Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Desarrollo de un sistema de Guerra Electrónica para la detección y perturbación de radares marinos en banda X

Grado en Ingeniería Mecánica

ALUMNO: Manuel González de Canales Martínez

DIRECTORES: José María Núñez Ortuño

CURSO ACADÉMICO: 2019-2020

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Desarrollo de un sistema de Guerra Electrónica para la detección y perturbación de radares marinos en banda X

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

El fin de este trabajo es despertar la conciencia sobre la importancia de la Guerra Electrónica en la formación de los futuros oficiales de la Armada, mediante el diseño de un sistema de detección y perturbación para radares marinos en banda X, compatible con el radar de las Lanchas de instrucción de la ENM.

Está compuesto por una primera fase de detección en la que el sistema es capaz de detectar, procesar y obtener los parámetros principales de la señal radar enemiga recibida. Esta fase es llevada a cabo a través de la generación de un algoritmo capaz de procesar la señal.

Una vez obtenidos estos parámetros e identificada la unidad emisora, se pasa a la fase de perturbación, donde el sistema es capaz de generar jamming sobre los pulsos recibidos, anulando en un sector toda recepción de blancos al radar enemigo y enmascarando todo el sector, incluso estando el sistema embarcado en navegación. El sistema fue probado en los radares Furuno de las Lanchas de instrucción, y también en el radar del sistema LIBRA del CEMEDEM.

PALABRAS CLAVE

Guerra Electrónica, Lancha de instrucción, Radar, Jamming, Detección

AGRADECIMIENTOS

Al profesor José María Nuñez Ortuño, por su constante apoyo y tiempo dedicado al proyecto, por su gran ayuda sin la cual este trabajo, tan experimental en ciertas partes, no podría haber salido adelante.

Al Capitán de Corbeta Antonio Valles Castro, por su consejo y ayuda durante el desarrollo del proyecto.

Al Centro de Medidas Electromagnéticas de la Armada (CEMEDEM), y al personal del Núcleo de Lanchas de instrucción por sus medios y recursos facilitados.

A mi familia, que desde que entré por la puerta de Carlos I, han sido mi apoyo fundamental durante estos cinco años de trabajo y dedicación.

A mi abuelo Fernando, que vivió los inicios de la Guerra electrónica en España.

A Luisete, que nos cuida desde allí arriba, y a toda la Promoción 420-150, en agradecimiento a estos años en los que me han demostrado ser como una segunda familia. Estoy seguro que lo seguiremos siendo durante toda la vida, sin dejar nunca solo a ningún compañero que nos necesite.

CONTENIDO

Contenido 1

Índice de Figuras 3

1 Introducción y objetivos 7

1.1 Contextualización 7

1.2 Motivación 8

1.3 Objetivos 9

1.4 Organización del trabajo 9

2 Estado del arte 11

2.1 La Guerra Electrónica 11

2.1.1 Historia de la Guerra Electrónica 11

2.1.2 La Guerra Electrónica en la Armada 12

2.1.3 Tipos de Guerra Electrónica 15

2.2 Sistemas de Guerra Electrónica. Equipos 17

2.2.1 Sistemas de detección 18

2.2.1 Sistemas de perturbación 20

2.3 Radar definido por software (SDR) 24

2.3.1 Down/Up-converter 24

2.3.2 SDR 26

3 Desarrollo del TFG 29

3.1 Investigación y recopilación de información 29

3.2 Hardware empleado 30

3.2.1 Radar Furuno 1944C 30

3.2.2 SDR HackRF 32

3.2.3 SDR Ettus N200 33

3.2.4 Oscilador 34

3.2.5 Alimentación del oscilador local 34

3.2.6 Mezclador 35

3.2.7 Antena 36

3.3 Software empleado 36

3.4 Diseño del sistema 37

3.4.1 Sistema receptor 37

3.4.2 Sistema de perturbación 44

4 Resultados / Validación / Prueba 49

4.1 Pruebas de detección 49
4.1.1 Pruebas con señal simulada 49
4.1.2 Pruebas con señal real 50
4.2 Pruebas de perturbación 51
4.2.1 Primeras pruebas 51
4.2.1 Pruebas de distintos tipos de señal 53
4.2.2 Pruebas en distancia 55
4.2.3 Pruebas en navegación 59
4.2.4 Pruebas Radar CEMEDEM 62
4.2.5 Calibración de radares 63
5 Conclusiones y líneas futuras 65
5.1 Problemas encontrados 65
5.1.1 Comportamiento interno del radar Furuno 1944C 65
5.1.2 Potencia de la antena jammer 65
5.2 Posibles líneas futuras 66
5.2.1 Sistema de perturbación inteligente 66
5.2.2 Calibrador de radares / Generador de diagramas de radiación 66
5.2.3 Perturbador de sistemas de comunicaciones o de otros radares 66
5.2.4 Sistema de jamming desde dron 66
5.2.5 Instalación fija del sistema de Guerra Electrónica en las lanchas de instrucción 67
5.3 Contrastación de resultados 67
5.4 Conclusión personal 68
6 Bibliografía 69
Anexo I: Siglas y Acrónimos 72
Anexo II: Contramedidas radar comunes 75
Anexo III: Código algoritmo de detección 76
Anexo IV: Código de carga de datos 79
Anexo V: Código de cálculo del PDW 80
Anexo VI: Código de diagrama de radiación de la antena 82
Anexo VII: Tabla de órdenes del ejercicio EWX 220 en la prueba de navegación 84
Anexo VIII: Código de generador de señal 85
Anexo IX: Especificaciones radar 1944C Furuno 87

ÍNDICE DE FIGURAS

Figura 1-1: Lanchas de Instrucción de la ENM [5] 9
Figura 2-1: Portaeronaves *Dédalo* con aviones Harrier sobre cubierta de vuelo [5] 12
Figura 2-2: Mástil de la Fragata *Asturias* con su sistema *Canopus* [2] 13
Figura 2-3: Mástil de la Fragata F-101 *Álvaro de Bazán* con sistema *Aldebarán* [7] 14
Figura 2-4: Ejemplo de Contramedida (ECM) de tipo Jamming sobre un radar 17
Figura 2-5: Diagrama esquemático de los componentes de un Sistema de Guerra Electrónica [8] .17
Figura 2-6: Ejemplo receptor ELINT en un sistema de Guerra Electrónica [40] 18
Figura 2-7: Pulso radar y parámetros principales [16] 19
Figura 2-8: Gráfica Burn-Through y Crossover Range [17] 21
Figura 2-9: Diagrama SSJ y ESJ Diagrama SSJ y ESJ [17] 22
Figura 2-10: Saltos de frecuencia de un Swept-spot Jammer [16] 23
Figura 2-11: Fragata *Álvaro de Bazán* lanzando chaff [18] 24
Figura 2-12: Funcionamiento de un Down/Up Converter [40] 25
Figura 2-13: Réplicas armónicas generadas en el mezclador para RF=9.41 GHz [21] 25
Figura 2-14: Esquema funcionamiento del SDR [20] 26
Figura 2-15: Mezclador IQ [23] 27
Figura 2-16: Representación vectorial de las señales I y Q [19] 27
Figura 3-1: Radar Furuno 1944C [24] 30
Figura 3-2: Vista superior de la Lancha emitiendo [24] 30
Figura 3-3: Vista longitudinal de la Lancha [21] 31
Figura 3-4: SDR Hack RF 33
Figura 3-5: SDR Ettus N200 33
Figura 3-6: Oscilador ADF 5355-EVAL 34
Figura 3-7: DC/DC Converter 34
Figura 3-8: Fuente de alimentación 35
Figura 3-9: Mezclador de frecuencia 35
Figura 3-10: Antena Microstrip SO4100-8N 36
Figura 3-11: Esquema de la estructura del sistema receptor 38
Figura 3-12: Detección de señal radar con el programa SDR Console 39
Figura 3-13: Diagrama explicativo del código *detection.m* 39
Figura 3-14: Detección de un barrido de señal radar 40
Figura 3-15: Detalle de los pulsos dentro de un mismo haz con las marcas de TOA Y TOD 41
Figura 3-16: Código de determinación de valores de ancho de pulso válidos 41
Figura 3-17: Código para el cálculo del Ancho de pulso y PRI 42

Figura 3-18: Señal detectada tras el procesado CFAR (PFA constante)....42
Figura 3-19: Diagrama de radiación del radar de la Lancha Guardiamarina Barrutia....43
Figura 3-20: Detalle del lóbulo principal o ancho de haz de la señal del radar....44
Figura 3-21: Esquema de la estructura del sistema de perturbación....45
Figura 3-22: Diagrama de funciones de GNU Radio para generación de la señal de jamming....46
Figura 3-23: Barras deslizantes (*sliders*) en el programa GNU Radio....46
Figura 4-1: Señal generada simulando pulsos radar....49
Figura 4-2: Espectograma de la señal generada....49
Figura 4-3: Señal generada con SNR de 15 dB....50
Figura 4-4: Detección y grabación de señal radar....51
Figura 4-5: Jamming de ruido blanco con pulso corto en escala mínima....52
Figura 4-6: Jamming de ruido blanco con pulso largo con escala menor a 5 MN....52
Figura 4-7: Jamming de barrera con señal cuadrada y pulso largo....53
Figura 4-8: Señal jamming cuadrada 500 KHz....54
Figura 4-9: Jamming con señal cuadrada al disminuir su frecuencia....54
Figura 4-10: Jamming de señal cuadrada desde 30 m [34]....55
Figura 4-11: Montaje del sistema en el muelle de Torpedos con las lanchas al fondo....56
Figura 4-12: Jamming de señal cuadrada desde 170 m [34]....56
Figura 4-13: Trayectoria salida de puerto lancha perturbada....57
Figura 4-14: Jamming de señal cuadrada durante la desatracada....57
Figura 4-15: Jamming de señal cuadrada desde 50 m durante la salida de puerto....58
Figura 4-16: Jamming de señal cuadrada a 250 m durante la salida de puerto....58
Figura 4-17: Disposición de equipos en el CIC e instalación de la antena en el puente alto....59
Figura 4-18: Recreación de jamming entre lanchas....59
Figura 4-19: Lanchas entrando en formación en columna durante el ejercicio....60
Figura 4-20: Formación para ejecución del ejercicio EWX 220....60
Figura 4-21: Guardiamarina Chereguini vista de través durante el ejercicio....60
Figura 4-22: Jamming en navegación desde una distancia de 100 yardas (91 m)....61
Figura 4-23: Jamming en navegación a una distancia de 150 yardas (137 m)....61
Figura 4-24: Sistema LIBRA de Medidas Electromagnéticas del CEMEDEM....62
Figura 4-25: Jamming con señal cuadrada Radar CEMEDEM....63
Figura 4-26: Comparación de la dirección del jamming obtenido en radar alto (izquierda) y bajo (detecha)....63
Figura 5-1: Recreación de Jamming desde dron....67

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contextualización

Cuando hablamos de Guerra electrónica nos referimos a una dimensión distinta dentro de lo que es el enfrentamiento de fuerzas navales, aéreas o terrestres en un escenario bélico o de crisis. Comúnmente en un buque hablamos de guerra de superficie, guerra antiaérea y guerra antisubmarina, a estas debemos añadir la EW (*Electronic Warfare*), fundamental para una fuerza desplegada.

Definimos como Guerra electrónica todas aquellas acciones militares que comprenden el uso de energía electromagnética para determinar, explotar, reducir o prevenir el uso del espectro electromagnético por parte del enemigo, y permitir el uso del espectro por parte de la fuerza enemiga. [1]

En definitiva, esta guerra es principal para la detección del enemigo en una situación de crisis o tensión, actualizando la situación de contactos de superficie, teniendo así claras las intenciones del resto de buques de interés y generando información que puede ser constatada como inteligencia. Cabe mencionar también el uso de las medidas electromagnéticas como un arma de ataque (perturbación), negando el uso de sus propios sensores al enemigo o realizando decepción o engaño, creando confusión al enemigo.

La Armada Española desde principios de los años 60, vio la necesidad de implementar en sus buques equipos con capacidad de Guerra electrónica. En aquel momento, se empezó de forma tímida incluyendo equipos de diseño estadounidense en los buques. Sin embargo, con el tiempo, la evolución de la capacidad tecnológica de la industria nacional a lo largo de los años ha permitido no solo diseñar y montar nuestros propios equipos de EW, sino también exportarlos al exterior [2].

Esta guerra solía ser tratada como una guerra de segunda categoría en cuanto a adiestramiento y equipos en las unidades. Además, con motivo de la crisis económica que sufrió nuestro país a partir del año 2008, se redujo el presupuesto destinado a equipos y adiestramiento, incrementándose la brecha con los nuevos avances tecnológicos y tácticos.

En primer lugar, era principal mantener los equipos en funcionamiento y formar al personal que los opera, para así mantener sus capacidades. Esto, sumado al gran coste de los componentes de equipos tanto de Guerra Electrónica de comunicaciones como electromagnética, motivó la llegada a esta situación.

En segundo lugar, se suprimieron temporalmente los cursos de Oficiales y Suboficiales de EW. Además, se dejaron de publicar plazas para cursos de este mismo ámbito en la OTAN y España retiró su asistencia a las Juntas de Doctrina de EW de la alianza.

Por último, hubo una reducción del adiestramiento de las unidades, con la desaparición de los ejercicios nacionales de guerra electrónica (EWX, *Electronic Warfare Exercises*), que sirven para adiestrar a varias unidades simultáneamente y evaluar y adiestrar a personal en la materia. Se pedían equipos cedidos de la OTAN para este tipo de ejercicios, como el *Transvan* (contenedor embarcable que genera señales electromagnéticas para adiestramiento en la mar).

Ante esta situación en septiembre de 2018 el ALFLOT convocó un Seminario de EW, donde mostró su preocupación sobre la situación y se tomó acción emitiendo un plan de recuperación de la capacidad de ASMD (*Anti-Ship Missile Defense*), donde se encuentran medidas importantes para la EW. De esta iniciativa parte la publicación por parte del Centro de Doctrina de la Flota de la DSF-55 (*Doctrina Táctica de la Guerra Electrónica en la Armada*), que actualiza los obsoletos procedimientos y da una renovación a todo lo referente a esta guerra [3].

Estas medidas devolvieron el adiestramiento al personal, recuperando los cursos de EW, renovación y mejora de mantenimiento de equipos, volviendo a organizar ejercicios nacionales EWX y participando en los ejercicios NEMO de la OTAN.

Por último, el CESEDEN (Centro Superior de Estudios de la Defensa Nacional) ha convocado este año un Plan de Campaña de Desarrollo de Doctrina (2020-2025), con conferencias y seminarios, dentro de los cuales se integra la Guerra Electrónica como uno de los pilares fundamentales [4].

En definitiva, la EW se está reactivando y recuperando la relevancia que esta merece dentro del ámbito naval, siendo España puntera en el desarrollo y exportación de este tipo de equipos.

1.2 Motivación

La razón de ser de este trabajo parte de la necesidad de este impulso hacia la Guerra Electrónica tanto en medios como en formación. Este tema sigue siendo una preocupación dentro del Estado Mayor de la flota, que vigila el progreso de las medidas tomadas para la reactivación de la EW.

La realidad es que, en los buques de la flota, es primordial el mantenimiento de la operatividad de los equipos y la formación y adiestramiento del personal a través de cursos y ejercicios. Los mandos deben buscar mantener las capacidades en EW en sus unidades

Si el personal que va a liderar los buques en el futuro no está concienciado, la dejaremos de lado y pasará a ser una guerra olvidada pese a tener los equipos necesarios, por descuido, falta de interés y de formación.

Por ello es primordial concienciar a los alumnos de la Escuela Naval Militar (ENM), futuros oficiales de la Armada, de la importancia de la Guerra Electrónica. Para cuando llegue el día en sus unidades, puedan explotar al máximo los medios y personal que se les asignen en cuanto a esta guerra.

El camino es aprovechar asignaturas tanto militares como técnicas que tratan temas muy relacionados, llevando a cabo una intensificación en la realización de laboratorios, prácticas o actividades de instrucción y adiestramiento sobre estos temas comunes. Para ello, se podría dar uso de las Lanchas de instrucción y laboratorios de Centro Universitario de la Defensa, o ciertos momentos incluso de las instalaciones del CEMEDEM (Centro de Medidas Electromagnéticas de la Armada).

En definitiva, el sentido de este trabajo es concienciar sobre la importancia de la Guerra Electrónica en la Armada y sacar provecho de la formación técnica que reciben los alumnos de la ENM, para complementar su formación como futuros oficiales.

1.3 Objetivos

El objetivo de este trabajo es diseñar un sistema de funcionalidades básicas de guerra electrónica contra radares marinos en banda X. El trabajo se realizará en dos fases diferenciadas, una fase de detección, en la que se identificarán los parámetros principales de la señal recibida [5]. En la segunda fase se perturbará ese radar. La idea es comprobar el funcionamiento del sistema con un radar de superficie en banda X de la marca Furuno instalado en las Lanchas de Instrucción de la ENM (Figura 1-1).

La fase de detección tratará de obtener los valores del ancho de pulso (PW), el periodo de repetición de pulsos (PRI) y la frecuencia central en la que se emite el radar enemigo, para luego con estos datos realizar un jamming sobre el radar desde nuestra posición. El jamming requerido deberá anular un sector del radar enmascarando todo contacto en esa zona.

Se pretende testear el sistema para comprobar sus alcances en distancia, su comportamiento con el radar enemigo en movimiento o la generación de jamming con distintos tipos de señal. El fin último es probar el sistema en las propias lanchas de instrucción en navegación, y así comprobar su funcionamiento y dar lugar a posibles ejercicios de Guerra Electrónica en las que los alumnos de la ENM, puedan ampliar sus conocimientos en este ámbito, y poder aplicar su formación técnica en el adiestramiento a flote.

Figura 1-1: Lanchas de Instrucción de la ENM [5]

1.4 Organización del trabajo

En primer lugar se realiza una contextualización del trabajo tratando la historia de la Guerra Electrónica (Apartado 2.1), para luego profundizar en los orígenes de esta guerra en la Armada Española hasta la actualidad (Apartado 2.1.2). Más tarde se analizan las tres categorías más relevantes en las que se divide la Guerra Electrónica, explicando cada una de ellas (Apartado 2.1.3). En el siguiente apartado se exponen los sistemas de detección (Apartado 2.2.1) y perturbación (Apartado 2.2.1), explicando sus conceptos básicos y sus técnicas más utilizadas. Después, el trabajo se adentra en el ámbito del radar definido por software, hablando de los equipos y su funcionamiento (Apartado 2.3).

A continuación se explica el proceso de recopilación e investigación (Apartado 3.1), además de los equipos (Apartado 3.2) y software (Apartado 3.3) empleados en el transcurso del proyecto Se incluye también la explicación de las dos fases diferenciadas pero interconectadas del proyecto, la fase de detección (Apartado 3.4.1) y la fase de perturbación (Apartado 3.4.2). En esta parte se define tanto la

estructura del sistema como la configuración y funcionamiento de este para ambas fases. También se describe el procedimiento de la obtención del diagrama de radiación de la antena del radar.

Después de haber definido el sistema, se procede a describir las distintas fases de pruebas que se llevaron a cabo, divididas en fase de detección, donde se muestran el desarrollo de las pruebas con señal generada (Apartado 4.1.1) o real (Apartado 4.1.2), y perturbación. Además se expone cómo se han realizado las pruebas iniciales (Apartado 4.2.1), pruebas con distinto tipo de señal (Apartado 4.2.1), pruebas en distancia (Apartado 4.2.2), pruebas en navegación (Apartado 4.2.3) y una última prueba con la colaboración del CEMEDEM (Apartado 4.2.4). Además se incluye un apartado que muestra el posible uso del sistema para la calibración de radares de navegación (Apartado 4.2.5).

Finalmente, se presentan una serie de conclusiones sobre el trabajo, detallando los problemas encontrados (Apartado 5.1), posibles líneas futuras (Apartado 5.2), la contrastación de resultados (Apartado 5.3), y por último unas conclusiones personales (Apartado 5.4).

2 ESTADO DEL ARTE

2.1 La Guerra Electrónica

Today, the ability to operate and maintain presence within the electromagnetic spectrum – as well as the ability to deny its use to enemies – is a battlespace all its own, and one of the biggest challenges our military leaders face today.

Steve Mensh

"En estos días, la habilidad para operar y mantener nuestra presencia dentro del espectro electromagnético – como la habilidad de negarle su uso a los enemigos – es un campo de batalla en sí, uno de los mayores desafíos a los que se enfrentan nuestros líderes militares de hoy en día."

Steve Mensh

En este apartado se va a explicar la historia de la Guerra Electrónica en el mundo, para después concretar en la historia de esta disciplina en España y las distintas variantes y técnicas de EW. En segundo lugar, se tratará de comprender el funcionamiento de los sistemas y equipos tanto de detección como de perturbación. Para finalizar, se analizarán los equipos de Radar Definido por Software (SDR).

2.1.1 Historia de la Guerra Electrónica

Como ya se ha explicado previamente, la Guerra Electrónica agrupa todo el conjunto de técnicas, equipos y sistemas que se ocupan a defender nuestro propio uso y explotación del espectro electromagnético, y además de negarle el uso de este espectro al enemigo, reduciendo su capacidad táctica [6].

Este campo bélico es relativamente reciente, y viene muy unido al desarrollo de los sistemas de radar y comunicaciones. Partiendo de las ecuaciones del comportamiento electromagnético de Maxwell, no fue hasta 1903, cuando se produjo el primer avance hacia lo que hoy llamamos radar. Fue el investigador alemán Christian Hulsmeyer, que desarrolló un equipo capaz de detectar ondas radio reflejadas en los buques como apoyo a la navegación. Este proyecto se presentó a la Armada Imperial del Kaiser, siendo rechazada por su corto alcance, más tarde Alemania pagaría caro no haber invertido en esa vía de investigación.

Utilizando investigaciones del científico italiano Marconi, en 1935 el inglés Watson-Watt diseñaría el "Radio Detection Finding" un aparato que conseguía detectar un avión a 15 millas de distancia a través de ondas de radio. Siguieron progresando las investigaciones en EEUU e Inglaterra, en muchos momentos de manera conjunta a iniciativa de Wiston Churchill, dejando muy por detrás tecnológicamente a las investigaciones alemanas.

Pese a ello, en 1942 los submarinos alemanes tipo *Metox* comienzan a llevar un simple receptor radio que les indicaba cuando eran iluminados por las armas enemigas, reduciendo la eficacia y superioridad radar de los británicos. Este hito puede considerarse como el inicio de la Guerra Electrónica, al menos en el ámbito de las ESM (Medidas Electrónicas de Apoyo). En respuesta a los ingleses diseñaron un atenuador que disminuía la potencia del radar una vez detectado el blanco, para hacer creer que al submarino que el radar enemigo estaba más lejos de lo que realmente estaba. Esto confirmaría el comienzo de una evolución enorme en la Guerra Electrónica a nivel mundial.

Los U-Boot alemanes comenzaron a usar también en la Segunda Guerra Mundial, globos de llenos de hidrógeno recubiertos de láminas de aluminio con gran RCS (*Radar Cross Section*), que engañaban a los operadores radar enemigos. En definitiva, estábamos ante el primer antecedente del chaff.

A partir de los años 50 hasta la actualidad la investigación y desarrollo de la Guerra electrónica se abrió a empresas civiles y no necesariamente para investigación exclusiva de las Armadas, lo que dio un impulso gigante a esta guerra, sus sistemas y equipos. Los receptores comenzaron muy pronto a procesar y reconocer señales de todo tipo, mientras que los transmisores de forma inteligente buscan los medios y bandas de frecuencia para evitar la detección o reconocimiento del enemigo. A continuación, explicamos cómo en España tardaría en llegar un poco más a través de equipos americanos, sin embargo, poco a poco nos hemos convertido en diseñadores punteros y exportadores de sistemas de Guerra Electrónica.

2.1.2 La Guerra Electrónica en la Armada

La aparición de la Guerra electrónica en la Armada Española fue tímida, sin embargo, la industria nacional ha conseguido no sólo cubrir con creces las necesidades tecnológicas de nuestras unidades, sino además conseguir clientes en el extranjero.

Figura 2-1: Portaeronaves *Dédalo* con aviones Harrier sobre cubierta de vuelo [5]

El sistema WLR-1 de origen americano fue el primer sistema EW (Electronic Warfare) montado en buques de la Armada. Concretamente en los destructores Clase "Churruca", transporte de ataque *Castilla* y el portaeronaves *Dédalo* (Figura 2-1). Este equipo era un receptor ESM de banda ancha con

capacidades ELINT (Inteligencia Electrónica), desarrollado en los años 50, requería un gran adiestramiento por parte del operador [5]. Además, no cubría el espectro electromagnético de *seekers* de misiles superficie-superficie, la capacidad de autodefensa era nula, puesto que no tenía posibilidad de medidas ECM (Contramedidas Electrónicas) ni de lanzamiento de señuelos.

Más tarde, ya en los años 70, las fragatas clase "Baleares" cambiaron sus equipos de EW WLR-1 por el llamado sistema beta, de origen italiano. Este equipo operaba con medidas tanto ECM como ESM, y estaba diseñado para buques de medio porte como corbetas o fragatas. El problema de este sistema era su poca precisión en demora y sensibilidad, además una gran dificultad de monitorización y almacenamiento de librerías de emisiones. También fue montado este equipo en el portaaviones *Dédalo*.

Habría que esperar hasta mediados de los años 80 para la aparición de los primeros equipos desarrollados en España. Todo esto partió de la creación a principios de década de la Sección de Guerra Electrónica dentro del Estado Mayor de la Armada (EMA). Ante la necesidad de medios de EW, se llevó a cabo el Programa *Santiago*, que trataba de realizar un análisis de la integración de Guerra Electrónica. Además, se realizó el primer curso de GE para oficiales.

Fue entonces cuando se empezó a gestar una base de datos de inteligencia de señales EW y aparecieron los primeros equipos en los tres ejércitos. Ejemplos son el equipo Mk-1000 de ECM del patrullero *Salcedo*, dos aviones de transporte de CASA o la creación del Batallón de EW y Unidad de transmisiones con equipos alemanes. No sería hasta finales de década cuando con la creación del Estado Mayor de la Defensa (EMAD), que agrupaba a los tres ejércitos, cuando se crearía la idea de una GE (Guerra Electrónica) conjunta unificando muchos proyectos.

Pero lo que verdaderamente marcó un cambio tecnológico y táctico fue la creación del *Plan General de Guerra Electrónica* a mediados de los años 80, que define las características básicas de los equipos y diferenciándolos por campo de actuación. Se apostaba por construir equipos españoles con nuestra tecnología, este plan que iniciado por la Armada y la empresa INISEL antecesora de la actual INDRA, fue el que inició la serie de sistemas llamados con nombres de estrellas, que culminaría con la llegada de las F100 y el sistema *Aldebarán*. El objetivo principal era dotar a la industria nacional de la capacidad para generar y diseñar equipos de Guerra Electrónica.

Figura 2-2: Mástil de la Fragata *Asturias* con su sistema *Canopus* [2]

De los primeros sistemas desarrollados en España destacan la modernización de media vida que se les hizo a las fragatas de la clase "Baleares", como la *Asturias* (Figura 2-2) y el equipamiento de las corbetas Clase "Descubierta" a mediados de los 80 [2]. Se decidió también modernizar los equipos existentes a través del programa *Deneb*, el principal freno que encontraron fue la poca sensibilidad de las antenas receptoras y la alta probabilidad de falsa alarma. Además, con los programas *Canopus* y *Elnath* se mejoraron la exploración del espectro, goniometría, lanzamiento de señuelos de tipo chaff y los receptores para sistemas de ECM de comunicaciones, llegando a conseguir capacidad de perturbación y *spoofing* [2].

