

Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Evaluación de resiliencia de sistemas AIS frente a jamming y spoofing: propuesta de un protocolo de pruebas para buques de la Armada

Grado en Ingeniería Mecánica

ALUMNO: Andrés Ayán Durán

DIRECTORES: José María Núñez Ortuño

CURSO ACADÉMICO: 2025-2026

Universidade Vigo



Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Evaluación de resiliencia de sistemas AIS frente a jamming y spoofing: propuesta de un protocolo de pruebas para buques de la Armada

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

El presente Trabajo de Fin de Grado aborda la vulnerabilidad crítica de los sistemas receptores AIS ante ataques de *jamming* (interferencia) y *spoofing* (suplantación), una amenaza creciente para la seguridad y conciencia situacional de los buques de la Armada. Dado que el protocolo AIS carece de cifrado y autenticación, el autor propone un protocolo de pruebas estandarizado para evaluar la resiliencia de los receptores a bordo.

Utilizando tecnología de Radio Definida por Software (SDR), se diseñó un banco de ensayos para recrear cinco escenarios de amenaza: saturación del procesador mediante envíos masivos de mensajes, inyección de ayudas a la navegación falsas, interferencia deliberada con ruido blanco y medición de los tiempos de recuperación del sistema tras un ataque. La metodología se validó en un receptor comercial básico y en receptores de las lanchas de instrucción de la Escuela Naval Militar.

Los resultados demuestran que, aunque los equipos de alta gama poseen algoritmos de filtrado más robustos, todos presentan vulnerabilidades ante ataques dirigidos. La conclusión fundamental subraya que el AIS debe utilizarse exclusivamente como un sensor de apoyo, cuya información debe ser siempre contrastada con la de otros equipos disponibles, como el radar. Este trabajo aporta una herramienta técnica esencial para que la Armada evalúe sus sistemas actuales y futuras adquisiciones en entornos de guerra electrónica.

PALABRAS CLAVE

AIS, *Jamming*, *Spoofing*, Resiliencia, Seguridad

AGRADECIMIENTOS

En primer lugar, quiero expresar mi agradecimiento a mi tutor, D. José María Núñez Ortuño, por su ayuda constante durante el desarrollo de este trabajo. Su disponibilidad para resolver dudas en cualquier momento y sacarme de más de un problema que ha surgido, ha sido fundamental.

También quiero agradecer al personal del Núcleo de Lanchas de la Escuela Naval Militar por facilitarme el acceso a las lanchas de instrucción en todo momento, permitiendo llevar a cabo las pruebas en condiciones óptimas y con total disponibilidad.

Por último, y no menos importante, agradecer al personal del comedor por su disposición y consideración, al proporcionarme comidas incluso fuera del horario habitual, permitiéndome continuar las pruebas sin interrupciones.

CONTENIDO

Contenido 4
Índice de Figuras 8
Índice de Tablas 9
Índice de Acrónimos 10
1 Introducción y objetivos 12
1.1 Contexto y motivación 12
1.2 Objetivos y metodología 13
1.3 Estructura de la memoria 14
2 Estado del arte 15
2.1 El Sistema de Identificación Automática 15
2.1.1 Antecedentes y necesidad operativa 15
2.1.2 El AIS como sistema de comunicaciones 16
2.1.3 Dependencia del AIS de GNSS 17
2.1.4 Extensiones del sistema 18
2.1.4.1 AtoN 18
2.1.4.2 SAT-AIS 18
2.1.4.3 AIS-SART 18
2.1.4.4 EPIRB-AIS 19
2.1.4.5 MOB-AIS 19
2.1.4.6 AIS R 20
2.2 Vulnerabilidades intrínsecas al AIS 20
2.2.1 Spoofing 20
2.2.2 Jamming 21
2.2.3 Hijacking 21
2.2.4 DoS 21
2.3 Comunicaciones VHF marítimas 21
2.4 Interferencias en la banda VHF marítima y estrategias de mitigación 22
2.4.1 Tipología de interferencias 22
2.4.2 Impacto operacional de las interferencias 23
2.4.3 Técnicas de mitigación 23
2.5 Limitaciones físicas del AIS en banda VHF 24
2.5.1 Propagación LoS como condicionante estructural 24
2.5.2 Horizonte radioeléctrico y alcance operativo real 24
2.5.3 Multitrayecto, reflexiones y pérdida de mensajes AIS 25

