre los RPAS	12	10	2
RPAS en España y Europa	28	20	8
Drones	50	46	4
TOTALES	**325**	**288**	**37**

Fuente: Elaboración propia.

La segunda fase, por su parte, consistió en el desarrollo de diversas entrevistas en reuniones físicas y personales o telefónicas, previamente pautadas, así como consultas electrónicas a través del correo, a expertos especializados en RPAS del ET: el Capitán Juan José Bermúdez Antona, Brigada. Miguel Ángel Llompart y el Sargento 1° Miguel Vasallo Ledo, así como a un experto en Guerra Electrónica: Francisco Javier Cruz Hernández. Dichas entrevistas han permitido el acceso a información de alta calidad sobre la operatividad, misiones, capacidades y limitaciones de los sistemas RPAS, así como sus vulnerabilidades en ambiente de GNSS denegado y los beneficios e inconvenientes evidenciados en la implementación de nuevos sistemas en la navegación. Las entrevistas pueden consultarse textualmente en los anexos del trabajo (Anexo I y Anexo II, respectivamente).

Cabe destacar que el informe del Oficial de Enlace de la US Army en el TRADOC (Tcol. D. José A. Fernández Alfaro), también ha permitido obtener una visión más amplia de los aspectos técnicos de los sistemas RPAS, así como sus beneficios e inconvenientes actuales. Además de los sistemas que hoy en día tienen la capacidad de enfrentar un ambiente GNSS denegado, y el uso de estos sistemas en Estados Unidos (véase Anexo III).

Finalmente, hay que mencionar que el presente trabajo, se estructura en seis apartados principales en los que convergen, además, una serie de subapartados necesarios para comprender los conceptos asociados. Como son las interferencias, su funcionamiento y su interacción con la señal GNSS para denegar un enlace del satélite con el RPA, además de las tecnologías actuales y aquellas en desarrollo, entre otros. Asimismo, se desarrollan algunas consideraciones preliminares importantes, la planificación de objetivos y el alcance de estos en torno al proyecto, el análisis de la información estudiada y las conclusiones a las que dicha información ha llevado.

Por otra parte, aun teniendo en cuenta el temprano desarrollo en el que se encuentran algunas nuevas tecnologías alternativas, se proponen algunas soluciones a corto plazo. Estas se reducen a las tecnologías existentes y ya aplicadas con éxito en algunos modelos, como las antenas CRPA que llevan ganando peso desde 2015. Sin embargo, se valorarán los costes de sistemas y del mantenimiento de estos, de acuerdo con los datos aportados por Francisco Javier Cruz Hernández como experto en Guerra Electrónica.

En la última década la necesidad creciente de combatir el jamming (interferencia) y spoofing (implantación de identidad) de la señal GNSS se ha plasmado en que las antenas CRPA previamente solo disponibles para militares autorizados de algunos ejércitos hayan acabado extendiéndose al mundo civil. Como ejemplo, podemos considerar como el Servicio Publico Regulado de Galileo (Galileo Public Regulated Service, Galileo PRS) ya está equipado con sistemas compatibles con las antenas CRPA. Además, el servicio abierto de Galileo requerirá, muy probablemente, una capacidad de protección contra estas interferencias, según un estudio publicado por Inside GNSS en Marzo de 2022.

3. VEHÍCULOS AÉREOS NO TRIPULADOS: UAV

Históricamente el ser humano ha logrado superar los diferentes obstáculos impuestos por la física y la gravedad, iniciando nuestra andadura en el aire en el siglo XX para más adelante viajar al espacio. Todos los esfuerzos que se han llevado a cabo nos han conducido a la era tecnológica actual. Aun así, se siguen presentando diversas vulnerabilidades, que nos obligan a trabajar en ofrecer respuestas satisfactorias a los nuevos dilemas, que, al mismo tiempo, nos hacen seguir evolucionando (Carrasco, 2017).

Ciertamente no es posible ahora determinar hasta qué punto llegarán en el futuro los avances del ser humano en términos que hoy se conocen como globalización, economía, comunicaciones e incluso RPAS, que constituyen "un eslabón más en la evolución tecnológica" (Carrasco, 2017).

Los sistemas aéreos tripulados remotamente o RPAS, han supuesto en estos avances históricos no sólo un eslabón más en la tecnología, sino también uno de los cambios más significativos generados en la operación militar. Estos sistemas, además, se han convertido en un foco de atención para las FAS y la Seguridad Mundial. De hecho, han pasado a ser un instrumento imprescindible en gran parte de las FAS del mundo dada su versatilidad, capacidad operativa, costos reducidos y gran prevalencia en las actuaciones eficientes sobre situaciones de conflictos generadas comúnmente entre países (Asensi, 2014).

En este punto, es importante mencionar el termino “Inteligencia en tiempo real” (figura 1), ya que la función más destacada de los RPAS se encuentra en su capacidad operativa para llevar a cabo misiones de inteligencia, vigilancia y reconocimiento (conocidas como ISR). Aunque se han considerado otras aplicaciones para el futuro en operaciones militares, como transporte aéreo, evacuaciones médicas, comunicaciones y otros, su función principal no será reemplazada (SOPT, 2013).

Figura 1 Representacion de la Inteligencia en tiempo real. Fuente: Aviaciondigital.com

Desde su creación hasta la actualidad, los UAS han aportado numerosos beneficios tanto en el ámbitos militar y de seguridad global como en el civil. Esto ha generado un aumento en la demanda del espacio aéreo para su implementación operativa, así como la necesidad imperativa de buscar soluciones alternativas para abordar sus vulnerabilidades y dependencias a través de esfuerzos dirigidos a la operación segura, la regulación y otros aspectos asociados a la navegación (Asensi, 2014).

Resulta innegable la popularidad entre países que ha tomado el campo de los vehículos aéreos no tripulados o UAV, debida principalmente a su gran capacidad tecnológica en la ejecución de operaciones militares complejas con rapidez y suficiencia, así como la cooperación en diversas tareas de manipulación y transporte, navegación autónoma, entre otros (Krajnik, 2014).

Sin embargo, pese a los avances y evolución que estos suponen, hoy en día es imperativo estudiar sus vulnerabilidades como obstáculos en el desarrollo de su plena autonomía y, por ende, de una capacidad operativa mayor o más eficiente (Krajnik, 2014).

3.1. Antecedentes Históricos

Según expertos como Carrasco (2017), el término UAV, nació aproximadamente en el siglo XIX con la implementación de globos cargados de explosivos (en el año 1849) que fueron dirigidos contra Venecia por parte del Ejército de Austria. Este inicio dio lugar al avance y desarrollo tecnológico paulatino en torno al control de movimiento para vehículos y buques, por lo que hasta 1917 aparece una versión bastante antigua de lo que hoy se conoce como un misil a control remoto (Carrasco, 2017).

En 1931, se creó un biplano no Tripulado, y en 1936 se prueba con éxito el primer UAV a control remoto desde una embarcación, al que se le dio nombre de "drone" que hacía referencia a aquellos vehículos aéreos que se controlaban a través de la radio (Carrasco, 2017).

En 1940 se crea la primera fabricación de UAVs a gran escala, y ya en 1942 estos vehículos ya eran dirigidos a control remoto gracias al empleo de un sistema de televisión a bordo que permitía obtener imágenes precisas para navegar el UAV (Carrasco, 2017).

El año 1951 marca una fecha importante la historia de los UAV, ya que Estados comenzó a fabricar estos vehículos para utilizarlos en misiones de reconocimiento, lanzándolos desde naves nodrizas en el espacio aéreo. Al cabo de unos 10 años, esta actividad se convirtió en algo habitual debido a la ventaja que proporcionaba en los conflictos bélicos (Carrasco, 2017). En la actualidad, los propios UAS están asumiendo este papel y también están llevando a cabo operaciones como naves nodrizas (ver figura 2).

Figura 2 Dron MQ- 25 T1, primer dron realizando funciones de avión nodriza en 2021. Fuente:larazon.es

Ya en 1980 se desarrollaban UAVs con mayor alcance, empleados en conjunto con aviones tripulados para aportar un señuelo electrónico y de reconocimiento aéreo, que sigue siendo una de sus funciones principales, como ya se ha mencionado al comienzo de este capítulo. Su uso estratégico generó la necesidad de seguir avanzando y desarrollando esta tecnología, por lo que para 1994 ya sus estructuras tenían más capacidades, cargas de pago y sistemas de posicionamiento basado en GPS (Carrasco, 2017).

Un hecho histórico en medio de estos antecedentes es la creación en 1998 de un UAV de largo alcance y gran capacidad operativa en Estados Unidos que fue denominado Global Hawk; su autonomía y carga de pago supusieron para la época un gran paso en la evolución tecnológica y la aplicación e impacto de este tipo de sistemas (Carrasco, 2017).

A partir del año 2010, la presencia cada vez más frecuente de vehículos no tripulados se ha vuelto común tanto en el ámbito militar como civil. Esto ha abierto un vasto campo de posibilidades para los países Este desarrollo representa una evolución progresiva de 167 años, en la que se han utilizado numerosos términos y variaciones (además de UAV) para referirse a estos sistemas. Los términos más comunes incluyen “drone” (para referirse a vehículos aéreos no tripulados, principalmente de uso militar), UAV (Unmanned Aerial Vehicle), UAS (Unmanned Aerial System), UCAV (Unmanned Combat Aerial System), RPA (Remotely Piloted Aircraft) y RPAS, siendo estos últimos dos los más usados en España en los últimos años. (Carrasco, 2017).

En otras palabras, estos sistemas aéreos no tripulados que se implementaron por primera vez hace tantos años y que surgieron como una respuesta a diversas necesidades de la época como su uso de señuelos o blancos móviles en situaciones de conflicto, han evolucionado al punto de ser hoy complejos sistemas de ISR (reconocimiento, vigilancia e inteligencia) de gran importancia para las FAS de España y la mayoría de los países del mundo que lograron desarrollar o importar su tecnología. (Ministerio de Defensa, 2016).

Si se suman los avances tecnológicos y de comunicaciones que han supuesto los UAVs, como el Searcher Mk III (figura 3), con su capacidad de navegación y el interés que han generado en los últimos años por su continuo desarrollo, podemos valorar su en el impacto en las FAS. Este se puede resumir al campo de posibilidades que suponen para las FAS en su adaptación a los retos y necesidades del mundo actual: reducir los riesgos para la vida humana en misiones internacionales; reducir costos de operación militar y seguridad nacional; entre otros. (Ministerio de Defensa, 2016).

Figura 3 Sistema Searcher Mk-III. Fuente: PD4-013, Anexo B, MADOC.

Sin embargo, no existen balanzas con sólo beneficios. Se deben considerar también algunas de sus vulnerabilidades, que suponen hoy en día una amenaza para la seguridad mundial. Como el hecho de que carecen de la operatividad necesaria, así como de la coordinación e integración con el resto de las fuerzas. Siendo el motivo principal la complejidad de la gestión de datos en una misión RPAS (ver figura 4). Además, ha proliferado considerablemente su uso en el ámbito civil debido a sus bajos costos actuales, generando así que casi cualquier persona o industria pueda acceder a su tecnología para amenazar los espacios aéreos civiles o en zona de operaciones. También se han desarrollado tecnologías que evaden las acciones de neutralización e identificación de los responsables de estas interferencias y amenazas. Por último, la dependencia considerable del GNSS de estos sistemas RPAS, entre otros. (Ministerio de Defensa, 2016).

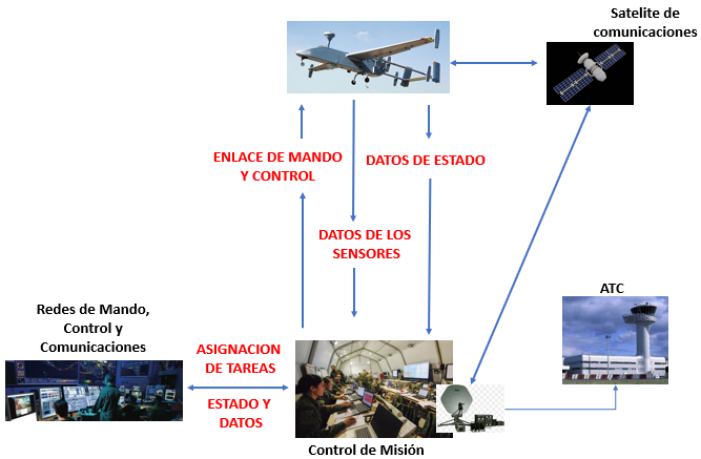


Figura 4 Complejidad de los enlaces de voz y datos para C2 de RPAS. Fuente: Elaboración propia a partir de PD4-013, MADOC.

3.2. Conceptualización

La etimología del término es propia del inglés Unmanned Aerial Vehicle, que representa sus siglas: UAV (García de la Cuesta, 2003). Estos vehículos constituyen como indica su nombre o denominación, una aeronave que ejerce sus funciones dirigidas de manera remota, sin tripulación, autónoma en el vuelo y posee un motor de explosión, eléctrico o de reacción (EASA, 2015). Su diseño es variado y corresponde a características propias de cada término empleado con las diferencias que suponen uno del otro (Ejemplo drone de RPA o RPA de UAV), pero existen básicamente dos categorías para definirlos: aquellos que se pueden dirigir desde una ubicación remota, y los que tienen un vuelo autónomo programado y dinámico (Organización De aviación Civil Internacional -OACI-, 2011).

Aunque en la actualidad existen sistemas de este tipo en el ámbito comercial y civil, a efectos de esta investigación resulta importante enfocarse en aquellos de aplicación militar, teniendo en cuenta además que fueron creados en propósito de la materia para su uso en operaciones militares de combate o conflicto.

Sin embargo, como se ha destacado en algunos puntos de esta fundamentación teórica, su popular actual uso civil supone un incremento de consumidores que está fuera del campo militar, y que, si bien puede aportar numerosos beneficios a otras industrias y empresas, también supone un riesgo por la proliferación de dicha aplicación (Axe, 2009).

Hoy en día, en el campo militar, las FAS y el Ejército Aéreo utilizan los UAVs para operaciones militares de reconocimiento y de combate, así como aquellas de salvamento y seguridad (Ministerio de Defensa, 2016).

Por otra parte, resulta imperativo en la conceptualización del término, tener en cuenta que su definición puede estar condicionada por el ámbito normativo y las exigencias asociadas a su empleo. Si se usa por ejemplo el término RPAS que ha sido protagonista en esta investigación y que es el más frecuentemente utilizado en las FAS, debe comprenderse que su uso supone la presencia humana en su control y dirección, aunque aún se mantiene en el campo de la conceptualización del Reglamento de Circulación Aérea Operativa: un vehículo propulsado que no lleva personal o tripulación a bordo (Asensi, 2014).

En el marco de sus características generales, destacan las siguientes: capacidad de mantenimiento de vuelo aerodinámico; operatividad con manejo remoto o programa de vuelo automático; capacidad de vigilar y reconocer factores importantes en situaciones complicadas; entre otros (Asensi, 2014).

Por último, cabe destacar la relación entre los términos UAV y RPA (o UAS y RPAS si hacemos referencia al sistema en su conjunto): "Todos los RPA son UAV, pero no todos los UAV son RPA, ya que para ello deben ser controlados por un operador" (Carrasco, 2017). Esta afirmación de Carrasco, nada menos que cierta, supone comprender que como se explicaba previamente, algunos UAVs son controlados y dirigidos por un operador remoto, considerándose así RPA, mientras que otros también cuentan con programas automatizados y dinámicos de vuelo (Gradiant, 2019).

La relación entre los términos ha surgido en la historia con los continuos avances tecnológicos que se han hecho en los sistemas, generando con nuevas características otros términos por los que se les ha llamado y que deben tenerse clarificados para evitar confusiones en su implementación. Ésta se encuentra además vinculada con su clasificación, por lo que es importante estudiarla a fines de hablar de los términos con la precisión requerida (Gradiant, 2019).

3.3. Clasificación UAV

Dentro de la clasificación de los UAV, según Carrasco (2017), se ha observado un desarrollo exponencial en los últimos años. Esto teniendo en cuenta que, en 2016, en España había 2380 vehículos y 1308 operadores habilitados. Desde entonces, la cantidad de operadores ha crecido continuamente de manera exponencial, alcanzando más de 71100 operadores al final de 2022, el doble que al final del año anterior (ver figura 5). Este aumento ha generado una serie de problemáticas relacionadas con las características de los modelos desarrollados y su clasificación, la cual se basa en el peso máximo al despegue, la altura de operación, certificado de aeronavegabilidad, uso del espacio aéreo operacional, características físicas, misión, sistemas de comunicaciones y aplicaciones civiles, según lo establecido por la Organización del Tratado del Atlántico Norte (OTAN) (ver tabla 2) (Carrasco, 2017).

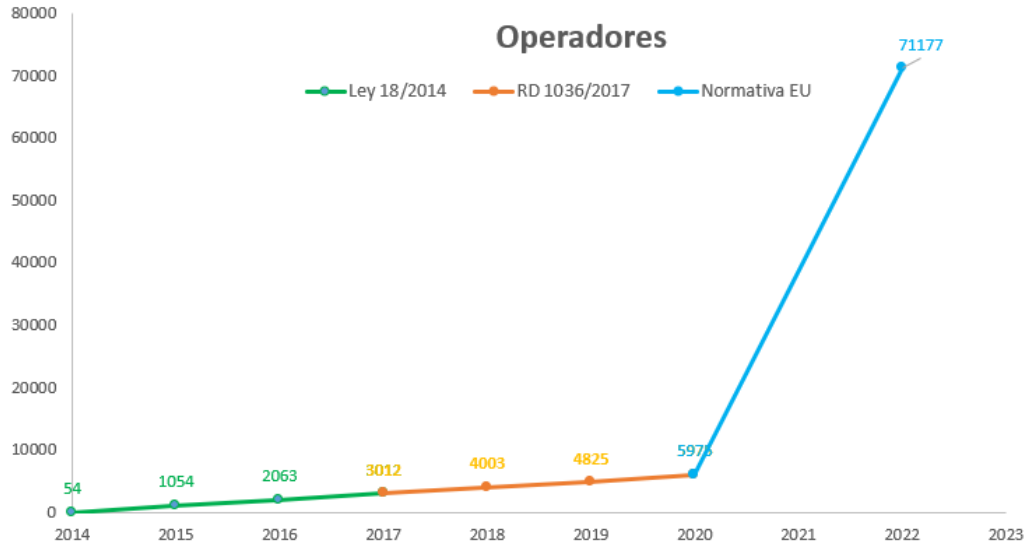


Figura 5 Gráfico evolución operadores drones registrados en AESA. Fuente: Agencia Estatal de Seguridad Aérea (AESA).

Los dos años de vigencia que lleva el actual reglamento de UAS ha supuesto un punto de inflexión para impulsar el sector, anteriormente regulado, desde 2018, por la normativa nacional del RD 1036/2017, que solo exigía el registro de los operadores profesionales. Con relación a la formación de pilotos, con la entrada en vigor de la nueva normativa, AESA ha emitido 131339 (hasta enero 2023) certificados de operación con drones para categoría abierta (la categoría abierta no requiere autorización ni declaración por parte del operador para poder operar los sistemas, se divide en subcategorías A1, A2 y A3).