El siguiente paso que dio la Armada Española fue volver a la tecnología italiana con el sistema *Nettunel*, instalado en las fragatas F-80 clase "Santa María". El sistema consiste en una antena de recepción, dos perturbadores de decepción y otros dos perturbadores de ruido. Tenía capacidad de seguir hasta 16 contactos en modo pasivo, trabajaba en digital y poseía una gran precisión en comparación con los equipos antiguos. También fue instalado en el portaaviones *Príncipe de Asturias*.

El impacto inesperado de dos misiles *Exocet* iraquíes en la fragata americana *Stark*, hizo saltar las alarmas en materia EW dentro de la US Navy, y como consecuencia España también impulsó el desarrollo de sistemas y equipos. El sistema Nettunel se convierte en el sistema EW por excelencia en la Armada, que se montaría también en el portaaviones *Príncipe de Asturias* y que forjaría las bases de los siguientes sistemas de Guerra Electrónica [7].

Figura 2-3: Mástil de la Fragata F-101 *Álvaro de Bazán* con sistema *Aldebarán* [7]

En 1986 se inicia el programa *Aldebarán*, que evolucionaría hasta acabar integrándose en el sistema de combate de las fragatas F100 clase "Álvaro de Bazán" (Figura 2-3). Se consigue generar módulos de medida instantánea de frecuencia (DIFM, *Digital Instantenous Frecuency Measurement*), antenas de apuntamiento electrónico y antenas multihaz para medir en ángulo de llegada (AOA, *Angle of Arrival*). En 1992 se empieza la fase de desarrollo empezando por sistemas ESM, y posteriormente equipos con capacidad ECM. Mientras el *Aldebarán* se ocupa de la parte de ECM/ESM, el sistema *Regulux* se ocupa de la Guerra Electrónica de comunicaciones. Las principales capacidades del sistema son: [8]

- Detección de emisores en banda ancha y estrecha.
- Determinación de parámetros de las emisiones.
- Clasificación e identificación en librería.
- Análisis intrapulso.
- Contramedidas (ECM) simúltaneas de ruido y engaño.

Por otro lado, cabe destacar dentro de la Infantería de Marina, la Sección de EW de la BRIMAR. Disponen de equipos pesados montados en vehículos *Piraña* o Mercedes *Unimog*, como es el sistema *Dubhe*, desarrollado por INDRA. Sin embargo, los equipos más utilizados son los *Lewt*, de ESM de comunicaciones, desplegados actualmente por los equipos operativos de seguridad en la operación Atalanta. [9]

Finalmente, el último sistema diseñado con tecnología española es el sistema *Rigel* que es de carácter ligero y con capacidad ESM. Ha sido adoptado por los Buques de Acción Marítima (BAM), el portaeronaves *Juan Carlos I* e implementado en la modernización de las fragatas F80. La empresa española INDRA ya está desarrollando el sistema de Guerra Electrónica de las futuras F110, las cuales llevaran unos equipos mucho más capaces y sensibles que los actuales. Son el sistema *Rigel* i110 y para las comunicaciones el *Regulux* i110. [10]

Además, las antenas de estos sistemas estarán integradas en un nuevo concepto de mástil integral (*Topside*) que reduce al mínimo la RCS. Estas antenas forman parte de la superestructura del barco y sobresalen lo mínimo posible haciendo al buque menos detectable con una superficie menos reflectante a las ondas radáricas. [11]

2.1.3 Tipos de Guerra Electrónica

Dentro de la Guerra electrónica, existen medidas electromagnéticas enfocadas tanto al espectro electromagnético del radar como al espectro de las comunicaciones.

Teniendo en cuenta la doctrina actual de la Armada, podemos dividirla en tres tipos o variantes diferenciadas. Esta clasificación es de carácter táctico o doctrinal, puesto que las tres comparten en muchos casos técnicas y modos de funcionamiento de sus equipos, pero con distinto uso estratégico. [8]

1. **Medidas de apoyo a la Guerra Electrónica (ESM).**

   Las ESM (*Electronic Support Measures*) son todas aquellas acciones utilizadas para interceptar, reconocer cualquier emisión electromagnética y localizar la fuente que la genera para reconocer una posible amenaza y sus intenciones. Estas medidas aportarán una información fundamental para tomar decisiones en cuanto a respuestas contra esa amenaza u otras acciones tácticas. Estas acciones pueden ser desde evasión, acercamiento al blanco, usar contramedidas electrónicas, que explicaremos posteriormente, o el empleo táctico de fuerzas.
   El uso de medidas ESM no tiene generalmente que alertar al enemigo de nuestra presencia, debido a que nosotros simplemente realizamos una escucha pasiva. Incluye 6 fases principales: [12]

   a. Búsqueda/Interceptación/Detección.
   b. Análisis de la emisión a través de bases de datos.
   c. Búsqueda dirección emisión.
   d. Reconocimiento de la emisión del blanco y equipo emisor.
   e. Identificación.

f. Grabación de las características de la emisión para análisis detallado e inteligencia.

Operativamente hablando las misiones principales son vigilar la amenaza, determinar las características técnicas del equipo emisor y localizar ubicación de los emisores.

Podemos clasificar estas medidas en SIGINT (*Signal Inteligence*), ELINT (*Electronic Inteligence*) y COMINT (*Communications Inteligence*), que conforman lo que llamamos Medidas de Inteligencia Electrónica. SIGINT son aquellas orientadas a la recolección y estudio de la información obtenida de las emisiones radar o de comunicaciones, y su posterior conversión en inteligencia útil para el desempeño táctico de la misión. La diferencia principal entre las medidas ESM corrientes y las SIGINT es esa, la obtención de inteligencia para uso estratégico a largo plazo, mientras que las Medidas de apoyo son tácticas (desarrollo en el momento del combate o enfrentamiento). ELINT y COMINT son las medidas englobadas dentro de SIGINT, dependiendo si están enclavadas dentro del campo de las emisiones de radar o de las comunicaciones.

Cabe mencionar también las Medidas de Inteligencia Óptica e IR, que dependen de la banda de frecuencias en la que trabajemos (OPINT, *Optical Inteligence* e IRINT, *Infrared Inteligence*).

2. **Medidas de protección electrónica (EPM).**

Las EPM (*Electronic Protective Measures*), también llamadas ECCM (*Electronic Counter-Countermeasures*), son todas aquellas medidas destinadas a garantizar el uso con seguridad y efectividad de nuestro propio espectro electromagnético, pese al uso del enemigo de acciones de EW. Tiene la función de proteger equipos y sistemas de las fuerzas propias, frente a la intención del enemigo de detectar, degradar, neutralizar o destruir la capacidad de combate propia. Es esencial para proporcionar la capacidad de mantener mando y control a través de las comunicaciones, y poder garantizar que los equipos electromagnéticos permitan el reconocimiento y uso de las armas de la unidad. [8]

Entre algunas de las medidas destacan el control de las emisiones, cambios de frecuencias en las comunicaciones, protección electromagnética de los equipos, etc. [12]

3. **Contramedidas electrónicas (ECM).**

Las ECM (*Electronic Countermeasures*) son la parte de la Guerra Electrónica que engloba las acciones encaminadas a prevenir o reducir el uso efectivo por parte del enemigo de sus emisiones electromagnéticas. En definitiva, el objetivo de estas medidas es reducir o deteriorar la capacidad de combate enemiga. Dentro de ella podemos dividir en 4 tipos: [13]

a. **Jamming.** Es la radiación deliberada o reflexión de energía electromagnética con la función de dañar la efectividad de los sistemas o equipos del enemigo. (Figura 2-4)
b. **Decepción.** Es radiación emitida, reflejada, absorbida o alterada, generada para confundir, distraer y seducir a los equipos del enemigo. Consiste en la creación, por ejemplo, de un contacto falso, bien de manera electrónica o con objetos físicos (decoys, chaff). La intención puede ser también que el enemigo pierda la pista del contacto real dejándose llevar por el que nosotros hemos generado.
c. **Confusión.** Está muy relacionado con la decepción, en cierto punto se pueden llegar a confundir. Se trata de la creación de muchos blancos falsos, generando incertidumbre y saturación al enemigo.

d. **Neutralización.** Es el uso de la energía electromagnética para dañar temporalmente o de forma definitiva los equipos del enemigo, sólo utilizando nuestras emisiones para inutilizar estos sistemas.

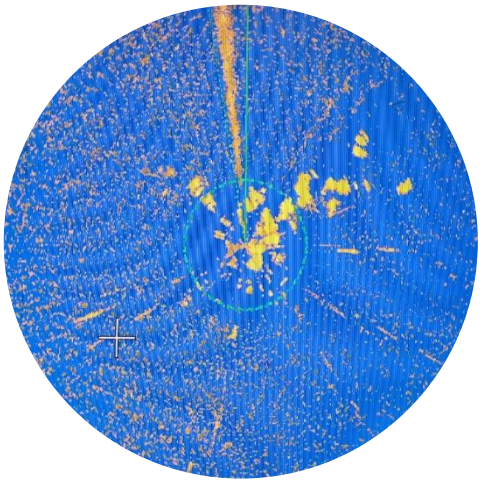


Figura 2-4: Ejemplo de Contramedida (ECM) de tipo Jamming sobre un radar

Las ECM son detectables por enemigo a diferencia de las ESM, ya que son una emisión deliberada y clara en dirección del enemigo. Eso significa que este puede detectar que está siendo perturbado, sin embargo eso no significa que pueda localizar la fuente que emite esta radiación, dependiendo del tipo de perturbación que utilicemos.

2.2 Sistemas de Guerra Electrónica. Equipos

Como ya comentamos al comienzo del apartado 2.1.3, podemos clasificar los sistemas de Guerra Electrónica dependiendo si son orientados a las comunicaciones o no (orientados a sistemas de navegación y detección). Pueden ser considerados pasivos o activos, si su objetivo es interferir o no, como hemos visto dependiendo si están diseñados para medidas ECM o ESM, o para ambas. En la Figura 2-5 se muestra un esquema general de los componentes de un sistema de EW, sus equipos principales son los sensores y los perturbadores. Un ejemplo claro de un sistema de este tipo es el sistema Aldebarán integrado en el sistema de combate de las fragatas clase F-100 *Álvaro de Bazán*. [8]

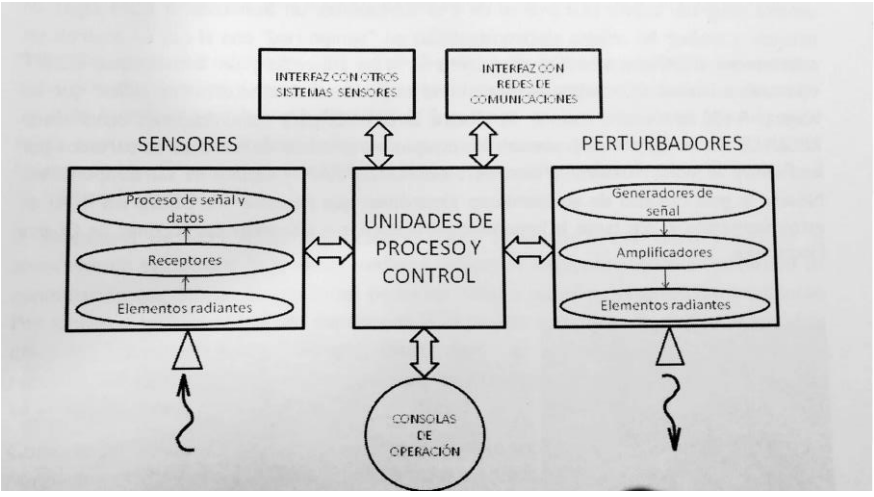


Figura 2-5: Diagrama esquemático de los componentes de un Sistema de Guerra Electrónica [8]

2.2.1 Sistemas de detección

Continuando con lo ya explicado previamente de las técnicas de ESM, estos equipos se ocupan de la detección de las señales incidentes y el proceso de análisis para identificar sensores y armas de la unidad enemiga.

El proceso de detección puede descomponerse en cuatro fases, exploración, interceptación, identificación y localización. [14]

1. **Exploración.** La principal misión de las acciones ESM en esta fase es buscar, dentro del rango de tiempo y frecuencia, cualquier emisión que pueda ser de interés con el objetivo de detectarla.
   Pueden realizar una búsqueda general, en la que se realiza una búsqueda de grandes proporciones en el espectro, usando receptores de banda ancha. Estos recogen todas las emisiones que estén dentro del margen de frecuencias que cubramos. Los receptores también pueden ser secuenciales e ir rastreando poco a poco el espectro. Estos últimos tienen mayor sensibilidad.
   Por otro lado pueden realizar una búsqueda inteligente, llamada búsqueda especial. En este caso se utilizan sistemas automatizados que seleccionan solo las emisiones consideradas de interés, a través de uso de bases de datos. (Figura 2-6)
2. **Interceptación.** Es el paso siguiente a la búsqueda y tiene como objetivo descubrir dentro del espectro las señales de interés. Es decir, dentro de todas las señales que llegan al receptor seleccionar aquellas que puedan potencialmente útiles para ser identificarlas.
3. **Identificación.** Consiste en determinar si las emisiones se corresponden a un emisor enemigo o amigo mediante un estudio más detallado de sus características y parámetros de señal. Comparación con bases de datos. Más tarde analizaremos que parámetros nos interesan para identificar la señal.
4. **Localización**. Determinación de la posición del emisor a través de la dirección en la que nuestra antena recibe esa emisión. Si tenemos la posibilidad de tener varias antenas receptoras podríamos cruzar demoras para sacar la posición del enemigo (triangulación), solamente teniendo su emisión electromagnética. Es lo que se llama la Radiogoniometría.

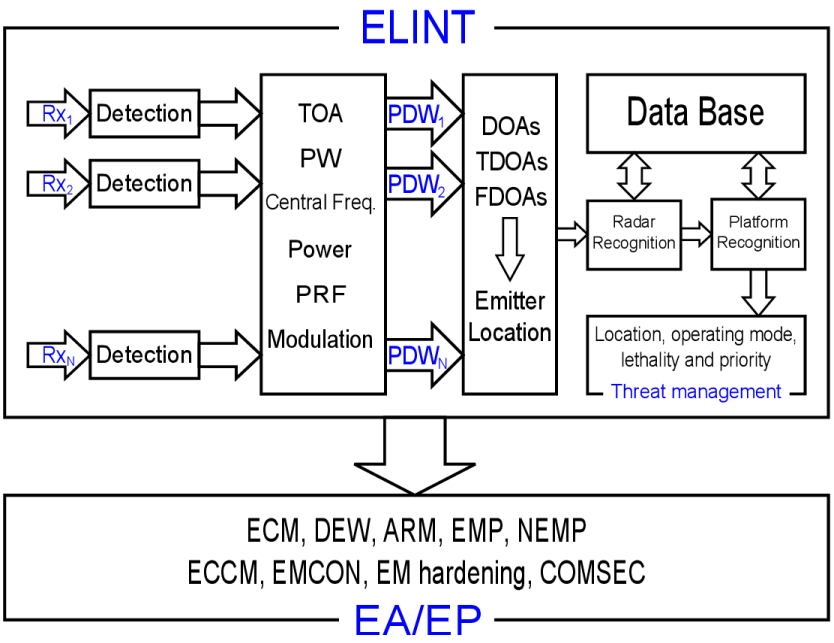


Figura 2-6: Ejemplo receptor ELINT en un sistema de Guerra Electrónica [40]

A continuación, describiremos los parámetros importantes para desarrollar la detección de una emisión a través de un receptor de Guerra Electrónica. Los receptores pueden ser de banda ancha o banda estrecha. Los receptores de banda ancha se utilizan normalmente para emisiones radáricas, mientras que los receptores de banda estrecha son usados para comunicaciones. [8]

Los parámetros más importantes que van a ser utilizados para reconocer la emisión amenaza son:

- Frecuencia
- Amplitud (potencia)
- Dirección de llegada (AOA)
- Tiempo de llegada (TOA)
- Intervalo de repetición de pulsos (PRI)
- Anchura de pulso (PW)
- Velocidad y tipo de exploración
- Anchura del haz
- Modulación de frecuencia del pulso
- Polarización del campo electromagnético

Los más relevantes son el AOA, que nos indica la dirección del radar enemigo y la frecuencia en la que este transmite. Otros parámetros importantes pueden agruparse en un conjunto denominado PDW.

El PDW (*Pulse Descriptor Word*) reúne los parámetros de los pulsos de un radar. Generalmente incluyen parámetros básicos como Ancho de pulso (PW), Intervalo de repetición de pulsos (PRI), Frecuencia de repetición de pulsos (PRF), Tiempo de llegada (TOA), Tiempo de salida (TOD), Diferencia de tiempo de llegada (DTOA), Ángulo de llegada (AOA), Amplitud (A), Relación señal a ruido (SNR), aunque puede incluir algunos otros. El PDW puede cambiar de sistema a sistema dependiendo de la aplicación o parámetros que sean más importantes para identificar determinados emisores. [15]

Para conseguir una detección e identificación clara, obteniendo los parámetros que nos caractericen la señal, debemos fijarnos en el PDW, y más en particular en el TOD y TOA. El tiempo de salida y llegada del pulso es primordial para poder obtener otros valores como el ancho de pulso o el PRI. Como se ve representado en la Figura 2-7, el TOA y TOD son los tiempos de llegada y salida del pulso radar.

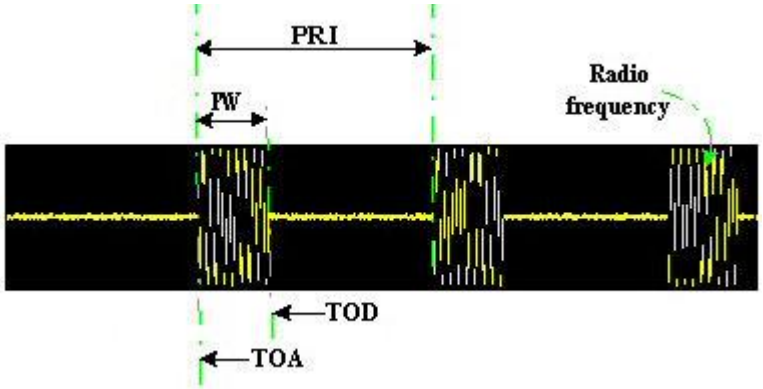


Figura 2-7: Pulso radar y parámetros principales [16]

2.2.1 Sistemas de perturbación

Como se ha comentado en el apartado 2.1.3, consideramos jamming o perturbación a aquellas medidas electromagnéticas que intentan disminuir la efectividad de los equipos del enemigo. Dependiendo del tipo emisión perturbadora respecto al radar enemigo y el objetivo de la técnica, podemos clasificarlos en distintos tipos. Todas estas técnicas se pueden agrupar según su tipo de función: Enmascaramiento (*Masking*), Decepción (*Deception*) o Confusión (*Confusion*) (Véase Anexo II).

Antes de pasar a explicar la variedad de técnicas se describirán algunos conceptos comunes a las tres citadas.

Los perturbadores son componentes principales dentro de los sistemas de Guerra Electrónica, no sólo por su función táctica e importancia estratégica. Son equipos críticos por su gran consumo, tamaño y coste de mantenimiento y piezas. Muchos buques tienen durante largos periodos equipos inoperativos por falta de presupuesto debido al alto coste de algunos componentes [13].

La efectividad de un perturbador o jammer viene dada por la relación entre la potencia de la señal interferente (J) y la potencia de la señal deseada (S), y se denomina relación jammer a señal (J/S). Cuanto mayor sea esta relación más efectiva será la perturbación.

La ERP (*Effective Radiated Power)* es la densidad de potencia enviada en la dirección del radar enemigo que se pretende perturbar y es función de la potencia del perturbador [13], ganancia de la antena y las posibles pérdidas que sufra (2-1):

$$ERP = \frac{P_J\, G_J}{L_J} \tag{2-1}$$

Dos conceptos importantes a tener en cuenta al hablar de jamming son la distancia ***Crossover*** y la distancia ***Burn-Through***. La primera es aquella distancia a la que la potencia recibida de señal del emisor (*S*) se iguala con la potencia recibida del jamming (*J*). Es decir, es el punto en el que el enemigo va a poder empezar a discernir el blanco sobre el que se está realizando el jamming. Mientras que la ***Burn-Through*** es la distancia mínima a la que el jamming realizado comienza a ser efectivo (Figura 2-8).

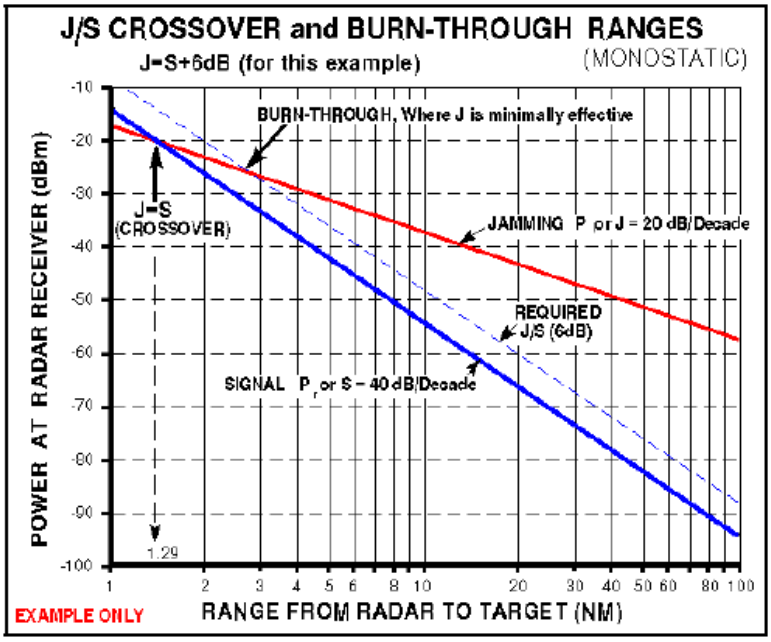


Figura 2-8: Gráfica Burn-Through y Crossover Range [17]

Se procede a analizar algunas de las técnicas de perturbación existentes:

a. N**oise Jamming.** Los jammers de ruido intentan enmascarar blancos radar simplemente aumentando el nivel de ruido, que compite con la señal radar. Se trata por tanto de degradar la relación señal a ruido (S/N) del receptor, añadiendo mayor cantidad de ruido (J). La nueva relación señal a ruido será (2-2):

$$\frac{S}{J+N} = \frac{1}{\frac{1}{S/J} + \frac{1}{S/N}} \qquad (2\text{-}2)$$

La perturbación sería simple si el radar mantuviese contante la frecuencia de operación, de esta forma sólo habría que perturbar dicha frecuencia. Sin embargo, si el emisor realiza cambios de frecuencia en el tiempo (*Frequency hopping*), tendríamos que realizar una perturbación en un ancho de banda B_J mucho mayor. Esta modalidad de perturbación se denomina jamming de barrera (*Barrage Jamming*).

b. **Support Jamming**. Son aquellas técnicas que tratan de enmascarar u ocultar nuestra posición o la de un contacto amigo frente a la detección o enganche de un radar hostil. Las técnicas de jamming utilizadas dependen de si la perturbación se realiza sobre el haz principal del radar o sobre uno de sus lóbulos laterales [13].

- **Jammers de lóbulo principal.** Las señales entran en el radar a través del haz principal. La unidad jammer puede tener la intención de realizar el jamming sobre su propio blanco, *Self Screnning Jammers* (SSJ), que sería utilizado por la unidad para

su propio enmascaramiento frente al enemigo [17]. O por otro lado, *Escort Jammers* (ESJ) donde la unidad realizaría funciones de escolta sobre otro blanco amigo, cubriéndole de una posible detección o enganche hostil (Figura 2-9). La relación señal a jamming **(2-3)** para este tipo de técnica es:

$$\frac{S}{J} = \frac{P_P \, \sigma \, G_\gamma \, PC \, B_J}{4\pi \, R^2 \, B \, L_\gamma \, ERP} \tag{2-3}$$

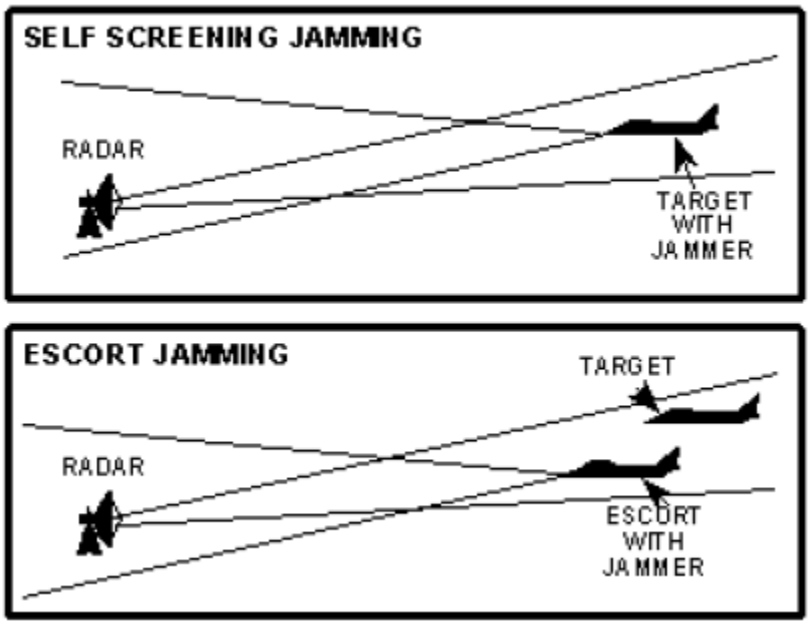


Figura 2-9: Diagrama SSJ y ESJ Diagrama SSJ y ESJ [17]

- **Jammers de lóbulo lateral (SLJ).** La señal entra en el radar por los lóbulos laterales. Este tipo de perturbadores son desplegados para largas distancias, fuera del alcance de los sensores y armas del enemigo. Suelen tener mayor potencia y ganancia que los de lóbulo principal. Los *Sidelobe cancellers* (SLC) como su nombre indica, eliminan los lóbulos laterales en la emisión del jammer. Funcionan con otra antena alternativa a la del perturbador. Pueden reducir los lóbulos laterales hasta 20 dB o más [13].

c. **Pulse jamming.** Consiste en producir gran número de falsos blancos que creen confusión y desconcierto al procesador de señal u operador del radar enemigo [13]. Algunos de los tipos más reseñables son:

- **Jammers de confusión de lóbulo lateral**. Producen gran número de falsos blancos en la zona de los lóbulos laterales y obliga al radar enemigo a confirmar o rechazar los ecos que recibe. Para ello puede utilizar los llamados *Sidelobe blankers* (SLB) que lo que hacen es utilizar una antena adicional para anular al jammer en sus periodos de perturbación. Si el jammer emite en onda continua el *blanker* sería inútil ya que dejaría ciego al radar.
- **Swept-spot Jammers.** Consiste en crear falsos ecos al mismo tiempo que el jammer va cambiando la frecuencia a lo largo del ancho de banda del radar perturbado. La rapidez en estos saltos de frecuencia, hace que el sistema introduzca ruido en el radar enemigo y además enmascare los blancos dentro de esa banda (Figura 2-10).