2.5.4 Implicaciones de las limitaciones físicas en escenarios de interferencia 25
2.6 El AIS en el entorno naval: exposición táctica y resiliencia 25
2.6.1 Uso del AIS en operaciones de conocimiento del entorno marítimo 25
2.6.2 Pattern of Life como herramienta operacional y vector OSINT 26
2.6.3 Exposición táctica del AIS no cifrado 26
2.6.4 Secure AIS y soluciones técnicas de mitigación 27
2.6.5 Gestión de emisiones y doctrina EMCON 28
2.6.6 El uso del AIS en CEVACO 28
2.7 Casuística documentada de *spoofing* de AIS 29
2.7.1 Incidentes documentados y tendencias actuales 29
2.7.2 Caso de estudio: evento de spoofing en la Isla de Elba (2019) 30
2.7.3 Evaluación institucional y marco estratégico – Informe RIN 2026 31
2.7.4 Estrategias de detección y mitigación 31
3 Desarrollo del TFG 33
3.1 Caracterización del escenario real 33
3.1.2 Caracterización estadística del tráfico AIS 33
3.1.3 Justificación de los vectores de ataque 34
3.2 Descripción del equipamiento hardware 34
3.2.1 Receptor QK-A026 34
3.2.2 Transpondedor SIMRAD V5035 35
3.2.3 Transpondedor FURUNO FA-170 36
3.2.4 Dispositivos SDR 36
3.2.5 Splitter ZX-10-2-20-S+ 38
3.2.6 HYS Antena Marina VHF 38
3.3 Entorno de software y visualización 39
3.3.1 AIS-Catcher 39
3.3.2 OpenCPN 39
3.3.3 Arquitectura de interconexión 40
3.4 Implementación lógica de los ataques 42
3.4.1 Lógica de construcción de tramas 43
3.4.2 Librería de funciones 43
3.5 Entorno de modulación y control 43
3.5.1 Spoofer 43
3.5.2 Jammer 44
3.6 Conexión del hardware a LLII 44

3.7 Validación y puesta a punto del código conforme a los estándares 45
3.7.1 Tipo 1 46
3.7.2 Tipo 5 47
3.7.3 Tipo 21 48
3.8 Metodología de evaluación y criterios de degradación 49
3.8.1 Variables controladas 49
3.8.2 Variables observables 50
3.8.3 Propuesta del protocolo de pruebas 50
3.8.4 Indicadores de evaluación del sistema 52
3.8.5 Marco de evaluación y rúbrica de resiliencia 52
3.8.6 Calificación final del receptor 53
3.8.7 Cálculo del Packet Error Rate 54
4 Aplicación y validación del protocolo 56
4.1 Caracterización de la capacidad del receptor QK-A026 56
4.1.1 PS1 Saturación con mensajes Tipo 1 56
4.1.2 PS2 Saturación con mensajes Tipo 5 57
4.1.3 PS3 Suplantación de AtoN 58
4.1.4 PJ1 Jamming AWGN 59
4.1.5 PJ2 Recuperación del sistema 59
4.1.6 Calificación final del receptor QK-A026 59
4.2 Caracterización de la capacidad del transpondedor SIMRAD V5035 60
4.2.1 PS1 Saturación con mensajes Tipo 1 60
4.2.2 PS2 Saturación con mensajes Tipo 5 61
4.2.3 PS3 Suplantación de AtoN 62
4.2.4 PJ1 Jamming AWGN 62
4.2.5 PJ2 Recuperación del sistema 63
4.2.6 Calificación final del transpondedor SIMRAD V5035 63
4.3 Caracterización de la capacidad del transpondedor FURUNO FA-170 63
4.3.1 PS1 Saturación con mensajes Tipo 1 63
4.3.2 PS2 Saturación con mensajes Tipo 5 64
4.3.3 PS3 Suplantación de AtoN 65
4.3.4 PJ1 Jamming AWGN 65
4.3.5 PJ2 Recuperación del sistema 65
4.3.6 Calificación final del transpondedor FURUNO FA-170 65
5 Conclusiones y líneas futuras 67
5.1 Conclusiones 67