Tabla 2 Clasificación OTAN sobre los RPAS.

Clasificación RPAS OTAN				
Clase	**Categoría**	**Empleo Habitual**	**Altura de Operación Normal**	**Radio de Misión**
Clase I (< 150kg)	MICRO <66J	-Subunidad táctica. -Lanzamiento manual. -Operadores individuales.	Hasta 200 ft AGL	Hasta 5KM (LOS)
	MINI <15kg	-Subunidad táctica. -Lanzamiento manual. -Operadores individuales.	Hasta 3.000 ft AGL	Hasta 25KM (LOS)
	SMALL 15kg-<150kg	-Unidad Táctica. -Sistema de lanzamiento.	Hasta 5.000 ft AGL	50KM (LOS)
Clase II (150kg - 600kg)	TÁCTICO	-Formación táctica.	Hasta 10.000 ft (AGL)	200KM (LOS)
Clase III (> 600kg)	MALE	-Operacional. -De teatro.	Hasta 45.000 ft MSL	Sin límite (BLOS)
	HALE	-Estratégico.	Hasta 65.000 ft	Sin límite (BLOS)
	ATAQUE / COMBATE	-Estratégico. -Operacional.	Hasta 65.000	Sin límite (BLOS)
Términos como *AGL, *MSL, *LOS y *BLOS pueden verificarse en la sección de abreviaturas ubicada en la página XX.				

Fuente: Elaboración propia, adaptación de Carrasco, J., (2017).

Esta clasificación de 2011 ha sido posteriormente contrastada hasta cierto margen por la Ley 18/2014 de 15 de octubre, en la que se aprobaron algunas medidas necesarias para la regulación de los avances científicos y técnicos que han tenido lugar en materia de aviación en los últimos años, específicamente en lo referente a UAVs y RPAS.

En el preámbulo V de la Ley, se plantea la necesidad del establecimiento de un régimen jurídico que pueda aplicarse a estos vehículos y a las actividades que estos desarrollan, así como a las condiciones de uso y explotación para la realización de diversos trabajos científicos o técnicos, las operaciones especiales, su aplicación, entre otros factores, teniendo en cuenta además, el abordaje único en la normativa nacional de vehículos civiles pilotadas a control remoto de peso <150kg y aquellas de peso >150kg destinadas a la operación de actividades como salvamento y lucha contra incendios (el resto se encuentran sujetos a la legislación regulada por la Unión Europea o UE) (véase tabla 3), (Carrasco, J., 2017).

Tabla 3 Clasificación de la Ley 18/2014, de 15 de octubre, sobre los RPAS.

<table>
<tr><th colspan="5">Clasificación RPAS según Ley 18/2014</th></tr>
<tr><th><u>MTOM</u></th><th><u>Ámbito Administrativo</u></th><th><u>Régimen Administrativo</u></th><th><u>Condiciones y Limitaciones Operativas</u></th><th><u>Cobertura de Seguro</u></th></tr>
<tr><td>< 2kg</td><td rowspan="5">Nacional</td><td rowspan="3">Habilitación</td><td>VLOS
BVLOS
(NOTAM)

Altura 120 m

Alcance: Según enlace de radio.</td><td rowspan="2">Ley 48/1960</td></tr>
<tr><td>>= 2kg
< 20kg</td><td rowspan="2">VLOS

Alcance: 500 m

Altura: 120 m</td></tr>
<tr><td>>=20 kg
<=25kg</td><td rowspan="4">Reglamento (CE) N°785/2004</td></tr>
<tr><td>>25kg
<=150kg</td><td rowspan="3">Autorización</td><td rowspan="2">Según certificado de aeronavegabilidad

Espacio aéreo no controlado</td></tr>
<tr><td>>150kg (salvamento, rescate, incendios).</td></tr>
<tr><td>>150kg (otras operaciones).</td><td>Europeo</td><td>Según certificado de aeronavegabilidad

Autorización ATC</td></tr>
<tr><td colspan="5">*Información verificada en el Título II de Infraestructuras y Transporte, Capítulo I de Aviación Civil, Sección 6 de Aeronaves Civiles Pilotadas por Control Remoto, Artículo 50 de Operación de Aeronaves Civiles Pilotadas por Control Remoto. *</td></tr>
</table>

Fuente: Elaboración propia, adaptación de Carrasco, J., (2017): información verificada en la Ley 18/2014.

De acuerdo con el autor, cuyo discurso ha sido de gran apoyo en esta investigación, aún y cuando todos los datos suministrados se han verificado en sus fuentes primarias, es necesario hacer una comparativa entre las tablas de clasificación vigentes en la actualidad por la normativa para evidenciar además de una clara diferencia entre pesos de despegue y alturas operacionales, que existe una problemática a nivel de integración de los RPAS en el espacio aéreo no segregado. Esto hace necesario a su vez, que, aunque no se ahonde sobre la normativa en el texto del presente trabajo, se consulte y analice el marco legal vigente para identificar la integración de los RPAS en el espacio aéreo español y europeo y determinar algunos puntos que serán definidos propiamente en los próximos apartados referentes a los beneficios y vulnerables de los vehículos en cuestión.

En la actualidad, las operaciones de UAS se realizan en zonas separadas de las utilizadas por la aviación convencional, eso significa una constante coordinación a la hora de afrontar las operaciones con seguridad. Por último, se muestra una previsión de la posible evolución del uso del espacio aéreo y sus aplicaciones, partiendo de la división del espacio aéreo en niveles de vuelo hasta la total integración de todos los usuarios del espacio aéreo (ver figura 6).

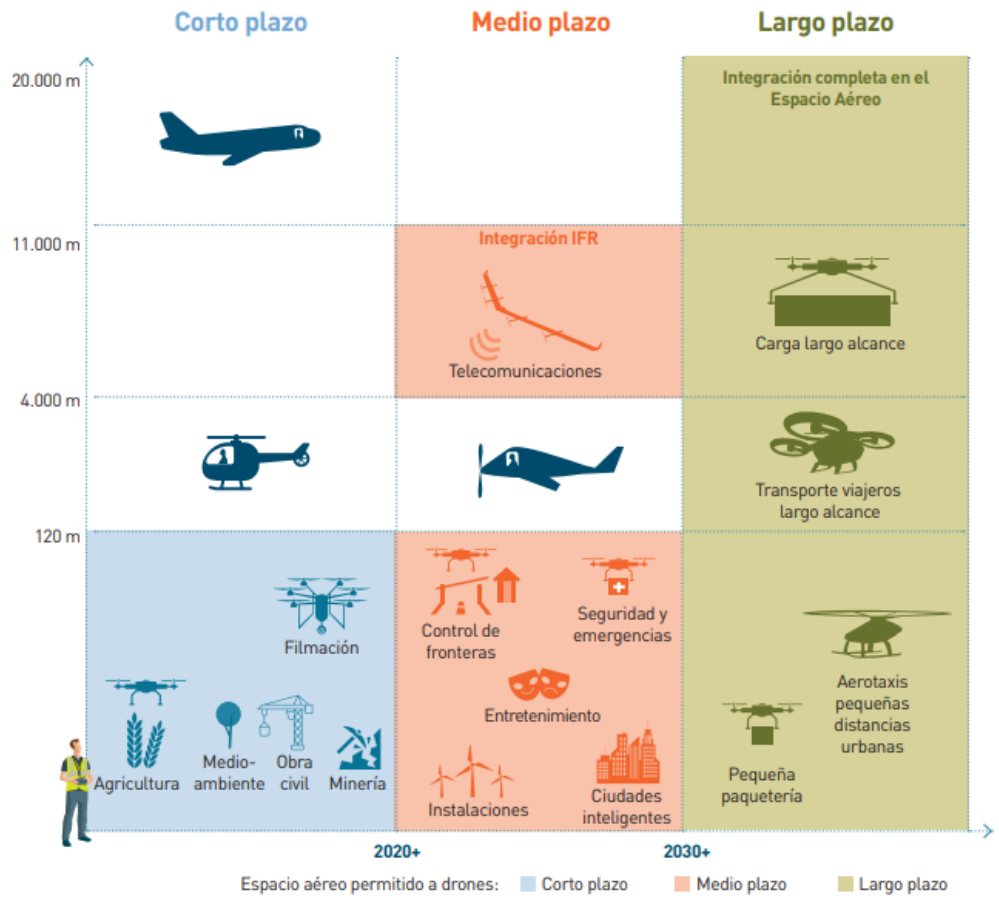


Figura 6 Evolución posible del uso compartido del espacio aéreo. Fuente: Ministerio de fomento (2018)

4. RPAS EN LA ACTUALIDAD: BENEFICIOS, VULNERABILIDADES Y AMENAZAS A LA SEGURIDAD

Desde hace varias décadas, los RPAS han sido motivo de interés internacional, especialmente en el ámbito militar, por lo que en los últimos años se han desarrollado diversos equipos más que aptos para su uso profesional en operaciones tácticas y de defensa.

Hoy en día como podemos ver por la Estrategia de Tecnología e Innovación para la Defensa (ETID 2020) elaborado por la DGAM para el Ministerio de Defensa estos vehículos tienen grandes capacidades para desarrollar misiones reales con utilidad, eficiencia y velocidad que hasta hace unas décadas eran impensables. Además, podemos ver los múltiples alcances del desarrollo de estas tecnologías para el mundo civil a través de la Estrategia Española de Ciencia, Tecnología e Innovación 2021-2027 (EECTI 2021-2027) elaborada por el Ministerio de Ciencia e Innovación y el plan Estratégico para el Desarrollo del Sector Civil de los Drones en España elaborado por el Ministerio de Fomento en 2018 además de otras agendas de carácter estratégico para el año 2030 como la de la plataforma tecnológica Aeroespacial Española.

Su implementación hasta ahora, con más éxitos que fracasos, en los últimos conflictos internacionales (por ejemplo, en el último año se ha visto imágenes de la guerra de Ucrania tomadas desde el aire, pero no por aviones o helicópteros, sino por RPAS, que están desplazando cada vez más a las aeronaves convencionales en el campo de batalla), han promovido que se continúen perfeccionando las tecnologías y elementos que conforman estos sistemas RPAS. Tales como la navegación, el control y las comunicaciones, entre otros.

Por lo que además de investigar la ampliación de sus aplicaciones, se trabaja actualmente en contrastar sus vulnerabilidades y las amenazas que pueden suponer para la seguridad mundial. Como podemos comprobar en el extenso informe realizado por el Ministerio de la Presidencia, que aborda un estudio de los drones y seguridad nacional en un informe de más de 400 páginas publicado en octubre de 2022. Todo indica que la flota de RPAS crecerá y se especializará originando una nueva arma, cuyo recorrido en las guerras del futuro parece ser muy prometedor. Todo ello, siempre que consigan no ser víctimas de contramedidas de guerra electrónica que interrumpan las comunicaciones del RPA (Diaz Villanueva, 2023).

Aunque en el ámbito civil estas tecnologías no se han desarrollado en la misma línea que en el ámbito militar, el interés mostrado por la evolución de estos queda patente por la mencionadas EECTI 2021-2027 desarrollada por el Ministerio de Ciencia e Innovación, el Plan estratégico para el desarrollo del sector civil de los drones en España por parte del Ministerio de Fomento además de otros planes estratégico por parte de plataformas civiles.

Por lo tanto resulta necesario a fines de esta investigación conocer el estado de la cuestión sobre los RPAS en la actualidad en forma general, así como comparar sus beneficios, vulnerabilidades y amenazas a la seguridad, teniendo en cuenta que estos han supuesto en la evolución humana, una revolución de la tecnología y del mercado de servicios, así como el surgimiento de un sector estratégico de primer orden sobre el que Europa se prepara actualmente para desarrollarse sin perder de vista las nuevas necesidades del continente en una época de crisis mundial en la que todas las decisiones tomadas tendrán repercusiones importantes en al menos las próximas décadas.

4.1. Beneficios

Los RPAS representan años de evolución, de diversos avances técnicos, tecnológicos y científicos en el mundo, de estudios y aplicaciones aparentemente desarrolladas en beneficio de la vida humana, la globalización y la optimización de recursos y procesos. Su uso ha abierto posibilidades que hasta hace unos años o décadas atrás no eran viables, como las pruebas de material aeronáutico en condiciones peligrosas para la vida humana, así como el comportamiento esperado del material expuesto a grandes cargas o los vuelos comerciales no tripulados. Asimismo, han supuesto un empuje al desarrollo y despliegue de otras tecnologías paralelas, como la fabricación de pilas de células de combustible de hidrógeno que les permiten a los RPAS triplicar su autonomía de vuelo.

Además, los RPAS han generado importantes beneficios a nivel laboral, con el crecimiento y la consolidación del mercado que ha supuesto la creación de puestos de trabajo para agentes cualificados capaces de desarrollar las distintas aplicaciones que utilizan los RPAS. Con esto entran en el marco de referencias las empresas de fabricación de equipos de radio frecuencias, sensores, telemetría, propulsores, sistemas de energía, cámaras, entre otros. También se han abierto nuevos puestos de trabajo para operadores calificados en manejar, mantener o reparar estos vehículos, así como para la formación de futuros operadores de RPAS (Ruiz Domínguez, 2013).

Las ventajas en el sector de las telecomunicaciones no hacen más que incrementarse, debido a sus aplicaciones en vuelos de larga duración controlados de forma remota en situaciones imposibles para vuelos tripulados. Y en materia de defensa sólo hay que mirar los resultados de la tecnología de los RPAS aplicada por países como Estados Unidos en diversas operaciones de seguridad internacional (donde el gobierno de Biden ha hecho hincapié en su capacidad para realizar ataques con drones “más allá del horizonte” que según sostiene, son necesarios. Además, se tienen constancia de algunas de sus misiones de ataque realizadas con éxito en Oriente próximo o de su vigilancia en el mar Negro con el dron MQ-9 Reaper (figura 7), donde tras el reciente accidente con los caza rusos y ser derivado, en marzo 2023, EEUU ha prometido continuar con sus misiones de vigilancia en el mar Negro) para comprender el alcance e importancia de los RPAS en la actualidad.

Figura 7 Un dron MQ-9 Reaper de la Fuerza Aérea de EEUU, Fuente: vozdeamerica.com

Estos vehículos aéreos no tripulados no sólo pueden volar en formaciones 2D y 3D (volando varias aeronaves con un separación constante en el mismo plano o nivel de vuelo o con separación vertical, según lo requiera la misión), evitar o esquivar obstáculos fijos o en movimiento, y efectuar diversos tipos de maniobras aéreas, sino que además funcionan de manera autónoma y segura mediante la navegación por GPS o con sistema de cámaras a bordo, sirviendo en distintas aplicaciones y usos para beneficiar el ámbito civil y militar (Ruiz Domínguez, 2013).

En el ámbito de la seguridad privada, por ejemplo, sirven para la vigilancia de grandes complejos turísticos y urbanizaciones, así como para la comprobación de alarmas de seguridad. Al mismo tiempo, en materia de seguridad pública, se usan para vigilancia de unidades especiales, lucha antiterrorista, investigaciones policiales, control y seguridad de las aglomeraciones de personas en entornos urbanos, entre otros (Ruiz Domínguez, 2013).

Ahora bien, en materia militar, los beneficios de los RPAS surgen de la necesidad de las fuerzas militares por realizar con éxito distintas operaciones de seguridad con el mínimo de riesgos posibles a la vida humana. Esta evolución en las tecnologías ha permitido al sector de la Defensa operar de forma remota en zonas peligrosas sin ningún tipo de limitaciones sabiendo que no se pondrán en riesgo las tripulaciones humanas. Aunque su precisión y otros factores necesarios para operar en zonas de conflicto los hacen más costosos que los drones utilizados en el entorno civil debido a la implementación de algoritmos y sensores avanzados para el estudio y detección del entorno y sus amenazas, las operaciones militares actuales se sirven de los múltiples beneficios y ventajas que supone el uso de los RPAS para contrarrestar sus propias vulnerabilidades (Fervimax group, 2019).

Es así como los RPAS pueden llegar a ser usados como señuelos, en una estrategia de defensa, donde se usen estos drones para engañar a los oponentes mientras se lanza un ataque desde otra dirección, sin poner así en riesgo una tripulación. Como también los RPAS pueden ser usados para misiones de combate ya que tienen la precisión para: determinar, enfocar el objetivo e impactar de manera eficiente, además de la capacidad de vigilancia y reconocimiento de los movimientos del enemigo incluso sin ser detectados para transmitir la información que pueda ser útil para la toma de decisiones en referencia a las operaciones, como el mencionado dron de ataque MQ-9 (figura 8) (Fervimax group, 2019).

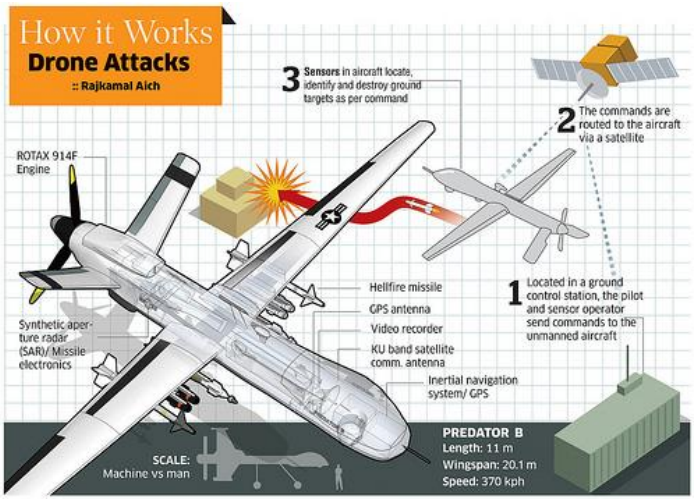


Figura 8 Esquema y características del dron de ataque MQ-9 Reaper o Predator B con su sistema de control y comunicaciones a través de un sistema satelital. Fuente: Blog de las Fuerzas de Defensa de la República de Argentina.

Entre las diversas aplicaciones en la actualidad de esta tecnología en diversos sectores pueden encontrarse la distribución de señal gratuita de Internet, la elaboración de ortofoto mapas en alta resolución, la monitorización de instalaciones, el transporte y entrega de mercancías, la gestión de cultivos, control de incendios, salvamento y rescate, auditoría de siniestros, filtrado de aire, entre otros (Muñoz, 2014).

4.2. Vulnerabilidades y amenazas a la seguridad

En referencia a las vulnerabilidades y amenazas a la seguridad de los RPAS, es destacable que éstas se hacen cada vez más evidentes debido al gran número de avances tecnológicos, científicos y técnicos que se han desarrollado en los últimos años en la materia, además del surgimiento de nuevas necesidades globales que suponen, por ende, otras adaptaciones y mejoras. Pueden categorizarse de la siguiente manera:

4.2.1. Vulnerabilidades

Marco Legal

Si se analiza un poco la Ley 18/2014, que se ha estudiado a fines de comprender la clasificación de los RPAS, se pueden identificar una serie de aspectos que no quedan completamente definidos en la normativa o que exigen que se hagan inversiones de tipo tecnológicas en los vehículos aéreos, suponiendo así parte de sus vulnerabilidades (si bien transitorias, mientras exista esta diferencia entre los requisitos de estas aeronaves y la situación actual). Estas vulnerabilidades, que por el momento se suplen manteniendo a estas aeronaves en espacios aéreos segregados, tienen que ver con la siguiente ambigüedad: si bien esta Ley modifica el artículo 11 de la Ley de Navegación Aérea (LNA), modificando la definición de aeronave para establecer sin lugar a duda que los RPAS o UAS son aeronaves, estas, no pueden operar como tales fuera de un espacio aéreo segregado. Así, estos sistemas pasan a tener que regirse bajo una normativa bajo la cual todavía no pueden operar con normalidad.