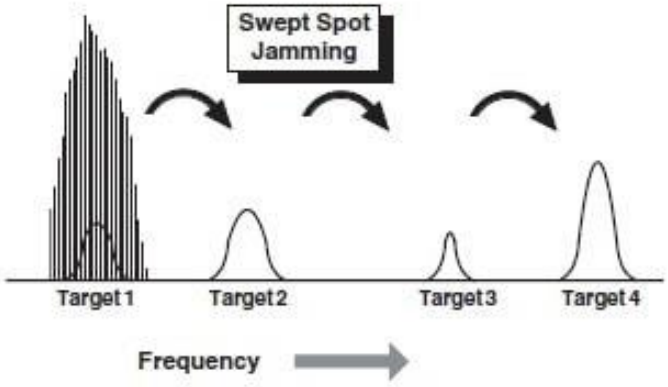


Figura 2-10: Saltos de frecuencia de un Swept-spot Jammer [16]

- **Jammers de repetición.** Transmite réplicas de la señal radar para crear falsos contactos. Se debe sincronizar con la transmisión del radar para que el contacto falso siga una trayectoria creíble. Normalmente la posición obtenida del falso contacto será mayor a la posición real desde que nuestra unidad está perturbando.
- **Track-breaking Jammers.** Son perturbadores que roban la puerta de distancia y de demora del blanco. Es decir, consiguen mover en distancia o demora un contacto adquirido por el radar, de forma que la traza de este se pierda. Funcionan emitiendo sofisticadas señales modificadas en fase y tiempo contra ese radar.

  La efectividad de nuestra perturbación se va a ver reducida si el enemigo utiliza saltos de frecuencia, PRF o anulación de los lóbulos laterales.

d. Chaff. Se trata de situar gran número de objetos reflectantes radar alrededor de un contacto de interés. Las reflexiones de estos objetos tratan de ocultar y crear confusión sobre la posición de nuestro blanco frente a un radar enemigo o *seeker* de un mísil (Figura 2-11). Hay distintos tipos de chaff utilizados en los buques: [18]

- **Chaff C.** Confusión, usado en la fase previa a la detección.
- **Chaff D.** Distracción, con la función principal de enganchar la dirección de tiro o el *seeker* del mísil al falso eco producido por el chaff. Uso sólo previo al enganche de nuestro blanco.
- **Chaff S.** Seducción, una vez hemos sido enganchados por el radar enemigo, intentar desviarlo a un blanco falso, que es más efectivo con pulso estrecho.

Figura 2-11: Fragata *Álvaro de Bazán* lanzando chaff [18]

Otros objetos o métodos que funcionan con los mismos principios que el chaff son los decoys, que son lanzados para evitar la detección o enganche de nuestro blanco. Suelen tener una gran RCS, y pueden ser lanzados al mar o aeropropulsados, para de esta forma hacer frente a distintas amenazas.

2.3 Radar definido por software (SDR)

Para implementar la fase de detección (ESM) de las señales enemigas, expuesta en el apartado 2.1.3 y su posterior perturbación (ECM), se necesita usar software de procesado de señal, tanto para interpretación y extracción de parámetros, como para definir una señal que tenga las características necesarias para interferir el radar enemigo.

El origen del radar definido por software está en la definición de ondas de radio a través de software informático, que más tarde daría lugar al mismo software para ondas radáricas. El concepto SDR se define como el hecho de usar soporte informático para manejar las funciones, comportamiento o características de un sistema de comunicaciones radio o un sistema radar. A través de procedimientos y técnicas de procesado de señales en equipos digitales programables, se obtienen señales de radio o radar específicas, modificables en cualquier momento a través este software. Consigue ser un sistemas de telecomunicaciones en el que un ordenador personal o sistema de computación hacer lo que físicamente lo realizaban componentes en hardware (como mezcladores filtros, amplificadores, moduladores, detectores de señal…) [19].

2.3.1 Down/Up-converter

Cuando la frecuencia de la señal que se quiere sintonizar es muy elevada, se suele utilizar un dispositivo, denominado *down-converter*, que traslada dicha frecuencia a otra más baja llamada frecuencia intermedia (IF). El down-converter es un mezclador como el de la Figura 2-12. La señal de radiofrecuencia f_{RF} se bate (mezcla) con la señal de un oscilador local f_{OL} dando lugar a la frecuencia intermedia f_{IF}.

Existe un dispositivo similar, denominado *up-converter*, que, a partir de una señal de frecuencia intermedia f_{IF}, obtiene una señal de RF tras la mezcla con la señal de un oscilador local (Figura 2-12).

Figura 2-12: Funcionamiento de un Down/Up Converter [40]

$$f_{IF} = |f_{RF} \pm f_{OL}| \quad (2\text{-}4)$$

El comportamiento de un mezclador ideal respondería a la Ecuación (**2-4)**, sin embargo, debido a la no-linealidad de estos dispositivos, se generan infinitos armónicos en las frecuencias derivadas de la Ecuación (**2-5)**. La señal de interés es la obtenida cuando m=1 y n=1, y el resto de las señales deberían ser filtradas [20].

En caso de que la frecuencia de salida deseada sea 9410 MHz, siendo la señal de frecuencia intermedia f_{IF} , 1000 MHz, la señal del oscilador local f_{OL} tendrá que ser 8410 MHz. Mientras si se quiere recibir una frecuencia RF de 9410 MHz, se debería configurar 10410 MHz para poder obtener 1000 MHz de frecuencia IF.

$$f_{IF} = |mf_{RF} \pm nf_{OL}| \quad (2\text{-}5)$$

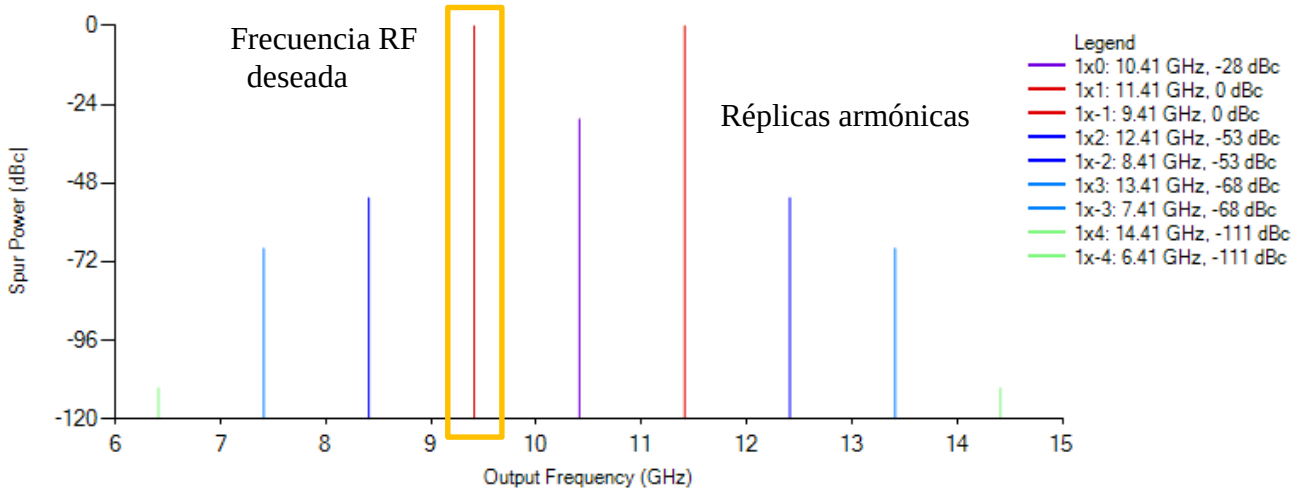


Figura 2-13: Réplicas armónicas generadas en el mezclador para RF=9.41 GHz [21]

La mayoría de réplicas armónicas son generadas por la intermodulación no linear de la señal RF y OL en la región de transmisión en el diodo del mezclador. Cuanto más baja sea la f_{RF} más limpia será la señal obtenida. La aparición de estas réplicas significa confusión y problemas a la hora de usar el mixer, por ello el clave la reducción de los armónicos en el diseño del mezclador. La Figura 2-13 muestra esas réplicas generadas al intentar obtener RF= 9.41 GHz, la frecuencia deseada, marcada en naranja.

2.3.2 SDR

Una de las piezas fundamentales del sistema que posteriormente será diseñado es el equipo SDR, que, junto al mezclador, oscilador local y el programa informático de tratamiento de señal, conforman la estructura del sistema básico de un equipo de Guerra Electrónica.

Nació de manos de la Air Force, a través del programa ICNIA (*Integrated Communication, Navigation, Identification and Avionics*) a finales de los años 70. A partir de entonces, el Departamento de Defensa Norteamericano inició el desarrollo de un sistema de radio VHF multibanda y posteriormente de sistemas SDR con el llamado proyecto SpeakEasy, un sistema que intentaba dotar de interoperabilidad entre las distintas tecnologías de comunicaciones, alrededor de 10 tipos diferentes en un solo equipo programable [22].

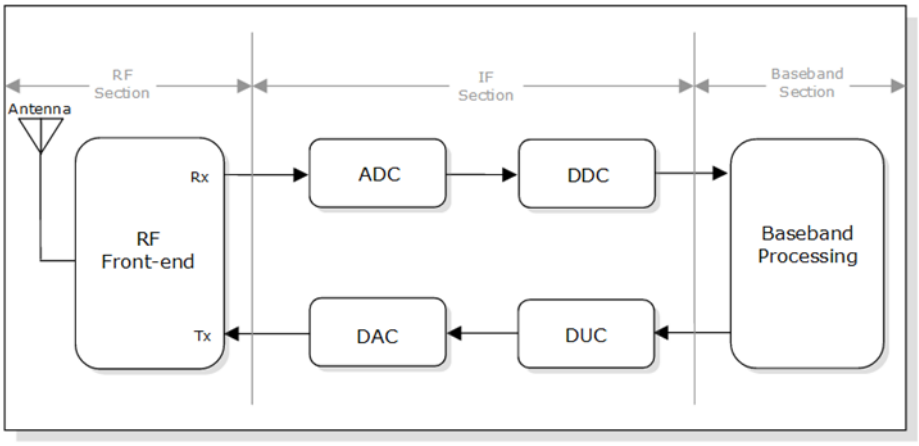


Figura 2-14: Esquema funcionamiento del SDR [20]

En cuanto a su funcionamiento, podemos distinguir varias etapas, expuestas en la Figura 2-14. En primer lugar, una etapa de radiofrecuencia, en la que la señal recibida se translada a una frecuencia muy inferior denominada frecuencia intermedia (IF). Para realizar esta operación, se utiliza un down-converter como el descrito en el apartado anterior [19]. Generalmente, los dispositivos SDR suelen trabajar con la denominada *Zero-IF*, es decir, con frecuencia intermedia cero, de forma que la señal se entrega directamente en banda base.

La señal pasa por un procedimiento de descomposición en fase-cuadratura o mediante un mezclador IQ que genera dos señales denominadas “en fase” y “en cuadratura” (Figura 2-15). La señal no desfasada se denomina señal en fase (Señal I, *Inphase-Signal*), y a la desfasada señal en cuadratura (Señal Q, *Quadrature-Signal*).

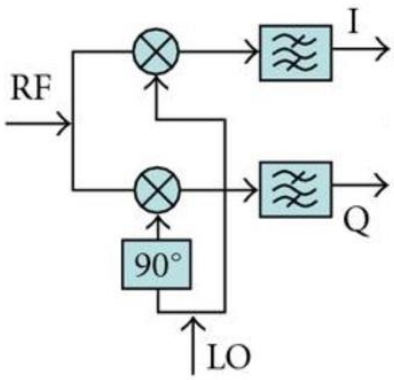


Figura 2-15: Mezclador IQ [23]

Como se ve en la Figura 2-16, las dos componentes Q e I pueden obtenerse a partir del módulo de la señal, R, y la fase β, empleando las ecuaciones (**2-7)** y (**2-6)**.

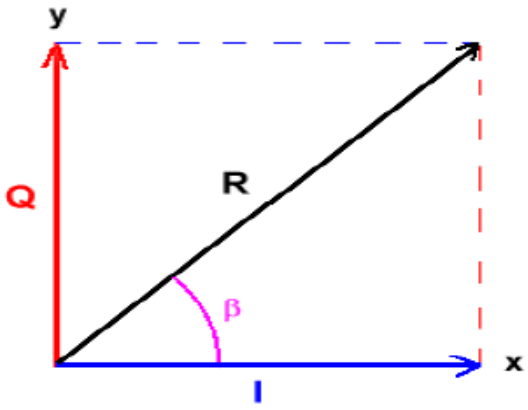


Figura 2-16: Representación vectorial de las señales I y Q [19]

$$\boldsymbol{R^2 = Q^2 + I^2} \tag{2-6}$$

$$\beta = \arctan\left(\frac{Q}{I}\right) \tag{2-7}$$

Estas dos componentes de señal son muestreadas mediante sendos conversores analógico-digitales (A/D) y llevadas al procesador/ordenador para su proceso. Para la transmisión de la señal, se realiza un proceso inverso en el que se convertiría la señal digital en analógica mediante un convertidor DAC.

3 DESARROLLO DEL TFG

3.1 Investigación y recopilación de información

El trabajo se compone principalmente de dos fases diferenciadas, una fase de detección (ESM), en la que se detectará la señal del radar y se obtendrán los parámetros de la emisión a través de algoritmos; y una segunda fase de perturbación (ECM), en la que se realizará una perturbación (jamming) sobre el radar enemigo para, de esta forma, negarle o dificultarle su uso normal de exploración y detección. Estas dos fases están relacionadas, puesto que para la realización del jamming, es necesaria la detección previa y procesado de la señal.

Se ha realizado un trabajo de investigación y estudio de otros proyectos ya existentes, sobre todo en lo relativo al desarrollo de algoritmos para determinación de parámetros de señales, y también sobre tratados sobre Guerra Electrónica, donde se pudo ver qué tipos de perturbaciones se podían realizar y las posibilidades del sistema. También ha sido indispensable el estudio de los distintos equipos utilizados durante el trabajo, primordial para conocer su funcionamiento, límites y posibles usos.

Además del análisis de los equipos usados en el sistema de detección y perturbación que posteriormente serán explicados con detalle, cabe destacar la importancia de la investigación de las características, modos de funcionamiento, filtros y opciones del radar con el que se realiza el trabajo, el radar Furuno 1944C. En resumen, las principales líneas de la fase de investigación fueron:

- Estudiar de las distintas posibilidades de jamming existentes, y al alcance de nuestro sistema.
- Investigar algoritmos para generar, representar y determinar los parámetros de una señal radar con Matlab.
- Conocer los equipos a utilizar y limitaciones de cada uno de ellos.
- Informarse del funcionamiento del software y programas informáticos a utilizar.
- Estudiar del radar Furuno banda X de las Lanchas de instrucción.

La investigación y el estudio han sido constantes. Este proceso de estudio ha ido surgiendo de la necesidad de ir profundizando en los temas en los que se adentraba el proyecto. Informándose en nuevos campos desconocidos hasta la realización de este proyecto.

3.2 Hardware empleado

A continuación, pasamos a describir los distintos equipos utilizados durante la realización del trabajo. En primer lugar, se definirá el radar marino con el que vamos a trabajar tanto para la detección como para la perturbación.

3.2.1 Radar Furuno 1944C

Figura 3-1: Radar Furuno 1944C [24]

El radar utilizado como ya se comentó en el inicio de este trabajo es el radar Furuno 1944C (Figura 3-1) instalado en las Lanchas de instrucción de la ENM. El elemento radiante es un array guiaondas ranurada con polarización horizontal y un ancho de haz ($\theta_{horizontal}$) a 3 dB de 1,9º. El receptor es de tipo MIC (*Microwave Integrated Circuit*, circuito integrado de microondas). La lancha dispone de dos equipos radar similares con sus respectivas antenas a una altura de 5,3 m y 7 m respectivamente.

Los dos radares transmiten en banda X, a una frecuencia de 9.410 MHz y una tolerancia de $\pm$30 MHz, la cual hace falta para intercalar radares iguales que se pueden llegar a interferir por su funcionamiento simultáneo, como es el caso de las lanchas de instrucción. Cuyos radares transmiten en frecuencias distintas, por ello, la tolerancia de 30 MHz es un factor determinante para poder diferenciar e identificar a las distintas lanchas.

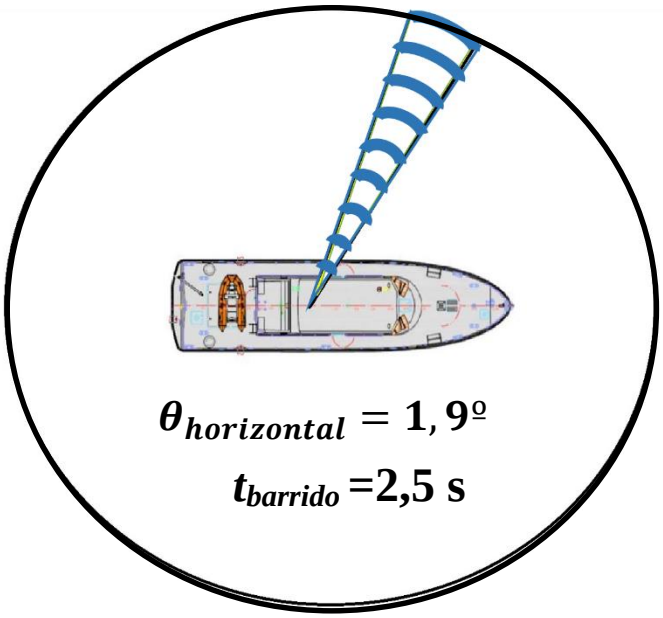


Figura 3-2: Vista superior de la Lancha emitiendo [24]

Según las especificaciones del manual (Anexo IX), el radar 1944C tiene una potencia de pico de 6 KW con una escala máxima de 64 MN. La antena gira a una velocidad de 24 rpm, lo que significa que su $t_{barrido}$ es 2,51 s, es decir la antena realiza un barrido sobre nuestra posición aproximadamente cada 2,5 s (Figura 3-2).

Teniendo en cuenta la Ecuación (**3-1)** , el tiempo durante el cual un blanco puntual es iluminado por el radar de la lancha es de 13 ms. Es igual al ancho de haz del radar dividido por la velocidad angular de la antena. Como veremos más adelante, este periodo de tiempo debe ser tenido en cuenta para realizar el jamming.

$$t_{obs}\ (s) = \frac{\theta_{horizontal}\ (rad)}{\omega\ (rad/s)} \tag{3-1}$$

$$N\ (pulsos) = \frac{t_{obs}\ (s)}{PRI\ (s)} \tag{3-2}$$

El umbral de detección de un radar marino suele oscilar sobre los -80 dBm, y el número de pulsos en el t_{obs} de este radar en particular, calculándolo a partir de la Ecuación **(3-2)** es de aproximadamente 7 pulsos. Por otro lado su ancho de haz vertical ($\theta_{vertical}$), alcanza los 22º (Figura 3-3).

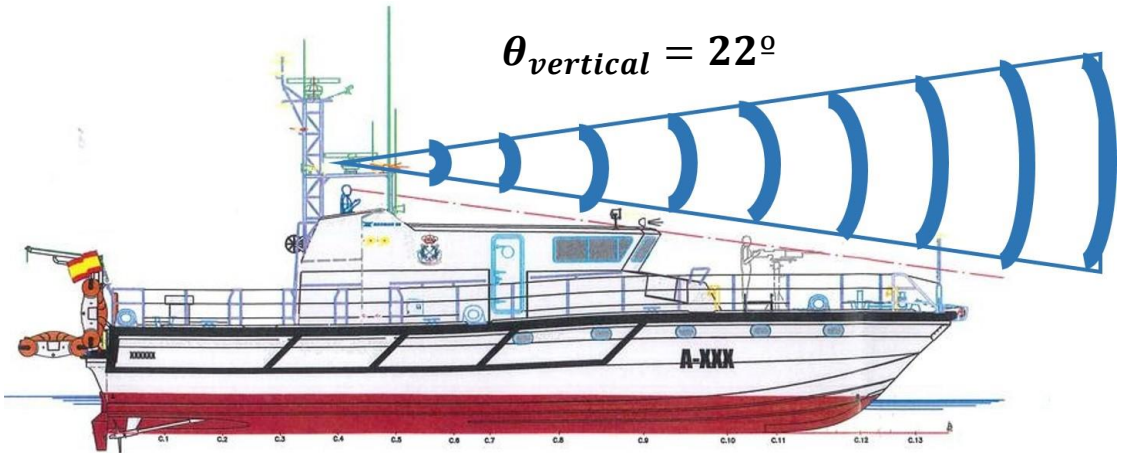


Figura 3-3: Vista longitudinal de la Lancha [21]

En cuanto al ancho de pulso, funciona en tres modalidades, corto, medio y largo. Dependiendo de la escala que esté seleccionada se utiliza un tipo de ancho de pulso [24].

Escala (MN)	Ancho de pulso (μs)	PRF (Hz aprox.)
De 0,125 a 1,5	0,08	2100
De 1,5 a 3	0,3	1200
De 3 a 64	0,8	600

Tabla 1: Modos de Ancho de pulso en radar 1944C [24]

Es importante destacar que el ancho de pulso elegido a la hora de realizar las pruebas fue determinante para la extracción de conclusiones. Por un lado, durante la detección, para interpretar e identificar los parámetros de la señal, y por otro, durante la fase de jamming y las pruebas de perturbación. En esta última fase, el ancho de pulso (PW) afecta a la señal que tenemos que emitir para perturbar y a su sincronización con los momentos de llegada y salida del pulso (TOA y TOD), explicados en el apartado 2.2.1. El ancho de banda (BW) vendrá determinado por el inverso del ancho de pulso.

A continuación, se procederá a explicar aquellos equipos utilizados tanto para la detección como para la realización del jamming o perturbación. En primer lugar, los dos SDR que se han utilizado para realizar las pruebas tanto en el proceso de detección como en el de perturbación.

3.2.2 SDR HackRF

Uno de los SDR que se utilizan en este trabajo es el Hack RF (Figura 3-4). Este SDR es capaz de transmitir y recibir señales de 1 MHz a 6 GHz. Está diseñado como un sistema de hardware abierto conectable a un dispositivo de proceso de datos (generalmente un PC) mediante USB. Funcionando en modo transmisor, su máxima potencia es de 15 dBm, factor que limitará, junto a la ganancia de la antena, la capacidad de perturbación del sistema. El dispositivo tiene dos puertos CLKIN/CLKOUT, utilizados para la sincronización en tiempo de dos SDR, dispone de un conector USB, y el correspondiente puerto SMA para la antena [25].

Internamente dispone una placa con un conmutador que conecta la antena con el bloque transmisor o receptor. Se trata de un sistema semi-duplex en el que el equipo no puede transmitir y recibir simultáneamente. También tiene dos conversores, uno digital-analógico (D/A) para la transmisión, y otro analógico-digital (A/D) para la recepción. Dispone de unos botones para el reseteo del equipo y cambio de firmware. El SDR permite trabajar con programas informáticos que se utilizan en este trabajo como SDR Console o GNU Radio.

Figura 3-4: SDR Hack RF

3.2.3 SDR Ettus N200

Este equipo USRP (*Universal Software Radio Peripheral*) (Figura 3-5) ofrece una gran velocidad de muestreo hasta 50 MS/s en ambas direcciones con muestras de 8 bits o 16 bits. En este caso se va a trabajar con muestras de 16 bits y un ancho de banda (BW) de la señal de RF de 25 MHz. Trabaja con conexión de red Ethernet y toma de corriente convencional. Dispone de dos puertos con conectores SMA, RF1 y RF2, el primero es válido para transmitir y recibir (TX/RX) y el segundo exclusivamente para recibir (RX2). Está compuesto de dos conversores y amplificadores de salida que le dan una máxima potencia de salida de 15 dBm, similar a la que aporta el Hack RF. Además de la disponibilidad de dos puertos de salida SMA, la otra diferencia con el HackRF es la banda de trabajo, puesto que el N200 alcanza solamente hasta 2,40 GHz. Esta frecuencia tan baja hace necesario el uso de un down-converter como el detallado en el apartado 2.3.1 cuando se precisa trabajar con frecuencias de microondas (banda X).

Figura 3-5: SDR Ettus N200

3.2.4 Oscilador

La función principal del oscilador local es conseguir poder sintonizar la elevada frecuencia del radar frente a las limitaciones de máxima frecuencia usable de los SDR. Tal y como se describió en el apartado 2.3.1, genera una f_{OL}, que combinada con f_{IF} genera la señal de salida requerida o en sentido de recepción, a partir de la recibida, la señal en banda base.

El oscilador de radiofrecuencia utilizado como oscilador local es el ADF 5355-EVAL (Figura 3-6), compuesto por dos placas intercambiables y alimentado con una tensión continua. La señal generada se entrega a dos salidas A y B, siendo la salida B de una frecuencia doble de la A.

Como se explicó previamente en el apartado 2.3.1, dependiendo de si estamos en fase de recepción o transmisión, utilizaremos de frecuencia del oscilador 10410 o 8410 MHz, para conseguir pasar de los 9410 MHz teóricos en los que trabaja el radar de la lancha, a los aproximadamente 1000 MHz con los que vamos a trabajar en el SDR y ordenador.

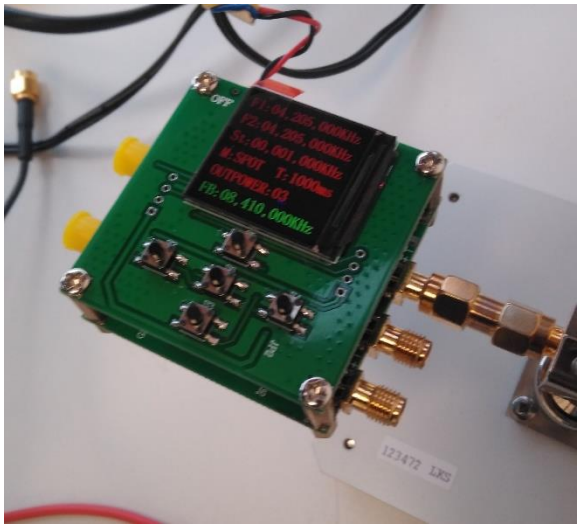


Figura 3-6: Oscilador ADF 5355-EVAL

3.2.5 Alimentación del oscilador local

La alimentación del oscilador local se obtiene a partir de una fuente de alimentación de 13,8 V de CC (Figura 3-8). Dicha fuente alimenta un conversor DC/DC (Figura 3-7) que entrega los 7 V deseados para el funcionamiento del oscilador local.