5.2 Líneas futuras 68
6 Bibliografía 69
Anexo I: Implicaciones Sociales, y/o Económicas, y/o Ambientales 72
Anexo II: Reflexiones Éticas y Sociales 73
Anexo III: TDMA 74
Anexo IV: Fichas técnicas de los receptores 75
Anexo V: Códigos 82

ÍNDICE DE FIGURAS

Figura 1-1 Principales rutas marítimas (Fuente: EOM 2021) 12
Figura 2-1 Conocimiento del entorno a través de AIS (Fuente: IMO) 16
Figura 2-2 Radiobaliza AIS-SART 19
Figura 2-3 Radiobaliza EPIRB-AIS 19
Figura 2-4 Radiobaliza MOB-AIS 20
Figura 2-5 Distribución de frecuencias VHF (Fuente: Apéndice 18 UIT) 21
Figura 2-6 Transmisión en línea de vista (Fuente: IN3ECI. Italian Amateur Radio Station) 24
Figura 2-7 Buques en el Mar Mediterráneo (Fuente: Marine Traffic) 26
Figura 2-8 Conexiones SAAB R6 Supreme AIS/VDES (Fuente: [29]) 28
Figura 2-9 Hotspots de interferencias GNSS y AIS 29
Figura 2-10 AIS *Spoofing* en la isla de Elba, 2019 (Fuente: [16]) 30
Figura 2-11 Recuperación del AIS tras un episodio de interferencias (Fuente: [33]) 32
Figura 3-1 Conexiones QK-A026 (Fuente: [35]) 35
Figura 3-2 Transpondedor SIMRAD V5035 de la primera serie de LLII de la ENM 35
Figura 3-3 Interfaz del transpondedor FURUNO FA-170 36
Figura 3-4 Unidad de recepción RTL-SDR 37
Figura 3-5 Unidad de transmisión ADALM-PLUTO 37
Figura 3-6 Divisor de potencia RF ZX-10-2-20-S+ 38
Figura 3-7 HYS Antena Marina VHF 38
Figura 3-8 Interfaz AIS-catcher (Ría de Pontevedra, 10/02/2026) 39
Figura 3-9 Interfaz OpenCPN (Ría de Pontevedra, 10/02/2026 1730) 39
Figura 3-10 Arquitectura de conexión para la fase de escucha 40
Figura 3-11 Estructura de conexión para validación *scripts* 40
Figura 3-12 Arquitectura de conexión para pruebas de *spoofing* (PS1 y PS2) 41
Figura 3-13 Arquitectura de conexión para pruebas de *spoofing* (PS3) 42
Figura 3-14 Arquitectura de conexión para pruebas de *jamming* (PJ1 y PJ2) 42
Figura 3-15 Bloques de procesamiento del *spoofer* en GNU-Radio 44
Figura 3-16 Bloques de procesamiento del *jammer* en GNU-Radio 44
Figura 3-17 Transmisión de mensaje AIS Tipo 1 47
Figura 3-18 Transmisión de mensaje AIS Tipo 1 + Tipo 5 48
Figura 3-19 Transmisión de mensaje AIS Tipo 21 49
Figura 3-20 Resumen de ponderación de cada prueba 54
Figura A3-1 Protocolo de transmisión de mensajes AIS (Fuente: [7]) 74

ÍNDICE DE TABLAS

Tabla 2-1 Intervalos de informe AIS (Fuente: [7]) 17
Tabla 2-2 Canales VHF marítimos más representativos (Fuente: Apéndice 18 ITU) 22
Tabla 3-1 Mensajes AIS captados en 9 horas de escucha pasiva en la Ría de Pontevedra 34
Tabla 3-2 Pruebas del protocolo y métricas de evaluación 52
Tabla 3-3 Rúbrica de puntuación de un receptor en base al protocolo 53
Tabla 3-4 Tabla a rellenar por el usuario tras obtener la puntuación de las pruebas 53
Tabla 4-1 Resumen de la prueba PS1 para el receptor QK-A026 57
Tabla 4-2 Resumen de la prueba PS2 para el receptor QK-A026 58
Tabla 4-3 Calificación final para el receptor QK-A026 59
Tabla 4-4 Resumen de la prueba PS1 para el receptor SIMRAD V5035 61
Tabla 4-5 Resumen de la prueba PS2 para el receptor SIMRAD V5035 62
Tabla 4-6 Calificación final para el receptor SIMRAD V5035 63
Tabla 4-7 Resumen de la prueba PS1 para el receptor FURUNO FA-170 64
Tabla 4-8 Calificación final para el receptor FURUNO FA-170 65