Esta vulnerabilidad se puede resumir en la necesidad de la integración de los RPAS en el espacio aéreo y la gestión del tráfico aéreo, que no resulta sencillo. Esto es debido a que previamente es necesario una inversión en sistemas de verificación y validación, el desarrollo de enlaces de comunicación de datos que incluyan espectro electromagnético, mayor inversión en el sistema para detectar y evitar, así como el uso de sistemas anticolisión, la consideración del riesgo que suponen los distintos tamaños de RPAS y sus tipos de operación; el estudio e inversión tecnológica en procedimientos y sistemas operativos de emergencia para distintas actividades y maniobras; la determinación de la responsabilidad civil a terceros y seguros; protección de datos y seguridad de la información, entre otros (Esteban Herreros, 2015).

Requisitos operación RPAS en base a la Ley 18/2014 (figura 9):

-Las operaciones se deben realizar de día y en condiciones visuales.

-Fuera zonas urbanas o reunión de personas al aire libre.

-Altura máxima 400 pies (120 metros).

-En espacio aéreo no controlado.

-Distancia de 8km de cualquier aeródromo (15km si tiene procedimientos instrumentales).

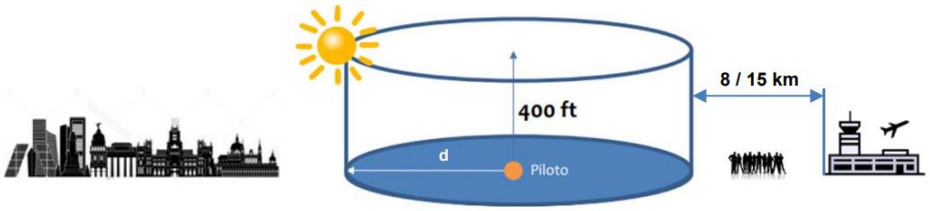


Figura 9 Esquema de los requisitos espacio aéreo segregado para vuelo de RPAS. Fuente: AESA

Dependencia al GNSS

Según los expertos consultados, todos los RPAS utilizan un sistema GNSS como base y, como medio redundante, también utilizan la Unidad de Medición Inercial (IMU). La IMU proporciona la tasa de cambio en los tres ejes, pero para obtener coordenadas precisas, estas deben ser inicialmente obtenidas del GPS o introducidas manualmente a partir de coordenadas conocidas. Además, para determinar la altitud, se utiliza un sensor barométrico (al menos los sistemas militares que tenemos en dotación: Raven, Wasp, Black Hornet II, Black Hornet III, Orbiter 3B, Searcher MKIII). Por lo tanto, la denegación o pérdida del GNSS no acarrea directamente la pérdida de la aeronave, pero sí resulta en un vuelo degradado y no operativo. En caso de pérdida del sistema GNSS, se pueden tomar medidas para recuperar el RPAS, como dirigirlo hacia la estación de control en tierra o utilizar referencias en el terreno a partir de la cámara integrada. Algunos sistemas también tienen un modo de vuelo denominado “Dead Reckoning” (navegación a la estima) que permite que la aeronave se posicione en el mapa mediante la IMU y la velocidad relativa al viento (Indicated Air Speed, IAS). Sin embargo, la perdida del sistema de posicionamiento conlleva una deriva en la posición estimada, y el error en la posición de la aeronave aumenta con el tiempo y los cambios de velocidad y altitud (comunicación personal Miguel Vasallo Ledo).

Muchos sistemas militares digitales dependen de GNSS para proporcionar los datos de Posición, Navegación y Sincronización (Positioning, Navigation and Timing, PNT) confiables, que permiten a las usuarios maniobrar, comunicarse, comprender y tomar decisiones en el campo de batalla moderno. Sin embargo, las señales GNSS son muy débiles cuando llegan a la Tierra, y dado que éstas son omnipresentes en el funcionamiento de los sistemas militares, las amenazas a la disponibilidad e integridad de la señal GNSS están en aumento. Los elementos hostiles y demás criminales tienen pocas dificultades para acceder a dispositivos portátiles, capaces de bloquear y falsificar señales. Por tanto, como se usa un mayor número de dispositivos que utilizan estos datos PNT, los usuarios afectados podrían ser mayores.

Una característica de los sistemas GNSS es que los receptores en la Tierra funcionan con señales de muy baja potencia. De hecho, incluso con un nivel de potencia que es menor que el ruido térmico de los propios sistemas. Esto provoca que el tipo de ataque más común y sencillo consista en ataques de denegación de servicio (Denial of Service, DoS), realizados mediante el jamming, creando interferencias. Existe otro tipo de ataque, mucho más peligroso, denominado spoofing. Este consiste en la suplantación de la señal GNSS, de manera que los receptores calculen posiciones incorrectas. Este ataque es mucho más peligroso que la simple denegación de señal, ya que permite que el usuario del RPAS obtenga una posición incorrecta por parte del receptor del RPA, sin que este sea capaz de detectar el fallo. Este ataque es posible debido a que las señales del satélite GPS no llevan ningún mecanismo de autenticación para determinar que la señal recibida es legítima (en la puesta en marcha del servicio GALILEO se ha previsto incluir un sistema de autenticación, aunque será de pago). Esta última es una amenaza real y creciente de acuerdo con el criterio de las fuentes entrevistadas (comunicación personal Francisco Javier Cruz Hernández).

Guerra Electrónica

El tipo de ataque más sencillo se realiza mediante simulador de señales GNSS. Este consiste en conectar un amplificador y una antena a un generador de señales GNSS (ver figura 10). Con esto se conseguiría radiar señales GNSS falsas con los datos que nosotros configuremos en el sistema generador. A pesar de ser el más sencillo por su eficacia, un simulador de señales GNSS puede costar más cien mil euros y no se encuentran ampliamente disponibles en el mercado. No obstante, hay alternativas de sistemas mucho más económicos, que pueden interferir la comunicación satélite a base de explotar la debilidad de la señal de los satélites con ruido

electromagnético generando así un ambiente de denegación. Los jammers de potencia inferior a 100w son los más peligrosos, al ser difíciles de detectar. Un inhibidor pequeño y barato de 1W podría cubrir unos 20km2. Como ejemplo tenemos los PPD (Personal Privacy Devices) o equipos SDR (Softwawre Defined Radio, radio definida por software) transmisores.

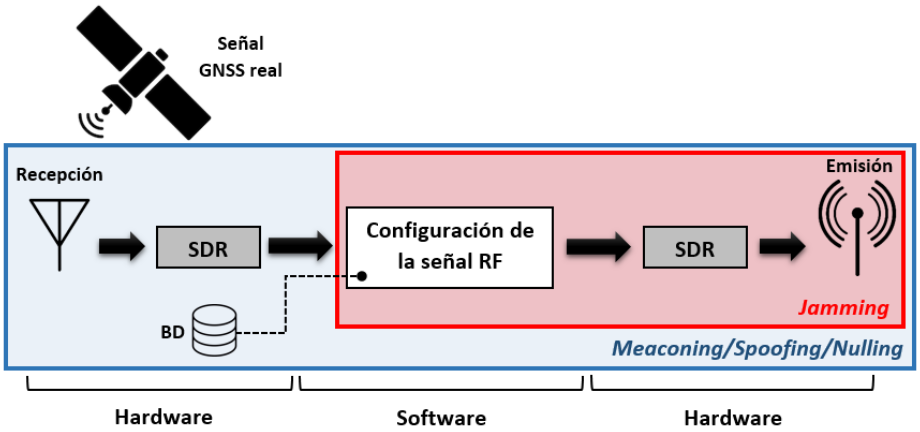


Figura 10 Diagrama de bloque para operaciones jamming y spoofing usando transmisores SDR. Fuente: incibe-cert.es

La libertad de acción que caracterizó las operaciones con RPAS en las últimas décadas está disminuyendo rápidamente, con la introducción e incremento de la guerra electrónica. Con las interferencias en las comunicaciones y sistemas antiaéreos, una parte significativa de los RPAS actuales no pueden llevar a cabo operaciones en espacio aéreo electromagnético denegado o disputado. Un ejemplo de esto, en palabras del experto Francisco Cruz, han sido los RPAS Bayraktar TB2 que fueron muy útiles para Ucrania al principio de la guerra contra Rusia, y que han perdido gran parte de su utilidad al ser incapaces de penetrar el espacio aéreo defendido por sistemas antiaéreos desplegados por las fuerzas rusas, y que se basan en una triple capa: Los S-400 y S-300 de largo alcance para defensa de media y gran altitud; los Buk-M2/M3 para defensa de media y baja altitud; y los TOR-M1/M2 para defensa de corto alcance a baja y muy baja altitud; junto con sistemas de defensa antiaérea cercana (Short Range Air Defence, SHORAD) como Tunguska, Sosna y MANPADS (Man-Portable Air-Defense System, misil tierra-aire lanzado por un solo soldado).

Por otra parte, los drones turcos Bayraktar TB2 han experimentado la interrupción o manipulación de sus enlaces satélite por parte de los rusos, y que conduce al fracaso de sus misiones de combate en conflicto actual de Ucrania. Se debe asumir entonces, que la mayoría de la generación actual de RPAS es incapaz de llevar a cabo las mismas misiones en entornos disputados, que ahora realizan en entornos no disputados. Esto sugiere que es necesario introducir cambios importantes en los RPAS actuales, para prepararlos para las operaciones en entornos con sistemas anti-acceso y denegación de área (A2/AD) (comunicación personal Francisco Javier Cruz Hernández).

Sistemas de comunicación

Según datos registrados por la DGAM para el Ministerio de Defensa en la ETID 2020, los sistemas de comunicación constituyen parte de las principales vulnerabilidades de los RPAS. Esto es debido a la saturación y resistencia de todos sus subsistemas frente a las distintas interferencias. En este sentido, desde los sistemas no tripulados que usan el cable como medio de comunicación, como sistemas de Radio Frecuencia (RF) y de comunicación láser, todas las partes de red de comunicación operativa padecen deficiencias importantes que generan diversas vulnerabilidades sobre los RPAS. Éstas pueden resumirse en una mala conectividad global o

insuficiencia en la distribución global de datos dentro del ancho de banda en tiempo real; altos costos de redes satelitales para la disposición de un ancho de banda capaz de desarrollar las comunicaciones de video en tiempo real; el empleo de procesamiento de explotación y difusión de datos de misión, impidiendo el intercambio rápido y efectivo entre los sistemas, los servicios y las organizaciones, permitiendo la detección y neutralización de la conexión; problemas como el jitter y latencia que pueden causar la pérdida de datos o la imposibilidad de detectar intrusos en el sistema; el uso de sistemas de múltiple entrada y múltiple salida (en referencia a como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos) (Múltiple-input Múltiple-output, MIMO-figura 11-), que son muy vulnerables a los perturbadores (DGAM, 2020).

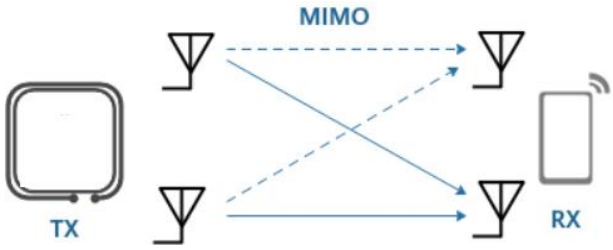


Figura 11 Esquema tecnologia MIMO. Fuente: Huawei.com

Sistemas de Propulsión

Las vulnerabilidades de estos sistemas pueden resumirse en aquellos de propulsión eléctrica, y en las limitaciones de carga, que se traducen en una sería dificultad para llevar armas o cargas explosivas. La sensibilidad EMP que hace referencia a vulnerabilidades ante impulsos electromagnéticos que neutralizan los sistemas de comunicación, y la baja velocidad de desplazamiento que los vuelve un objetivo fácil de abatir o neutralizar. Como ejemplo, tenemos el sistema RAVEN (figura 12) impulsado eléctricamente, con gran limitación de carga y baja velocidad que lo hacen un objetivo muy vulnerable.

Figura 12 Sistema RAVEN Fuente: PD4-013, Anexo B, MADOC

En los de propulsión por motores de combustión, las vulnerabilidades se encuentran por su parte en motores de dos tiempos de tecnología obsoleta que genera un consumo superior a otras más actuales desarrolladas.

Y en cuanto a las tecnologías de turbinas de reacción, puede decirse que son muy costosas, logística y operativamente, y por ende menos usadas en las operaciones militares. (Ministerio de Defensa, 2016).

4.2.2. Amenazas a la seguridad

En el caso de las actividades molestas en el ámbito civil, el uso ilegal de los RPAS en la interferencia con el público puede generar molestias e incluso estrés o miedo a personas y animales al ubicar estos sistemas en su ámbito personal o cercano, violando incluso un derecho civil. Estas actividades pueden afectar negativamente la percepción que esas personas tienen de su propia seguridad y se la seguridad nacional (Ministerio de Defensa, 2016).

En relación con la interferencia del espacio aéreo, muchos RPAS operados ilegalmente han ocasionado accidentes aéreos con aviones en el tráfico aéreo en todo el mundo, convirtiéndose en una amenaza para las operaciones de aviación comunes, operaciones de salvamento, de extinción de incendios, e incluso de colisiones. Estas interferencias pueden ser empleadas por terroristas y delincuentes para sabotear el trabajo de los aeropuertos, la policía, aduana, los bomberos y otros organismos de seguridad (Ministerio de Defensa, 2016).

El monitoreo, la grabación y la fotografía de personalidades públicas y otros particulares o empresas en sus actividades privadas, puede usarse para fines ilícitos como el espionaje industrial, que suponen una amenaza a la seguridad y a la privacidad. Algunos usos negativos que se han dado a los RPAS se resumen en el seguimiento y la vigilancia de personas sin su consentimiento o un motivo legal, lo cual pone en peligro su seguridad, en especial porque es sumamente complejo determinar quiénes son los responsables de dichas acciones (Ministerio de Defensa, 2016).

En cuanto al reconocimiento en el ámbito civil está aplicación de los RPAS puede suponer una amenaza a la seguridad personal cuando se usa para recoger información privada para utilizarla con fines ilícitos en actividades delictivas. En materia militar, por otra parte, todas estas actividades son fundamentales para acceder a información pertinente sobre el enemigo durante la toma de decisiones en distintas operaciones, por lo que la vulnerabilidad no viene de la aplicación en si misma sino del uso que se le dé a la misma por personal militar y de seguridad, o por delincuentes, que lamentablemente también tienen acceso a estas tecnologías (Ministerio de Defensa, 2016).

También existe el riesgo de amenaza cinética ya que estas provienen de la capacidad de los RPAS de causar lesiones a las personas y a sus propiedades debido a la velocidad alcanzada por los mismos en distintas operaciones, puesto que pueden ser utilizados por delincuentes para estos fines pretendiendo hacer pasar las consecuencias como accidentales. (Ministerio de Defensa, 2016).

En cuanto a la carga útil, el tráfico y contrabando suponen una amenaza a través de los terroristas o delincuentes, que pueden utilizar RPAS como un vehículo de transporte para evadir los sistemas de seguridad. Así pueden ser capaces de suministrar drogas, teléfonos móviles e incluso armas para actividades ilícitas, como vemos en el reciente ejemplo donde la policía Nacional incauta en Málaga en 2021 el mayor dron dedicado al transporte de droga (El país, 2021).

Por último, los RPAS como portadores de armas, explosivos o sustancias nocivas, representan una amenaza a la seguridad mundial que ha generado gran discusión entre los expertos, por la necesidad de combatir la situación de manera efectiva para evitar posibles tragedias. Debido a que grupos terroristas internacionales pueden acceder a estas tecnologías para producir ataques importantes a particulares o personalidades. También se pueden usar RPAS para hacer robos electrónicos, disponiendo de información personal contenida en cualquier dispositivo móvil con Wifi que lo hace vulnerable al sistema Snoopy, por ejemplo. Con esta tecnología pueden ubicar cualquier dispositivo móvil con el fin de secuestrar, además de otros fines ilícitos como robo de identidad, chantaje y espionaje (Ministerio de Defensa, 2016).

5. RPAS: LAS NUEVAS TECNOLOGÍAS Y LOS MODELOS EN DESARROLLO

Son las nuevas tecnologías desarrolladas en diferentes ámbitos los que posibilitan la concepción y el desarrollo de una navegación sin GNSS. Esta meta, como hemos visto, se debe a las vulnerabilidades en cuestión que han motivado numerosos cambios (avances tecnológicos y técnicos) en materia de RPAS y sistemas de posicionamiento, con miras a resguardar la información y la seguridad nacional y global. Estos cambios que han tenido origen principalmente en el ámbito militar suponen grandes avances en el sector. Sin embargo, no pretenden por sí mismos reemplazar o abandonar el GNSS, sino más bien identificar soluciones tecnológicas para minimizar las vulnerabilidades y amenazas (Ruiz Domínguez, 2014).

Así algunas alternativas pasan por la robustez del sistema de navegación mientras otros pueden aplicarse al vuelo autónomo. Estos pueden asociarse a:

- Microchips: Los ingenieros de la DARPA (Defense Advanced Research Projects Agency) lograron dentro del programa Micro-PNT (consiste en integrar un sistema PNT de precisión en un microchip) integrar tres datos imprescindibles en la navegación: la orientación, aceleración y el tiempo, en un dispositivo de tamaño diminuto (Timing and Inertial Measurement Unit, TIMU -figura 13-). Éste es un microchip con seis capas y 1W de potencia que contiene siete dispositivos; sus principales aplicaciones militares se asocian a los UAVs: sistemas de guiado de las municiones y los misiles, navegación de los soldados en tierra, acreditación de seguridad, facilitación de información precisa sobre la ubicación real del enemigo, entre otros. En agosto de 2013 se probaba un nuevo misil en el proyecto de la DARPA, con una TIMU integrada, que puede prescindir de la señal GNSS para su guiado hacia el objetivo, es decir, puede hacerlo aún y cuando dicha señal sea interferida (Ruiz Domínguez, 2014).

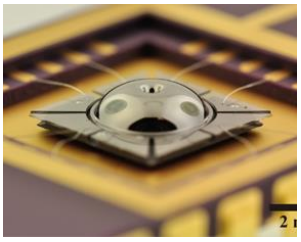


Figura 13 Microchip de última generación (next Generation) TIMU. Fuente: darpa.mil

Tecnologías de reconocimiento de imágenes: Google Vision, OpenCV, Pyzbar o más recientemente Machine learning (capaz de aprendizaje), son aplicaciones con librerías y capacidad de reconocimiento de patrones para diferentes usos que han sido el origen del modelo de navegación visual (VNS) (Acelera pyme, 2022).