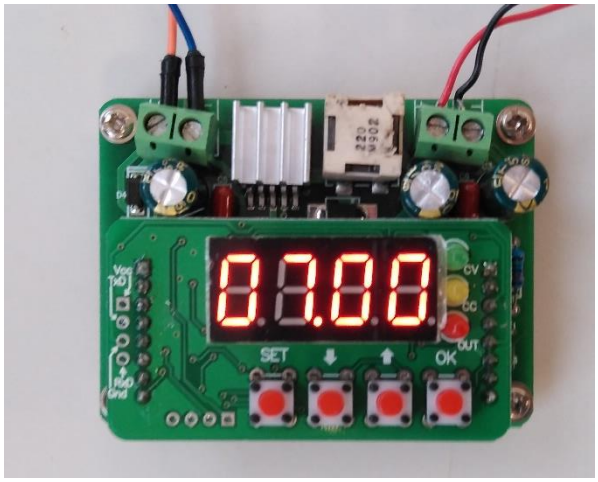


Figura 3-7: DC/DC Converter

Figura 3-8: Fuente de alimentación

3.2.6 Mezclador

El mezclador (Figura 3-9) es el modelo B3603 de la casa Mini-Circuits. Junto al oscilador local cumple la función de Up/Down Converter, su función es transformar f_{IF} con f_{OL} en f_{RF}, como se describe en el apartado 3.2.4 y viceversa, de f_{RF} a f_{IF} con f_{OL}.

Figura 3-9: Mezclador de frecuencia

3.2.7 Antena

La antena utilizada es de la casa alemana Lucas Nülle. Esta antena fue adquirida a partir de un kit de antenas, donde se incluían antenas de monopolo, dipolo, de tipo Yagi, helicoidales o patch con polarización lineal y circular. Además incluye un soporte con trípode giratorio y oscilador en banda X. La antena utilizada es el modelo SO4100-8N (Figura 3-10).

Figura 3-10: Antena Microstrip SO4100-8N

3.3 Software empleado

Para el tratamiento de la señal recibida, y generar una señal de jamming se debe usar un software informático que sea capaz de procesar la señal, extraer unos determinados parámetros de la señal y generar a partir de estos una señal de transmisión. Existen diversos programas de este ámbito, tanto aquellos que presentan la señal recibida, como los que la pueden estudiarla y pueden generarla.

- **SDR Console**. Este programa es capaz de recibir los datos recogidos en recepción por el SDR, y presentarnos el espectro en pantalla. Es indispensable para la localización de la frecuencia central de la emisión enemiga y la posterior identificación y estudio de la señal. Tiene la capacidad también de grabar señal en archivos *.wav* que luego pueden ser tratados por otro tipo de programas de procesado.

- **GNU Radio.** Es un programa para procesado de señal de SDR. Funciona con una interfaz sencilla de bloques que simulan elementos reales de filtrado, conversión, designación de variables o generación de distintas señales. Puede tanto generar señal como procesarla en recepción.

- **Matlab.** Es un software de procesado de arrays de datos mediante códigos y funciones. En este caso es útil para interpretar archivos .wav generados por SDR, y de esta forma procesar la señal recibida.

3.4 Diseño del sistema

El primer objetivo es diseñar un sistema de recepción que permita obtener los parámetros de transmisión del radar. A partir de la señal de radar almacenada en el PC, es posible obtener dichos parámetros mediante un código desarrollado en Matlab. Una vez determinados, se podrá generar la señal perturbadora. El segundo sistema desarrollado, correspondiente a la fase de jamming, generará una señal que perturbe el radar. Es importante que ambos sistemas sean compatibles y formen un sistema único.

3.4.1 Sistema receptor

Dentro de esta fase el objetivo es diseñar el sistema que recibe la señal transmitida por el radar enemigo. Además del sistema, se debía generar un algoritmo capaz, no sólo de cargar el fichero con los datos de la señal en el procesador, sino también sacar los parámetros y gráficas más relevantes de la señal recibida.

3.4.1.1 Preparación

En esta fase, se identificará la señal radar mediante el programa SDR Console, que permitirá almacenarla, localizar la frecuencia de trabajo y calcular su ancho de banda. Posteriormente, mediante funciones desarrolladas en Matlab, se realizará el procesado de datos.

Para poder comprobar el funcionamiento del sistema, debe ponerse en marcha el radar Furuno 1944C de una de las lanchas de instrucción. Se debe conectar la lancha a una toma de corriente en tierra, o en su defecto arrancar el diésel generador a bordo y además activar las baterías de servicio en la cámara de máquinas. Al arrancar el radar se le configurará el modo de pulso largo (escala mayor de 3 MN).

Este radar en transmisión emitirá una señal que interpretaremos como señal radar enemiga detectada por el sistema de Guerra Electrónica. De esta señal, de la que desconocemos su procedencia, trataremos de sacar la máxima información para identificar y clasificar el buque emisor, y por supuesto, para tener la información paramétrica suficiente para poder perturbar a ese radar.

3.4.1.2 Estructura del sistema

El sistema tiene varias partes diferenciadas que se ocupan de las distintas fases de la recepción. El procedimiento es ligeramente distinto para la conexión del SDR Ettus N200 o HackRF. Las conexiones a nivel RF y FI se realizan siempre con cable coaxial conectorizado con conectores SMA y RP-SMA.

Una vez recibida la señal radar por la antena receptora pasa al mezclador (Figura 3-11). Allí dicha señal se mezcla con la señal generada por el oscilador local, obteniéndose la señal en frecuencia intermedia, tal como se explicó en el funcionamiento del Up/DownConverter en el Apartado 2.3.1.

En este caso se ha ajustado el oscilador local a una frecuencia de 10410 MHz. Según la Ecuación (**2-4)**, para un radar que trabaja a 9410 MHz, se generará una señal a una frecuencia intermedia de 1000 MHz.

La señal obtenida a frecuencia intermedia, f_{IF}, entra en el SDR. Para el desarrollo del trabajo se utilizaron indistintamente el SDR Ettus N200 y el SDR HackRF, pese a que finalmente, en las pruebas se optó por usar el Ettus. En este, se usó la entrada SMA RF1, la cual funciona indistintamente en recepción y transmisión (RX/TX), lo que facilita la realización de ambas operaciones sin modificar el cableado: primero se recibiría la emisión del radar víctima, se obtendrían los parámetros de la señal, y se cambiaría al modo de transmisión para así perturbar esa emisión (Figura 3-11).

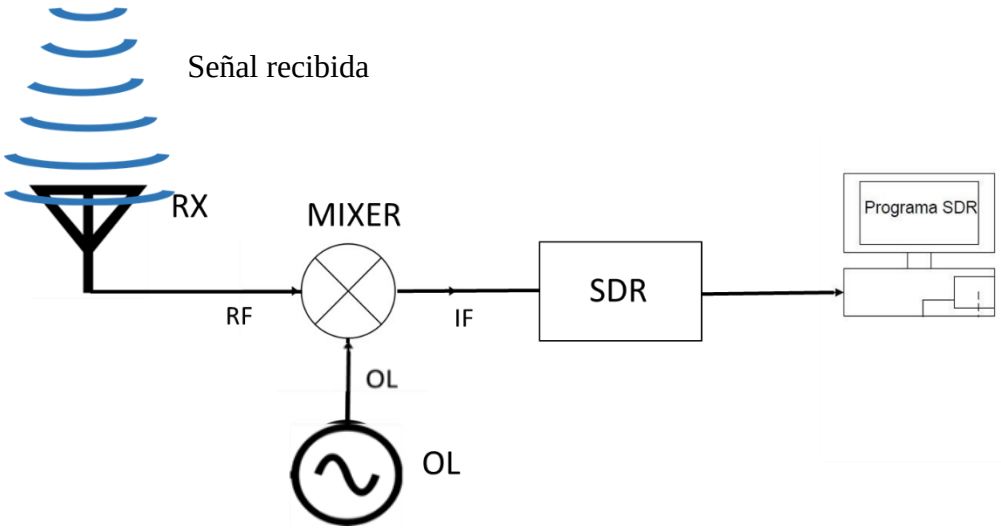


Figura 3-11: Esquema de la estructura del sistema receptor

La señal digitalizada se obtiene del SDR gracias a su puerto Ethernet que lo conecta con el ordenador. En primer lugar, la señal será identificada mediante el programa SDR Console y se almacenará una porción de ella. Posteriormente, se procesará mediante Matlab. Todo este proceso será explicado con detalle en el apartado siguiente.

3.4.1.3 Generación de algoritmos de detección

Para el diseño de los algoritmos se tomaron de referencia distintos trabajos que versaban sobre códigos que interpretaban señales radar y obtenían sus parámetros principales [16]. El software desarrollado carga el archivo de señal en Matlab y representa la señal gráficamente, mostrando su diagrama polar. Por último, un código obtiene los parámetros del ancho de pulso (PW), periodo de repetición de pulsos (PRI), fundamentales para poder identificar la emisión y realizar la perturbación.

En primer lugar, la señal debe ser localizada en el espectro de frecuencias, utilizando el programa SDR Console. En él se localiza manualmente la frecuencia intermedia f_{IF}, a la que recibimos la señal desde el SDR (Figura 3-12).

En este programa, una vez localizada la emisión y la frecuencia, se graba una porción de señal de muestra, aproximadamente 10-11 segundos. Esta señal se carga posteriormente en Matlab para obtener un array con los datos muestreados con una determinada frecuencia de muestreo (f_S).

El programa almacena un archivo de formato *.wav*, en una carpeta determinada del disco duro para su carga posterior en el algoritmo.

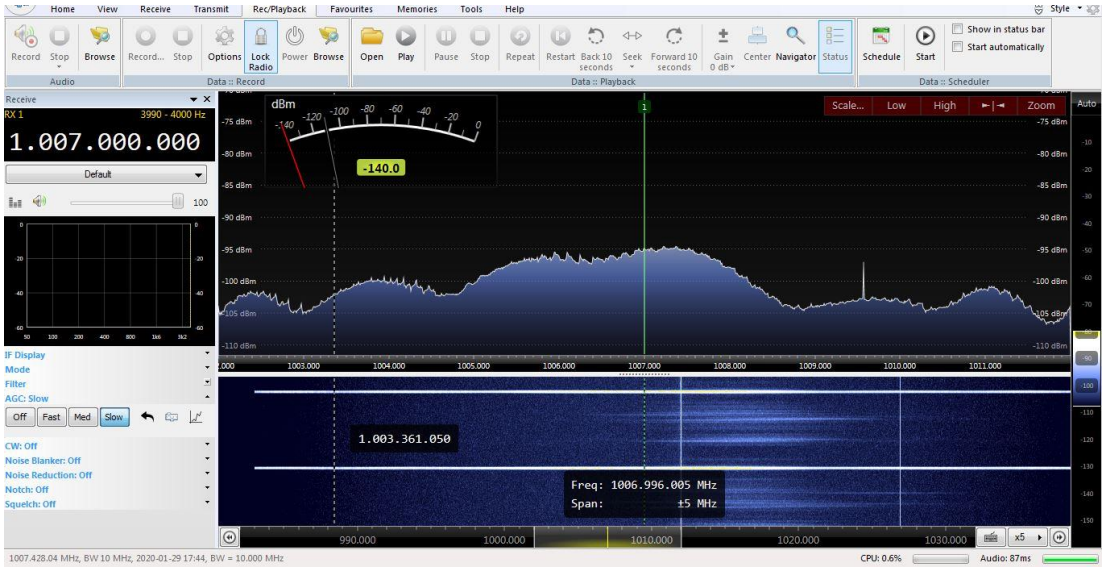


Figura 3-12: Detección de señal radar con el programa SDR Console

El algoritmo de detección generado con Matlab puede dividirse en 4 partes principales:

- Algoritmo de detección (*detection.m*).
- Algoritmo de cálculo de los parámetros principales del radar (*calculate_PDW.m*).
- Algoritmo de carga de datos de la señal (*load_radar_data.m*).
- Algoritmo de generación de diagramas de radiación (*polar_dB.m*).

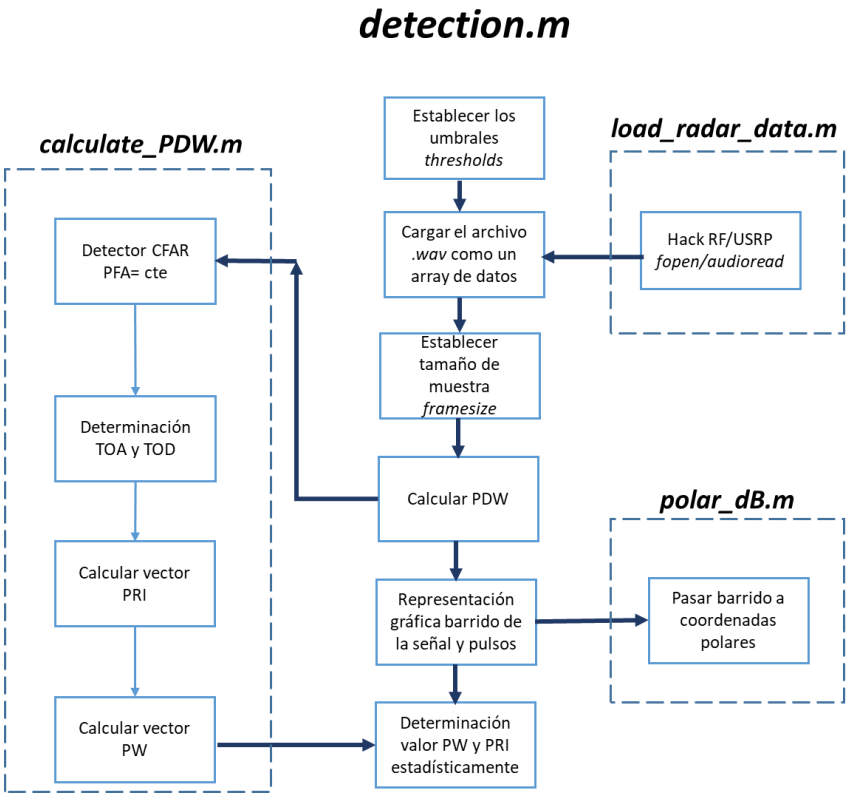


Figura 3-13: Diagrama explicativo del código *detection.m*

El código *detection.m* (Anexo III), como se muestra en la Figura 3-13, incluye la ejecución de las funciones *calculate_PDW.m* y *load_radar_data.m*, que serán explicadas a continuación. Además, se encuentra también el código *polar_dB.m* sirve para obtener el diagrama de radiación de la antena emisora, obteniendo su representación polar, que será explicado en el apartado 3.4.1.4.

El código de la función *load_radar_data.m* es el código de carga de datos, viene contenido en el Anexo IV. El objetivo de esta función es cargar el archivo *.wav* generado por el SDR Console con el comando *audioread* y pasar el formato de enteros de 16 bits a un formato *double*, en el caso del uso del Ettus N200. En el caso del HackRF se utilizaría el comando *fope*n.

En cuanto al código *calculate_PDW.m*, es el código de cálculo del PDW, y como se ve en el Anexo V, muestra los comandos necesarios para sacar los parámetros principales del radar detectado: ancho de pulso (PW) y periodo de repetición de pulsos (PRI), que son presentados al final de la ejecución del código.

3.4.1.4 Determinación de parámetros de la señal

Para que el programa detecte los flancos del pulso, es decir su llegada y final se utiliza un sistema de *thresholds*, es decir dos niveles que se determinan dependiendo del pulso de la señal recibida. Estos marcan el margen dentro del cual la detección de los TOA y TOD (parámetros que marcan el comienzo y la finalización del pulso) va a ser fiable y donde se reduce la posibilidad de falsos pulsos [16]. Los niveles deben ser introducidos manualmente una vez recibida la señal y registrada su amplitud. En la Figura 3-14, se ven los dos niveles de *threshold* establecidos en el barrido.

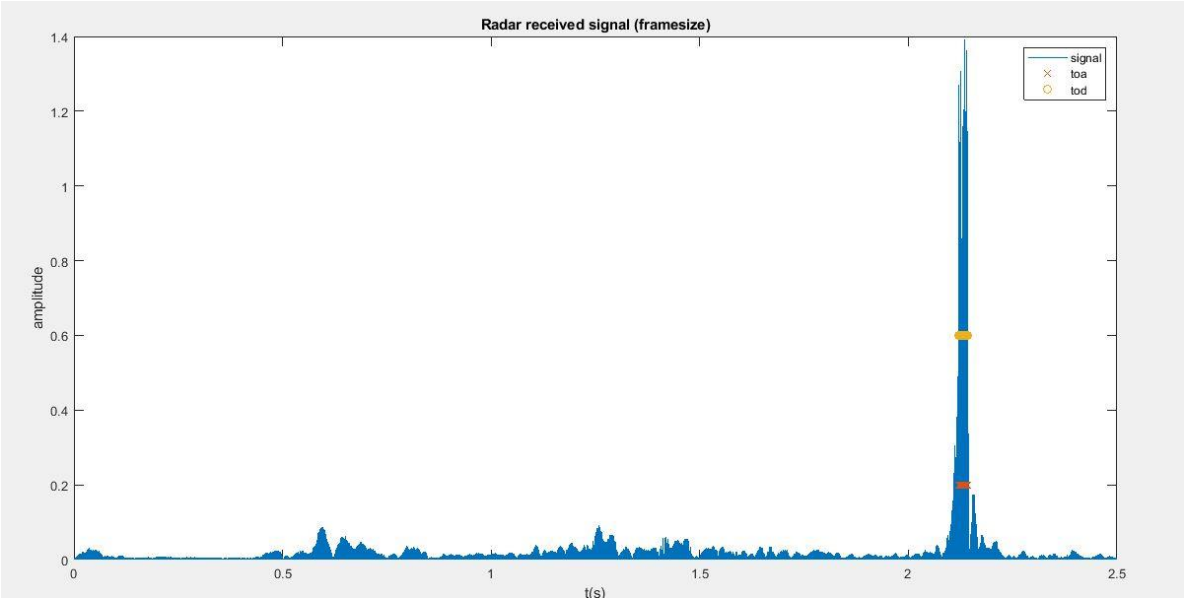


Figura 3-14: Detección de un barrido de señal radar

Como se ve en la Figura 3-15, se establecen dos niveles de *threshold* que marcan los puntos de amplitud donde la detección del pulso va a ser certera. Se marcan en amarillo la detección de los TOD y en rojo la detección de los TOA. Entre los pulsos detectados dentro del haz hay pulsos falsos, es decir pulsos que son detectados pero no se corresponden con los pulsos que el radar ha transmitido realmente, sin embargo el algoritmo aproxima los anchos de pulso estadisticamente fuera de un determinado rango y los descarta, obteniendo los valores de ancho de pulso correctos (Figura 3-16). Lo mismo ocurre con

los valores de PRI calculados e introducidos en un array, estos datos son procesados y se eliminan los valores sin sentido, demasiado desplazados de la media.

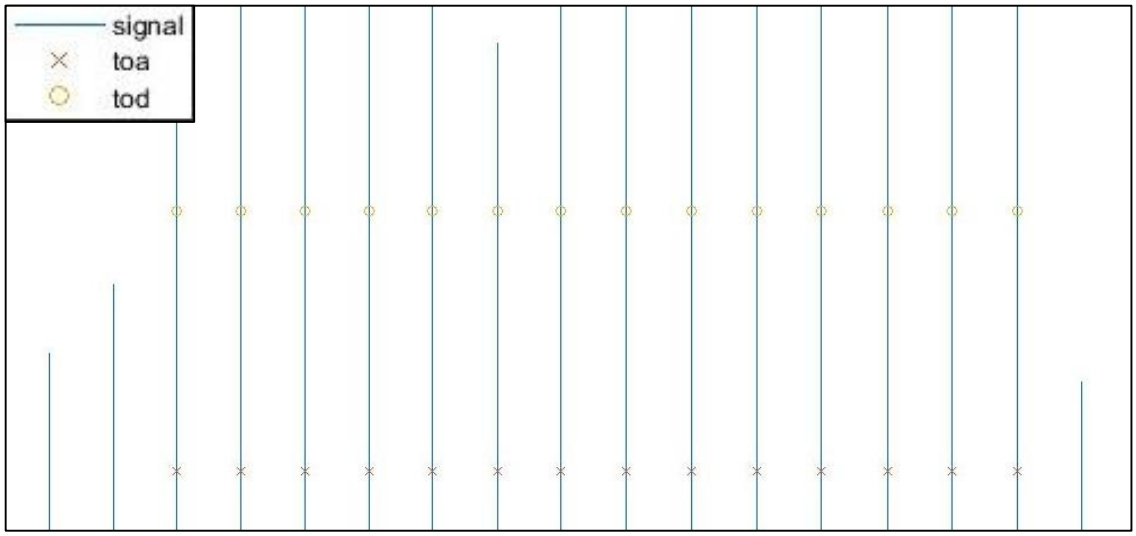


Figura 3-15: Detalle de los pulsos dentro de un mismo haz con las marcas de TOA Y TOD

```
% remove outliers
% criteria:  remove points more than three standard deviations from the
% mean of the data
threshold = 1 * std(pw);
validRange = mean(pw) + threshold;
pwo = pw(pw <= validRange);
pdpwo = fitdist(pwo','Normal');
fprintf('Detected PW: %4.2f us \n',pdpwo.mu*1e6);
```

Figura 3-16: Código de determinación de valores de ancho de pulso válidos

Después de seleccionar la duración de la señal a analizar y la frecuencia de muestreo, el funcionamiento principal de la determinación del parámetro del ancho de pulso se basa en el uso del TOA y el TOD, previamente calculados. La diferencia entre ambos parámetros es el ancho de pulso (PW), el problema es determinar los TOA y TOD de la señal detectada, que pasa a ser un array de datos, y conseguir que un bucle detecte el valor lógico entre las muestras.

Por otro lado, la determinación del PRI pasa simplemente por la diferencia entre dos llegadas de pulso consecutivas (TOA). Como se observa en la Figura 3-17, el código funciona con un bucle que va calculando el PW y PRI para cada TOD y TOA, obteniendo un array de valores que son divididos por la frecuencia de muestreo con el fin de obtener los valores del ancho de pulso y PRI en número de muestras.

```
% Calculate PRI vector
if toa_cnt>1
    for idx = 2:toa_cnt-1
         pri(idx) = toa(idx) - toa(idx-1);
    end
else
     disp('Not enough data to calculate PRI');
end

% Calculate PW vector
if (toa_cnt >= 1) && (tod_cnt >= 1)
    for idx = 1:tod_cnt-1
        pw(idx) = tod(idx) - toa(idx);
    end
else
    disp('No hay datos suficientes para calcular el PW');
end

toa = toa/fs;
tod = tod/fs;
pw  = pw/fs;
prf = fs./pri;
```

Figura 3-17: Código para el cálculo del Ancho de pulso y PRI

Además el código incluye un detector CFAR, que mantiene la probabilidad de falsa alarma constante (PFA) (Figura 3-18), que evita la detección de falsos pulsos o ruido. Este detector asegura que los pulsos detectados son reales. Finalmente, el algoritmo presenta el valor final obtenido de PW y PRI.

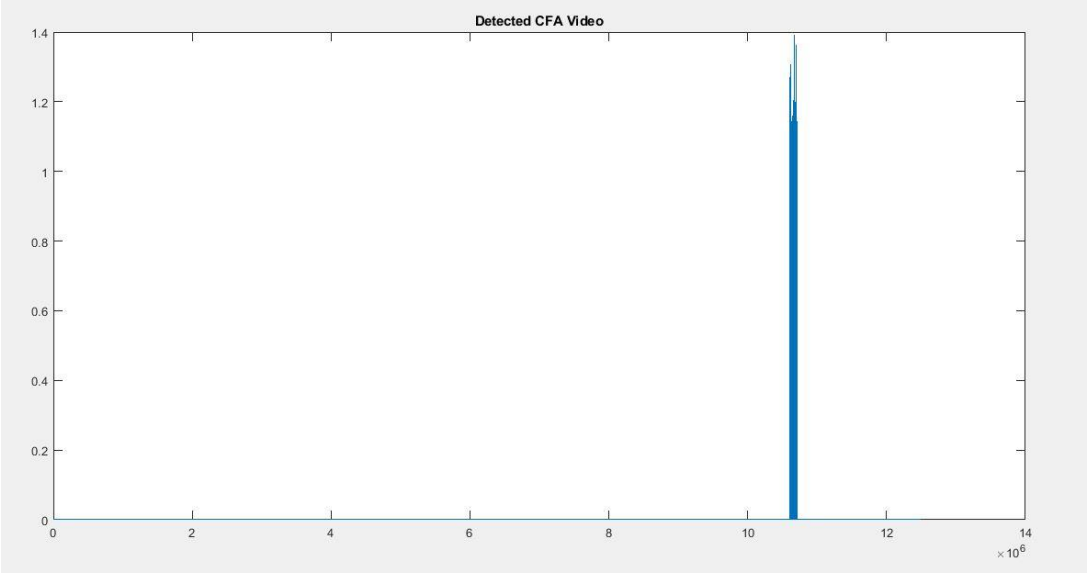


Figura 3-18: Señal detectada tras el procesado CFAR (PFA constante)

Por último, cabe destacar que todas estas gráficas y diagramas son presentados por pantalla a través de la ejecución del algoritmo principal *detection.m* y sus funciones internas.

3.4.1.5 Diagramas de radiación de las antenas

Una vez obtenidos los valores de ancho de pulso y PRI necesarios para identificar y clasificar el tipo de señal radar que se está recibiendo, surge otro problema, que es diferenciar señales procedentes de radares del mismo tipo y obtener su diagrama de radiación. Es cierto que incluso radares del mismo tipo emiten en frecuencias ligeramente distintas, pero existe la necesidad de identificar la forma de radiar del radar, para así relacionarlos con una unidad en particular dentro de un modelo o clase de buque. Es decir, se quiere dotar a nuestro sistema de capacidad de discernir equipos radares similares de buques de la misma clase.

En nuestro caso diferenciaremos los radares por el diagrama de radiación las antenas y las frecuencias de trabajo de las cuatro lanchas de instrucción: A-121 Guardiamarina Barrutia, A-122 Guardiamarina Chereguini, A-123 Guardiamarina Rull y A-124 Guardiamarina Salas.

El código *polar_dB*.m, que se encuentra en el Anexo VI, representa en coordenadas polares la señal recibida en el tiempo de un barrido, es decir la señal recibida durante un giro completo de la antena del radar, de esta forma se obtiene el diagrama de radiación de la antena [26] . En el diagrama, mostrado en la Figura 3-19, se observa como destaca el lóbulo principal, así como los lóbulos laterales y el posterior.

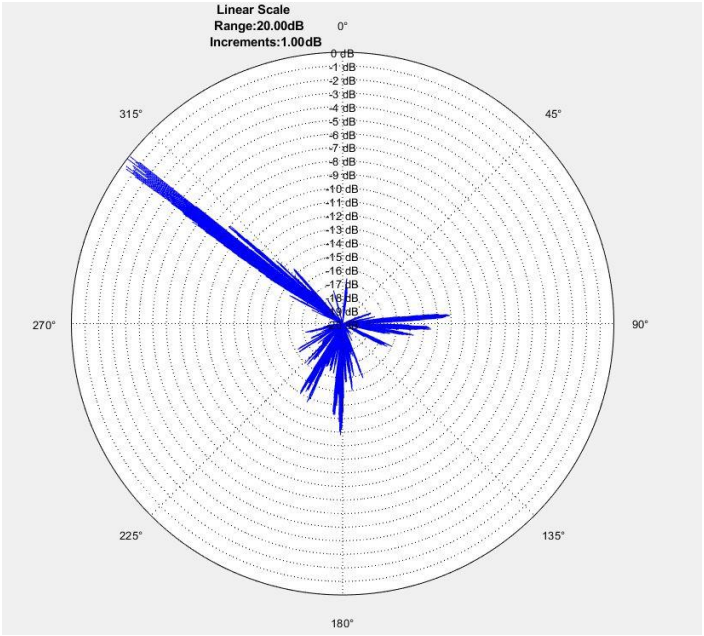


Figura 3-19: Diagrama de radiación del radar de la Lancha Guardiamarina Barrutia

En el diagrama polar de la Figura 3-20 se puede observar perfectamente ampliando la imagen el ancho de haz emitido por el radar. Cuya anchura se corresponde con los aproximadamente 2º que cita el manual de dicho radar. Además de ver el ancho de haz, en la se diferencian también los pulsos integrados dentro de cada haz, calculados en el apartado 3.2.1.