ÍNDICE DE ACRÓNIMOS

AIS	Automatic Identification System
AtoN	Aid to Navigation
AWGN	Additive White Gaussian Noise
CEVACO	Centro de Valoración y Apoyo a la Calificación Operativa para el Combate
COVAM	Centro de Operaciones y Vigilancia de Acción Marítima
CPA	Closest Point of Approach
DoS	Denial of Service
ECDIS	Electronic Chart Display and Information System
EMCON	Emission Control
EW	Electronic Warfare
GNSS	Global Navigation Satellite System
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
IMO	International Maritime Organization
ITU	International Telecommunication Union
LoS	Line of Sight
MARS	Maritime mobile Access and Retrieval System
MMSI	Maritime Mobile Service Identity
MSA	Maritime Situational Awareness
OGP	Oficial de Guardia en Puente
OSINT	Open Source Intelligence
PER	Packet Error Rate
PNT	Positioning, Navigation and Timing
PoL	Pattern of Life
RMP	Recognized Maritime Picture
SAR	Search and Rescue
SART	Search and Rescue Transponder
SDR	Software Defined Radio
SLOC	Sea Lines of Communication
SNR	Signal-to-Noise Ratio

SOLAS	Safety of Life at Sea
SOTDMA	Self-Organizing Time-Division Multiple Access
STANAG	Standardization Agreement
TCPA	Time to Closest Point of Approach
TDMA	Time-Division Multiple Access
UTC	Coordinated Universal Time
VTS	Vessel Traffic Services

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contexto y motivación

El conocimiento del entorno y de lo que nos rodea en el ámbito marítimo es esencial para garantizar la seguridad en la navegación. Por ello, la mejora de la conciencia situacional constituye uno de los objetivos principales del concepto de e-navigation introducido en 2018 por la Organización Marítima Internacional (IMO) [1]. Buenos sistemas de navegación y su correcto uso equivalen a una navegación segura. Pese al avance tecnológico que están experimentando los sistemas de navegación, con la automatización como principal objetivo de los fabricantes, se consideran elementos críticos de seguridad susceptibles a manipulaciones [2].

En la actualidad, gran parte del comercio mundial se transporta por vía marítima [3] por medio de las líneas de comunicación marítimas (SLOC). Como en todo, se busca rapidez y bajo coste en transporte. Es por ello por lo que las navieras tratan de atravesar las rutas a la mayor brevedad para obtener un elevado beneficio económico. En estrechos y canales artificiales como el Estrecho de Ormuz o el Canal de Suez, donde el margen de maniobra es limitado y el tráfico intenso, los sistemas de seguridad de los barcos tienen que estar en su máximo nivel de operatividad y sus operadores monitorizando cada anomalía que pueda surgir.

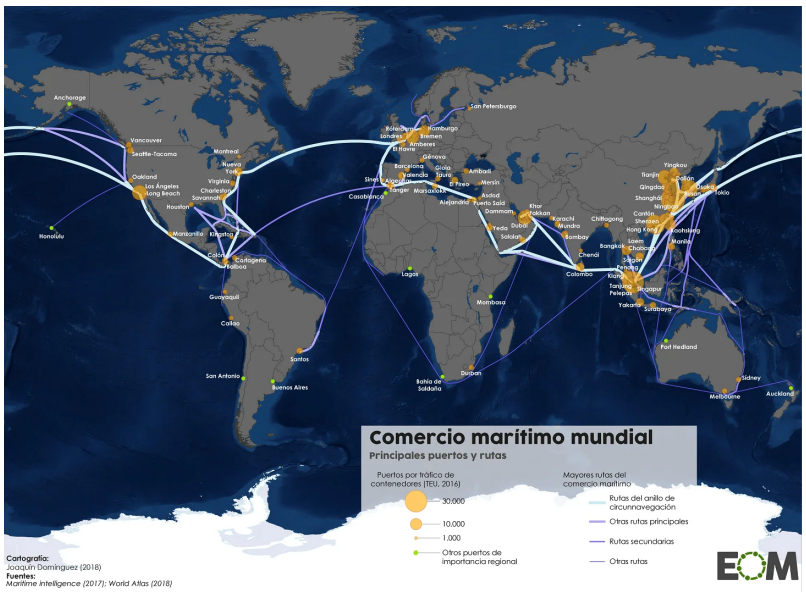


Figura 1-1 Principales rutas marítimas (Fuente: EOM 2021)