Además de estas hazañas, se han conocido otros modelos en desarrollo que buscan mitigar las amenazas que han supuesto para los RPAS su dependencia al GNSS en operaciones de seguridad y situaciones de conflicto. Sin embargo, son muchas las limitaciones de información y son muchos más aún los sesgos en la que puede hallarse en la búsqueda bibliográfica, por lo que sólo se ha contemplado aquella que ha sido confirmada por fuentes verificables y calificadas.

Tenemos así dos líneas de desarrollo principales. Por un lado, las tecnologías que buscan sustituir el GNSS completamente, más robustas, pero menos desarrolladas hoy en día. Mientras, la otra línea de desarrollo busca mantener esa dependencia de los satélites a base de mayor robustez y seguridad en el enlace, evitando así una degradación de la calidad de recepción de los sistemas de navegación por GNSS.

5.1. Alternativas al GNSS

En primer lugar, tenemos el LIDAR es el acrónimo de Light Detection and Ranging, es decir, detección por luz y distancia (ver figura 14). Se trata de un sistema láser que permite medir la distancia entre el punto de emisión de ese láser hasta un objeto o superficie. El tiempo que tarda ese láser en llegar a su objetivo y volver del mismo es lo que nos dice la distancia entre los dos puntos. El resultado es que se puede obtener un mapa en 3D de alta resolución para conocer el terreno en cuestión. LIDAR es una tecnología tremendamente útil para conocer el terreno y sus características, pero también para alcanzar un navegación autónoma de los RPAS siendo capaz de navegar en lugares previamente mapeados en ambiente de negación de GNSS.

Los RPAS equipados con cámaras ofrecen un par de ojos adicionales en el cielo, proporcionando una nueva perspectiva a las operaciones que se realizan sobre el terreno. Al desplegar un RPAS equipado con un sensor LIDAR, las FAS podrían realizar lecturas aéreas más precisas, creando modelos 3D con una precisión centimétrica, y detectando características que serían invisibles con métodos menos sofisticados. Lejos de ser un área tecnológica de nicho, el LIDAR está llegando a todo tipo de industrias que necesitan de cartografía y recopilación de datos geoespaciales. Si seguimos los últimos usos de los UAS con sensor LIDAR, podremos determinar si los RPAS militares pueden encajar en los planes estratégicos de las FAS.

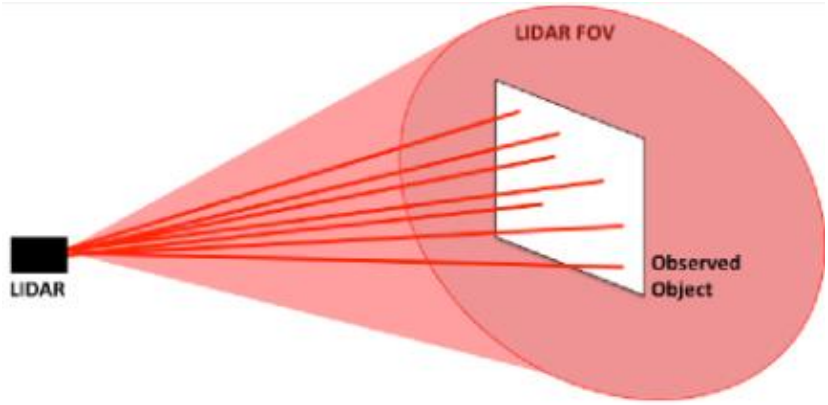


Figura 14 Esquema funcionamiento tecnología LIDAR. Fuente: rpas-drones.com

Francisco Javier Cruz Hernández también menciona (además de las antenas CRPA para proteger enlace GNSS, extendido en el siguiente punto) sobre la tecnología LIDAR, que constituye un sistema láser que permite medir la distancia entre el punto de emisión de éste hasta un objeto o superficie determinados, y cuyos resultados se pueden obtener en un mapa en 3 D de alta resolución para conocer el terreno en cuestión.

Las aplicaciones de esta tecnología tienen lugar principalmente en la geodesia, ya que garantiza la captación de datos precisos en el aire a alturas considerables, pudiendo generar Modelos Digitales de Elevación del terreno (MDE), lo cual a su vez le permite a los RPAS navegar en lugares previamente mapeados en ambiente de denegación de GNSS; es decir, con mayor seguridad porque tienen información más precisa y confiable (véase Tabla 4).

Tabla 4 Aplicaciones de la tecnología LIDAR en las alternativas al GNSS.

Creación de modelos 3D	Lecturas aéreas precisas, creando modelos 3D con una precisión centimétrica y detectando características que serían invisibles con métodos menos sofisticados.
Asequibilidad y menor peso	Los módulos de los sensores son cada vez más asequibles y mucho más ligeros.
Amplitud de aplicaciones	Esta tecnología ha llegado a distintos nichos de trabajo que requieren de la captación y recopilación de datos geoespaciales precisos, por lo que sus aplicaciones no se limitan al ámbito militar.
Exactitud y rapidez	La tecnología de teledetección que aplica supone la oportunidad de captar información con gran exactitud y rapidez.
Alta calidad de imagen	Los modelos 3D se crean con rapidez y alta calidad en archivos pequeños y poco pesados.
Tecnología no monopolizada	Los sistemas con esta tecnología están siendo desarrollados por múltiples empresas en todo el mundo.
Captación de detalles importantes	Los pulsos del LIDAR pueden captar las líneas eléctricas mientras que las fotos tomadas por los módulos de fotogrametría podrían no detectar los cables.
Innovaciones futuras	En la medida en que se reduce el peso del LIDAR, se pueden desarrollar nuevos RPAS que incorporen la tecnología para crear modelos sobre los que se pueda navegar de forma autónoma.

Fuente: Elaboración propia, adaptación de entrevista a Francisco Javier Cruz Hernández (2022).

Por otro lado, el VNS (figura 15), que también depende de cámaras en el RPAS, es una unidad compacta y ligera que permite un uso seguro y navegación precisa de RPAS en ambientes de GNSS denegado. El VNS fusiona 'Odometría visual' y 'técnicas de reconocimiento de patrones con otros sensores a bordo. Con esto consigue determinar con precisión la posición absoluta, la orientación y el movimiento relativo de la plataforma sobre el suelo.

Como hemos visto, las operaciones donde toda o parte de una misión debe ser llevada a cabo sin acceso a los datos GNSS son cada vez más comunes. Las soluciones de control de vuelo de los RPAS en estos ambientes, como el mencionado Dead Reckoning, son compatibles con la navegación VNS. A pesar de que estos sistemas complementarios ya se han mostrado capaces de conformar un vuelo seguro, en una situación prolongada de falta de datos GNSS llevan a una gran deriva. Es aquí donde el VNS provee ventaja vital.

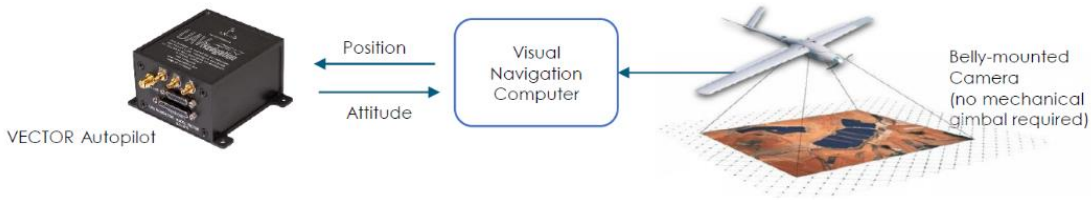


Figura 15 Esquema Navegación VNS con el FCS VECTOR. Fuente: uavnavigation.com

La navegación con el sistema VNS, combinado con los nuevos sistemas de control de vuelo (Flight Control System, FCS), como el sistema VECTOR, resuelve de manera eficiente y autónoma el problema de la deriva de navegación. La computadora a bordo de la unidad procesa las imágenes capturadas por la cámara incorporada, identificando patrones y movimiento sobre el terreno que sobrevuela. Esto permite que el FCS cancele cualquier error absoluto y operar por largos periodos de tiempo sin perder la posición. Gracias a su pequeño tamaño y peso, también puede ser instalado en pequeños y medianos RPAS, permitiéndoles aprovechar este nuevo y revolucionario sistema sin comprometer autonomía o capacidad de carga útil.

En los sistemas que menciona Miguel, hace una mención especial sobre el Black Hornet III (figura 16), que asegura posee un modo de vuelo sin GPS para operar en zonas denegadas, acercarse con precisión a paredes y ventanas e incluso para el vuelo en interiores de edificaciones. Su mecanismo de posicionamiento se basa en cámaras y software; con una nueva versión de éste en caso de pérdida de enlace, la aeronave es capaz de recorrer el camino para recuperarlo. Donde cabe destacar su gran conectividad (puede conectarse a él con cable ethernet para introducir o extraer información), su enlace robusto que permite que dificulta su perdida, así como una cámara térmica con capacidad nocturna muy por encima de otros sistemas RPAS similares (véase Tabla 4).

Figura 16 Black Hornet 3. Fuente: infodefensa.com

Tabla 5 Ventajas y Desventajas del Black Hornet III.

Ventajas	Desventajas
Peso: Cuenta con una huella logística mínima, todo el empaque pesa 2kg y se puede portar en el chaleco.	*Autonomía:* Sólo 20 minutos.
Velocidad: Tiene una rápida puesta en servicio equivalente a menos de 2 minutos.	*Cámara:* La resolución del video es escasa en BH", así como de la cámara IR.
Operatividad: Lo opera un solo operador y requiere poco mantenimiento.	*Capacidad de vuelo:* Límites de viento reales bajos (10kt-15kt) que suponen dificultades a la operatividad del vuelo.
Conectividad: Se considera muy buena, a través de un cable ethernet video con metadatos en STANAG 4609 con IP multicast.	*Operatividad:* Requiere alta destreza de manejo del operador, ya que, aunque cuenta con modos automáticos de vuelo su forma de operar y estabilizarse es de tipo "manual".
Detección: Es un sistema muy discreto y por ende, de difícil detección: unos 5 metros por sonido y unos 10 metros en visual.	*Mantenimiento:* El mantenimiento de las baterías debe ser exquisito para no sufrir una degradación temprana de estas; el BH3 posibilita su intercambio, por lo que la esperanza de vida de la plataforma aérea se alarga, en caso del BH" la batería está integrada lo que resulta en que una batería dañada deja inoperativa a toda la aeronave, y la esperanza de vida de las baterías es de 18 meses.
Enlace: Es robusto, por lo que se dificulta su pérdida.	
Capacidad de vuelo: Tanto en exteriores como en interiores.	
Cámara: Su cámara térmica muy superior a otras de sistemas similares, le otorga además una capacidad nocturna que beneficia su funcionamiento.	

Fuente: Elaboración propia, adaptación de entrevista a Miguel Vasallo Ledo (2022).

Al respecto, Miguel Ángel Llompart agrega que el mecanismo de funcionamiento de este sistema (BH3) en ambiente degradado funciona tomando como referencia diferentes puntos sobre una imagen de la zona de vuelo. Sin embargo, cuando se vuela en ambientes con superficies monocromas o con poco contraste de colores, el sistema se comporta de una forma errática, pudiendo producirse un “derrape” del aparato en el aire, que a su vez puede producir un golpe contra una pared o incluso la caída del aparato. Destaca además que un sistema BH3 no puede trabajar en ambientes degradados usando la antena como punto de referencia, como el caso del ORBITER 3. Aunque no de manera exclusiva, desde su perspectiva y experiencia, este tipo de sistemas usan la localización de la antena, que es conocida, y el ángulo de elevación y azimut de dicha antena para mejorar la localización del RPA en el espacio.

En otras palabras, según los expertos consultados, no hay competidores para el BH3. Aparte de ser el único en servicio de su clase (MICRO), posee una tecnología innovadora y difícil de duplicar en nuevos sistemas por diversos aspectos económicos y técnicos, entre otros. De allí su importancia en este apartado, ya que, podría decirse, que es el modelo más viable que contemplar una vez se estudien las alternativas correspondientes al GNSS, según las necesidades identificadas y las vulnerabilidades ya expuestas.

En referencia a las limitaciones de la navegación visual, puede decirse que ésta requiere de un mapa almacenado en el RPA con imágenes aéreas de la zona de operaciones, ya sea que hayan sido descargadas del satélite u obtenidas por el mismo en tiempo real, u otras aeronaves en misiones anteriores de reconocimiento sobre la zona de operación, lo cual no siempre es factible a nivel operacional.

Por último, como alternativas sin necesidad de servicio GNSS, tenemos la más antigua, usada por la aviación convencional desde sus orígenes hasta nuestros días, la radionavegación. Esta tecnología depende de una infraestructura terrestre muy amplia y costosa logísticamente. Por tanto, proporciona una limitada operatividad en zonas de conflicto. Esta tecnología necesita estaciones como el VOR/DME (figura 17) (Very High Frequency -Directional Range/Distance Measuring System), o similares. Estas son estaciones terrestres que emiten continuamente y en todas direcciones ondas de alta frecuencia para que un equipo a bordo interprete desde donde se están recibiendo estas señales y la distancia.

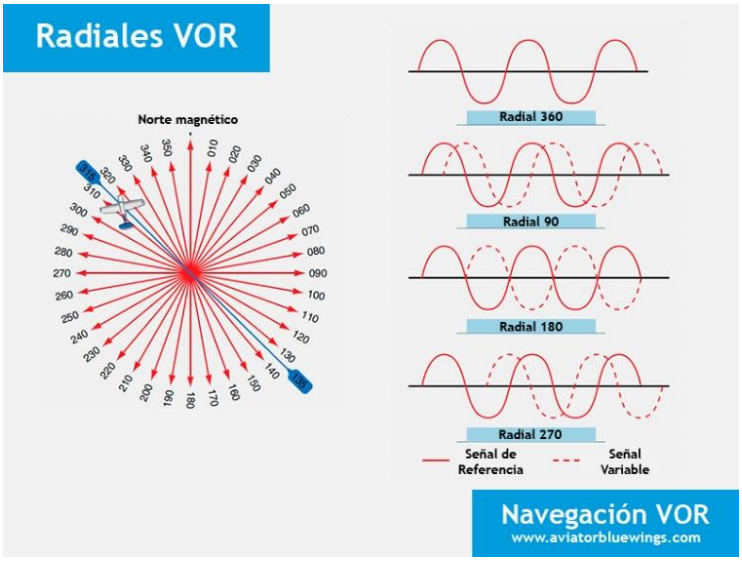


Figura 17 Radiales VOR que recibe una aeronave. Fuente:aviatorwings.com

Por otra parte, los avances tecnológicos han derivado en el conocimiento de la localización del RPA a través de la visualización del terreno, comparándola con una imagen guardada en la "memoria" del vehículo; la diferencia entre esa imagen guardada y la que se ve en tiempo real, se salva mediante inteligencia artificial. Incluso, asegura Miguel, que ya hay empresas que están estudiando este método para poder proporcionar coordenadas CAT I (categoría más básica de capacidad y precisión de posicionamiento radioeléctrico, y su precisión va de 30 a 60 metros) sin necesidad del posicionamiento satélite, aunque eso no puede ser usado hoy en día por el BH3.

5.2. Refuerzo a la Navegación basada en GNSS

Aunque esta investigación se centra en las vulnerabilidades que supone la dependencia al GNSS de los RPAS por las amenazas a la seguridad que ha experimentado, este sistema ha evolucionado en los últimos años. De acuerdo con Miguel Vasallo Ledo, los RPAS se posicionan mediante una IMU y mantienen la altitud a través de un sensor barométrico, al menos en sistemas como Raven, Wasp, BH II, BH III, Orbiter 3B, Searcher MKIII. Por este motivo, la denegación o pérdida del GNSS no acarrearía la pérdida de la aeronave. Por lo tanto, contar con un sistema redundante para el posicionamiento, sería el primer paso para reforzar la navegación basada en GNSS.

Hay que recalcar que esto es solo el principio. Ya que las misiones en las cuales están implicados los RPAS, suponen que no contar con estos medios redundantes a la hora de planear y conducir cualquier tipo de acción militar, podría suponer una clara desventaja en los escenarios actuales. Por ello, los sistemas deben estar diseñados para operar en cualquier condición, incluyendo la denegación o degradación de los GNSS. El avance más grande realizado en este sentido se ha centrado en asegurar, proteger y robustecer el enlace del RPA con el sistema satelital. Esta ha sido la línea de desarrollo principal tanto en el mundo civil como en el entorno militar mundial. La intención ya no es: no depender de los satélites, si no como asegurarnos que somos capaces de mantener este enlace en cualquier situación.

Como se ha remarcado desde el inicio del planteamiento de la investigación, las necesidades identificadas se resumen a las problemáticas que puede originar en materia de seguridad mundial el hecho de que las señales GNSS pueden ser interferidas o reemplazadas (figura 18). Por ende, que los RPAS sean ciertamente bastante vulnerables a este tipo ataques. Esto se ve agravado debido a la presencia en el mercado internacional de armas tecnológicas, que están al alcance de muchos países con intereses económicos diversos y en conflicto (Pedro Cervera, 2016).

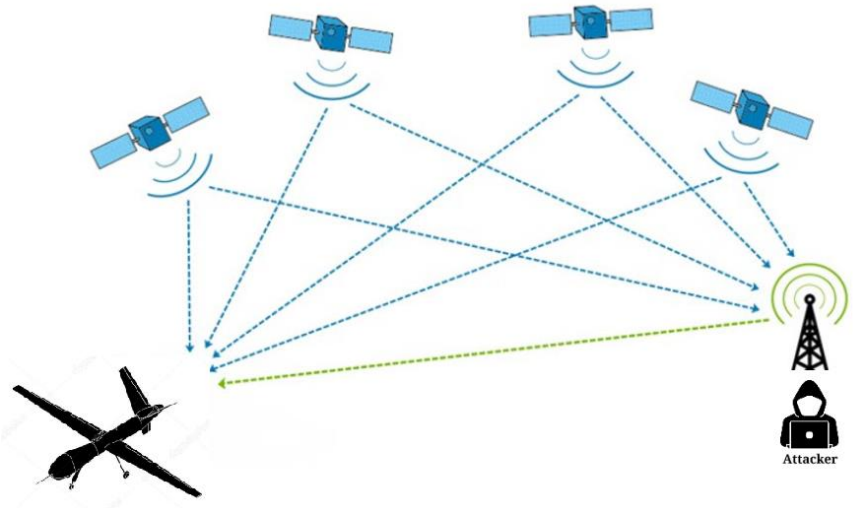


Figura 18 Interferencia de las señales GNSS. Fuente: dronescelab.com

En el conjunto de alternativas y nuevas creaciones tecnológicas, puede mencionarse el nuevo sistema de control GPS OCX (figura 19) y a los satélites GPS III, que se apoyarán en el sistema GPS OCX para su lanzamiento. Además, tenemos los receptores MGUE o "Military GPS User Equipment", que tienen como objetivo incrementar la precisión de posicionamiento aprovechando el sistema GPS OCX. Estos ya están integrados en sistemas portátiles que llevan operando desde 2015 en la US Army como el DAGR (figura 20). Con esto se consigue ser menos vulnerable ante los ataques cibernéticos, las interferencias y el spoofing (suplantación de la señal GNSS, de manera que los receptores calculen la posicione de manera incorrecta), utilizando una nueva encriptación de la información de alto nivel y disponible para los usuarios militares calificados y autorizados. Esto podría suponer la base de un sistema de posicionamiento más robusto para los RPAS del futuro (Pedro Cervera, 2016).