Hay que resaltar que, pese a que el resultado obtenido en el diagrama de radiación es coherente, al encontrarnos en la zona de campo cercano de la antena del radar (las medidas se ha realizado a unos 30 m), , el diagrama no es totalmente real y debería obtenerse en campo lejano, Teniendo que la longitud de onda es $\lambda = c/f = 3 \cdot 10^8/9410 \cdot 10^6 = 0{,}032\, m$ y la antena tiene unas dimensiones de $D = 1{,}2$ m (Anexo IX), la distancia de campo lejano vendrá determinada por la expresión siguiente (3-3) [23]:

$$d_{CL} = \frac{2D^2}{\lambda} \approx 90\ m \tag{3-3}$$

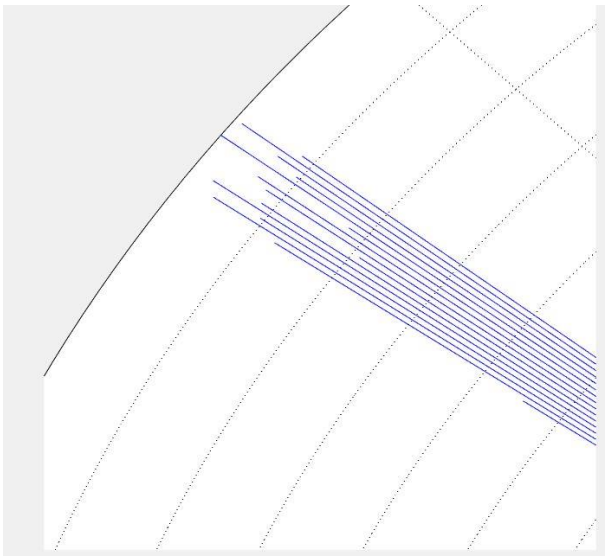


Figura 3-20: Detalle del lóbulo principal o ancho de haz de la señal del radar

3.4.2 Sistema de perturbación

Una vez se obtienen a través de nuestro sistema de ESM, los parámetros fundamentales del radar para la perturbación, como pueden ser la frecuencia en la que trabaja el radar, ancho de pulso (PW), período de repetición de pulsos (PRI), etc. El sistema de Guerra electrónica ya tiene localizado e identificado el radar enemigo, gracias a los parámetros y a haber obtenido el diagrama de la antena de ese buque en concreto, en este caso el radar Furuno 1944C de una de las Lanchas de instrucción.

3.4.2.1 Preparación

En esta etapa el principal objetivo es diseñar un sistema capaz de realizar jamming sobre el radar de la lancha (ECM). Este montaje es muy similar al del sistema receptor y tiene como objetivo emitir una señal en la misma frecuencia del radar en dirección opuesta a la onda emitida por este. La generación de la señal perturbadora se realiza con el programa GNU Radio, probando distintos tipos de señal y comprobando la eficacia del jamming sobre la pantalla del radar. Posteriormente analizaremos las distintas variantes de jamming que se han realizado, que pasan desde la emisión de ruido blanco, a la perturbación a través de una señal pulsada.

Como se ha comentado en el apartado 3.2.1, la lancha tiene dos radares a distintas alturas. Se realizaron las pruebas con el radar bajo para coger un mayor ángulo de haz vertical a la hora de perturbar, sin embargo después durante el desarrollo de las mismas, se comprobó que el jammer afectaba por igual a ambos radares pese a la diferencia de altura.

Otro factor determinante es la distancia de la antena jammer al radar emisor, esta afectará tanto sobre el ancho del sector de jamming generado, como a la potencia necesaria para crear esa perturbación.

El proceso de preparación del sistema es simple, en primer lugar, se debe poner el radar a emitir, simulando que una exploración enemiga intentando localizar nuestro blanco. Una vez encendido el radar previamente alimentado, se selecciona el pulso largo (escala mayor de 3 MN) y se aumenta la ganancia.

El aumentar la ganancia viene motivado por el aumento proporcional de la ganancia y la ERP del jamming como se ve en la Ecuación (**2-1)**. Sin embargo, para reconocer bien el sector o área perturbada, es mejor empezar con una ganancia media e ir aumentándola progresivamente, y así de esta forma diferenciar más claramente los ecos o ruido de entorno con nuestro jamming.

Es importante marcar con la línea de demora radar (EBL) y el anillo de distancia (VRM), la dirección y distancia de la perturbación en las distintas pruebas, para que así sea más fácil identificar en la pantalla si el jamming ha sido efectivo o no.

3.4.2.2 Estructura del sistema

Una vez dispuesto el radar emisor, se realiza el montaje de nuestro jammer o perturbador. El sistema tiene la misma disposición de sus componentes que en la fase de detección, a excepción de algunas configuraciones.

El sistema es muy similar al del sistema receptor (Figura 3-21). Se dispone el ordenador con el software del GNU Radio instalado, este conectado al SDR y Up /Down Converter, compuesto por el mezclador y el oscilador local. El mezclador recibe las frecuencias IF y OL, y pasa la RF a la antena, que transmite en la frecuencia deseada para la realización del jamming.

En este caso se ha ajustado el oscilador local a una frecuencia de 8410 MHz. Según la Ecuación (**2-4)**, para un radar que trabaja a 9410 MHZ, se generará una señal a una frecuencia intermedia de 1000 MHz.

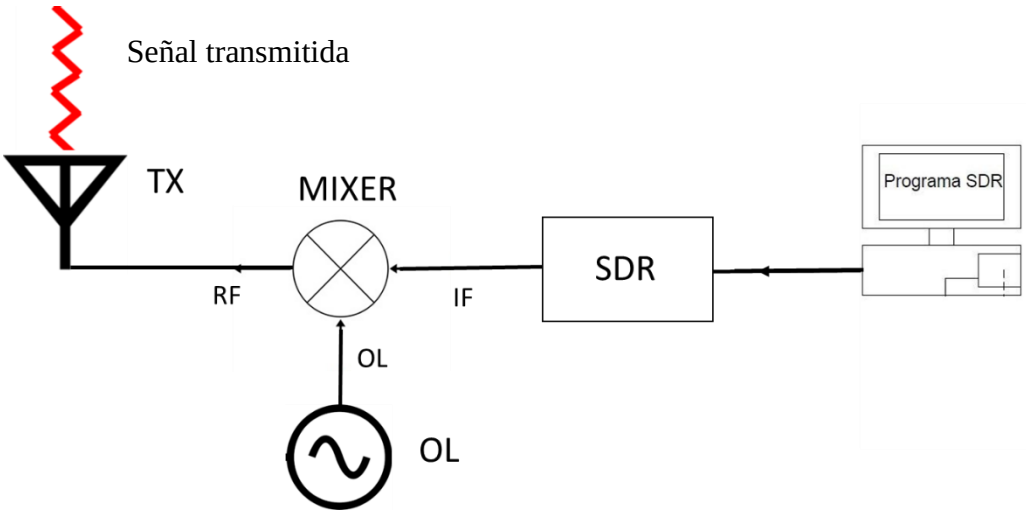


Figura 3-21: Esquema de la estructura del sistema de perturbación

3.4.2.3 Configuración GNU Radio

En este apartado pasamos a explicar el proceso de generación de la señal de jamming a través del esquema desarrollado en entorno GNU Radio. Este programa genera la señal deseada con unos determinados parámetros, frecuencia y tipo de señal, y la pasa al SDR para su emisión. En el esquema desarrollado (Figura 3-22) se pueden diferenciar los siguientes elementos:

- Los bloques correspondientes a las variables que entran en juego, ganancia de la antena (g), ancho de pulso (tau), periodo de repetición de pulsos (PRI) y frecuencia central a la que vamos a perturbar (center_freq). (SLIDE). Destacar también la introducción de la variable de la frecuencia de muestreo (sample_rate).
- Las funciones que generan los distintos tipos de señal, la fuente de señal cuadrada, triangular sinuidal o cosinuidal, el generador de ruido blanco o ruido rápido o aleatorio (Gaussiano).
- Los bloques de salida y enlace a los puertos del SDR, existen dos bloques de salida distintas configuradas en función de si el SDR elegido es el Ettus N200 o el HackRF.

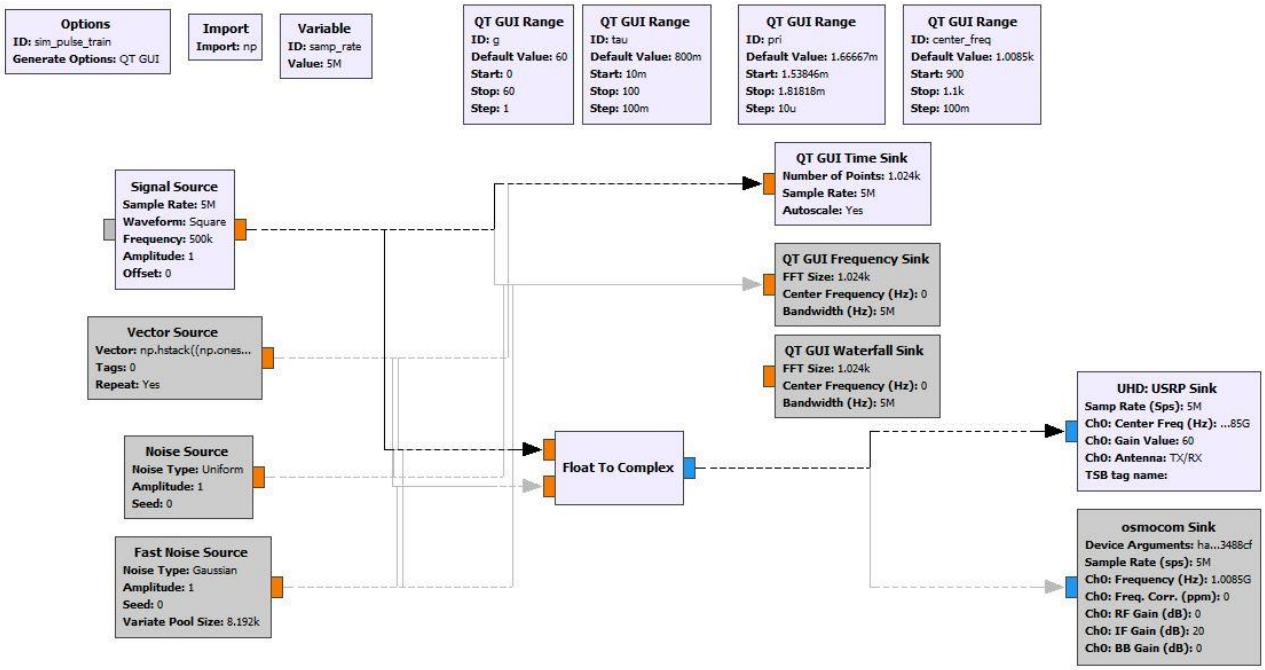


Figura 3-22: Diagrama de funciones de GNU Radio para generación de la señal de jamming

Los bloques QT GUI Sink permiten representar en tiempo real la señal que se está generando. Así de esta forma, se puede comprobar la señal que se está enviando al SDR, es decir, la señal de perturbación. Una vez se ha decidido con qué tipo de señal se quiere perturbar, se habilitan las conexiones en el diagrama de funciones y se ejecuta el programa. En ese momento se generan cuatro barras deslizantes (*sliders*) que nos permiten desplazar tanto la frecuencia de transmisión, ganancia de antena, PRI como el ancho de pulso (Figura 3-23). Cabe destacar que la frecuencia con la que estamos trabajando es la frecuencia intermedia, f_{IF}.

Figura 3-23: Barras deslizantes (*sliders*) en el programa GNU Radio

4 RESULTADOS / VALIDACIÓN / PRUEBA

Tras haber analizado el desarrollo del trabajo, este apartado aglutina las distintas pruebas o ensayos que han sido realizados en cada una de las fases, y sus correspondientes resultados y conclusiones. Las cuáles nos confirman la efectividad y sugerirán las mejoras del sistema de Guerra electrónica desarrollado.

4.1 Pruebas de detección

4.1.1 Pruebas con señal simulada

Los primeros pasos en esta fase han sido la generación de códigos de Matlab, capaces de generar una señal simulada para probar los algoritmos de obtención de parámetros radar sin emplear el sistema físico de recepción (Figura 4-2).

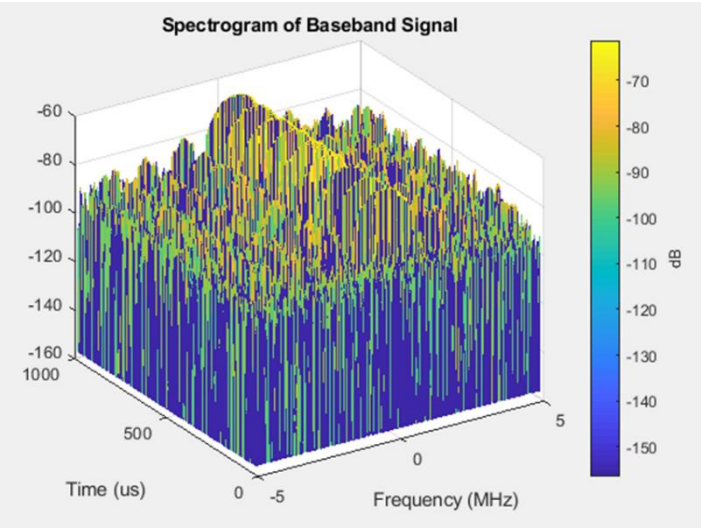


Figura 4-2: Espectograma de la señal generada

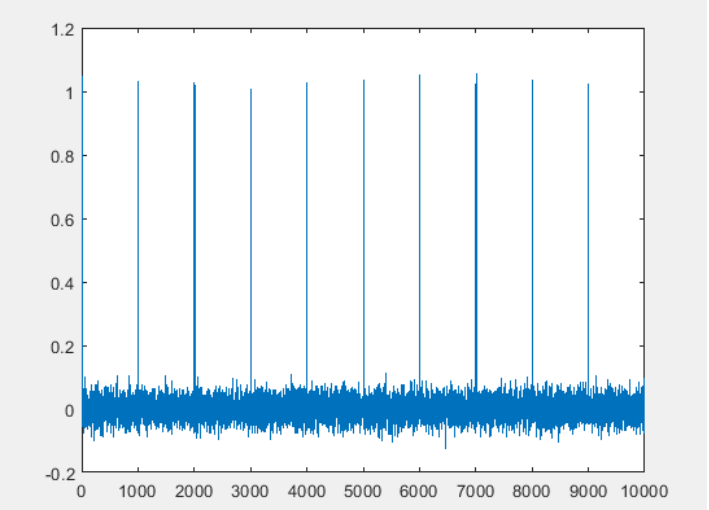


Figura 4-1: Señal generada simulando pulsos radar

El código desarrollado (Anexo VIII), genera señal a partir de ciertos parámetros introducidos: Ancho de pulso (PW), frecuencia de muestreo (f_S), PRF, Número de pulsos y Relación Señal a Ruido (SNR). De esta forma los resultados de los parámetros que debe dar el algoritmo de detección al ejecutar esta señal ya son conocidos desde un principio.

Por otro lado, es muy importante el concepto de la SNR, ya que al generar una señal ideal se ve todo muy limpio y claro, sin embargo, cuando la detección tenga que actuar con una señal real con ruido e interferencias puede tener problemas identificar los pulsos. Por ello, durante las pruebas se fue probando con señales simuladas cada vez con menor SNR, comprobando así la efectividad y preparando la detección frente a una posterior señal real.

Para la señal generada en la Figura 4-1, se ha seleccionado una SNR de 30 dB, por lo tanto los pulsos se distinguen mejor y la señal sale mucho más limpia que en el caso de la Figura 4-3, en el que se ha generado la señal con una SNR de tan sólo 15 dB.

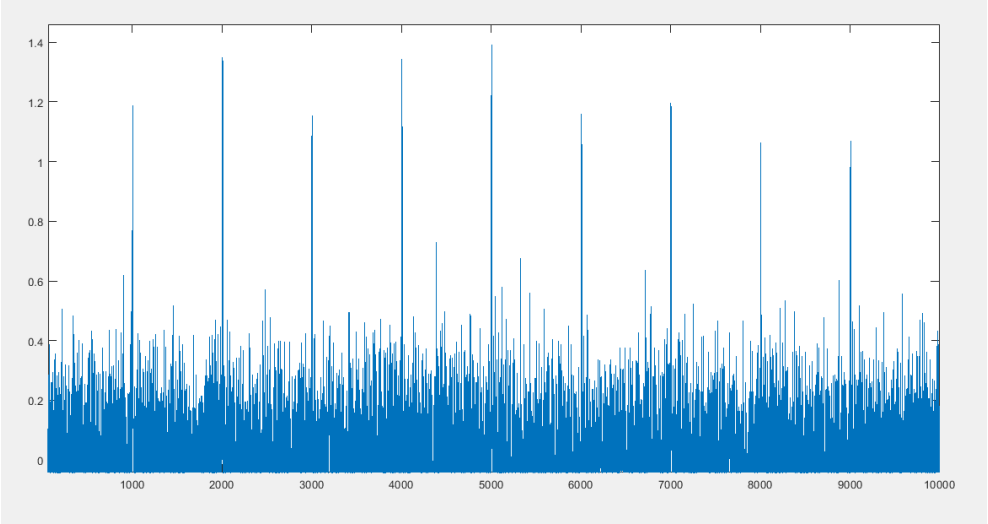


Figura 4-3: Señal generada con SNR de 15 dB

Los resultados de estas pruebas acabaron siendo satisfactorios ya que se obtenía el valor de los parámetros con los que se había configurado la señal generada.

4.1.2 Pruebas con señal real

La segunda fase fue conseguir grabar señal real del radar mediante el programa SDR Console y nuestro sistema de detección. De esta forma se podría trabajar posteriormente con esa señal con el Matlab.

Para realizar las pruebas es necesario ajustar el radar de la lancha en pulso largo. Durante la mayoría de las pruebas se utilizó el radar bajo de la lancha Guardiamarina Barrutia, sin embargo, posteriormente se realizaron pruebas con los radares de otras lanchas, comprobando el ligero desfase en frecuencia que tienen entre ellos.

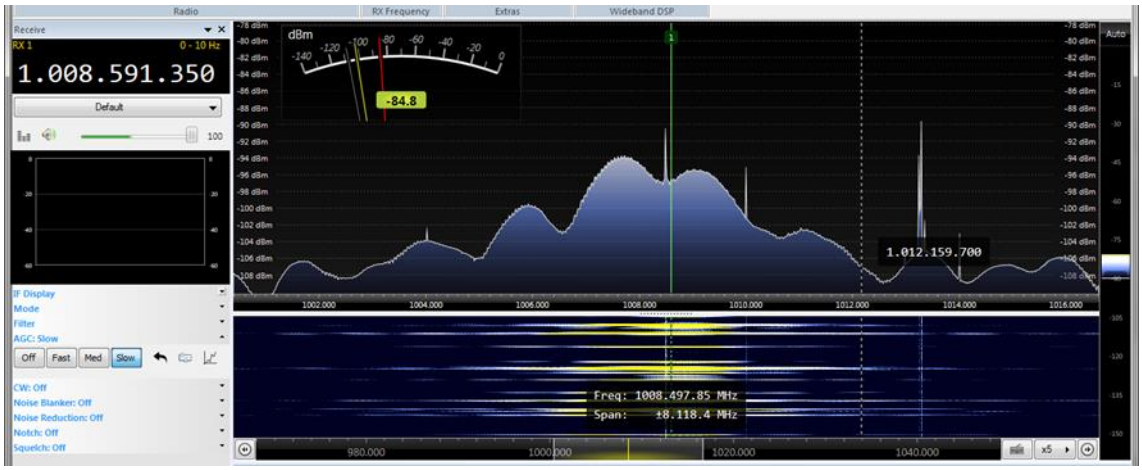


Figura 4-4: Detección y grabación de señal radar

El sistema de detección fue montado en el laboratorio de simulación, a 30 m del radar de la lancha, desde el cual con la antena situada sobre un trípode a la altura de la ventana se exploraba la multitud de señales recibidas.

Una vez identificada la señal del radar en el espectro (Figura 4-4) y centrada en la presentación del SDR Console, se realiza la grabación de la señal, normalmente de entre 8 y 11 segundos para coger varios barridos. El tiempo de barrido de la antena depende del ancho de haz horizontal ($\theta_{horizontal}$) y de la velocidad de giro de la antena (ω), como se muestra en la Ecuación (**3-1)**. Esto no significa que se vaya a muestrear el periodo completo de tiempo, luego en el código se selecciona el tiempo de muestreo.

4.2 Pruebas de perturbación

4.2.1 Primeras pruebas

Los ensayos de esta fase comenzaron una vez desarrollado el sistema y montaje con los distintos componentes, como la configuración del programa generador de señal. El principal problema en los primeros días era la falta de conocimiento del equipo radar al que se pretendía perturbar. Eso llevó a cometer errores en el tratamiento de la configuración interna del radar y comprobación de los resultados.

En primer lugar se intentó realizar una perturbación de ruido blanco, también llamada perturbación de barrera en onda continua (Noise jamming), explicada en el apartado 2.1.3, generando una señal que fuese capaz de perturbar el radar a una distancia de 7 m. Se eligió para las pruebas el radar bajo de la lancha *Guardiamarina Barrutia*, atracada en el muelle, eligiendo este radar en vez del alto por estar ser más directivo dentro del ancho de haz vertical ($\theta_{vertical}$).

Después de poner el sistema en detección para identificar la frecuencia a la que estaba transmitiendo el radar, se cambió la configuración a transmisión para realizar el jamming. Esta serie de perturbaciones se realizaron con el pulso largo y pulso corto, en escala siempre menor a 5 millas, probando distintos tipos de señales que serán citados posteriormente.

La prueba sí confirmó que la perturbación se estaba realizando adecuadamente. Ya que el radar alto también se veía afectado y al variar la frecuencia central del jamming de la del radar a perturbar, el jamming desaparecía completamente de la pantalla del radar.

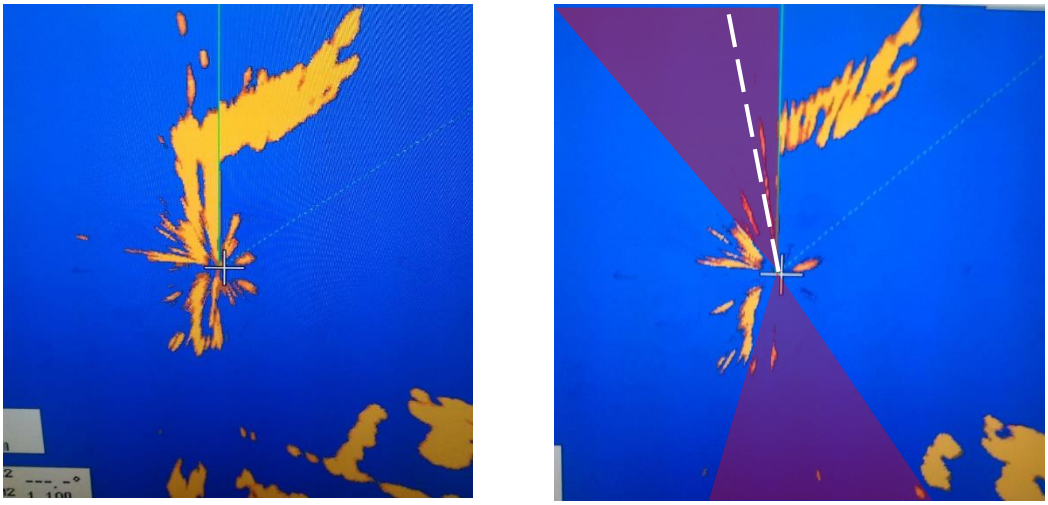


Figura 4-5: Jamming de ruido blanco con pulso corto en escala mínima

Sin embargo, la prueba no mostró el resultado esperado, en vez de generar una zona de ruido que solapase todos los crudos existentes en ese sector, anulaba un sector en la zona del lóbulo principal, un sector menor que entraba por lóbulo trasero, y finalmente una disminución de los crudos en ciertas zonas de ambos lados diagonales o perpendiculares a la dirección del jammer. Ocurría dentro de las escalas menores a 5 MN, tanto en pulso corto como largo, eliminando posibles contactos, muelles, objetos o tierra.

En la Figura 4-5 podemos observar que la perturbación sectorial deja ciego al radar en 16º, siendo la dirección del jammer la demora indicada con línea blanca discontinua, entrando por el lóbulo principal y también afectando al lóbulo trasero en menor proporción (Figura 4-6).

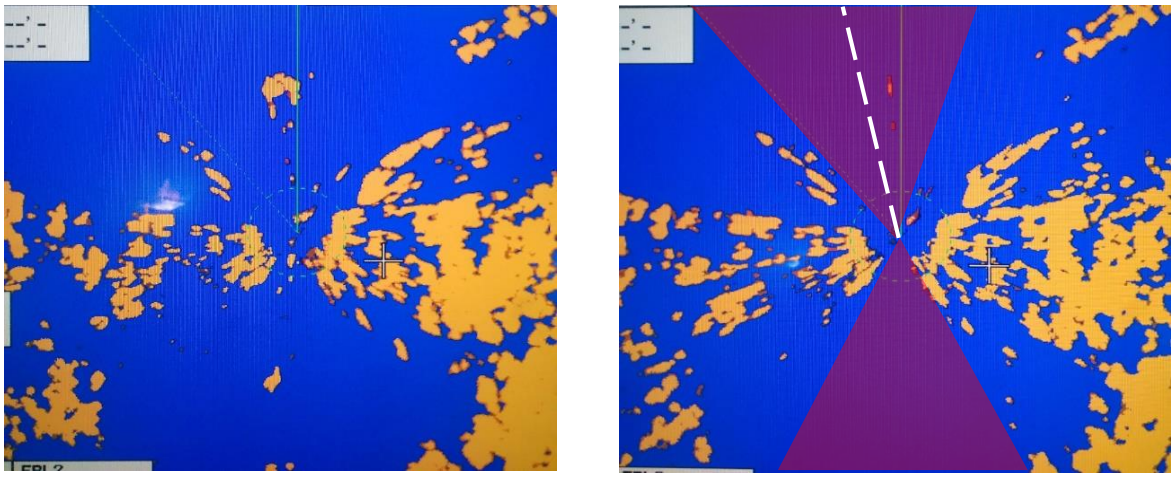


Figura 4-6: Jamming de ruido blanco con pulso largo con escala menor a 5 MN

La presentación de los sectores como zonas anuladas, donde el radar no es capaz de detectar ningún crudo puede venir motivada por la saturación de alguna etapa del sistema radar. Los radares utilizan amplificadores que amplifican más la señal recibida de blancos lejanos y menos la recibida de blancos cercanos. Esto puede explicar la anulación de los crudos recibidos por el radar dentro de las 5 MN. [27]

Inicialmente el problema se atribuyó a la poca potencia del perturbador por lo que se decidió realizar una prueba a mayor distancia, 28 m, comprobando que en esa escala no era posible apreciar perturbación a cierta distancia.