El creciente uso de sistemas electrónicos en el entorno marítimo ha incrementado la exposición a vulnerabilidades y riesgos asociados a la ciberseguridad [2]. Estos sistemas requieren un mantenimiento adecuado para garantizar la fiabilidad de la información que procesan. Si bien el Oficial de Guardia en Puente (OGP) conserva la responsabilidad última de la navegación, debe mantener un control riguroso de sus sistemas y verificar la información que estos proporcionan [4]. La toma de decisiones ya no se basa exclusivamente en la observación directa como en el pasado, sino que la integración de diversas fuentes digitales [1] configura el entorno situacional de la tripulación.

Los radares, sistema de información y visualización de cartas electrónicas (ECDIS) y sistema de identificación automática (AIS), entre otros, son los principales sistemas de navegación y vigilancia que incorpora cada buque [5]. Al integrar estos sistemas de manera correcta, el OGP tiene la capacidad de gobernar el buque sin comprometer su integridad [1]. Tras la promulgación de la regla V/19 del Convenio Internacional para la Seguridad de la Vida Humana en la Mar (SOLAS) [5] por parte de la IMO en el año 2000, se estableció la obligatoriedad, a determinadas categorías de buques, de contar con un AIS capaz de transmitir su velocidad, identificación y rumbo, entre otros datos, [6] a diferentes buques y autoridades costeras. Por este motivo, se concibe el AIS como una herramienta de apoyo más para mejorar la conciencia situacional.

En este contexto, el presente trabajo propone un protocolo experimental destinado a evaluar la resiliencia de receptores AIS frente a diferentes escenarios de manipulación y saturación de tráfico. Para ello se ha desarrollado un entorno de pruebas basado en radio definida por software (SDR), capaz de generar tráfico AIS controlado y analizar la respuesta del sistema receptor.

1.2 Objetivos y metodología

Este trabajo pretende ofrecer a la Armada un protocolo de pruebas para sus receptores AIS. Mediante este protocolo se busca detectar el nivel de resiliencia del receptor y evaluar sus vulnerabilidades, con el fin último de estudiar cómo reacciona el sistema frente a *jamming* y *spoofing.*

- En primer lugar, se realizará un estudio a fondo del receptor AIS QK-A026 de la marca Quark-Elec propiedad del Centro Universitario de la Defensa.
- En segundo lugar, se procede a llevar a cabo las diferentes perturbaciones en un ambiente controlado en laboratorio, del receptor QK-A026 y de los receptores AIS embarcados en las lanchas de instrucción de la Escuela Naval Militar.
- En tercer lugar, se evalúa la resiliencia del sistema y se redacta un protocolo de pruebas a partir de los ataques realizados para su posterior estandarización con el fin de ofrecérselo a la Armada.

Objetivo general

Analizar la resiliencia de receptores AIS frente a escenarios de saturación y manipulación de tráfico mediante el desarrollo de un entorno experimental basado en SDR y proponer un protocolo de pruebas estandarizado para buques de la Armada.

Objetivos específicos

- Diseñar un entorno experimental para generación controlada de tráfico AIS.
- Evaluar el comportamiento de los receptores frente a diferentes escenarios de perturbación.
- Definir métricas cuantitativas que permitan evaluar de forma objetiva la degradación de los receptores.
- Proponer un protocolo estandarizado de pruebas de resiliencia para receptores AIS.
- Validar experimentalmente el protocolo propuesto mediante su aplicación a distintos receptores AIS.

1.3 Estructura de la memoria

El presente Trabajo de Fin de Grado se estructura en cinco capítulos principales y sus cinco anexos. Se desarrolla de forma progresiva el análisis de la resiliencia de los receptores AIS descritos frente a escenarios de perturbación, utilizando el protocolo de pruebas propuesto.