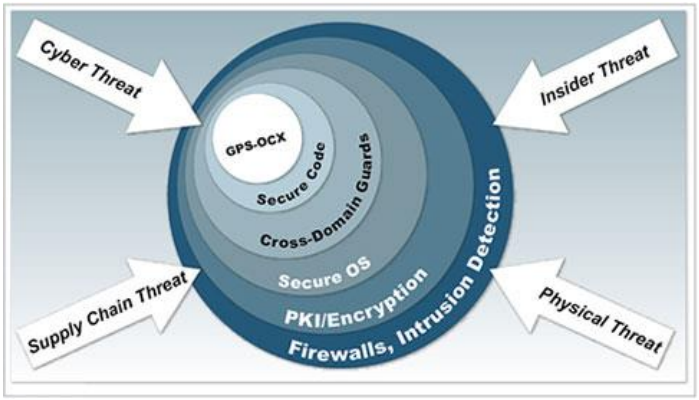


Figura 19 GPS OCX, sistemas de seguridad del remplazo del GPS y apoyo para los satelites GPS III. Fuente: Breakingdefense.com

Figura 20 Defense Advance GPS Receiver (DAGR). Actualmente con MGUE incorporado para aumento de precisión. Fuente: GPS.gov

El programa GPS OCX, en primer lugar, se propone una renovación de la infraestructura de control de sistema en tierra para hacer el sistema más robusto, preciso y menos vulnerable. Esto lo conseguirá utilizando un nuevo software con un algoritmo matemático mejorado. Este busca reducir específicamente la posibilidad del spoofing, comunicaciones encriptadas y firmadas. Mientras tanto, los satélites GPS III han tenido algunos problemas de implantación por componentes defectuosos. Sin embargo, EE UU sigue trabajando en nuevos modelos y conceptos tecnológicos que implementarán satélites y sistemas inerciales en pleno rendimiento en un futuro cercano. Es posible, de hecho, que el geoposicionamiento que hoy se conoce, a mediados del siglo ya sea obsoleto. Esto se debe a que tanto los países, como las empresas encargadas del desarrollo de estas tecnologías, avanzan sin cesar según cambian las necesidades globales. Todo ello con el fin de no atrasarse o hacerse más vulnerables en materia de seguridad (Pedro Cervera, 2016).

Cabe mencionar aquí que, Orolia (empresa líder en ofrecer software de PNT resiliente -figura 21-), tiene una larga historia colaborando con las agencias de defensa sobre el acceso a soluciones para asegurar el PNT, prácticamente, a prueba de fallos. En este sentido el software ofrecido por esta empresa proporciona datos PNT extremadamente veraces, seguros y de alta precisión en condiciones duras y móviles de las operaciones militares. Su experiencia ha resultado en un enfoque innovador, usando las estaciones terrestres, que a través de su software son capaces de mantener un enlace virtual a los datos del satélite. Esto los ha convertido en el líder mundial de un PNT Resiliente y, además, en una referencia para buscar soluciones sin prescindir del servicio GNSS en las navegaciones RPAS.

Figura 21 Logo empresa Orolia, lider mundial en PNT resiliente. Fuente: Orolia.com

La importancia de este último está en el impacto operativo de la Resiliencia PNT en la capacidad de detectar vulnerabilidades en GNSS, como incidentes de suplantación de identidad o interferencia, emitir alertas y proporcionar fuentes alternativas de navegación y posicionamiento. Así, determinar una u otra posición precisa a partir del satélite, depende de medir con precisión las distancias entre el receptor y éste, lo cual a su vez depende de una medición muy precisa del tiempo de viaje de la señal de radio desde el satélite hasta el receptor, que requiere una gran sincronización en el receptor.

También existen otros sistemas, como el mencionado por Francisco Javier Cruz Hernández, las antenas CRPA (figura 22). Estas permiten una protección frente al jamming de GNSS, ya que obligan a que el jammer requieran mucha más potencia, para ser efectivos. Con estos sistemas, la potencia de interferencia requerida para denegar la señal GNSS a 10 km en un RPA es de entre 800w y 80 KW, dependiendo de los sistemas que se combinen. En este caso, ya no sería tan fácil ni tan económico para el adversario perturbar el GNSS.

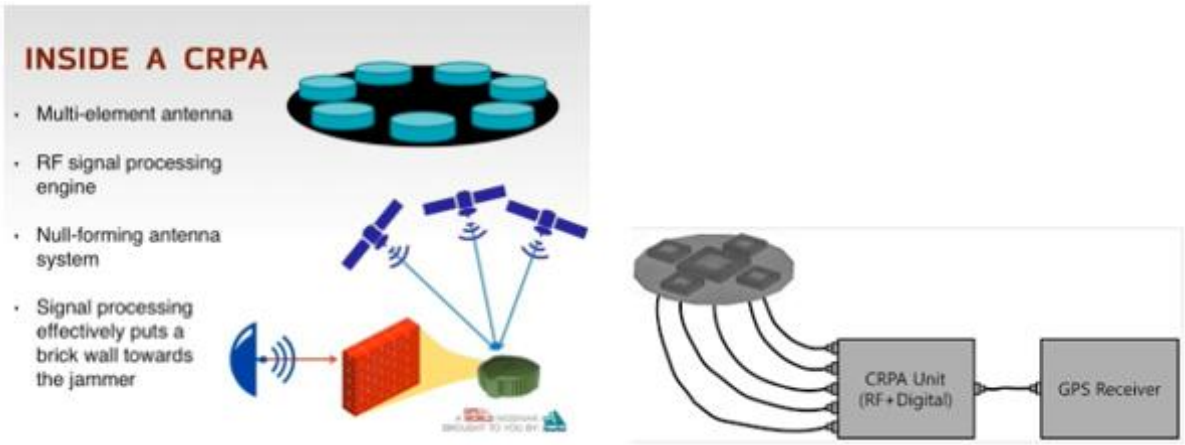


Figura 22 Funcionamiento de una antena CRPA. Fuente: novatel.com

Las antenas de patrón de recepción controlado o CPRA son antenas de dirección de haz adaptativo cuyo patrón de recepción se puede ajustar para crear nulos en la dirección de las señales de interferencia (figura 23). Crean una especie de filtro espacial que elimina las señales de una dirección particular mientras deja pasar señales de otras direcciones. La antena CPRA está conectada a una unidad de procesamiento que se encarga de controlar el patrón de recepción de la antena. Entonces, en el caso de jamming de la señal GNSS, la antena CPRA identifica la interferencia y controla el patrón de recepción dirigiendo los haces hacia los satélites y anulando el lugar de donde proviene la interferencia (comunicación personal Francisco Javier Cruz Hernández).

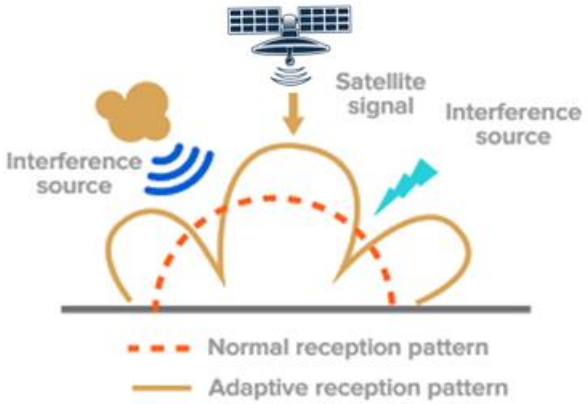


Figura 23 Patrón de recepción con una antena CRPA. Fuente: everything.com

Por lo tanto, si se quiere lograr una protección de +90dB frente al jamming de GNSS en el RPAS, considerando que el GPS C/A (servicio GNSS más ampliamente utilizado) es notablemente vulnerable a las interferencias, las antenas CRPA son una buena medida para los RPAS con capacidad de integrarlos. Hay que tener en cuenta que sin estas antenas este servicio tiene una tolerancia limitada a las interferencias. El nivel general de la señal GNSS en el receptor es de -163 dBW, esto quiere decir que está por debajo del nivel de ruido del receptor. Por ello, una interferencia de 2 W ubicada a 100 km del receptor GNSS podría impedir la adquisición del código C/A. Con esto en consideración y sabiendo que un perturbador comercial de entre 30€ y 300€ bastaría para inutilizar este servicio GNSS de un RPA de varios miles de euros, una antena CRPA es un opción a considerar (comunicación personal Francisco Javier Cruz Hernández).

Lo que Francisco sugiere con esto es que, aunque la confianza del ámbito militar en el GNSS sea consecuente, es necesario tener en cuenta que no se puede garantizar la calidad de las señales. Además, aclara que la antena CRPA está conectada a una unidad de procesamiento que realiza una suma destructiva de fase de las señales de interferencia entrantes, siendo este proceso equivalente a anular las interferencias en el patrón de radiación del conjunto. En pocas palabras, las antenas CRPA se han desarrollado para rechazar la interferencia de radiofrecuencia.

Según la opinión de este experto (Francisco) lo que hace que el sistema CRPA sea especialmente atractivo es el hecho de que no requiere ningún cambio en el propio receptor GPS. Simplemente reemplaza la antena existente. Dado que las antenas con patrón de recepción controlado se basan en la formación de haces, requieren varios elementos. El número de elementos de antena ayudará a determinar la resolución de los haces en el patrón de antena. Por lo tanto, cuantas más antenas, la capacidad de discriminar direcciones de recepción será mayor. Finalmente, Francisco estimo un presupuesto para este trabajo, mencionando que cada antena mas el control antijamming tendrían un coste unitario aproximado de 4000€. Un precio muy razonable teniendo en cuenta el valor que tienen los RPAS en las FAS.

Para finalizar este apartado me gustaría mencionar la opinión del Brigada Miguel Ángel Llompart, operador de varios sistemas RPAS, en relación con algunos de los sistemas de navegación resiliente mencionados en este trabajo. Según su opinión no debe haber un sistema único, si no que un sistema debe complementar a otro. En Iraq, por ejemplo, ha volado el ORBITER en aquellas ventanas en las que otros medios ISR no han podido volar o en donde un medio ISR no veía nada, el ORBITER 3 sí. De hecho, ha manifestado que en un reciente Ejercicio con los de la Fuerza de Guerra Naval Especial, posicionaban el BH3 observando una avenida de aproximación, durante el tiempo que tardaban en recuperar el RAVEN, cambiar la batería, y volver a lanzarlo. Al final se trata de que el Force Commander engrane de una forma adecuada sus medios, teniendo en cuenta sus fortalezas y debilidades. Pudimos al final estar de acuerdo que eso es el "Arte de la Guerra": adaptarse a la situación, con los medios que disponemos (SUN TZU, s IV a.C.-figura 24-).

Figura 24 Imagen con el arte de la guerra en el espacio aéreo. Fuente: rtve.es

6. CONCLUSIONES

Con el desarrollo del presente trabajo se han extraído diversas conclusiones que se exponen a continuación:

I. Tras analizar los RPAS en dotación del ET; a pesar de las vulnerabilidades que presentan y de las características de sus sistemas de navegación (dependiente del GNSS), se puede concluir que los sistemas estudiados han cumplido sus cometidos en aquellos escenarios donde han sido desplegados. Los RPAS han supuesto, sin duda, una revolución en las operaciones militares de las dos últimas décadas, convirtiéndose en un elemento indispensable por su contribución a estas operaciones, tanto a nivel táctico, operacional y estratégico o político. Su polivalencia, versatilidad y discreción, unido a su persistencia en la zona de misión y a sus reducidos costes (tanto de adquisición, como de operación y de mantenimiento), han permitido a los ejércitos integrar una capacidad fundamental para obtener información en tiempo real, y que puede ser difundida a miles de kilómetros en tan sólo unos segundos; además, posibilitan la difusión de esas imágenes a través de diferentes medios de comunicación, para lograr el apoyo u otras reacciones en la opinión pública. A pesar de todas sus ventajas, con la proliferación de estas aeronaves, también se han visto aumentadas sus vulnerabilidades. La principal, objeto de este trabajo, es la dependencia de un GNSS para su navegación y posicionamiento. El resultado de una acción contra este sistema de navegación o posicionamiento se traduce en una imposibilidad de la aeronave para realizar su vuelo, o realizarlo de forma que pueda resultar peligrosa para la operación o para el aparato.

II. Tras las diferentes entrevistas por operadores de RPAS; actualmente las operaciones militares se realizan tanto en territorio nacional como en misiones internacionales. En las operaciones nacionales, donde se realizan vuelos de enseñanza, instrucción y adiestramiento (y esporádicamente en apoyo a Fuerzas y Cuerpos de Seguridad del Estado), prima la operación de forma segura; hoy en día, se realiza en espacio aéreo segregado. A pesar de una nueva regulación a nivel europeo, que permitirá el uso compartido del espacio aéreo entre aeronaves tripuladas y no tripuladas, actualmente no hay sistemas robustos para permitir este entorno colaborativo (aunque se están desarrollando para ser implementados en los próximos meses). Con la proliferación de RPAS en nuestro espacio aéreo se generará, sin duda, la misma duda que ha motivado la realización de este trabajo: alternativas al GNSS para el posicionamiento de RPAS.

III. El uso de receptores GNSS se ha extendido masivamente y las técnicas de jamming y spoofing suponen una amenaza en constante evolución. Con este avance también se consiguen equipos de bajo coste y menor tamaño, pero con amplias capacidades de ataque y estrategias más sofisticadas. Para protegernos ante esta situación se han seguido las dos líneas de acción desarrolladas en el punto cinco. Una de ellas es buscar la independencia de los RPAS de los servicios GNSS, buscando alternativas a los satélites para el posicionamiento. Por otro lado, la otra línea va dirigida a fortalecer esta conexión con los satélites, por las grandes ventajas que estos aportan. Aunque en la actualidad el avance principal se ha realizado en esta segunda dirección, hay alternativas cada vez más interesantes para desprendernos de la dependencia satelital. Desde un punto de vista personal y tras el desarrollo del trabajo, hoy en día la mejor opción se encuentra en esta vía: una conexión más robusta con los satélites. Esto es debido a que hoy en día los sistemas alternativos no proporcionan las capacidades que ofrece el sistema GNSS.

IV. En cuanto a la búsqueda de la independencia satelital, las opciones contempladas más interesantes en este trabajo son la navegación VNS, y la implementación de la tecnología LIDAR en la navegación. Tecnologías que hoy día siguen evolucionando y probándose en nuevos prototipos de RPAS con un futuro muy prometedor. También se ha mencionado la clásica navegación radioeléctrica. No obstante, la finalidad más habitual de la utilización de los RPAS en las FAS es su empleo operativo para misiones ISR. Este hecho lo hace incompatible con tener que hacer una preinstalación de una gran antena en las inmediaciones de las zonas que se quiere operar (en espionaje, por ejemplo). No obstante, la navegación radioeléctrica es una posibilidad muy conveniente para territorio nacional o ciertos territorios donde ya existen las instalaciones terrestres necesarias para realizar este tipo de navegación.

V. Por otro lado, la industria y los países de todo el mundo han centrado su atencion en mantener su dependencia de los satélites y han desarrollando nuevas tecnologías y software para proteger los enlaces del servicio GNSS. Entre las tecnologías más interesantes se encuentran los nuevos sistemas de refuerzo satelital, como el GPS OCX o los nuevos satélites GPS 3. A nivel nacional y europeo, una vez consolidada la fase de desarrollo de la infraestructura y con los sistemas E-GNSS (EGNOS y Galileo) en diversos grados de operación, la fase de explotación se convertirá en un aspecto cada vez más relevante, con una previsión de crecimiento en los próximos años. Esto permitirá capitalizar el conocimiento y la experiencia obtenidos por la industria española a través de su participación en estos proyectos europeos (EGNOS y Galileo). También se han desarrollado microchips dentro del programa Micro-PNT, logrando integrar tres datos imprescindibles en la navegación: orientación, aceleración y tiempo. Estos chips han sido probados en misiles que no dependen del GNSS para alcanzar su objetivo. Por último, en lo que respecta al refuerzo de los enlaces satelitales, destacan las antenas CRPA, que, según el experto Francisco Javier Cruz Hernández, son una solución muy versátil y operativa. Este sistema solo implica el cambio de las antenas actuales por estas nuevas antenas, que tienen la capacidad de discriminar la dirección de recepción para evitar cualquier interferencia. En mi opinión, después de evaluar las diferentes posibilidades, mi propuesta inicial sería adoptar las antenas CRPA en los modelos del ET que puedan incorporarlas, lo cual no impediría el aprovechamiento de los nuevos sistemas de E-GNSS cuando se encuentren totalmente operativas.

VI. Todos estos pasos han llevado a evaluar las alternativas al GNSS de RPAS y el impacto que supone la vulnerabilidad del sistema del cual son dependientes en gran medida en la navegación, para las FAS, España y el mundo en general. Especialmente en medio de situaciones de crisis o conflicto. Es esencial considerar que, si la señal GNSS es interferida o reemplazada por información errónea, las decisiones que se tomen sobre el reconocimiento de una zona en conflicto (como se ha visto recientemente en Europa) también serán fatídicas. Con ello, se pondrán en riesgo no solo la seguridad de la misión sino incluso vidas civiles y militares. Por ello, es imperativo minimizar cuanto antes las amenazas que el jamming y el spoofing suponen actualmente en términos de información para el GNSS en el posicionamiento de RPAS. A pesar de las limitaciones de acceso a información en aspectos relacionados con el tema a tratar, se han extraído estas conclusiones, y se proponen como alternativa a la solución de este problema a corto plazo. Además, se han contemplado tal como se había planificado, las diversas opciones al alcance de la investigación realizada.

VII. Por otro lado, se puede identificar una necesidad por parte de las FAS de colaborar activamente con los ministerios y organismos regionales en la gestación de sus planes y estrategias de I+D+i (Investigación, Desarrollo e innovación), presentando ante ellas las opiniones y necesidades de nuestras FAS de cara al desarrollo de programas de financiación más adecuados. El interés de plasmar nuestras prioridades en las agendas estratégicas, además, es doble: dotar de coherencia a los esfuerzos de los diferentes actores del ecosistema innovador, e interpelar a las administraciones, que deben articular formulas y herramientas que ayuden al desarrollo de las líneas de acción detalladas en estas agendas. Por último, y tras comprobar la falta de coordinación en algunos elementos de las FAS con la industria nacional, propondré algunas acciones que podrían tenerse en cuenta: en primer lugar, sería crear un grupo de expertos que pudiera asesorar sobre la investigación en materia de RPAS. Se definirían líneas de colaboración entre las FAS y la industria además de centros de I+D+i. Estas líneas de colaboración podrán proponerse los aspectos que se consideren prioritarios, como, por ejemplo, enlaces de comunicación satélite, software, entre otros. Por último, sería publicar un análisis prospectivo sobre objetos futuros en materia de investigación de RPAS.