Sin embargo, gracias a probar distintas escalas del radar, se descubrió que el jamming si estaba siendo efectivo, es decir, si estaba generando un sector de ruido al radar de la lancha. Este jamming es efectivo solo a partir de las 5 MN en adelante con su correspondiente pulso largo. Esta comprobación descartó completamente el problema de potencia como razón de los problemas que se habían encontrado al intentar conocer la efectividad del jamming.

En definitiva, si se realiza un jamming en barrera, el radar es perturbado en un sector de 10º, cubriendo todo el sector desde las 4,15 MN hasta el máximo alcance. Como se muestra en la Figura 4-7, el jammer transmite su emisión desde el 355º, obteniendo un sector totalmente interferido, ocultando todo posible contacto en ese sector incluido el barco emisor, en el caso del jammer esté instalado a bordo y no en tierra.

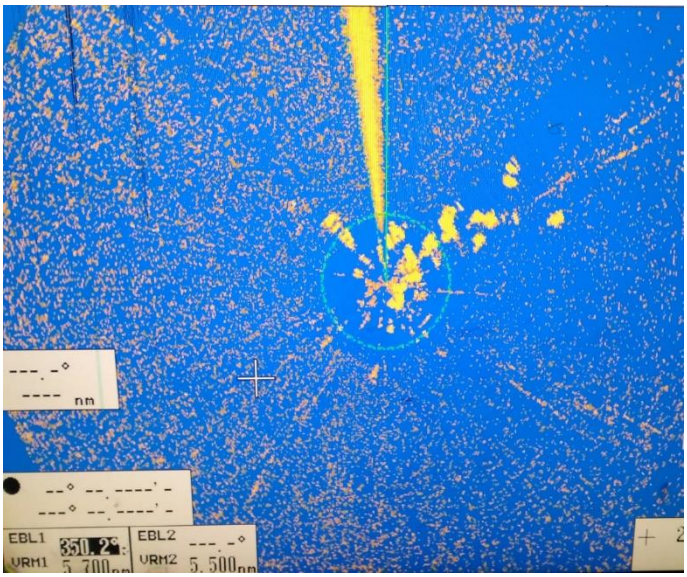


Figura 4-7: Jamming de barrera con señal cuadrada y pulso largo

4.2.1 Pruebas de distintos tipos de señal

Una vez obtenida la confirmación de que el jamming era efectivo, se realizó una segunda fase de pruebas usando distintos tipos de señal, variando ganancia de la antena jammer y la frecuencia de la señal cuadrada.

Con diferencia el jamming más efectivo es el realizado con señal cuadrada, debido a que la forma de la señal se aproxima a un tren de pulsos (Figura 4-8). Con este tipo de señal se consiguió un sector de jamming eficaz y capaz de enmascarar por completo blancos o crudos de poco porte.

Otro factor muy importante es la ganancia del transmisor, al disminuirla modifica la efectividad del jamming (ERP) tal como muestra la Figura 4-9, disminuyendo notablemente la densidad del ruido generado en el sector, además de también el ancho de sector perturbado. Sin embargo, al cambiar la ganancia de 5 dB a 10 dB y luego a 30 dB, se mantiene el ancho del sector perturbado alrededor de los 10º.

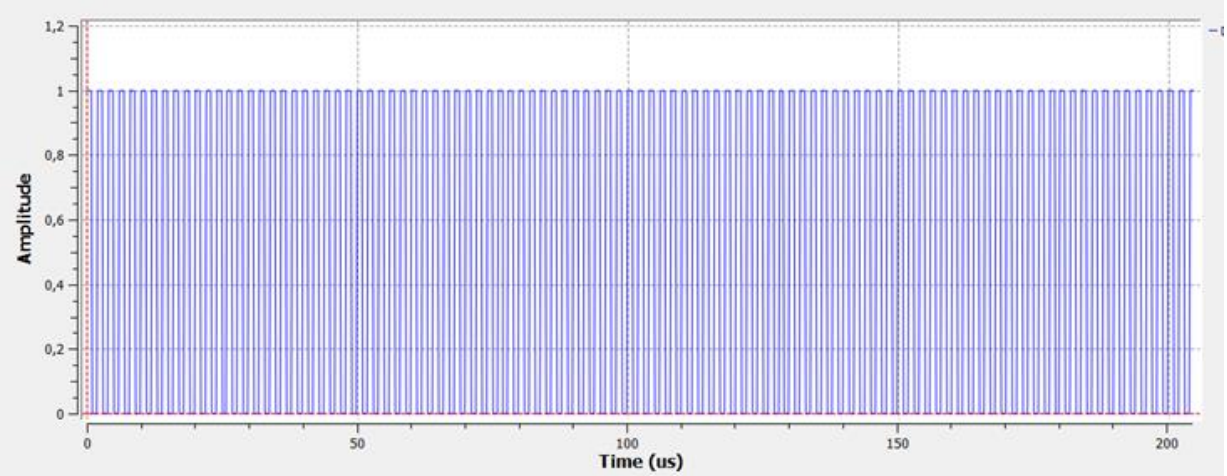
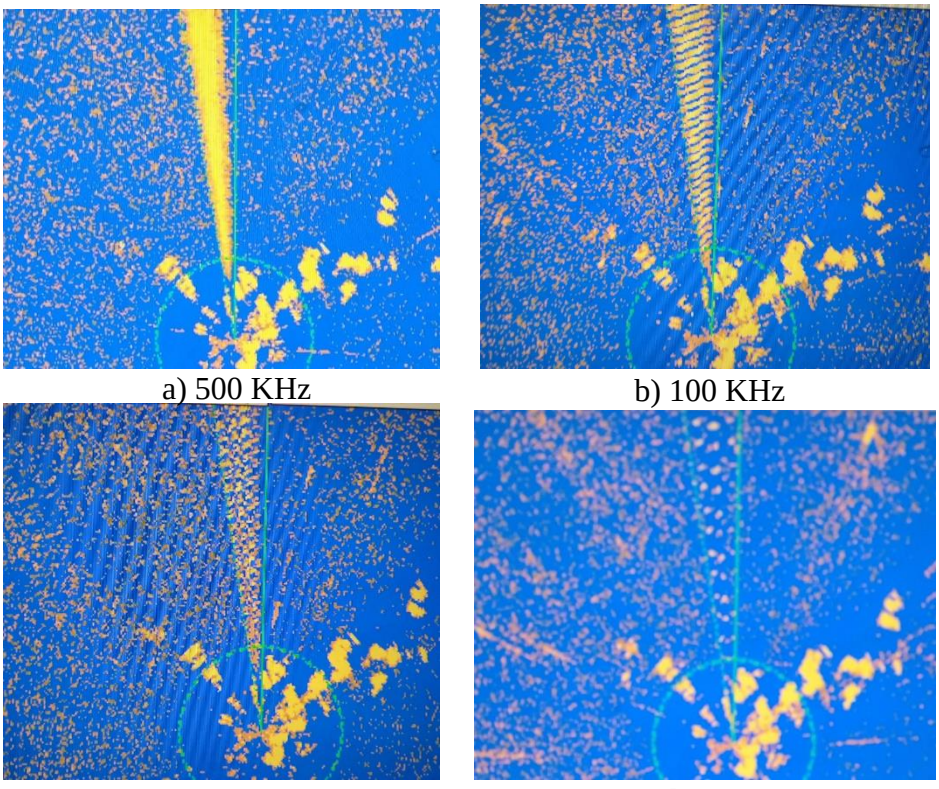


Figura 4-8: Señal jamming cuadrada 500 KHz

Con la señal cuadrada las pruebas se basaron en variar la frecuencia inicial de la señal de 500 KHz, lo que hace variar el ancho de pulso y distancia entre ellos. A menor ancho de los pulsos de la señal cuadrada, más fácil es que coincidan con los TOA de los pulsos emitidos por el radar.



a) 500 KHz b) 100 KHz

c) 75 KHz d) 50 KHz

Figura 4-9: Jamming con señal cuadrada al disminuir su frecuencia

En la Figura 4-9 se observa que cuando vamos disminuyendo la frecuencia de 500 KHz a 50 KHz, el jamming comienza a convertirse en un sector anillado, debido al aumento del periodo entre pulsos de la señal cuadrada. Al llegar a las frecuencias más bajas c) y d) el radar recibe crudos de puntos en demora separados por igual entre ellos.

Es importante destacar que la señal cuadrada cuando se la baja la frecuencia llega un momento que los pulsos de la señal sólo son recibidos por el radar cada cierto número de barridos, debido a que al bajar la frecuencia aumentamos el tiempo de espaciado entre los pulsos, por lo tanto, hasta que se produce la sincronización no vemos el tren de pulsos en la pantalla del radar.

Se realizaron pruebas con otros tipos de señal, como la señal triangular y la onda continua, cuya efectividad fue nula en el radar. También se utilizó señal sinuidal o cosinuidal que consiguió un jamming parecido a la señal cuadrada pero mucho más débil debido a que es muy parecida a un tren de pulsos rectangular. Y por último se probó con ruido blanco, que fue efectivo en menor proporción que la señal cuadrada, pero sí que consiguió generar falsos ecos y ruido en el sector, pero sin llegar a tener entidad como para enmascarar un blanco.

4.2.2 Pruebas en distancia

Otra de las pruebas a las que sometimos al sistema de perturbación es al alcance en distancia. Por un lado, para comprobar el alcance dependiente de la potencia emitida por la antena jammer, y por otro lado, comparar los anchos de los sectores de jamming dependiendo de la distancia entre el radar de la lancha y el perturbador. El objetivo principal es determinar la máxima distancia de alcance de la perturbación.

Toda esta fase de ensayos se realizó en tierra desde el muelle comenzando por una distancia inicial de prueba de 7 m. Después de comprobar que el jamming era efectivo en distancia cercana se probó a situar la antena jammer a una mayor distancia del radar. Se utilizó una señal cuadrada con una frecuencia de 500 KHz y ganancia de la antena máxima 30 dB, configuración que se había comprobado que generaba un mayor sector de jamming.

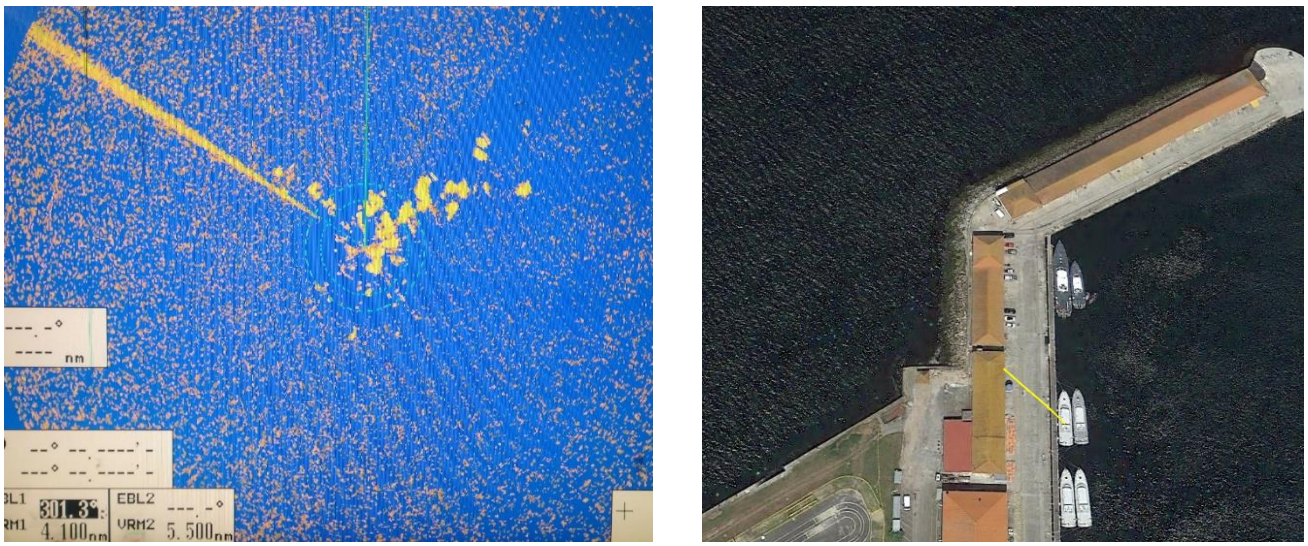


Figura 4-10: Jamming de señal cuadrada desde 30 m [34]

Se comenzó colocando la antena en la ventana del laboratorio de simulación, desde donde se realizaron la mayoría de pruebas de la fase de detección como se comentó en el apartado 4.1. Eso suponía

una distancia de 30 metros (32,8 yardas) entre el equipo y el radar a perturbar, y a demora del 301º desde la lancha. Se comprobó que la potencia era suficiente para generar jamming con la misma efectividad y grado de enmascaramiento que desde la distancia inicial de prueba. Es verdad que el ancho del sector del jamming se ve ligeramente reducido hasta los 8º (Figura 4-10).

La dirección en la que el radar recibe la perturbación también es relevante, no por los lóbulos o diagrama de la antena, ya que la antena es bastante directiva, sino porque todos los radares tienen un sector ciego o atenuado. En el caso del radar Furuno de la lancha tiene atenuación de la señal en el sector popel, por lo tanto, el jamming realizado desde esa dirección será recibido con una menor efectividad.

Figura 4-11: Montaje del sistema en el muelle de Torpedos con las lanchas al fondo

La segunda prueba consistió en colocar la antena jammer en la punta del muelle de Torpedos, alimentado el sistema por la batería de un coche a través de un inversor (Figura 4-11). El montaje se colocó orientado hacia el 215º, donde se encontraba el radar emitiendo, quedando situado a una distancia de 170 m (186 yardas). La señal utilizada fue la misma señal cuadrada que en la prueba desde los 30 m. Antes de comenzar a perturbar se puso el sistema en sentido receptor, para identificar la frecuencia en la que estaba emitiendo el radar en ese momento, y así posteriormente centrar el jamming en esa frecuencia.

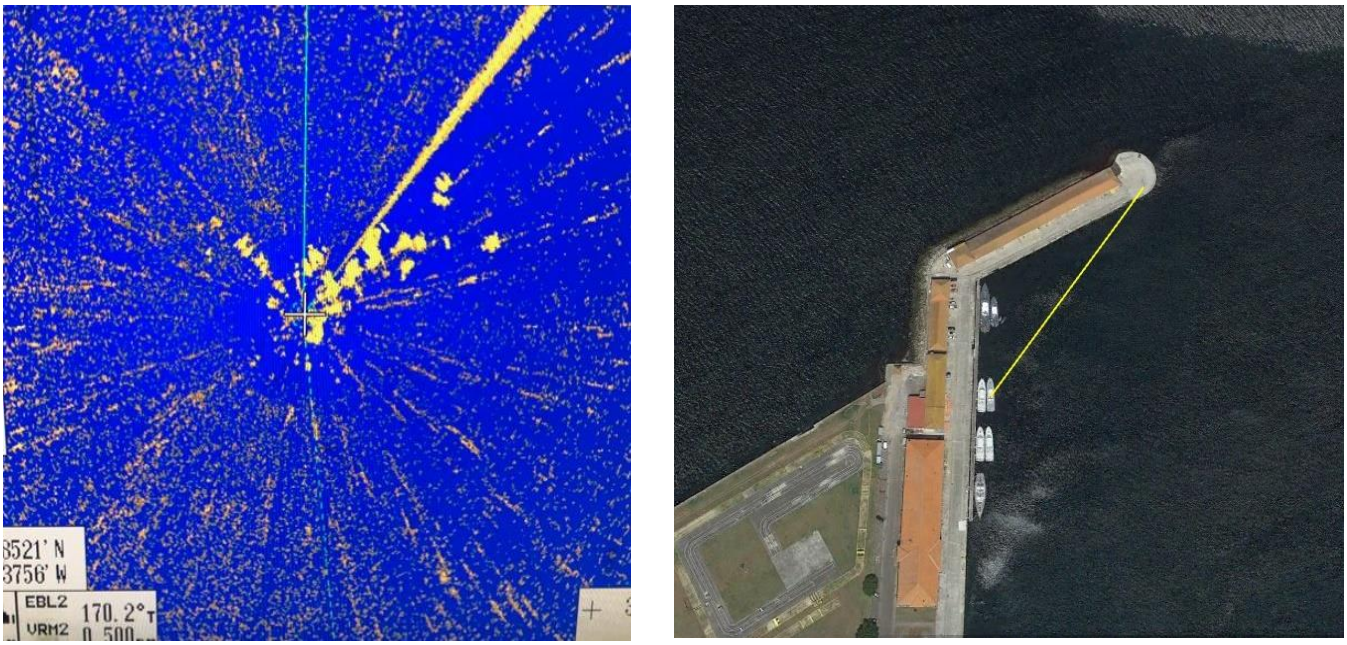


Figura 4-12: Jamming de señal cuadrada desde 170 m [34]

El resultado fue una recepción de un jamming igualmente efectivo que el de 30 m, aunque ligeramente inferior en ancho del sector perturbado, unos 5º (Figura 4-12).

Antes de la prueba de perturbación en navegación, se quiso realizar una prueba estableciendo el perturbador estático en una lancha atracada, y realizar jamming sobre una lancha en navegación, desde su desatraque hasta su llegada a la línea entre las puntas de Torpedos y el muelle comercial de Marín (Figura 4-13). El objetivo era comprobar la variación del jamming en demora y distancia mediante la filmación de la pantalla del radar. Para su análisis se han extraído fotogramas del video en ciertos momentos donde podemos obtener la distancia del jammer al radar por medio de demoras.

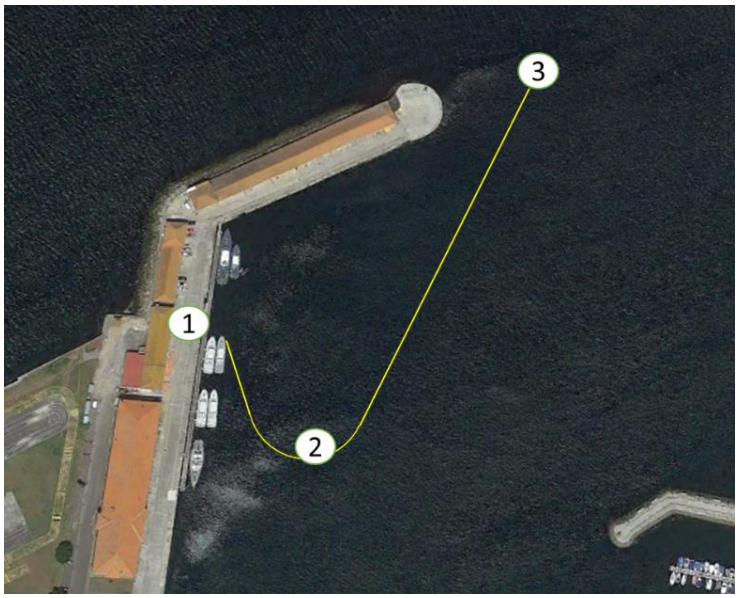


Figura 4-13: Trayectoria salida de puerto lancha perturbada

1. La distancia inicial entre antena perturbadora y radar en situación de atraque es de 5 metros, distancia incluso menor a las primeras pruebas que se realizaron en el trabajo. En la Figura 4-14 vemos como el jamming disminuye en sector pero se mantiene en efectividad al dar atrás durante la maniobra de desatraque.

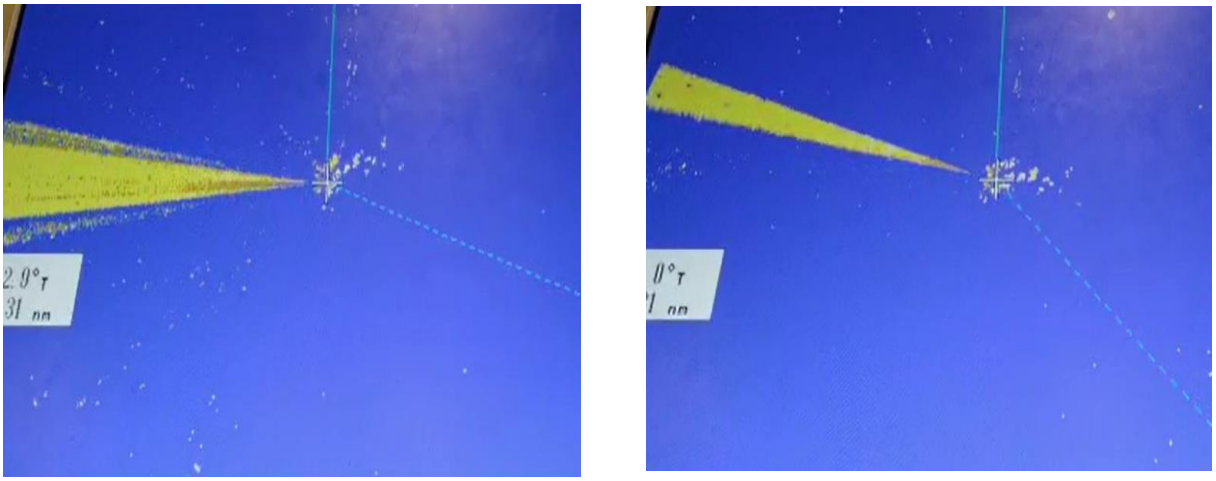


Figura 4-14: Jamming de señal cuadrada durante la desatracada

2. El siguiente fotograma (Figura 4-15) fue obtenido en el momento en que la lancha comienza a dar avante ya librando el muelle y el resto de lanchas. A una distancia de unos 50 m, el sector del jamming comienza a reducirse, a pesar de seguir entrando por el través.

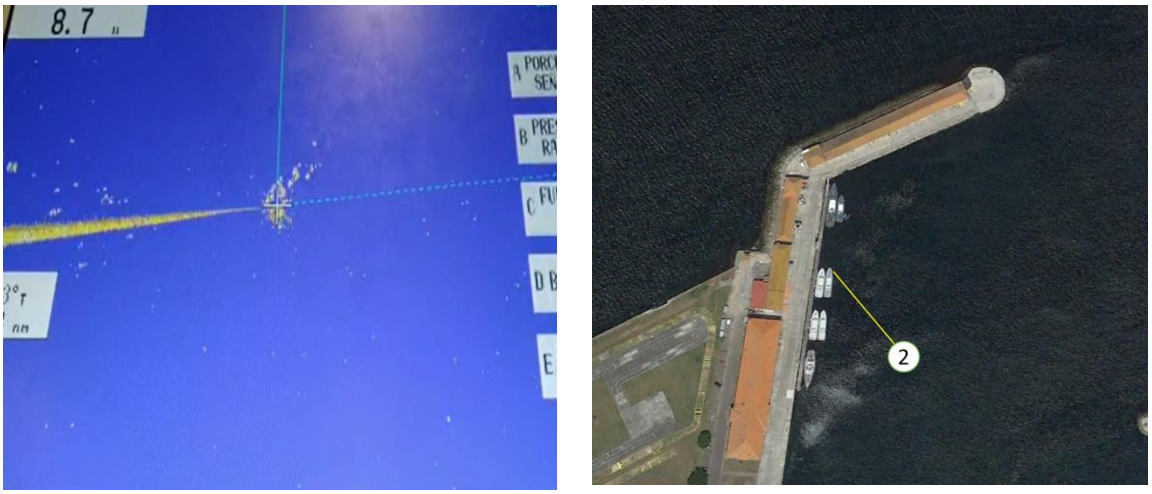


Figura 4-15: Jamming de señal cuadrada desde 50 m durante la salida de puerto

3. Y en la Figura 4-16 tenemos la captura del final de la perturbación, quizás provocado por distancia o por entrar en un sector popel del radar donde el mástil o elementos de la superestructura podrían provocar atenuación a la señal recibida. Pese a que el radar no tiene designado un sector ciego de transmisión, (modo opcional en la configuración del mismo), la atenuación por su sector popel es evidente, tanto en las pruebas realizadas en este trabajo como en los numerosos ejercicios que realizan los alumnos en las lanchas cada año.

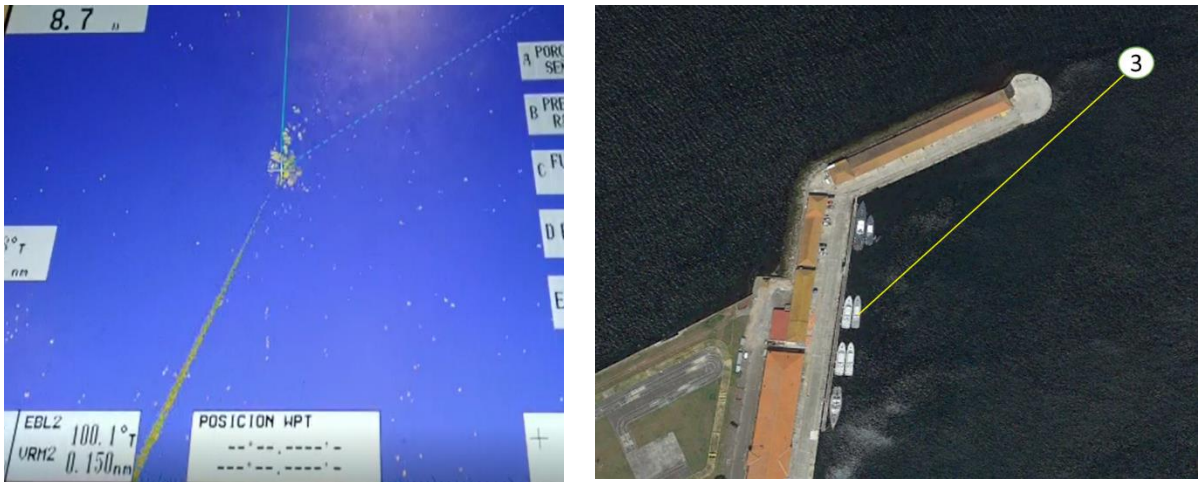


Figura 4-16: Jamming de señal cuadrada a 250 m durante la salida de puerto

La distancia a la que se consiguió ejercer este jamming es de 250 m, espacio que recorre la onda perturbadora desde la antena transmisora hasta su recepción en el radar.

La conclusión que se obtuvo de las pruebas en tierra fue que la atenuación con la distancia no suponía un problema para la potencia, es decir el jamming seguía siendo efectivo en este margen de distancias. El siguiente paso sería comprobar que el sistema de detección y perturbación funcionase en navegación entre dos lanchas y comprobar el límite máximo de distancia.

4.2.3 Pruebas en navegación

El siguiente paso fue probar el sistema funcionando en el ambiente natural de un equipo de Guerra Electrónica, en el mar. La idea era comprobar si el sistema podía realizar jamming a cierta distancia entre dos lanchas en movimiento, tanto de avance como balance y cabezada por efecto del mar.

Se colocó la antena perturbadora fijada en el puente alto de la lancha, conectada al resto de equipos a través de las lumbreras que tiene el aula del CIC de la lancha, donde estaban estibados el SDR, generador y ordenador conectados a la red 220V del barco (Figura 4-17).