- Capítulo 1: Se introduce el contexto general del trabajo, justificando la importancia del AIS en los escenarios geopolíticos complejos de la actualidad. Se presentan, además, los objetivos que se persiguen durante el desarrollo del estudio.
- Capítulo 2: En este capítulo se recoge el estado del arte. Se describen las bases de funcionamiento del AIS, haciendo hincapié en su necesidad operativa, su funcionamiento dentro del ámbito de comunicaciones VHF marítimas y sus principales vulnerabilidades con ejemplos documentados.
- Capítulo 3: El capítulo desarrolla la metodología experimental utilizada, describiendo el entorno de pruebas creado, el equipamiento hardware y software, la lógica de generación de mensajes (desarrollado en más detalle en el Anexo V) y, por último, el protocolo de pruebas propuesto.
- Capítulo 4: Se aplica el protocolo propuesto a los dos receptores estudiados. Se presenta el análisis de los resultados obtenidos durante la fase experimental.
- Capítulo 5: Recoge las conclusiones y posibles líneas futuras del trabajo.
- Anexo I: Se desarrollan las implicaciones sociales, y/o ambientales, y/o económicas, y/o ambientales del trabajo realizado.
- Anexo II: Se desarrollan las reflexiones éticas y sociales del presente trabajo.
- Anexo III: Explica el funcionamiento de TDMA.
- Anexo IV: Presenta las fichas técnicas de los receptores estudiados.
- Anexo V: Desarrolla la elaboración de los códigos empleados para llevar a cabo las diferentes pruebas del protocolo propuesto.

2 ESTADO DEL ARTE

El presente capítulo expone el marco teórico de referencia sobre el que se basa este TFG. Se abordan los fundamentos técnicos, los estándares y las principales vulnerabilidades asociadas al sistema AIS. Asimismo, se analizan las amenazas más relevantes con el objetivo de darle contexto al desarrollo del trabajo para justificar la necesidad de un método de evaluación de la resiliencia de los receptores AIS.

2.1 El Sistema de Identificación Automática

El AIS se define formalmente como un sistema cooperativo y abierto de radiodifusión en la banda VHF marítima diseñado para mejorar la seguridad en la navegación y la gestión del tráfico mediante el intercambio de información automática de posición, identificación, rumbo, velocidad y destino, entre otros, entre buques y estaciones costeras [7]. Su configuración estándar no incorpora mecanismos de cifrado ni autenticación [6], lo que habilita la manipulación de datos y ataques de disponibilidad [8, 9].

Desde el punto de vista operativo, el sistema organiza sus transmisiones mediante Acceso Múltiple por División en el Tiempo Autoorganizado (SOTDMA) y Acceso Múltiple por División en el Tiempo (TDMA), cuyo funcionamiento se describe en el Anexo III, en "*slots*" temporales, en los que cada canal cuenta con 2.250 *slots* por minuto, lo que permite una coordinación eficiente en zonas de alta densidad de tráfico. La estructura y mecanismos de acceso vienen descritos en la Recomendación ITU-R M.1371-6 [6] en su Anexo II, donde se fija la asignación de *slots* y las tasas de reporte en función del tipo de mensaje, considerando la coexistencia de dos canales.

Sin embargo, la creciente dependencia del AIS como fuente primaria de información presenta diversas vulnerabilidades técnicas y operativas que pueden ser explotadas mediante interferencias o manipulación deliberada del tráfico AIS.

2.1.1 Antecedentes y necesidad operativa

Antes de la implementación obligatoria del AIS como elemento complementario, la conciencia situacional se basaba en su totalidad en tres fuentes principales de información: la observación visual, el radar y las comunicaciones por voz a través de VHF. Una de las principales herramientas del oficial de guardia en puente ha sido tradicionalmente el radar, ya que permite detectar y seguir contactos en el entorno inmediato del buque [4]. Sin embargo, la información que proporciona es meramente cinemática.

Para evaluar de forma correcta la situación táctica o de navegación resulta necesario disponer de información adicional, como el nombre del buque, su tipo, su bandera o la identidad del servicio móvil marítimo (MMSI) [6], entre otros. Estos datos aportan un contexto que permite mejorar la interpretación de las intenciones de los barcos que operan en la zona. La ausencia de esta información en escenarios

con alta densidad de tráfico o condiciones meteorológicas adversas puede incrementar la carga de trabajo del personal de puente [1], desviando su atención de otros aspectos más relevantes para la seguridad en la navegación. Así, aumenta la probabilidad de confusiones en la identificación de contactos o en la interpretación de sus maniobras futuras.