En cuanto a las limitaciones y prospectiva sobre el estudio del tema abordado, estas radican en que hay muchos lagunas de información sobre el tema a tratar. La búsqueda bibliográfica es compleja porque la información se vuelve redundante y, en muchas ocasiones, no se reflejan las fuentes para cotejar o contrastar la información revelada en los artículos de prensa (que son los principales resultados de búsqueda). Por otra parte, se espera poder realizar más entrevistas a expertos en la materia en un futuro estudio, que pueda ampliar los fundamentos aquí desarrollados en una parte más práctica, que pudiera incluso permitir determinar cuáles son las alternativas más viables al GNSS como sistema de posicionamiento de RPAS en un futuro cercano para España.

REFERENCIAS BIBLIOGRÁFICAS

AEROSPACE, SECURITY AND DEFENSE (ASD Eurospace). The Unmanned Aircraft Systems Traffic Management (UTM) Regulation (2022). Disponible en https://asd-europe.org/the-unmanned-aircraft-systems-traffic-management-utm-regulation.

ACELERA PYME. Machine learning. ¿Qué es y cuáles son sus utilidades?, 2022. Disponible en https://www.acelerapyme.gob.es [Consultado el 13-03-2023].

AGENCIA ESTATAL DE SEGURIDAD AEREA (AESA). España ha terminado 2022 con más de 71.100 operadores de drones registrados en AESA (Enero 2023).Disponible en https://www.seguridadaerea.gob.es/es/noticias/españa-ha-terminado-2022-con-más-de-71100-operadores-de-drones-registrados-en-aesa [Consultado el 10-03-2023].

AGENCIA EUROPEA DE SEGURIDAD AEREA (EASA). EASA presents new regulatory approach for Remotely Piloted Aircraft (RPAS). 2015Disponible en https://www.easa.europa.eu/en/newsroom-and-events/news/easa-presents-new-regulatory-approach-remotely-piloted-aircraft-rpas [Consultado el 10-03-2023].

ASENSI MIRALLES, José Ramón. LA OPERACIÓN DE LOS SISTEMAS AÉREOS TRIPULADOS REMOTAMENTE EN ESPAÑA. 2014. Ejército del Aire. p 1-10. Email: jasensim@ea.mde.es.

ASESORÍA DRONES ESPAÑA. ¿Qué es un RPA, RPAS, UAS y un DRON? 2020. Disponible en https://www.asesoriadron.com/que-diferencia-hay-entre-los-terminos-rpa-rpas-uav-uas-y-dron [Consultado el 10-03-2023].

AXE, D. Strategist: Killer Drones Level Extremists' Advantage. 2009. Disponible en https://www.wired.com/2009/06/strategist-killer-drones-level-extremists-advantage/ [Consultado el 10-03-2023].

BANDERA, María Paula. Drones: creció la demanda de pilotos profesionales y hay lista de espera en los cursos. [Clarín.com] Publicado el 17 de diciembre de 2017. Disponible en https://www.clarin.com/sociedad/drones-crecio-demanda-pilotos-profesionales-lista-espera-cursos_0_r12R5NVMf.html [Consultado el 10-03-2023].

BERNÉ VALERO, José Luis. (2019). Universitat Politècnica de València. GNSS: GPS, GALILEO, GLONASS, BEIDOU. Fundamentos y métodos de posicionamiento.

CARRASCO, J. LOS RPAS, UN ESLABÓN MÁS EN LA EVOLUCIÓN TECNOLÓGICA. Discurso leído en el acto de su recepción como Académico Numerario por D. Juan Antonio Carrasco Juan el día 30 de enero de 2017. Academia De Ciencias, Ingenierías y Humanidades de Lanzarote. p 1-45.

CONSEJO NACIONAL DE SEGURIDAD AEROESPACIAL (CNSA). Drones y seguridad Nacional, un estudio multidimensional. 2022. Disponible en https://www.dsn.gob.es [Consultado el 11-03-2023].

DEPARTMENT OF DEFENSE (DoD). Unmanned Systems integrated roadmap 2017-2042. 2017. Disponible en https://apps.dtic.mil/sti/citations/AD1059546 consultado [Consultado el 11-03-2023].

DIAZ VILLANUEVA, FERNANDO. La guerra de los drones, 2023. Disponible en https://diazvillanueva.com/la-guerra-de-los-drones/ [Consultado el 11-03-2023].

DIRECCION GENERAL DE ARMAMENTO Y MATERIAL (DGAM). Estrategia de Tecnología e Innovación para la Defensa (ETID). 2020. Disponible en https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/t/etid_estrategia_de_tecnolog_a_e_innovaci_n_para_la_defensa_2020.pdf [Consultado el 10-03-2023].

EL CONFIDENCIAL. Prueban con éxito el primer dron nodriza de la historia. 2021. Disponible en https://www.elconfidencial.com/tecnologia/novaceno/2021-08-24/avion-nodriza-dron-boeing-pentagono_3247218/ [Consultado el 10-03-2023].

EL PAIS. La Policía confisca en Málaga el mayor dron dedicado al transporte de droga, publicado 13 julio 2021. Disponible en https://elpais.com [Consultado el 10-03-2023].

ESTEBAN HERREROS, JOSE LUIS. Los Drones y sus aplicaciones a la ingeniería civil. 2015. Disponible en https://www.fenercom.com/wp-content/uploads/2015/03/Los-Drones-y-sus-Aplicaciones-a-la-Ingenieria-Civil-fenercom-2015.pdf [Consultado el 10-03-2023].

FERVIMAX. Drones en el sector militar y cómo aprovechar al máximo esta tecnología. [Internet] Publicado el 27 de noviembre de 2019. Disponible en https://fervimax.com/drones-en-el-sector-militar-y-como-aprovechar-al-maximo-esta-tecnologia/ [Consultado el 10-03-2023].

FUERZAS DE LA DEFENSA DE LA RÉPUBLICA ARGENTINA (FDRA). UCAV: Infografías MQ-9 Reaper. 2012. Disponible en https://fdra.blogspot.com/2012/07/ucav-infografias-mq-9-reaper.html [Consultado el 15-03-2023].

GARCÍA DE LA CUESTA, Jorge. Terminología aeronáutica. Ediciones Díaz de Santos, S.A. ISBN 84-7978-579-9, 2003. Disponible en https://books.google.co.ve/books [Consultado el 10-03-2023].

GARCÍA, Rosario. Thales realiza una demostración de su sistema Antidron (Hours Shield) y Los Sistemas más avanzados de Drones y Antidrones. RPASDrones. 2022, nº1, p 38-39 y p 26-27.

GRADIANT. DRON, RPA, RPAS, UAS y UAV: ¿Qué son y en qué se diferencian? 2019. Disponible en https://www.gradiant.org/blog/dron/ [Consultado el 10-03-2023].

INFODEFENSA. Las fuerzas especiales de la Armada recibirán el mini dron Black Hornet 3. Marzo 2023. Disponible en https://www.infodefensa.com [Consultado el 18-03-2023].

INSIDE GNSS. CRPA for GNSS: Benefits, Challenges and Testing. 2022. Disponible en https://insidegnss.com/crpa-for-gnss-benefits-challenges-and-testing/ [Consultado el 10-03-2023].

KRAJNIK, J. A simple visual navigation system for an UAV. Conference Paper. March 2012. p 1-8. DOI: 10.1109/SSD.2012.6198031.

LEY 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia. Publicado en: «BOE» núm. 252, de 17 de octubre de 2014, páginas 83921 a 84082 (162 págs.). Disponible en https://www.boe.es/eli/es/l/2014/10/15/18 [Consultado el 10-03-2023].

MARTÍNEZ, JORGE. Prioridades de I+D+i en sistemas aéreos no tripulados (UAS). 2020. Disponible en https://plataforma-aeroespacial.es/wp-content/uploads/2020/10/Documento-Prioridades-IDI-en-UAS-FINAL.pdf [Consultado el 20-03-2023].

MINISTERIO DE CIENCIA E INNOVACIÓN. EECTI 2021-2027 (Estrategia Española de Ciencia, Tecnología e Innovación 2021-2027). 2020. NIPO: 83120021X.

MINISTERIO DE DEFENSA. Proyecto RAPAZ y tecnologías anti-RPAS. Diciembre 2016. p 1-194. NIPO: 083-16-434-X.

MINISTERIO DE FOMENTO. Plan Estratégico para el desarrollo del sector civil de los drones en España (2018-2021). Disponible en https://www.mitma.gob.es/recursos_mfom/paginabasica/recursos/plan_estrategico_drones_2018-2021_0.pdf [Consultado el 10-03-2023].

MUÑOZ, Fernando. Los usos más increíbles de los «drones». ABC.es Publicado el 07 de agosto de 2014. Disponible en https://www.abc.es [Consultado el 10-03-2023].

ORGANIZACIÓN DE AVIACION CIVIL INTERNACIONAL (OACI). Sistemas de aeronaves no tripuladas (UAS). 2011. ISBN 978-32-9231-809-3.

PLATAFORMA TECNOLOGIA AEROESPACIAL ESPAÑOLA. Agenda estratégica de investigación e innovación en aeronáutica 2019-2030, 2018. Disponible en https://plataforma-aeroespacial.es/wp-content/uploads/2019/12/Agenda-Final-5-web.pdf [Consultado el 10-03-2023].

PÉREZ QUINTANA, ADRIAN. Estudio de Array de Atenas de Referencia para GNSS. Trabajo Fin de Master. Escuela Politécnica Superior. UAM. 2019.

RUIZ DOMÍNGUEZ, Fernando. Instituto Español de Estudios Estratégicos. La importancia de los RPAS/UAS para la Unión Europea. Documento de Opinión 78/2013. Publicado el 28 de agosto de 2013. p 1-15.

SISTEMA DE OBSERVACIÓN Y PROSPECTIVA TECNOLOGICA (SOPT): Monografía 13, Monografía 15 y Monografía 17. 2013, 2015 y 2017 respectivamente. NIPO 083 -13-196-3, 083-16-433-4 y 083-18-179-9 respectivamente.

VENTURA, Javier, ESA. “La navegación por satélite es una de las tecnologías que más va a cambiar el mundo”. [Atlantico.net] Publicado el 6 de junio de 2015.

VOZ DE AMERICA. EEUU promete continuar con sus misiones de vigilancia en el mar Negro. 2023. Publicado el 15 de marzo de 2023.Disponible en https://www.vozdeamerica.com/a/eeuu-promete-continuar-misiones-vigilancia-mar-negro-/7006735.html [Consultado el 15-03-2023].

ANEXOS

Anexo I Entrevistas a expertos especializados en RPAS

Miguel Vasallo Ledo (Sgto1)

Todos los RPAS se posicionan mediante una IMU (unidad de medición inercial) para posicionarse y aparte la Altitud la mantiene mediante sensor barométrico (al menos los sistemas militares que tenemos en dotación, Raven, Wasp, Black Hornet II, Black Hornet III, Orbiter 3B, Searcher MKIII) por lo que la denegación o pérdida del GNSS no acarrea la pérdida de la aeronave.

Dicho esto, la emergencia de pérdida de GNSS conlleva un vuelo degradado y no operativo por lo que las acciones a tomar son traerlo con rumbo inverso al bearing de la GCS o por referencias en el terreno hasta la zona de aterrizaje.

Según la doctrina y los mismos operadores, se considera la capacidad de poder seguir desempeñando la operación y posicionarse la aeronave mediante otro método. En este caso algunos sistemas tienen un modo de vuelo que se llama dead reckoning (navegación a la estima) que la aeronave se posiciona en el mapa teniendo en cuenta las aceleraciones, rumbo y velocidad dados por la IMU/ IAS. El problema es que no es apto para un buen desempeño de la operación pues los datos de viento no los tiene en cuenta por lo que la aberración que sufre la posición de la aeronave sobre el plano es mayor con el tiempo y los cambios de velocidad y altitud no los tolera bien para los cálculos.

Otros sistemas tienen posicionamiento por comunicaciones (Orbiter 3B y Searcher MKIII) la posición la obtiene sabiendo la posición de la antena, la distancia a esta (mediante el tiempo que tardan los paquetes de datos en retornar) y más el magnetómetro de la antena (GDT). Con todo esto se posiciona con bastante precisión la aeronave, el problema de estos sistemas es la forma de aterrizar, pues el Orbiter tiene que ser mediante indicaciones de personal en tierra y apertura de paracaídas manual y el Searcher que aterriza en pista mediante el RPAPS (dispositivo parecido goniómetro que busca catadióptrico de la aeronave y lo mete en eje y senda para el aterrizaje)

-El black Hornet los hay modelo II y III

Respecto a la capacidad de vuelo con GNSS denegado el black hornet II precisa de GPS para el vuelo solo puede despegar sin GNSS empleando la cámara y un software, está pensado para despegarlo en sitios confinados y una vez en el aire activar el GPS y empezar la operación.

El Black Hornet III sí que posee un modo de vuelo sin GPS, para operar en zonas denegadas, acercarse con precisión paredes y ventanas (sombra GNSS) e incluso el vuelo en interiores de edificaciones, la forma de posicionarse es mediante cámaras y software, incluso con una nueva versión de software en caso de pérdida de enlace la aeronave es capaz de recorrer el camino andando para recuperar el enlace.

-Ventajas en general e inconveniente del sistema Black Hornet

Ventajas

+Huella logística mínima, todo el empaque pesa 2kg y se puede portar en el chaleco.

+Extremadamente discreto siendo muy difícil detectarlo, unos 5 metros por sonido y unos 10 metros en visual.

+Enlace robusto, siendo difícil la pérdida de este.

+Capacidad nocturna gracias a la cámara térmica (muy superior la del BH3)

+rápida puesta en servicio, menos de 2 minutos.

+lo opera un solo operador.

+requiere poco mantenimiento.

+Muy buena conectividad sacando a través de un cable ethernet video con metadatos en STANAG 4609 con IP multicast.

+Capacidad de vuelo en exteriores e interiores (solo BH3).

-Inconvenientes:

+Autonomía de 20 minutos.

+Resolución del video escasa (BH")

+Resolución baja de la cámara IR

+Límites de viento reales bajos (10kt-15kt ya dificulta el vuelo)

+Requiere destreza por el operador pues, aunque tiene modos automáticos de vuelo su forma de operar es en "manual" (la aeronave se estabiliza automáticamente).

+Mantenimiento de la baterías y esperanza de vida de estas, por experiencia el mantenimiento de las baterías debe ser exquisito para no sufrir una degradación temprana de estas, el BH3 posibilita el intercambio de baterías por lo que la esperanza de vida de la plataforma aérea se alarga, en caso del BH" la batería está integrada lo que resulta en que una batería dañada deja inoperativa a toda la aeronave, la esperanza de vida de las baterías es de 18 meses.

Miguel Ángel Llompart (Brigada)

Tema muy interesante, y más en estos días viendo lo visto en el este de Europa, y además lo ha podido comprobar personalmente en un teatro de Operaciones como es Iraq. El poder trabajar en un ambiente degradado lo considero un requisito Obligatorio para un RPAS de las FAS.

En primer lugar, el modo de trabajo del Black Hornet 3(BH3) en ambiente degradado es tomando como referencia diferentes puntos en la imagen (muy resumido). He tenido la oportunidad de observar modelos Beta del software en los que se aprecian esos puntos, (en los sistemas de serie no se pueden ver), por eso cuando se vuela en ambientes con superficies monocromas, o con poco contraste de colores el sistema se comporta de una forma errática, pudiendo producirse un "derrape" del aparato en el aire dando como resultado el golpeo a una pared o incluso la caída del aparato.

El BH3 no puede trabajar en ambientes degradados usando la antena como punto de referencia,

como el caso del ORBITER 3 (aunque no exclusivo). Este tipo de sistemas usan la localización de la antena, que es conocida, y el ángulo de elevación y azimut de dicha antena. Además de esta información, puede verse complementada por información proporcionada por otros sensores embarcados en el RPA, y que mejoran la localización del RPA en el espacio.

La tecnología está derivando a que se pueda conocer la localización del RPA mediante la visualización del terreno, comparándola con una imagen guardada en la "memoria" del RPA. La diferencia entre esa imagen guardada y la que se ve en tiempo real, se salva mediante inteligencia artificial. Incluso ya hay empresas que están estudiando este método para poder proporcionar coordenadas CAT I sin necesidad del posicionamiento satélite. Pero nada de eso puede ser usado hoy en día por el BH3.

En segundo lugar, creo que el BH3 no tiene ni ventajas ni inconvenientes con otros sistemas de su categoría, dado que es el único en servicio de su clase. El BH3 pertenece a la clase MICRO, aquella que puede infligir una energía cinética menos a 66 Julios (Anexo A del RCAO), actualmente no conozco a ningún otro sistema en servicio o pretendiendo serlo, que pueda competir con él. La DGAM, (y en ocasiones el MALE), habla de clase MICRO, en especial a la hora de hablar de adquisiciones a aquella que va de 0 a 2 kilos, que coincide con la anterior clasificación de UAS, dado que, si se atiende a la de RCAO, (o del STANAG 4670), solo habría un competidor: El BH3, no dando oportunidad a la industria nacional, (implicaría muchos años e inversión llegar a desarrollar un sistema como el BH3 actual).

Pero intentando "mojarme" diría que:

-Los puntos fuertes del BH3 son tres: su baja firma sonora, que una aeronave puede ser empleada de día como de noche, y que puede ser usada tanto outdoor como indoor, y todo ello sin necesidad de disponer de varios sistemas para cada situación.

-Como puntos en contra: la "baja" calidad de su imagen térmica, (la pongo entre comillas puesto que existe una duda razonable de si se puede considerar "baja" la calidad proporcionada a una cámara térmica montada en una aeronave de 34 gr de MTOW). Podríamos hablar de su tolerancia al viento, pero en mi opinión está más que bien en un aparato de ese MTOW.

Anexo II Entrevista a experto en guerra electrónica

Francisco Javier Cruz Hernández (correo trabajador en guerra electrónica en TecnoVit)

Cómo mejorar la capacidad de operaciones RPAS en entorno GNSS denegados

Las antenas de patrón de recepción controlado o CPRA son antenas de dirección de haz adaptativo cuyo patrón de recepción se puede ajustar para crear nulos en la dirección de las señales de interferencia. Crean una especie de filtro espacial que elimina las señales de una dirección particular mientras deja pasar señales de otras direcciones. La antena CPRA está conectada a una unidad de procesamiento que se encarga de controlar el patrón de recepción de la antena. Entonces, en el caso de jamming de la señal GNSS, la antena CPRA identifica la interferencia y controla el patrón de recepción dirigiendo los haces hacia los satélites y anulando el lugar de donde proviene la interferencia

La potencia de interferencia requerida para denegar el GPS a 10 Km en un RPA que emplea GNSS C/A + INS, considerando que el nivel de potencia de señal que llega a los receptores es de alrededor de -160 dBW, es de 0,2W. Puesto que la potencia recibida por el GPS es muy baja, la relación señal a interferencia (J/S) que se requiere es muy modesta. Un perturbador comercial, fácilmente adquirible, bastaría para inutilizar la señal del satélite en un RPA.