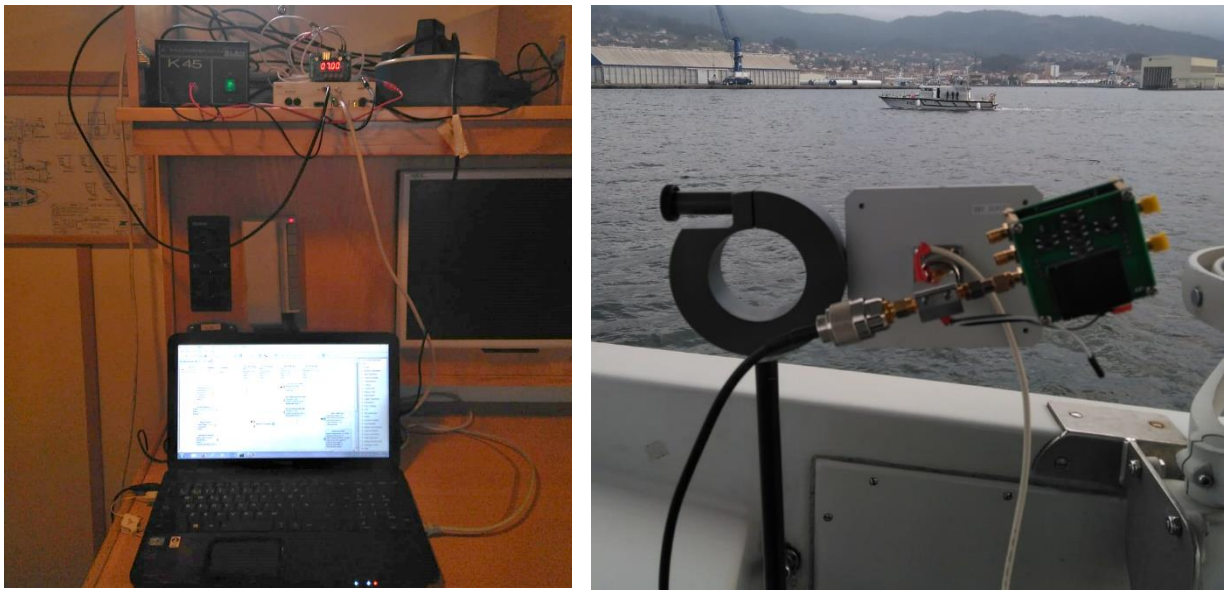


Figura 4-17: Disposición de equipos en el CIC e instalación de la antena en el puente alto

La idea era realizar aproximaciones entre una lancha jammer (con el sistema perturbador montado) y otra lancha que emitiendo con su radar bajo identificase la efectividad del jamming realizado a distintas distancias (Figura 4-18). Para ello se preparó una tabla de órdenes (TABORD) del ejercicio de pruebas a realizar, tal como se adjunta en el Anexo VII . Siguiendo el formato de la AXP-02, *The Allied Maritime Above Water Warfare Exercise Manual*, se decidió llevar a cabo un ejercicio EWX 220 definido en la publicación como “Elementary Demonstration of Electronic Jamming”.

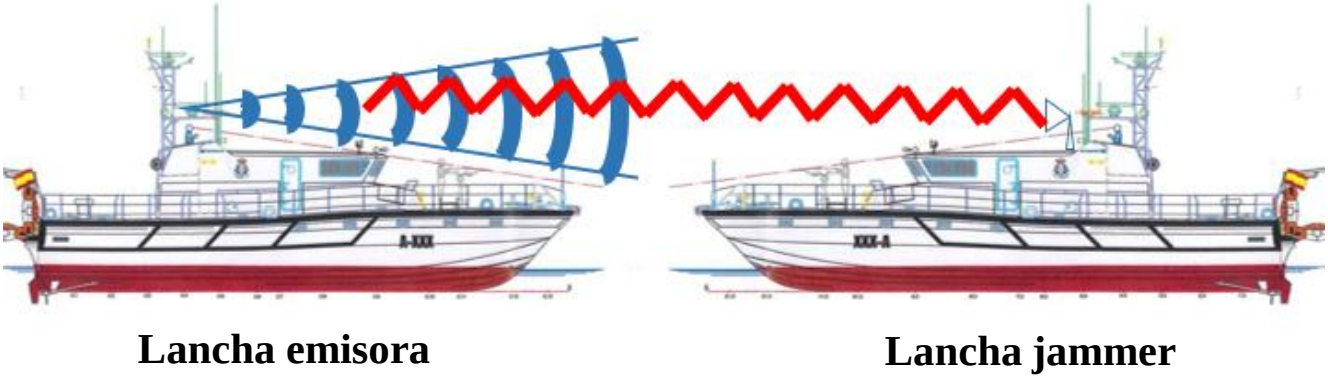


Figura 4-18: Recreación de jamming entre lanchas

El ejercicio consiste en formar a las cuatro lanchas (Barrutia, Salas, Rull, Chereguini) en formación en columna (FORM 1) a una distancia de 100 yardas entre unidades y una velocidad de 6 nudos. Después se ordenaría adoptar STATION L-2 a la primera lancha a ser perturbada, es decir, colocarse por el través de la lancha jammer a 25 yardas (Figura 4-20). En ese momento se comenzaría a realizar el jamming. Entonces la lancha receptora tomaría muestras e informaría a lancha jammer través del procedimiento *Jamming State*, recogida en la publicación APP-1. Cuando el jamming se verificase, se incrementaría la distancia entre ambas lanchas para buscar el límite en distancia de la perturbación.

Figura 4-19: Lanchas entrando en formación en columna durante el ejercicio

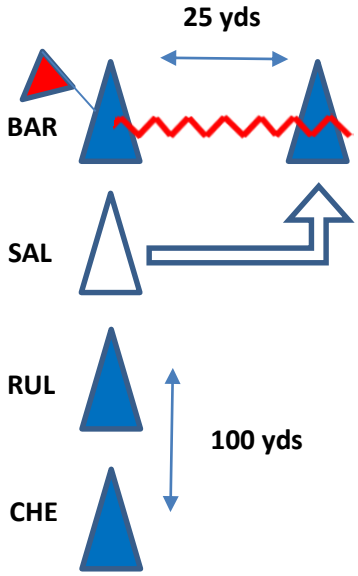


Figura 4-20: Formación para ejecución del ejercicio EWX 220

La prueba se realizó desde la lancha Guardiamarina Barrutia, siendo esta la lancha jammer. Las lanchas realizaron la prueba en orden Salas, Rull y Chereguini (Figura 4-19). Siendo la prueba con la Rull la más concluyente. Una vez encontrada la frecuencia del radar a perturbar, se introdujo la frecuencia en el programa GNU Radio y se ejecutó. La señal utilizada fue nuevamente la señal cuadrada con una frecuencia de 500 KHz. Durante la realización del jamming, se llevó la coordinación entre lancha jammer y emisora por el circuito táctico 269.0 MHz, mandando los correspondientes cambios de distancia para ver el límite (Figura 4-21).

Figura 4-21: Guardiamarina Chereguini vista de través durante el ejercicio

Los resultados fueron satisfactorios a distintas distancias, sin embargo, los alcances fueron menores a los obtenidos en tierra. Esto principalmente debido al desapuntamiento de la antena perturbadora respecto al radar víctima debido movimiento de balance y cabezada de la lancha por acción del mar. Las condiciones de la mar el día de la prueba eran de mar marejadilla (0,5 m) y viento bonancible (13 kts) del Oeste. Pese a las buenas condiciones, la gran directividad de la antena hizo que los resultados conseguidos fueran peores que en las pruebas en tierra.

Durante las pruebas se mantuvo la ganancia del radar emisor entre 50 y 80, obteniendo una efectividad de jamming muy similar en 150 yardas (137 m), la distancia más larga de las probadas, que en distancias más cortas como 120 yardas (109 m) y 100 yardas (91 m) (Figura 4-22). Siendo en el caso mostrado en la Figura 4-23, a una distancia de 150 yardas, el sector cubierto por el jamming de unos 4º.

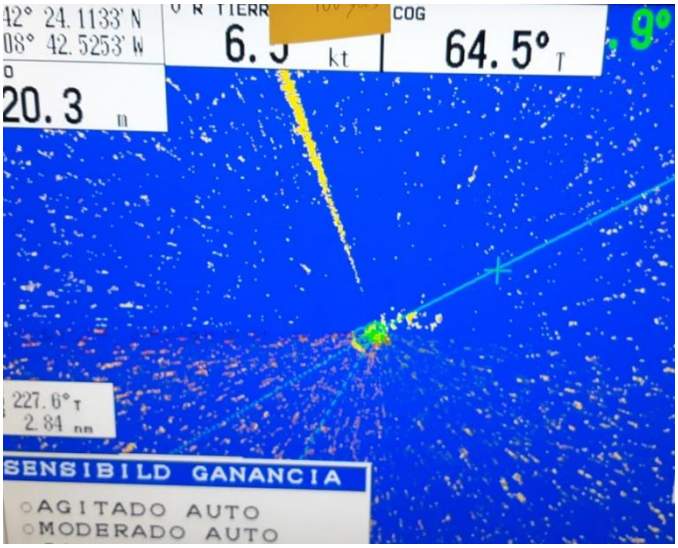


Figura 4-22: Jamming en navegación desde una distancia de 100 yardas (91 m)

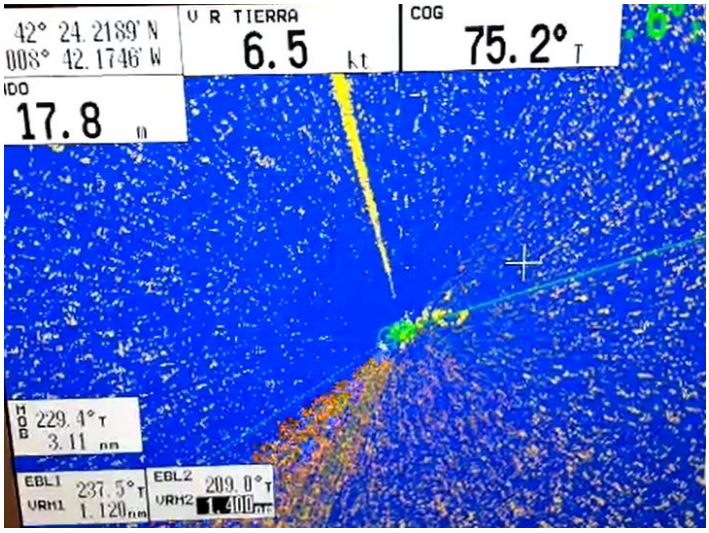


Figura 4-23: Jamming en navegación a una distancia de 150 yardas (137 m)

4.2.4 Pruebas Radar CEMEDEM

Antes de comenzar las pruebas con las lanchas, se intentó probar con el radar Furuno 1934C del CEMEDEM (Centro de Medidas Electromagnéticas de la Armada), muy similar al montado en las lanchas. Este radar está montado sobre el contenedor del LIBRA, un sistema utilizado en el pasado por el CEMEDEM para la medición de RCS (Figura 4-24).

Figura 4-24: Sistema LIBRA de Medidas Electromagnéticas del CEMEDEM

Surgió la idea de intentar generar jamming sobre el radar del CEMEDEM. Además de dar la posibilidad de testear el sistema con un radar distinto, también ayudó a comprender los límites del sector de jamming generado, así como la profundidad en distancia del jamming dentro de las 5 MN.

El proceso fue el mismo que en otras ocasiones, montaje del sistema a una distancia de 36 m, puesta del radar a transmitir e identificación de la señal recibida a través del SDR Console. Una vez la frecuencia fue identificada, cambio del sistema a perturbación, cambiando la frecuencia del oscilador y comienzo del jamming.

Se optó por señal cuadrada, se fue variando la frecuencia comprobando la separación de los anillos que conformaban la señal, sin embargo, la mayor efectividad se obtuvo con frecuencia de 500 KHz. También se probó con señal de onda continua, ruido y sinuidal sin obtener resultados muy satisfactorios. El sector de jamming en el radar del CEMEDEM alcanzaba desde la escala máxima hasta una distancia de 2,5 millas, donde se empezaba a atenuar, mientras que en el radar de las lanchas la perturbación desaparecía dentro las 5 millas.

Además de la perturbación sectorial de 10º del lóbulo principal, como se puede observar en la Figura 4-25: Jamming con señal cuadrada Radar CEMEDEM, se generan varias réplicas de la señal perturbadora en demoras distintas. Esto es debido a que el jamming entra por los lóbulos laterales, mostrando el mal funcionamiento del radar. De hecho, se informó de este problema a la dotación del CEMEDEM, quienes no se habían percatado del problema de los lóbulos laterales.

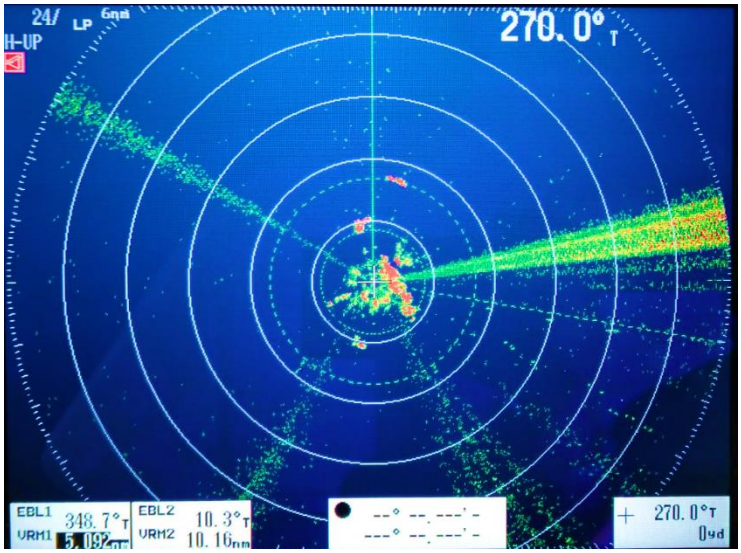


Figura 4-25: Jamming con señal cuadrada Radar CEMEDEM

La principal conclusión de esta prueba es que el sistema puede funcionar con diferentes radares y su sector de jamming no viene limitado por una distancia determinada, sino por como el radar amplifica su señal dependiendo si los blancos recibidos son cercanos o lejanos.

4.2.5 Calibración de radares

Por otro lado cabe destacar que en estas pruebas se vio que el sistema de perturbación creado podía tener una utilidad alternativa. Esta sería la calibración de radares en demora respecto a la giroscópica.

Al realizar las pruebas desde la proa desde distintas lanchas y tomando referencias también del radar alto, se observó la desalineación en demora respecto al norte de ambos radares. El haz de la perturbación vale para poder calibrar y sincronizar con el norte magnético los radares del buque. Simplemente produciendo el jamming desde el Norte, y orientando la calibración del radar para obtener una posición certera y segura propia y de otros buques, vital no sólo para mantener clara la situación táctica, sino también para poder llevar una navegación segura y sin riesgos en la mar.

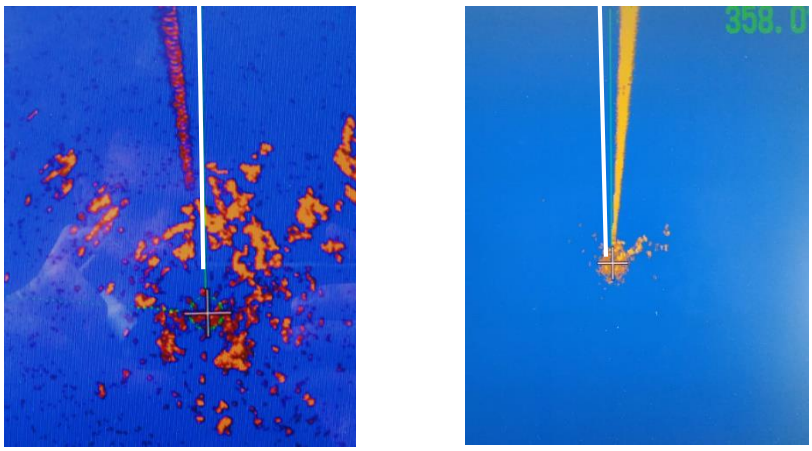


Figura 4-26: Comparación de la dirección del jamming obtenido en radar alto (izquierda) y bajo (detecha)

En la Figura 4-26 podemos observar la presentación del jamming a través de los distintos radares. Mientras el primero, el radar alto, muestra la perturbación a Babor, el radar bajo la muestra a Estribor. Es un claro ejemplo de la mala calibración de ambos radares. No están calibrados con la giroscópica, ya que no marcan las mismas demoras respecto al Norte y proa de la lancha.

5 CONCLUSIONES Y LÍNEAS FUTURAS

Para finalizar el trabajo se va a realizar un análisis de si se han alcanzado los objetivos que se marcaron en un inicio, y también un estudio de los problemas o barreras que se han encontrado a lo largo de las distintas fases de desarrollo del proyecto.

5.1 Problemas encontrados

5.1.1 Comportamiento interno del radar Furuno 1944C

Durante las pruebas de jamming a distancia de 7 m en el radar de la lancha, se comprobó que el jamming era efectivo hasta una distancia de 5 MN, para distancias inferiores, el radar respondía generando en el PPI sectores angulares ciegos correspondientes a las posiciones de los lóbulos principal y posterior en los que atenuaba, total o parcialmente, los crudos recibidos en esa área. Se intentó buscar una respuesta a este problema específico del radar contactando sin resultado con la empresa Furuno y talleres náuticos de la zona. También se consultó a ingenieros del Ramo de Sistemas del Arsenal de Ferrol sin obtener respuesta.

Tras la prueba con el radar 1934C del CEMEDEM, se comprobó que, con dicho radar, el problema expuesto en el párrafo anterior no existía. Por ello, se acabó pensando que este comportamiento es exclusivo del radar 1944C a cortas distancias. Aparentemente, alguna etapa de amplificación o detección del radar, puede llegar a saturarse cuando es perturbado en las cortas distancias, cuando el amplificador presenta su mayor ganancia. En cualquier caso, la respuesta del radar es crear un sector ciego para el operador del radar y por tanto, se consigue el efecto perturbador deseado.

5.1.2 Potencia de la antena jammer

Otro de los problemas de este proyecto es la poca potencia de salida del sistema. Debido a la inexistencia de un amplificador de RF a la salida del transmisor y a la baja ganancia de la antena microstrip, y pese a que se lograron alcances de hasta 200 m, la potencia siempre fue un factor limitante durante las pruebas realizadas. Otro problema fue la gran directividad de la antena. Aunque en principio este hecho era una ventaja por su mayor ganancia respecto a otro tipo de antena omnidireccional, los propios movimientos del buque durante la navegación, desapuntaban la antena.

Además, el montaje y su transporte en una caja siempre fueron procesos muy delicados por la fragilidad de los equipos. Esto sumado al trabajo en un medio poco estable como es un buque.

5.2 Posibles líneas futuras

5.2.1 Sistema de perturbación inteligente

La idea es intentar conseguir una sincronización entre la perturbación y los pulsos del radar. El problema es emitir jamming en cualquier instante, sin tener en cuenta cuando el pulso sale del radar y cuando vuelve a él. Si se pudiera conseguir sincronizar el tiempo de salida y llegada del pulso (TOD y TOA) con nuestro comienzo de emisión de la señal perturbadora, se podrían crear blancos falsos en movimiento, que simulasen nuestra posición. Esto sería posible realizando jamming con un pulso igual al recibido, tratando de hacer creer al radar que es su propio pulso volviendo. Además, al modificar el retardo de vuelta de este pulso perturbador, se le podría mover en distancia. Sería usar la decepción para crear falsos blancos.

Este sistema podría funcionar mediante un algoritmo que además de sincronizar la detección con la perturbación, automáticamente al detectar una emisión enemiga, realizase una perturbación inteligente sobre ella. Además, podría archivar todas las señales en una base de datos de inteligencia, y cada vez que detectase una nueva emisión, comprobaría si se corresponde con una emisión conocida. De esta forma reconoceríamos a las unidades emisoras automáticamente gracias al archivo de emisores amenaza.

5.2.2 Calibrador de radares / Generador de diagramas de radiación

Otra de las aplicaciones que se le ha sacado al proyecto es la de creación de un aparato de calibración de radares. Durante las pruebas de perturbación se comprobó que hay lanchas donde los radares alto y bajo no están alineados igual respecto al norte de giroscópica, como se mostró en el apartado 4.2.5. Algo que el personal del núcleo de lanchas no había tenido en cuenta, lo que supone un error en demora bastante grave que puede llevar a situaciones de riesgo durante la navegación.

Además de intentar buscar crear un calibrador de este tipo de radares, el sistema también puede ser útil para generar diagramas de radiación de las antenas, utilizando los códigos generados para este trabajo. Habría que conseguir realizar las mediciones en campo lejano para obtener un diagrama de radiación fiable. De esta forma, obteniendo los diagramas de radiación de radares iguales montados en distintos buques, se podrían diferenciar los buques dentro de una misma clase obteniendo su “huella” radárica.

5.2.3 Perturbador de sistemas de comunicaciones o de otros radares

Debido a la flexibilidad del diseño del transmisor, es posible generar prácticamente cualquier tipo de señal desde 0 hasta 13,8 GHz. De esta forma podrían perturbarse radares marinos de otras bandas, abriendo el abanico de posibilidades. Por otro lado, está otra posibilidad muy interesante, que sería usar el sistema como perturbador de sistemas de comunicaciones, parte fundamental de la EW en un buque. Interceptación de comunicaciones, decepción o jamming, negando la posibilidad de comunicación entre unidades.

5.2.4 Sistema de jamming desde dron

Debido al poco volumen y peso del sistema desarrollado, una posible línea futura de desarrollo de este proyecto sería el diseño de un equipo de Guerra Electrónica embarcable en un dron (Figura 5-1). La idea sería diseñar un dron generador de jamming que pueda moverse y libremente y realizar ataques cercanos a las unidades emisoras amenaza. Esto abriría un trabajo también de estudio de la estabilidad del dron y se colocaría como un proyecto muy actual. Rusia ya ha realizado incursiones con dron para obtener inteligencia a sensores de buques españoles en el mar Báltico. Es un proyecto de extrema actualidad dentro del marco de la nueva guerra híbrida y asimétrica.

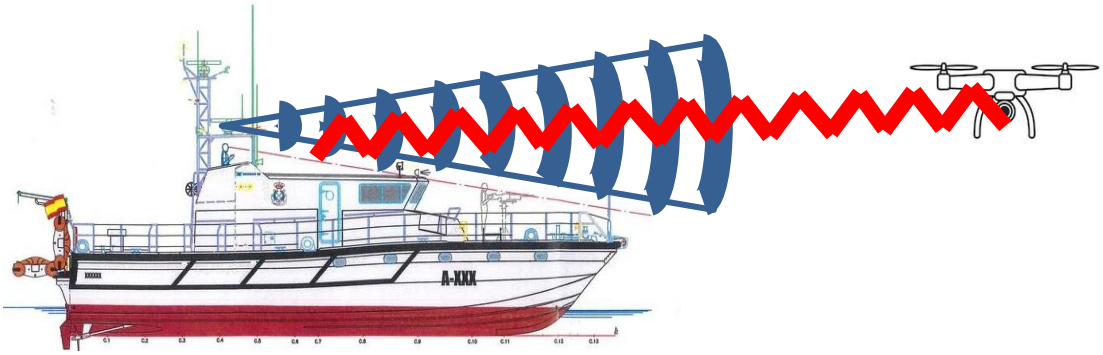


Figura 5-1: Recreación de Jamming desde dron

5.2.5 Instalación fija del sistema de Guerra Electrónica en las lanchas de instrucción

Finalmente, la última propuesta es la de usar el proyecto que se ha realizado, para llevar a cabo la instalación de un sistema fijo de Guerra electrónica en las lanchas para adiestramiento de los alumnos. Sería una instalación de equipos en el aula de CIC de la lancha, utilizando una pantalla de las ya presentes para la presentación y configuración de los programas, además de la instalación de una antena en el techo de la embarcación.

Este sistema daría lugar a numerosos ejercicios EWX durante las salidas de adiestramiento a flote, enseñando a los alumnos procedimientos de EW, que complementarían la escasa formación en este ámbito que se recibe en la escuela. Además, el sistema en la lancha de instrucción sería ideal para realizar prácticas de la asignatura de *Sensores Navales*, lo que sería en definitiva un paso adelante en la aplicación de conocimientos técnicos en el ámbito de la formación naval-militar.

5.3 Contrastación de resultados

Si se evalúa la consecución de los objetivos planteados al comienzo de este trabajo, se salda con una valoración muy positiva. No sólo por obtener resultados concluyentes y diseñar un sistema que funciona correctamente en sus dos fases relacionadas, detección y perturbación; sino también por haber realizado pruebas en distintos escenarios, con configuración de equipos y señales distintas, a diferentes distancias, etc. Además, se ha realizado la perturbación sobre 9 radares distintos, y 2 modelos diferentes.

En primer lugar, se ha demostrado que el sistema es capaz de detectar y determinar los parámetros principales de una señal (ESM), además de tener la posibilidad de obtener el diagrama de radiación. Con ese mismo sistema, modificando su configuración, las pruebas han mostrado que es capaz de realizar jamming (ECM) hasta una distancia de 250 m desde tierra a buque, y 137 m de buque a buque en navegación con mar marejadilla, generando sectores de enmascaramiento de hasta 5º.

En segundo lugar, se ha diseñado y ejecutado por primera vez un ejercicio de Guerra Electrónica (EWX) en las lanchas de instrucción (Anexo VII), suponiendo un hito y un punto de comienzo para el adiestramiento de los alumnos de la ENM en materia de EW.

Los resultados conseguidos son más satisfactorios cuando analizamos el reducido coste de los equipos utilizados, y que, pese a las limitaciones en potencia encontradas, esto no ha supuesto un freno para el desarrollo del sistema de Guerra Electrónica.

5.4 Conclusión personal

Desde el primer momento lo que me llevó a proponer este proyecto fue diseñar algo relacionado con la labor que vamos a realizar como oficiales en un futuro próximo. Pienso que es primordial intentar unir esfuerzos para conseguir integrar la parte técnica de nuestra formación con nuestra formación militar, y eso me hizo ir por este camino. Dejar patente la necesaria convergencia de ambos planes de estudios que por unos u otros motivos, muchas veces se ven separados y sin relación alguna.

Realizar un proyecto de fin de carrera sin relación alguna con la profesión para lo que nos preparamos aquí no me motivaba. Por ello me llamó la idea de la Guerra Electrónica, en primer lugar, por ser una guerra secundaria dentro de las enseñadas en la ENM, por los intentos de potenciarla por parte de la flota en los últimos años y por las grandes posibilidades de desarrollo y aplicación en las lanchas de instrucción. De la idea inicial que era generar un simple jamming, el trabajo ha dado sus frutos, y ha demostrado que deja muchas puertas abiertas a futuros proyectos.

El proyecto me hizo conocer más a fondo el funcionamiento del radar, la programación y las técnicas de Guerra electrónica. En los inicios del trabajo, tuve que ponerme al día en materias en las que no me manejaba, como el uso de los programas y equipos, pero ahora echando la vista atrás me doy cuenta del gran aprendizaje realizado.

Uno de los puntos más determinantes en el transcurso del proyecto desde mi perspectiva fue la prueba del sistema en la mar con las lanchas de instrucción, con la realización de un ejercicio EWX. Fue gratificante ver que el sistema funcionaba en su ambiente natural, y donde podría dar mucho juego para la enseñanza y adiestramiento de los alumnos.

En definitiva, estoy realmente satisfecho con la realización de este trabajo, que, aunque con un mayor periodo de tiempo se habrían conseguido mejores resultados, creo que se han cumplido con creces los objetivos iniciales. Creo que además de despertar el ámbito de la Guerra electrónica en la ENM, sobre todo, he disfrutado mucho realizándolo y he ganado unos conocimientos que estoy seguro me servirán, en un futuro muy cercano, como oficial en las unidades.

6 BIBLIOGRAFÍA

[1] ENM, *Electronic Warfare, Táctica Naval,* 2019.

[2] G. L. M. Mezo, «Foro Naval,» 19 Julio 2016. [En línea]. Available: https://foronaval.com/2016/07/19/sistemas-de-ew-en-la-armada-espanola/. [Último acceso: 21 1 2020].

[3] NATO, DSF-55, Electronic Warfare Procedures.

[4] CESEDEN, Ministerio de Defensa, «Plan de Campaña de Desarrollo de Doctrina,» 2020.

[5] Armada Española.

[6] J. P. Sanfuentes, *Historia del Radar. Revista de Marina nº 854,* Armada de Chile, 2000.

[7] J. Alcalde, «Analisis Naval,» 30 10 2016. [En línea]. Available: http://josenaval63.blogspot.com/2016/10/. [Último acceso: 23 1 2020].

[8] COIT, *Introducción a la Guerra Electrónica: conceptos, técnicas y tecnologías,* 2012.

[9] Departamento Infantería de Marina ENM, «Sistemas de control y Sensores Navales en la Infantería de Marina,» 2020.

[10] J. M. N. García, «Defensa.com,» 2018. [En línea]. Available: https://www.defensa.com/espana/sistema-guerra-electronica-fragata-f-110. [Último acceso: 21 1 2020].

[11] Navantia, «Situación Diseño F110 y Problemas Pendientes,» 2020.

[12] NATO, *ATP-31, Nato Above Warfare Manual.*

[13] G. R. Curry, Radar Essentials, Scitech Publishing, 2012.

[14] ENM, Guerra Electrónica E.W. Pub. 5351, 2005.

[15] M. K. Aslan, *Emitter Identification Techniques in Electronic Warfare,* Turquía: Middle East Technical University, 2006.

[16] B. M. Albaker, «Signal Acquisition and Parameter Estimation of Radio Frecuency Pulse Radar Using Novel Method,» University of Malaya, 2011.

[17] Naval Air Warfare Center Weapons Division, Electronic Warfare and Radar Systems Engineering Handbook, 2013.

[18] ENM, Defensa AntiMisil, Táctica Naval, 2019.

[19] D. J. I. Hernández, *Diseño y puesta en marcha de un receptor SDR de bajo coste para experimentación en la banda de HF*, 2015.

[20] F. Marki y C. Marki, *Mixer Basics Primer*, Marki Microwave, Inc., 2010.

[21] «Marki Microwave,» 2020. [En línea]. Available: https://www.markimicrowave.com/spur-calculator.aspx. [Último acceso: 6 3 2020].

[22] S. Srikanteswara, R. Palat, J. Reed y P. Athanas, «An Overview of Configurable Computing Machines for Software Radio Handsets,» *IEEE Communications Magazine*, vol. 41, nº 7, pp. 134-141, 2003.

[23] C. A. Balanis, Antenna Theory: Analysis and Design, 1982.

[24] Furuno, Radar marino Modelo 1944C, 2005.

[25] Sparkfun, «Sparkfun start something,» 2 2 2020. [En línea]. Available: https://www.sparkfun.com/products/13001#description-tab. [Último acceso: 1 2 2020].

[26] H. Cakmak, «General and Theorical Electrical Engineering,» University of Duisburg-Essen, 2020.

[27] F. Neri, Introduction to Electronic Defense Systems, Artech House Publishers, 1991.

[28] J. Rodríguez y V. Fernández, Cómo redactar el estado del arte de un trabajo, Editorial Genios, 2010.

[29] R. L. Cuquerella, *Fabricación y puesta en marcha de un radar FMCW de bajo coste en banda S*, 2015.

[30] ENM, Manual de las Lanchas de Instrucción.

[31] E&Q, «E&Q Engineering,» 2010. [En línea]. Available: http://www.eqeng.com/site/es/node/38. [Último acceso: 18 1 2020].

[32] Matlab and Simulink, «Signal Parameter Estimation in a Radar Warning Receiver,» 2019. [En línea]. Available: https://www.mathworks.com/help/matlab/ref/isinf.html. [Último acceso: 2 17 2020].

[33] Google, «Google Earth,» 5 02 2020. [En línea]. Available: http://www.googleearth.com. [Último acceso: 11 2 2020].

[34] Korabli, «Korabli Gallery,» 2009. [En línea]. Available: http://www.korabli.eu/galleries/oboi/voennye-korabli/alvaro-de-bazan. [Último acceso: 13 Enero 2020].

[35] P. Choudhari, «Full Afterburner,» 28 4 2018. [En línea]. Available: http://fullafterburner.weebly.com/next-gen-weapons/electronic-warfare-radar-noise-jamming. [Último acceso: 13 Enero 2020].

[36] R. T. Fernández, *Selección, dimensionamiento y estudio de adaptación de sistema POD para la propulsión de las lanchas de instrucción*, 2015.

[37] Wipro Technologies, ««Software defined radio. A technology overview»,» 2002.

[38] «QLS,» 24 1 2020. [En línea]. Available: https://www.qsl.net/ea3du/2010/12/SDR-IQ.html. [Último acceso: 24 1 2020].

[39] V. I. Muñoz, *Diseño de Algoritmos de Guerra Electrónica y Radar para su implementación en tiempo real*, Universidad Politécnica de Madrid, 2015.

[40] E. RF, «Everything RF,» 23 1 2020. [En línea]. Available: https://www.everythingrf.com/community/understanding-rf-mixer-isolation. [Último acceso: 23 1 2020].

ANEXO I
Siglas y Acrónimos

AOA: Angle Of Arrival

BAM: Buque de Acción Marítima

BW: Band Width

CEMEDEM: Centro de Medidas Electromagnéticas

CESEDEN: Centro Superior de Estudios de la Defensa Nacional

COMINT: Communications Inteligence

DIFM: Digital Instantenous Frecuency Measurement

EBL: Electronic Bearing Line

ECCM: Electronic Counter-Counter Measure

ECM: Electronic Counter Measure

ELINT: Electronic Inteligence

ENM: Escuela Naval Militar

EPM: Electronic Protective Measure

ERP: Effective Radiated Power

ESJ: Escort Screening Jammer

ESM: Electronic Support Measure

EW: Electronic Warfare

GE: Guerra Electrónica

IRINT: Infrared Inteligence

MOPS: Mando de Operaciones

NEMO: Naval Electro-Magnetic Operations

OPINT: Optical Inteligence

PDW: Pulse Description Word

PRF: Frecuencia de Repetición de Pulsos

PRI: Intervalo de Repetición de Pulsos

PW: Pulse Width

RCS: Radar Cross-Section

RX: Recepción

SDR: Software Defined Radio

SIGINT: Signal Inteligence

SLB: Sidelobe Blankers

SLC: Sidelobe Cancellers

SMA: SubMiniature version A

SNR: Signal-to-Noise Ratio

SSJ: Self-Screening Jammer

TOA: Time Of Arrival

TOD: Time Of Departure

TX: Transmisión

USRP: Universal Software Radio Peripheral

VHF: Very High Frequency

VRM: Variable Range Marker

ANEXO II

Contramedidas radar comunes

Category	Countermeasure	Counter-Countermeasures
Masking	Mainlobe jammer	Frequency agility
		Burnthrough
		Passive tracking
	Sidelobe jammer	Low sidelobes
		Frequency agility
		Burnthrough
		Sidelobe cancellers
	Volume chaff	MTI and pulse Doppler
		Range resolution
		Velocity resolution
Confusion	Pulsed jammer	Sidelobe blanker
		Frecuency agility
		Tracking
	Traffic decoys	Range resolution
		Bulk filtering
		Tracking
	Debris	Bulk filtering
		Tracking
Deception	Repeater jammer	Frequency agility
		PRF agility
		Signal processing
	Track-breaking jammer	Signal processing
		Tracking
	Spot chaff	MTI and pulse Doppler
		Radar measurements
		Tracking

ANEXO III

Código algoritmo de detección

detection.m

```
clear all
close all

% Radar parameters
ta = 4;          % analysis duration (s)
fs = 5000000;       % sampling rate (Hz)
tb = 2.5;           % radar antenna scan time (s)
% TODO: calculate automatically radar antenna scan time
fif = 1008.005;   % Intermediate frequency (MHz)
fol = 10410;        % local oscillator frequency (MHz)

% Threshold levels
% TODO: calculate automatically threshold levels
th1 = 0.2;
th2 = 0.6;
fprintf('Threshold level 1: %2.2f \n',th1);
fprintf('Threshold level 2: %2.2f \n',th2);
% File path
filename = 'C:\04-Feb-2020 093008.038 1008.005MHz';
%file
name = 'D:\hackrf.iq';

% USRP
y = load_radar_data(filename,fs,ta,'usrp');

% HackRF

% -r <filename> # Receive data into file (use '-' for stdout).
% [-f freq_hz] # Frequency in Hz [0MHz to 7250MHz].
% [-a amp_enable] # RX/TX RF amplifier 1=Enable, 0=Disable.
% [-l gain_db] # RX LNA (IF) gain, 0-40dB, 8dB steps
% [-g gain_db] # RX VGA (baseband) gain, 0-62dB, 2dB steps
% [-s sample_rate_hz] # Sample rate in Hz (4/8/10/12.5/16/20MHz, default 10MHz).
% [-n num_samples] # Number of samples to transfer (default is unlimited).

% command = strcat('"hackrf_transfer.exe" -r'," ",filename,' -f 1060000000 -a 1 -l 10 -g
20 -s 10000000 -n 50000000');
% [~,cmdout] = dos(command)
% y = carga_datos(filename,fs,ta,'hackrf');

% Frame size: ONLY one antenna scan
framesize = 1*tb*fs;
fprintf('Frame size: %d samples (%4.2f s)\n',framesize,framesize/fs);

fprintf('Analysis time: %2.2f s\n',ta);
fprintf('Antenna rotation time: %2.2f s\n',tb);

% Estimate radar parameters
[toa,tod,pw,prf,fp] = calculate_PDW(y,th1,th2,framesize,fs);
```

```
    %fprintf('PRF: %5.0f Hz \n',prf);
    %toa
    %tod

    %fprintf('PW: %2.1f us\n',pw*1e6);
    fprintf('IF frequency: %f MHz \n',fp+fif);
    fprintf('Detected radar carrier frequency: %f MHz \n',fol-(fp+fif));

    % Plot waveform
    figure
    plot(0:1/fs:framesize/fs-1/fs,abs(y(1:framesize)))
    title('Radar received signal (framesize)')
    ylabel('amplitude')
    xlabel('t(s)');
    hold on
    plot(toa,th1*ones(size(toa)),'x')
    plot(tod,th2*ones(size(tod)),'o')
    legend('signal','toa','tod')

    % Plot spectrogram
    figure
    spectrogram(abs(y(1:framesize)),      512,      400,      512,      fs,'centered');      %
X,WINDOW,NOVERLAP,NFFT,Fs,type

    % Pintamos un barrido de antena en rectangulares
    figure
    yb = abs(y(1:tb*fs));
    plot(linspace(0,tb,max(size(yb))),yb)
    title('Radar received signal (tb)')
    ylabel('Amplitude')
    xlabel('time(s)')

    % hold on
    % [yu ~] = envelope(yb,100,'peak');
    % plot(linspace(0,tb,max(size(yu))),yu,'linewidth',1.5)
    % legend('y','yup')
    % hold off

    % Pintamos un barrido de antena en polares
    figure
    theta = linspace(0,2*pi,max(size(yb)));
    % polar_dB(phi, gain, rangedb, increments, rays)
    % rangedb    = maximum range for the plot
    % increments= increments for the gain circles
    % rays      = number of rays default is 16  use series of 4
    polar_dB(theta,yb/max(yb),20,3,8);

    % figure
    % % polar_dB(phi, gain, rangedb, increments, rays)
    % % rangedb   = maximum range for the plot
    % % increments= increments for the gain circles
    % % rays      = number of rays default is 16  use series of 4
    % polar_dB(theta,yu/max(yu),10,1,8);
```

```
% PRF processing
% remove outliers
% size(prf)
% prfo = rmoutliers(prf);
% size(prfo)

% Remove outliers
% first remove Inf,NaN and Zero elements
prf(isinf(prf) | isnan(prf) | prf == 0) = [];

% now remove points more than one standard deviations from the
% mean of the data
threshold = 1 * std(prf);
validRange = mean(prf) + threshold;
prfo = prf(prf <= validRange);
pdprf = fitdist(prfo','Normal');
fprintf('Detected PRF: %4.0f Hz \n',pdprf.mu);

% figure
% h=histogram(prf,'Normalization','probability')
% title('PRF (Hz)')

% Remove outliers
% first remove Inf,NaN and Zero elements
pw(isinf(pw) | isnan(pw) | pw == 0) = [];

% remove outliers
% criteria:  remove points more than three standard deviations from the
% mean of the data
threshold = 1 * std(pw);
validRange = mean(pw) + threshold;
pwo = pw(pw <= validRange);
pdpwo = fitdist(pwo','Normal');
fprintf('Detected PW: %4.2f us \n',pdpwo.mu*1e6);

% figure
% histogram(pw*1e6,'Normalization','probability')
% title('Pulse width (\mus)')
```

ANEXO IV

Código de carga de datos

load_radar_data.m

```
function y = load_radar_data(filename,fs,ta,sdr_type)
% filename: file path
% fs: sampling rate
% ta: analysis duration
% sdrtype: Type of SDR HW 'usrp' or 'hackrf'

% y: data vector

samples = [1,2*ta*fs];

if strcmp(sdr_type,'usrp')
    % USRP
    % Read samples
    y = audioread(filename,samples,'native');
    % Convert int16 to double and normalize
    y = double(y(1:2:end))/32768 + j*double(y(2:2:end))/32768;
elseif strcmp(sdr_type,'hackrf')
    % HackRF
    fid = fopen(filename,'r');
    y = fread(fid, 2*max(samples), 'int8');
    y = y(1:2:end)/128 + j*y(2:2:end)/128;
    fclose(fid);
else
   y=[];
end
```

ANEXO V

Código de cálculo del PDW

calculate_PDW.m

```
function [toa,tod,pw,prf,fp] = calculate_PDW(y,th1,th2,framesize,fs)
% Calculates the Pulse Descriptor Word (PDW) of a pulsed radar waveform
%
% y: signal vector
% th1: threshold level nr. 1
% th2: threshold level nr. 2
% framesize: data frame size
% fs: sampling rate (Hz)

% toa: pulse time of arrival (s)
% tod: pulse time of departure (s)
% pw: pulse width (s)
% prf: pulse repetition frequency (Hz)
% fp: detected pulse intermediate frequency (MHz)

toa = [];
tod = [];
pri = [];
pw = [];

% initialize counters
toa_cnt = 1;
tod_cnt = 1;
counter = 1;

% Pre-processing
video = abs(y(1:framesize));

% Create constant false alarm rate detection video
while counter < framesize
    if (video(counter)>th2)
        while (video(counter)>th1) & (counter<framesize)
            counter = counter+1;
        end
    else
        video(counter) = 0;
        counter = counter+1;
    end
end

figure
plot(video)
title('Detected CFA Video')

% Calculate TOA and TOD vectors
counter = 1;
while counter < framesize
    if (video(counter)<th2) & (video(counter+1)>th2)
        toa(toa_cnt) = counter;
```

```
            toa_cnt = toa_cnt+1;
        end
        if (video(counter)>th1) && (video(counter+1)<th1)
            tod(tod_cnt) = counter;
            tod_cnt = tod_cnt+1;
        end
        counter = counter+1;
    end

    % Calculate PRI vector
    if toa_cnt>1
        for idx = 2:toa_cnt-1
             pri(idx) = toa(idx) - toa(idx-1);
        end
    else
         disp('Not enough data to calculate PRI');
    end

    % Calculate PW vector
    if (toa_cnt >= 1) && (tod_cnt >= 1)
        for idx = 1:tod_cnt-1
            pw(idx) = tod(idx) - toa(idx);
        end
    else
        disp('No hay datos suficientes para calcular el PW');
    end

    toa = toa/fs;
    tod = tod/fs;
    pw  = pw/fs;
    prf = fs./pri;

    % Calculate data frame FFT
    frame_fft = fft(y(1:framesize));
    [~,ifftmax] = max(abs(frame_fft));
    fp = ifftmax*fs/framesize/2/1e6;
```

ANEXO VI

Código de diagrama de radiación de la antena

polar_dB.m

```
% polar_dB makes plot of gdb=10*log10(g) versus phi
% phi       = polar angles over [0,2*pi]
% gain      = gain (gain is in absolute units)
% rangedb     = maximum range for the plot
% increments= increments for the gain circles
% rays      = number of rays default is 16  use series of 4
% examples: polar_dB(phi, gain);
%           polar_dB(phi, gain, 20, 2.5, 16)
% Hakan Cakmak
% University of Duisburg-Essen,
% General and Theoretical Electrical Engineering
% hakan.cakmak@stud.uni-due.de
function h = polar_dB(phi, gain, rangedb, increments, rays)
if nargin < 5, rays = 16; end
if nargin < 4, increments = 2.5; end
if nargin < 3, rangedb = 20; end
% phi=linspace(0,2*pi,1000); % test
% gain=(sin(phi));
if nargin < 2
    warning('myApp:argChk', 'Not enough input arguments.');
    help polar_dB;
  return;
end
gain1 = 10 * log10(abs(gain));        % test = (isinf(gain1)-1).*gain1;
gain1(gain1==-Inf) = -rangedb;        % avoids -Inf's
gain1 = gain1 .* (gain1 > -rangedb) + (-rangedb) * (gain1 <= -rangedb);
% lowest is rangedb dB
gain1 = (gain1 + rangedb)/rangedb;
 % scale to unity max.
x = gain1 .* cos(phi);
y = gain1 .* sin(phi);

%R = 1.2; axis([-R, R, -R, R]);
N0 = 360;
phi0=linspace(0,2*pi,N0);
x0 = sin(phi0); % gain circles
y0 = cos(phi0);
patch('xdata',x0,'ydata',y0, ...
     'edgecolor','black','facecolor','w');
 hold on

%changed coordinates
h = plot( y, x,'LineStyle','-','color','blue');  %,'LineWidth', 2
hold on
title({'Linear Scale               ',...
  sprintf('Range:%3.2fdB           ',rangedb),...
  sprintf('Increments:%3.2fdB      ',increments)},'horizontalalignment','right');%
c_log=(-rangedb:increments:0);
c = (c_log)/-rangedb;
```

```
for k=2:length(c_log) %gain circles
    plot(x0*c(k), y0*c(k),'LineStyle',':','color','black');
end
for k=1:length(c_log) %gain circles markers
    text(0,c(k), sprintf('%.3g dB',c_log(length(c_log)-k+1)),...
            'horiz', 'center', 'vert', 'middle'); %,'fontsize', 13
end
phi_s=linspace(0,2*pi,rays+1);
x_s = sin(phi_s); % rays
y_s = cos(phi_s);
for k=1:rays
    line([x_s(k)/rangedb*increments,x_s(k)],...
        [y_s(k)/rangedb*increments,y_s(k)],'LineStyle',':','color','black');
    text(1.1*x_s(k),1.1*y_s(k),...
        sprintf('%.3g°',phi_s(k)/pi*180),...
        'horiz', 'center', 'vert', 'middle'); %,'fontsize', 15
end
axis square;
axis off
%hold off
```

ANEXO VII

Tabla de órdenes del ejercicio EWX 220 en la prueba de navegación

R 051200A FEB 20
FM BARRUTIA
TO CHEREGUINI
SALAS
RULL
INFO DIRENAM
NATO-UNCLASSIFIED
SIC/LAA//
XXXXX
BT
SUBJ/TABORD EWX 220 SRL 012XXX//
REF/A/ AXP-02(D)//
REF/B/ ATP-1(F) VOL 1//
RE/C/APP-1//
A/ SRL 12XXX EWX 220//
B/ DIRENAM//
C/ BAR//
D2/ BAR//
F1/CHE/RUL/SAL//
G/BAR//
H/ ALFA//
J1/ 121700A FEB 20//
JJ/ 121750A FEB 20//
N2/ PONTEVEDRA STUARY//
N5/ MUSSEL FARMS AND SHALLOW WATERS//
QQ2/ INITIAL FORMATION WILL BE FORM 1. BAR- SAL -RUL- CHE. BAR WILL BE GUIDE. DISTANCE BETWEEN UNITS WILL BE 100 YARDS//
ST1/ SAL WILL APROACH BAR BY HER STARBOARD SIDE, TO BE IN STATION LIMA TWO AT 25 YDS OF BAR. WHEN UNITS ARE IN DISTANCE, BAR WILL START NOISE JAMMING ON SAL. WHEN JAMMING IS RECEIVED BY SAL, SAL IS TO REPORT IAW ANNEX C REF C. THEN, AN INCREASE OF DISTANCE BETWEEN UNITS WILL BE ORDER BY BAR. THE DISTANCE IS TO BE INCREASED FROM 25 YDS IN INTERVALS OF 25 YDS, REPORTING CHE ONCE JAMMING NOT BE DETECTED. AT BAR ORDER, THE JAMMING WILL BE CONCLUDED//
ST2/ GADGET TO BE JAMMED WILL BE FURUNO LOW RADAR (OPS ROOM RADAR)//
ST3/ THE JAMMED RADAR WILL BE AT MAXIMUM ESCALE RANGE AND HIGH GAIN//
ST4/ JAMMING STATE REPPORT WILL BE DONE BY JAMMED UNIT IAW ANNEX C REF C.
ST5/ IF IT WORKS SUCCESFULLY, PROCESS WILL BE REPEATED WITH RUL AND SAL//
ST6/ N SPEED WILL BE 6 KNOTS//
U/ FREQPLAN/REPORTING UHF1/FL213/A/281.800 MHZ/A2E//
BT

ANEXO VIII

Código de generador de señal

Simulatorsignal.m

```
clear all;

% Radar signal generation
SampleRate = 10000000;
PulseWidth = 8e-07;
PRF = 10000;
NumPulses = 10;
SNR = 30;

N = 32;

% Create a Rectangular Waveform object
h = phased.RectangularWaveform;
h.SampleRate = SampleRate;
h.PulseWidth = PulseWidth;
h.PRF = PRF;
h.NumPulses = NumPulses;
snr = SNR;

%Create figure, panel and axes
fig = figure;
panel = uipanel('Parent',fig);
hAxes = axes('Parent',panel,'Color','none');
Fs = h.SampleRate;
x = step(h);
xn = awgn(x,snr);

win = kaiser(floor(length(xn)/N),38); % 38 is beta parameter
Threshold = -100;

Nf = 256;
fin = linspace(-Fs/2,+Fs/2-Fs/Nf,Nf);
%fin = Fs*(-1/2:1/256:127/256);
% Plot a spectrogram of xn
% [s,f,t] = spectrogram(x,window,noverlap,f,fs)
[~,f,t,p] = spectrogram(xn,win,floor(length(xn)/(N+1)),fin,Fs,'yaxis', ...
    'MinThreshold',Threshold, 'reassigned');

[~, t_scale, t_Units] = engunits(max(t));
[~, f_scale, f_Units] = engunits(max(f));
%set all 0 with next smallest value;
p(p<eps) = eps;
surf(f*f_scale,t*t_scale,(10*log10(abs(p'))),'EdgeColor','none');
%axis([f(1)*f_scale f(end)*f_scale t(1)*t_scale t(end)*t_scale]);

ylabel('Time (us)');
xlabel('Frequency (MHz)');
title('Spectrogram of Baseband Signal');
```

```
    axis xy;
    ch = colorbar;
    xlabel(ch, 'dB');

    figure
    %trange =
    plot(xn)

    % figure
    % plog=10*log10(abs(p'));
    % plot(plog(:,1:1))
```

ANEXO IX

Especificaciones radar 1944C Furuno

ESPECIFICACIONES DEL RADAR MARINO

MODELOS 18x4C/19x4C [24]

1 GENERAL

- Escala, longitud del impulso (PL) y frecuencia de repetición de impulsos (PRR)

Escala (MN)	Ancho de pulso (μs)	PRF (Hz aprox.)
De 0,125 a 1,5	0,08	2100
De 1,5 a 3	0,3	1200
De 3 a 64	0,8	600

- Escala máxima:
  - M1934C: 48 mn
  - M1944C: 64 mn
- Resolución de escala: 15 m
- Resolución de demora:
  - M1934C: 2,4°
  - M1944C: 1,9°
- Escala mínima: 42 m
- Precisión de demora ±1°
- Precisión del anillo fijo de escala 0,9% de escala o 8 m; se utilizará la que sea más alta

2 UNIDAD DE ANTENA

- MODELO 1934C:
  - Radiador Array guíaondas ranurada
  - Polarización Horizontal
  - Rotación de la antena 24 o 48 rpm (nominal)
  - Longitud del radiador 100 cm (XN10)
  - Ancho del haz horizontal 2,4°
  - Ancho del haz vertical 27°
  - Atenuación del lóbulo lateral -20 dB como máximo (hasta ±20º del lóbulo principal) -28 dB como máximo (±20º del lóbulo principal o más)
- MODELO 1944C:
  - Radiador Array guíaondas ranurada
  - Polarización Horizontal
  - Rotación de la antena 24 o 48 rpm (nominal)
  - Longitud del radiador 120 cm (XN12)
  - Ancho del haz horizontal: 1,9°
  - Ancho del haz vertical: 22°
  - Atenuación del lóbulo lateral -24 dB como máximo (hasta ±20º del lóbulo principal) -30 dB como máximo (±20º del lóbulo principal o más)

3 MÓDULO TRANSCEPTOR

- Frecuencia y modulación 9.410 MHz ±30 MHz (banda X), P0N
- Potencia de salida máxima
    - M1934C: 4 kW (nominal),
    - M1944C: 6 kW (nominal), M1954C: 12 kW (nominal)
- Modulador Método de conmutación de FET
- Frecuencia intermedia 60 MHz
- Sintonización Automática o manual
- Receptor (Front End) MIC (Microwave Integrated Circuit, circuito integrado de microondas)
- Ancho de banda Longitud del impulso Tx 0,08 μs y 0,3 μs: 25 MHz
- Longitud del impulso Tx 0,8 μs: 3 MHz
- Duplexor Circulador con diodo limitador
- Calentamiento 90 s aprox.

4 ALIMENTACIÓN

- Tensión/corriente nominal
    - M1934C 12-24 VCC: 8,9-4,3 A
    - M1944C 12-24 VCC: 9,3-4,4 A
- Rectificador (opción) 100-115/220-230 VCA, monofásico, 50/60 Hz

5 CONDICIONES AMBIENTALES

- Temperatura ambiente Unidad de antena: de -25 °C a +70 °C
- Unidad de presentación: de -15 °C a +55 °C
- Control remoto de +5 °C a +45 °C
- Unidad de alimentación: de -15 °C a +55 °C
- Humedad relativa 93% o inferior a +40 °C
- Resistencia al agua Unidad de antena: IPX6 Unidad de presentación: IPX5 (monitor
- externo conectado: IPX0) Control remoto, unidad de alimentación: IPX0
- Vibración de demora IEC 60945-4