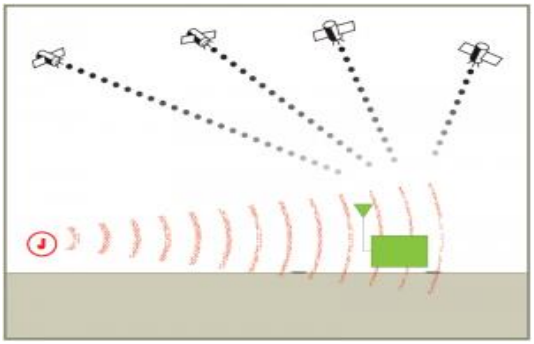
Por lo tanto, aquellos RPAS que solo recurran al empleo de un inercial como complemento al GNSS para intentar operar con GNSS denegado, por muy bueno que sea el INS y el filtro Kalman que fusiona los datos de los sensores para proporcionar la solución de navegación, se verán abocados a no poder continuar su misión.

Aunque puedan mantener la estabilidad del RPA, el INS experimentará una deriva creciente a lo largo del tiempo que hará inviable completar la misión. En términos de precisión de navegación, la perturbación del GNSS durante una hora puede suponer entre 11 y 16 Km, en función de la calidad del INS. Conviene aclarar que completar la misión no es mantener la estabilidad del RPA ni regresar de forma segura a un punto de recuperación.

Se han propuesto alternativas al GNSS tales como la navegación visual, las señales de oportunidad y las radiobalizas.

En el caso de la navegación visual, se requiere un mapa almacenado en el RPA, con imágenes aéreas de la zona de operaciones, ya sea descargada de satélite u obtenidas por el mismo en tiempo real, u otras aeronaves, en misiones anteriores de reconocimiento sobre la zona de operación. Esto no siempre es factible.

Sin embargo, existen otros sistemas que permiten una mayor protección frente al jamming de GPS. Estos sistemas obligan a que el jammer requiera J/S de 40 dB o incluso más, para ser efectivos. Con estos sistemas, la potencia de interferencia requerida para denegar la señal GNSS a 10 km en un RPA es de entre 800w y 80 KW dependiendo de los sistemas que se combinen. En este caso, ya no sería tan fácil y ni tan barato para el adversario perturbar el GNSS.



Si nos interesara lograr una protección de +90dB frente al jamming de GNSS en nuestro RPAS

El GPS C/A es notablemente vulnerable a las interferencias, con una tolerancia limitada a las interferencias (típicamente J/S entre 20y 30 dB gracias a la ganancia de procesamiento que introduce el empleo de DSSS). El nivel típico de la señal GNSS en el receptor es de -163 dBW, es decir, por debajo del nivel de ruido del receptor (potencia ruido, N=K·T·B, por ejemplo, -138 dB para una señal en banda L de ancho de banda de 20 MHz).

Por ello, una interferencia de 2 W ubicada a 100 Km del receptor GNSS podría impedir la adquisición del código C/A. Un perturbador comercial de entre 30€ y 300€ bastaría para inutilizar el GNSS de un RPA de varios miles de euros.

Incluyendo ciertos sistemas se puede lograr una protección J/S= +90 dB. Es decir, entre 60 y 70 dB por encima de un receptor GPS C/A + INS.

Por lo tanto, al aumentar la J/S necesaria para que el jamming sea efectivo, el adversario tendrá que consumir más energía y dinero para intentar perturbar con éxito la señal GNSS.

Entender la necesidad en un PNT Resiliente para Defensa

La confianza de los militares en el GNSS es omnipresente, y los RPAS es una más de estas dependencias. Dependiendo de los datos de posicionamiento, navegación y sincronización (PNT) para la navegación y el posicionamiento de nuestros vehículos ya sean terrestres, marinos o aéreos y hasta la guía de armas de sincronización C4ISR. Sin embargo, no se puede garantizar la calidad de las señales GNSS. Imagínese si un oficial de inteligencia militar no pudiera acceder a información esencial para las operaciones de la misión o recibir datos precisos. El papel del PNT asegurado en los programas de defensa actuales es de vital importancia para la seguridad en todo el mundo.

Orolia tiene una larga historia de brindar a las agencias de defensa acceso a soluciones para asegurar el PNT prácticamente a prueba de fallos. Deben ofrecer datos PNT extremadamente confiables, seguros y de alta precisión en condiciones duras y móviles de las operaciones militares. La experiencia de Orolia en diversas tecnologías PNT ha dado como resultado un enfoque innovador en capas para las soluciones PNT. Orolia ofrece una plataforma configurable que combina productos de tamaño, peso y potencia pequeños con software de dirección de interferencias y una gama de fuentes de referencia PNT robustas para cumplir con requisitos específicos para tierra, mar o aire. Orolia es el líder mundial en un PNT Resiliente.

¿Qué es la Resiliencia en PNT?

El PNT Resiliente o RPNT es la convergencia de la tecnología tradicional de posicionamiento, navegación y sincronización con tecnología no tradicional y emergente para mejorar la confiabilidad, el rendimiento y la seguridad de las aplicaciones de misión crítica. La resiliencia ofrece información confiable de tiempo y ubicación al proteger, autenticar y ofrecer alternativas a las fuentes PNT existentes, como GNSS.

El impacto operativo de Resiliencia es la capacidad de detectar vulnerabilidades en GNSS, como incidentes de suplantación de identidad o interferencia, emitir alertas y proporcionar fuentes alternativas de navegación y posicionamiento.

¿Por qué es importante la sincronización en el PNT?

Determinar una posición precisa a partir de satélite depende de medir con precisión las distancias entre el receptor y el satélite, y eso depende de una medición muy precisa del tiempo de viaje de la señal de radio desde el satélite hasta el receptor, de ahí la importancia de la sincronización en el PNT.

Las señales proporcionadas por GNSS representan el estándar de oro en términos de disponibilidad y precisión. Sin embargo, la proliferación de dispositivos que degradan y niegan el GNSS entre actores estatales y no estatales pone en peligro esta información crítica. Los dispositivos PNT tradicionales utilizan varios componentes internos alternativos para mantener la retención de los datos PNT durante la pérdida de la entrada GNSS, pero son susceptibles de desviarse con el tiempo, lo que significa que la información se vuelve menos precisa. El PNT Resiliente hace que las aplicaciones PNT sean resistentes a la interferencia, el jamming y el spoofing de señales GNSS, y que sean adecuadas para operar en entornos con GNSS denegado.

¿Por qué podríamos necesitar PNT resiliente?

Las soluciones PNT resistentes se pueden implementar en la defensa en los centros de comando y en vehículo, barcos, personal y además aeronaves como las RPAS donde una discrepancia en la precisión, disponibilidad o estabilidad de los datos puede afectar la seguridad y el éxito de la misión de operaciones militares.

Las amenazas al GNSS afectan a numerosos sistemas de defensa militar entre los que están los RPAS, que dependen del GNSS confiable para la posición, la navegación y la sincronización. La pérdida de accesibilidad e integridad del GNSS se traduce directamente en operaciones degradadas y puede significar la diferencia entre el éxito y el fracaso de la misión o incluso la vida o la muerte.

Un investigación del Reino Unido en 2017 identificó que una pérdida de GNSS de 5 días le costaría a su economía más de 12 mil millones de Libras, destacando el valor fundamental de la señal y la creciente comprensión de que el GNSS como fuente de PNT debe ser tanto protegido como confiable, naciendo así el término de PNT Resiliente o RPNT.

¿Cuáles son las amenazas más comunes para el GNSS?

Muchos sistemas militares digitales dependen de GNSS para proporcionar los datos PNT confiable que permiten a las Fuerzas Armadas (FA) maniobrar, comunicarse, comprender y tomar decisiones en el campo de batalla moderno. Las señales GNSS son muy débiles cuando llegan a la Tierra y, dado que estas señales son omnipresentes en el funcionamiento de los

sistemas militares, las amenazas a la disponibilidad e integridad de la señal GNSS están aumentando. Los actores de amenazas estatales y criminales modernas tienen pocas dificultades para obtener acceso a dispositivos portátiles y que pueden bloquear y falsificar señales. A media que el uso de GNSS se extiende a más aplicaciones móviles más lejanas, se debe tener en cuenta incluso el terreno natural y urbano al considerar la disponibilidad de PNT.

Jamming e interferencia se usan con frecuencia como sinónimos. La interferencia generalmente se refiere a la interferencia intencional por medio de una señal de radiofrecuencia. La interferencia a veces se usa en el contexto de causas naturales como los fenómenos atmosféricos. El efecto es el mismo para ambos: la capacidad del receptor GNSS para extraer información de la señal GNSS del ruido de fondo se ve afectada y se vuelve imposible interpretarla. La suplantación de identidad (Spoofing) es el acto de transmitir señales falsas con la intención de engañar a un receptor GNSS para que acepte las señales falsas como genuinas. Desde una perspectiva técnica, el spoofing de receptores GNSS es más desafiante que la interferencia y las consecuencias son más graves porque el receptor en realidad usa las señales manipuladas para los cálculos de PNT. Ni el sistema ni el operador se dan cuenta de que los datos PNT indicados se han dañado. El spoofing puede reubicar el receptor, lo que no es posible con la interferencia o jamming. El spoofing no es una tarea fácil, especialmente si el objetivo del spoofing se está moviendo rápidamente. Pero ya se ha hecho, y tanto las agencias gubernamentales como los operadores privados de infraestructura crítica consideran que la amenaza es real y creciente.

¿Cómo protege el PNT resiliente contra las discrepancias de GNSS?

Las tácticas y la tecnología utilizadas para combatir la interferencia y la suplantación de identidad se conocen como interferencia, detección y mitigación (IDM). La integración de una solución IDM sólida y bien coordinada en un sistema PNT lo hace resistente contra interferencias y spoofing, lo que garantiza la continuidad de los datos PNT críticos incluso en entornos con GNSS denegado.

¿Cómo se puede detectar la interferencia de la señal PNT?

La detección rápida y correcta de un evento de interferencia implica el uso de toda la información disponible para alertar y notificar a los usuarios de un sistema PNT basado en GNSS sobre la presencia de una amenaza. Los receptores GNSS están cada vez más equipados con funciones de detección de interferencias que informarán al usuario de una situación de interferencia / negación GNSS, ofreciendo al menos una opción de un diagnóstico más rápido en caso una pérdida de señal inesperada. Un enfoque relativamente nuevo para detectar ataque de interferencia o spoofing es una solución software que se puede instalar en sistemas basados en GNSS, donde monitorea la banda de frecuencia de la señal mediante la aplicación de algoritmos de detección de errores. El software puede detectar si un receptor GNSS está recibiendo un spoofing o jamming o si la señal se vuelve demasiado débil o se pierde, el servidor de tiempo emitirá una alarma e invalidará la información PNT antes de que pueda contaminar la solución de navegación interna o la base de tiempo.

¿Cómo se puede mitigar la interferencia de la señal?

La mitigación en el PNT significa que, después de aislar la señal no deseada, se rechaza y reemplaza rápidamente, lo que provoca una degradación mínima del sistema o RPAS. Para el RPAS militar, la primera medida de mitigación suele ser el uso de antenas anti-interferencias ya sean CRPA activas (Controlled Radiation Pattern Antennas) o pasivas. La siguiente medida de

mitigación puede incluir el uso de tecnología encriptada como SAASM/M-Code (Selective Availability Anti-Spoofing Module) siempre que sea posible, y/o el uso de receptores multifrecuencia. Otro enfoque es utilizar receptores GNSS que sean capaces de recibir y procesar de forma independiente cada constelación y luego comparar las señales en vivo para detectar cambios sospechosos. Otros enfoques técnicos bien establecidos para hacer frente a la pérdida temporal de señales GNSS son a través de soluciones de reserva, como osciladores para temporización y sistemas de navegación inercial (INS) para sistemas de navegación.

¿Qué más se necesita para el PNT resiliente?

Otro aspecto vital del PNT resiliente es probar el equipo PNT para determinar su vulnerabilidad real contra jamming y spoofing. Esto implica el proceso de mejora continua a través de la replicación de amenazas en el laboratorio para innovar y adoptar nuevas estrategias de detección y mitigación. Las amenazas se pueden simular con simuladores GNSS en el laboratorio de pruebas para comprender cómo reacciona un receptor RPAS en una situación de spoofing o jamming, o para evaluar las estrategias de mitigación existentes. El objetivo de la prueba es fortalecer un sistema PNT mediante la compresión de cómo reacciona el receptor GNSS de nuestros sistemas RPAS ante jamming o spoofing, implementando una técnica de mitigación y luego probando y modificando el sistema mejorado.

¿Es real la amenaza al PNT?

Hay una creciente comprensión de los riesgos de PNT sin garantía. Los ejemplos recientes de vulnerabilidades incluyen una interrupción prolongada del GPS en el norte de Noruega durante un ejercicio militar ruso en 2017, la conocido como el spoofing del GNSS/AIS del Mar Negro donde se informó posiciones de alrededor de 20 barcos en 2017; otro donde un conductor de furgoneta interrumpió un aterrizaje basado en GPS que se estaba probando en el aeropuerto internacional de Nueva Jersey; y un caso de jamming a barcos pesqueros que provoco un gran atasco de barcos atribuido el ataque a Corea del Norte. Las capacidades resistentes de ONT son fundamentales para la continuidad de las operaciones de apoyo a las fuerzas militares terrestres, marítimas y aéreas que operan en condiciones con GNSS limitado o denegado.

Tecnología LIDAR

LIDAR es el acrónimo de Light Detection and Ranging, es decir, detección por luz y distancia. Se trata de un sistema láser que permite medir la distancia entre el punto de emisión de ese láser hasta un objeto o superficie. El tiempo que tarda ese láser en llegar a su objetivo y volver del mismo es lo que nos dice la distancia entre los dos puntos. El resultado es que se puede obtener un mapa en ·D de alta resolución para conocer el terreno en cuestión.

El escáner láser de LIDAR funciona de forma aerotransportada y trabaja con dos movimientos: el de trayectoria de la RPA (longitudinal) y el del espejo que refleja la luz que llega desde el láser (transversal). Con ellos, es capaz de obtener un completo mapa de puntos del terreno que permite conocer su geografía de manera detallada. Para realizar sus mediciones, emplea un sistema GNSS, una Unidad de Medición Inercial (IMU) y el sensor láser.

Las aplicaciones de LIDAR se dan, sobre todo, en el mundo de la geodesia: el estudio de la geología que establece la forma y magnitud de una superficie, y mediante la cual se pueden diseñar los mapas que todos necesitamos usar. LIDAR permite captar los datos desde las alturas.

Su uso es un gran avance respecto a los métodos analógicos pues los datos resultan mucho más precisos al poderse generar Modelos Digitales de Elevación del terreno (MDE).

LIDAR es una tecnología tremendamente útil para conocer el terreno y sus características, pero también para alcanzar un navegación autónoma de los RPAS siendo capaz de navegar en lugares previamente mapeados en ambiente de negación de GNSS.

Los usos de LIDAR son muchos y nos abren un gran mundo de posibilidades.

Los RPAS equipados con cámaras ofrecen un par de ojos adicionales en el cielo, proporcionando una nueva perspectiva a las operaciones que se realizan sobre el terreno. Al desplegar un RPAS equipado con un sensor LIDAR, las empresas pueden realizar lecturas aéreas más precisas, creando modelos 3D con una precisión centimétrica y detectando características que serían invisibles con métodos menos sofisticados.

Lejos de ser un área tecnológica de nicho, el LIDAR está llegando a todo tipo de industrias que necesitan de cartografía y recopilación de datos geoespaciales. Si seguimos los últimos usos de los drones con sensor LIDAR, podremos determinar si los RPAS militares pueden encajar en los planes estratégicos de las FAS.

El LIDAR es una forma de tecnología de teledetección. En lugar de emplear cámaras fotográficas convencionales, los sensores LIDAR envían rápidos impulsos láser y captan las respuestas, utilizando esos puntos de datos para cartografiar una zona con gran precisión y exactitud.

El sistema LIDAR crea una nube de puntos con los datos que devuelven los objetos sobre el terreno. Estos puntos son la materia prima de los modelos 3D. Aunque el ensamblaje de estos modelos requiere un software especializado y expertos que sepan utilizarlo. El proceso es relativamente rápido y genera mapas de alta calidad con archivos de pequeño tamaño.

Sin embargo, hay que tener en cuenta que estas imágenes 3D no tienen detalles fotográficos. Por ejemplo, los propios impulsos láser no permiten conocer los colores de los objetos del suelo. Esos datos tendrán que proceder de una fuente alternativa, como un sensor adicional.

La tecnología LIDAR ha experimentado algunos avances en los últimos años: los módulos de los sensores son cada vez más asequibles y mucho más ligeros. Esto ha permitido la rápida evolución de los sistemas de RPAS equipados con LIDAR, con la aparición de nuevos modelos que permiten aplicar la tecnología a más casos de uso.

En lugar de ser obra de una sola empresa, los sistemas LIDAR, están siendo desarrollados por múltiples proveedores, como Livox y Velodyne. Integradores de sistemas como GreenValley, YellowScan, Emescent y LiDARUSA se encargan de convertir los componentes tecnológicos en módulos comercialmente utilizables.

En comparación con el LIDAR, los sistemas de fotogrametría pueden tener dificultades para captar objetos muy pequeños y con detalles muy precisos: por ejemplo, mientras que los pulsos del LIDAR pueden captar las líneas eléctricas, las fotos tomadas por los módulos de fotogrametría podrían no detectar los cables. El LIDAR también es capaz de penetrar a través de la vegetación para captar la forma del terreno subyacente, e incluso puede trabajar en la oscuridad.

La principal razón para elegir la fotogrametría ha sido su relativa accesibilidad. Con módulos más ligeros que se adaptan mejor al vuelo de los RPAS en sus misiones actuales dentro de los ejércitos.

A medida que el peso del LIDAR se reduzca, las matemáticas pueden cambiar para el desarrollo de nuevos RPAS que incorporen esta tecnología para crear modelos sobre los que poder navegar de manera autónoma.

El Ejército de Tierra lidera el desarrollo del nuevo RPAS táctico europeo

El denominado NGSR (Next Generation Small RPAS) involucra a España y a otros seis países. Deberá estar listo en 2028

A la hora de hablar de cualquier programa militar los titulares suelen centrarse en los grandes proyectos cuando, en realidad, muchas veces son igual de importantes aquellos que pasan más desapercibidos. Ese es el caso del NGSR. Su hermano mayor, el denominado Euromale o Eurodrón, el gran RPAS europeo (26 metros de envergadura) que competirá en los mercados del mundo con el mítico Predator estadounidense siempre se ha llevado todas las portadas, pero el programa del pequeño NGSR y sus menos de 150 Kg de peso ya está en marcha y España liderara el proyecto.

Es importante tener en cuenta que Europa siempre ha ido por detrás de EE. UU. o Israel en tecnologías dron, un sector que la UE ha querido potenciar dentro de su estrategia común en un momento (guerra de Ucrania) en el que, encima, estos sistemas se han revelado como imprescindibles. El desarrollo del sector es uno de los puntos de referencia para lograr la autonomía estratégica impulsada por la Brújula Estratégica de la UE, publicada hace escasos meses.

Siete países, España, Alemania, Portugal, Francia, Austria, Hungría y Países Bajos, y una institución supranacional, la Agencia de Defensa Europea del Estado Mayor de la UE, han dado los primeros pasos para el desarrollo del nuevo dron táctico europeo, el NGSR, un proyecto incluido en la denominada Cooperación Estructurada Permanente (Pesco). El RPAS no es el único proyecto de este programa ni el único en que está implicada España. Junto al NGSR está el proyecto Amida para desarrollar un sistema de mapeo e identificación de estructuras urbanas utilizando tecnología 3D basado en los RPAS fabricados en España.

El programa NGSR estará dirigido por el Ejército de Tierra español que, a finales del pasado mes de junio, organizo las primeras sesiones de los grupos de trabajo. Los países socios y la UE, bajo la coordinación española, volverán a verse las caras durante noviembre en las instalaciones de la Agencia de Defensa Europea.

El RPAS no será diseñado únicamente para uso militar, sino también civil, una dualidad que ya se ha convertido en habitual en los sistemas militares por varias cuestiones, que van desde conseguir una mayor rentabilidad para la industria implicada a la cada vez mayor tendencia a compartir sistemas, conceptos e incluso personal entre los diferentes Ministerios, de Defensa a Interior pasando por Infraestructuras o Agricultura, por ejemplo.

En el ámbito puramente militar, el proyecto nace ante la necesidad de las Fuerzas Armadas europeas de un RPAS táctico capaz de despegar y aterrizar sin necesidad de contar con una

pista de aterrizaje o cualquier otra infraestructura compleja y no portátil para dar servicio a unidades de tipo brigada/división. Su misión será mejorar las capacidades en ISR (reconocimiento, vigilancia e inteligencia), C2 (mando y control), Early Warning (alerta temprana), Targeting (designación de objetivos), NRBQ (guerra nuclear, radiología, biología y química), C-IED (explosivos y operaciones cinéticas, también tendrá la posibilidad de ir armado.

El dron deberá incluir “sensores y designador láser, comunicaciones y diferentes módulos en función de las cargas de pago cuyo desarrollo e integración se acuerde por la naciones”, es importante esa versatilidad para que el sistema pueda adecuarse a las necesidades de cada país comprador. El objetivo es desarrollar un sistema basado en cuatro principios: arquitectura abierta, capacidades autónomas, modularidad e interoperabilidad.

El encargado de fabricarlo será el consorcio industrial europeo en el que España se espera que tenga un peso importante. En este sentido, desde Tierra se recordó que el proyecto “constituye una oportunidad para que las empresas de la industria de la defensa desarrollen proyectos de I+D y expandan su negocio en áreas en las que la UE aspira a incrementar capacidades como en inteligencia artificial, sistemas no tripulado, armamento o comunicaciones.

Operación NAVWAR para denegar Posicionamiento, Navegación y referencia de tiempo

Se emplea un supuesto táctico en el cual un adversario antes de iniciar un despliegue de fuerza realiza una denegación de GNSS en la Zona de Operaciones.

Su objetivo es impedir el acceso, en un área circular con un radio de hasta 100 Km, del servicio de Posicionamiento por satélite GNSS con código C/A y del Servicio de Posicionamiento Preciso (PPS) con código P (Y) en las bandas L1 y L2. Para ello, se posiciona a 10 Km del borde de dicha área.

Su Unidad de Guerra Electrónica dispone de tres tipos de jammers: J1 con una potencia de transmisión de 10W; J2 con una potencia de 100W y J3 con una potencia de 1Kq. En todos los casos, se emplean antena con ganancia 10 dB.

Los satélites GNSS orbitan a una altitud de 20200Km.

Banda L1 (1575.42 MHz) -> código C/A (SPS), código P (Y) para PPS.

Banda L2 (1227.6 MHz) -> código P (Y) para PPS.

La potencia radiada efectiva ERP = Pt + Gt es:

56,8 dBm para C/A

53,8 dBm para P (Y) en L1

49,7 dBm para P (Y) en L2

Con Gt= 13 dB

Tomaremos la ganancia de antena en un receptor GPS como Gr= 4 dB

GPS utiliza DSSS. De tal modo que, el código C/A emplea un ancho de banda de 2 MHz para

transmitir señales de 50 MHz. Esto le proporciona una Ganancia de Procesamiento Gp = 46 dB. Mientras que el código (Y) emplea un ancho de banda de 20 MHz para transmitir señales de 50 Hz. Esto le proporciona una Gp = 56 dB.

La potencia recibida es:

Pr=Pt + Gt – [32,44 + 20 Log D + 20Log F + Latm] +Gr

Para L1 C/A: Pr = -125,64 dBm

Para L1 P (Y): Pr = -130, 64 dBm

Para L2 P (Y): Pr= -132, 74 dBm

La potencia de reído para C/A en el ancho de banda de 2 MHz es de -110 dBm. Sin embargo, debido al empleo de DSSS, se introduce Gp = 46 dB. Por lo tanto, las señales pueden recuperarse recibiendo por debajo del ruido de fondo -100-46=-156 dBm.

La relación interferencia a señal es:

J/S= ERPj -ERPs -Lj + Ls + Grj – Gr

Para L1 C/A

J/S=38,8 dB

[J/S] eff=J/S -Gp=38,8-46dB= -7,2 dB< 0

Con un jammer de 10W no es factible.

J/S=48,8 dB

[J/S] eff = J/S -Gp=48,8-46dB= 2,8 dB> 0

Con un jammer de 100W si es factible.

Para L1 P(Y):

J/S=41,8 dB

[J/S] eff=J/S -Gp=41,8-56dB= -14,2 dB< 0

Con un jammer de 10W no es factible.

J/S=51,8 dB

[J/S] eff = J/S -Gp=51,8-56dB= -4,2 dB< 0

Con un jammer de 100W no es factible.

J/S=61,8 dB

[J/S] eff = J/S -Gp=61,8-56dB= 5,8 dB> 0

Con un jammer de 1KW sí es factible.

Para L2 P(Y):

J/S=45,9 dB

[J/S] eff=J/S -Gp=45,9-56dB= -10,1 dB< 0

Con un jammer de 10W no es factible.

J/S=55,9 dB

[J/S] eff = J/S -Gp=55,9-56dB= -0,1 dB< 0

Con un jammer de 100W no es factible.

J/S=65,9 dB

[J/S] eff = J/S -Gp=65,9-56dB= 9,9 dB> 0

Con un jammer de 1KW sí es factible.

La Vulnerabilidad de los RPAS Bayraktar TB2 en Ucrania

La libertad de acción que caracterizó las operaciones con RPAS en las últimas décadas está disminuyendo rápidamente, con la introducción de guerra electrónica, interferencias en las comunicaciones y sistemas antiaéreos. Gran parte de los RPAS actuales no pueden llevar a cabo operaciones en espacio aéreo/electromagnético denegado o disputado.

Los RPAS Bayraktar TB2 que fueron muy útiles para Ucrania al principio de la guerra contra Rusia, han perdido gran parte de su utilidad al ser incapaces de penetrar el espacio aéreo defendido por sistemas antiaéreos desplegados por las fuerzas rusas, y que se basa en una triple capa:

(1) Los S-400 y S-300 de largo alcance para defensa de media y gran altitud;

(2) Los Buk-M2/M3 para defensa de media y baja altitud; y

(3) Los TOR-M1/M2 para defensa de corto alcance a baja y muy baja altitud; junto con sistemas SHORAD como Tunguska, Sosna y MANPADS.

Por otra parte, esta capacidad defensiva de tipos cinéticas, consistentes en una gran concentración de medios que han identificado las frecuencias de transmisión de los TB2, las cuales están siendo interferidas, provocando la pérdida de control de los RPA. Los TB2han experimentado la interrupción o manipulación por parte de los rusos de sus enlaces C2 desprotegidos, lo que conduce al fracaso de sus misiones de combate.

Se debe asumir que, la mayoría de la generación actual de RPAS son incapaces de llevar a cabo las mismas misiones en entornos disputados/ contestados, que ahora realizan en entornos no disputados, no contestados. Por lo tanto, es necesario introducir cambios importantes en los RPAS actuales, para prepararlos para las operaciones en entornos anti-acceso y de zona denegada (A2/AD).

Los RPAS deben transformarse para poder sobrevivir y operar en entornos no benignos, donde el adversario dispone de medios para evitar la libre circulación y proyección de fuerzas enemigas. Estos cambios afectan a tres áreas principales:

A. La integración de ayudas a la navegación protegidos,

B. Enlaces C4ISR protegidos,

C. Sistemas de autodefensa en los casos que proceda por misión y tamaño.

EW: actividad tecnológica y electrónica con el fin de determinar, explotar, reducir o impedir el uso hostil de todos los espectros de energía, por parte del adversario y a la vez conservar la utilización de dicho espectro en beneficio propio.

La PI 17/28 solicita literalmente la siguiente información:

“Capacidad de neutralización de RPAS mediante la inhibición / interferencia de su señal de mando (jamming). Se tiene conocimiento del amplio empleo de esta TTP durante el conflicto de Ucrania”.

“La finalidad de la solicitud es conocer el grado de implementación de este tipo de contramedidas en el ámbito de otros ejércitos, al objeto de impulsar e incorporar esta capacidad a las Organizaciones Operativas nacionales que se constituyan, atendiendo a las necesidades de Protección de la Fuerza en Operaciones”.

Anexo III Informe del Oficial de Enlace de la US Army en el TRADOC

Tcol D. José A Fernández Alfaro (OFEN en el TRADOC)

“La información disponible sobre este tema en el US Army es únicamente la procedente de fuentes abiertas, ya sean del propio US Army o de publicaciones en páginas web.”

La información accesible y disponible para este OFEN en el Mando de Adiestramiento y Doctrina del US Army (TRADOC) acerca de cómo las unidades del US Army están organizadas o las técnicas, tácticas y procedimientos (TTP) que emplean para interferir un RPAS es realmente mínima.

Russian New Generation Warfare Handbook

Interesante para conocer la evolución del concepto de guerra (asimétrica, hibrida, etc.) o como las fuerzas rusas han evolucionado en un nuevo tipo de conflicto, como es el de Ucrania, en este caso, el interés viene dado por la descripción de los medios EW empleados por las fuerzas rusas para interferir los RPAS.

En concreto, en las páginas 14 y 15 se detallan las características del RP-377 L/LA de los R330 y SPR-2 (RTUIT):

En la página 23 trata los sistemas RPAS (empleo, medios disponibles, tácticas, etc.) y en la 37 y siguientes, como operar en entorno de presencia de unidades de EW y cómo reaccionar ante la presencia de RPAS.

El documento en su conjunto es muy válido en opinión de este OFEN TCol Fernández Alfaro destinado en el TRADOC, y es uno de los pocos documentos que he podido tener acceso del US Army que describen las TTP rusas empleadas en Ucrania.

Noticias en fuentes abiertas

Aunque las noticias aparecidas en fuentes abiertas son difíciles de contrastar, se detallan aquí algunas de las informaciones recibidas acerca de interferidos de RPAS.

La página web del US Army publicaba información sobre el denominado High Energy Laser Tactical Vehicle Demonstrator (HEL TVD), cuya finalidad es la protección contra amenazas tipo misiles, munición de artillería y de morteros y RPAS

Se trata de un sistema de 60 kilovatios, con anterioridad ya se ha probado el High Energy Laser Mobile Test Truck (HELMTT), con capacidad de emisión de hasta 10 KW.

La Página web C4ISRNET cita el desarrollo de iniciativas como la de Boeing, que han creado el Compact Laser Weapon System (CLWS), un sistema capaz de derribar un RPA de Clase I, con una emisión de 10 segundos de láser, durante el ejercicio Black Dart.

Como mejorar la resistencia al jamming de enlace de datos en RPAS

La mayoría de los RPAS disponibles comercialmente operan con radio módems en 433 MHz,

869MHz, 915 MHz, 2400 MHz o 5800 MHz. Por lo tanto, los sistemas C-UAS recuren a inhibir dichas frecuencias.

Suponemos un rifle anti RPA operando en 2400 MHz (el 80% de los drones comerciales operan 5,8 GHz y/o 2,4 GHz) con una potencia de transmisión de 50 dBm y una ganancia de antena de 5 dBi.

Por otra parte, los RPAS emplean un radioenlace de 2,4 GHz con una potencia de transmisión de 3 dBm, antena en RPA con ganancia de 5 dBi y antena con ganancia en estación de tierra de 14 dBi.

Por simplicidad, consideraremos una distancia de 10 Km entre la estación de tierra y el RPA, e igualmente otros 10 Km de separación entre el sistema anti-dron y el RPA.

La relación entre la señal de interferencia (en el receptor) y la señal deseada (en el receptor) es lo que denominamos relación de interferencia a señal (J/S. Esta relación se puede calcular como:

J/S = ERPj – ERPs – Lj + Ls + Grj – Gr

Calculando la Perdida de propagación como L(dB)= 20log10(d) + 20log10(f) + 32,44(dB)

Cuando se interfieren señales de comunicación moduladas analógicamente, normalmente, es necesario lograr un J/S de al menos 10 dB.

En cambio, cuando interferimos señales de comunicación modulados digitalmente, cuando J/S llega a 0 dB, la tasa de error de bit está muy cerca del 50%. Por lo tanto, cualquier J/S superior a 0 dB interferirá con éxito al RPA.

Si el enlace de datos del RPAS opera en frecuencia fija a 2,4 GHz, considerando que el jammer y la estación de tierra están equidistantes del RPA, y que la antena receptora del RPA tiene la misma ganancia hacia el jammer y hacia el transmisor de la estación de tierra:

J/S = 55 dBm – 42 dBm = 13 dBm

Por lo tanto, el jamming del RPA será efectivo.

La modulación de espectro ensanchado introduce una ganancia de procesamiento Gp, que permite mitigar las interferencias de un jammer. La ganancia de procesamiento disminuye la potencia de interferencia efectiva en el receptor por la cantidad de Gp. Por lo tanto, en el receptor, el J/S efectivo se reduce por dicha ganancia de procesamiento.

Cuanto mayor sea Gp, mayor será el grado de rechazo a las interferencias.

Supongamos un sistema DSSS con una tasa de código (Rc) de 15 Mbps frente a una tasa de datos (Rb) de 500 Kbps □Gp = 10log (Rc/Rb) =15dB

Supongamos un sistema FHSS con 1000 frecuencias de salto□Gp~30dB

En estos casos:

Si el enlace de datos del RPA opera un DSSS: J/S=-2 dB

Si el enlace de datos del RPA opera en FHSS: J/S= -17dB

Por lo tanto, introduciendo medidas de protección electrónica el jamming del RPA ya no será efectivo.

Autodefensa para RPA frente a amenazas radar

Supongamos un radar de vigilancia con una potencia de transmisión de 100 KW (80dBm), antena con ganancia 30 dBi, sensibilidad del receptor de -96 dBm, operando con una frecuencia de 10 GHz (Banda X).

Supongamos un RPA de clase I con sección radar RCS=-15dBSm ($0.03m^2$) en la banda X. El RPA dispone de un alertador Radar (RWR) que opera de 0,5 a 18 GHz con una sensibilidad de -35 dBm. RWR emplea antenas con una ganancia de 0dBi a 10 GHz.

¿Cuál es la máxima distancia a la que el alertador radar puede detectar la señal del radar de vigilancia? Necesitamos conocer la distancia de detección del Radar vs la distancia de detectabilidad del Radar por el Alertador Radar.

40 log(D)=-103 + Pt + 2G- 20log(f) + 10 log (RCS) - Sen(s)

Donde:

D: la distancia desde el radar hasta el objetivo (Km);

Pt: potencia del transmisor del radar (dBm);

G: ganancia de antena del radar (dBi);

f: frecuencia de operación del radar (MHz);

RCS: sección radar del objetivo (m2);

Supondremos que la potencia recibida es igual a su sensibilidad.

Por lo tanto:

40 log (D) = -103 + 80 dBm + 2(30) dBi – 20 log (10000) dB + 10 log (0,03) – (-96) dBm=38 dB
 D=8,9 Km

Es decir, la distancia de detección del radar para blancos con RCS típicos del RPA es 8,9 Km.

Por otra parte, el balance de potencia en el enlace del radar RWR es:

Pr =Pt +Gt - 32 - 20 log(f) - 20 log(d) + Gr

Donde:

Pr=potencia recibida en RWR (dBm);

Pt= potencia del transmitida por radar (dBm);

Gt= ganancia de la antena del radar (dB);

f = frecuencia transmitida (MHz);

d = distancia del radar al RWR (Km);

Gr= ganancia de la antena del RWR (dB).

Consideraremos que la potencia recibida por RWR es igual a la sensibilidad de su receptor. Es decir:

Pr= Sen(s)= Pt + Gt -32 – 20 log(f) – 20 log (d) + Gr

20log (d) = Pt + Gt – 32 – 20log(f) + Gr – Sen(s)

Así pues:

20 log(d) = 80 dBm + 30 dBi - 32 – 20 log (10000) + 0 dBi – (-35dBm) =33 dB □ d = 44,7Km

Por lo tanto, el RWR del RPA puede detectar al radar de vigilancia a casi 50 km; mientras que el radar puede detectar al RPA a mucha menos distancia, casi 9 Km. Es decir, el RPA será consciente de la presencia del radar hostil mucho antes de que este se percate de su presencia. Esto se traduce en una ventaja para su capacidad de supervivencia.

Supongamos ahora que el RPA dispone de un jammer para autodefensa con una potencia de transmisión de 10 W y una antena con una ganancia de 6 dBi. La relación señal a interferencia del jammer es:

J/S= ERPj – ERPs + 71 + 20 log R – 10 log RCS = 24,6 dB

Por lo tanto, el RPA conseguirá perturbar al radar hostil antes de que este pueda detectar su presencia.

Suite de autodefensa

La autoprotección de las aeronaves depende de conocer fiablemente si algún adversario está empleando un sistema de armas para un ataque potencial. Esto requiere proporcionar una información fiable de las posibles amenazas, descartando las falsas alarmas y detectando e identificando las amenazas reales para aplicar las contramedidas oportunas.

Para ello, el personal de mantenimiento y las tripulaciones deben comprobar la efectividad operacional de su suite de autodefensa durante la pre-vuelo antes de ejecutar una misión, asegurando la plena confianza en el sistema de autoprotección de su aeronave.

Además, los equipos de prueba en ML1 permiten reducir la tasa de No-Fault-Found, detectando fallos no cubiertos por el BIT de los sistemas.

Hasta hace poco, solo se disponía de equipos dedicados para probar Alertadores Radar, otros equipos específicos para probar Alertadores de Misiles y otros para Alertadores Láser. Sin embargo, ahora se disponen de equipos multi-role que permiten probar todos los alertadores.