En este contexto, nace el AIS como sistema cooperativo destinado a facilitar el intercambio de información entre buques y estaciones costeras [7]. A través de este sistema automatizado, cada barco emite en intervalos de tiempo establecidos en función del mensaje, como muestra la Tabla 2-1, datos relativos a su identidad, posición y estado de navegación [6], contribuyendo a mejorar la conciencia situacional compartida.

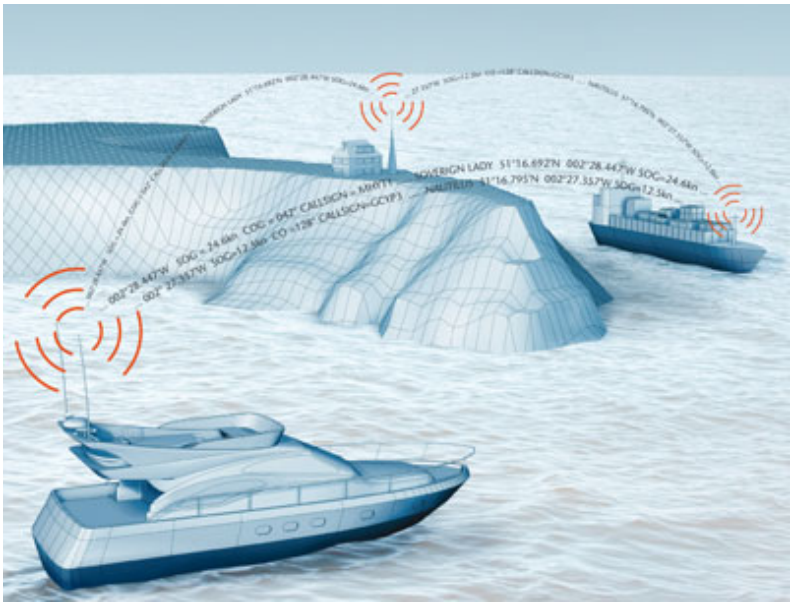


Figura 2-1 Conocimiento del entorno a través de AIS (Fuente: IMO)

No fue hasta finales de la década de los 90 cuando la IMO estableció los primeros requisitos formales para el funcionamiento del AIS [10]. De esta manera, el AIS pasó a convertirse en un sistema reglamentado dentro del marco de la seguridad marítima. La Unión Internacional de Telecomunicaciones (ITU) define en [6] las características técnicas del enlace radioeléctrico, en la que se describen el mecanismo TDMA y el uso de la banda VHF marítima, entre otros.

Finalmente, entre los años 2002 y 2004, el Convenio SOLAS introduce la obligación de instalar equipos AIS en determinados tipos de buques. Esta decisión normativa marca un punto de inflexión, ya que convierte al AIS en una infraestructura global ampliamente extendida y en fuente de datos omnipresente. No obstante, aunque la instalación es obligatoria en buques que superen determinados tonelajes, su uso obligatorio no es aplicable en unidades militares [5], que pueden limitar o incluso suprimir la transmisión de datos AIS en función de sus necesidades operativas.

2.1.2 El AIS como sistema de comunicaciones

El sistema facilita la operación simultánea de un número considerable de estaciones sin requerir coordinación centralizada. Su arquitectura se fundamenta en TDMA, organizando la transmisión de datos en mensajes estandarizados que incorporan información dinámica, información estática e información relativa al viaje [6]. Esta estandarización asegura la interoperabilidad entre equipos de diferentes fabricantes y sistemas embarcados.

Se distinguen dos tipos de equipos: Clase A y Clase B. Los transpondedores Clase A están destinados a buques sujetos al Convenio SOLAS [5], operando con potencias de transmisión de 12,5 W, tasas de actualización en información dinámica superiores [6] y mecanismos de acceso que, en entornos de alta densidad de tráfico, priorizan la fiabilidad del intercambio de datos. El comportamiento de estos

equipos facilita la interoperabilidad e integración completa con otros sistemas del barco. Los transpondedores Clase B están orientados a embarcaciones no obligadas a portar AIS, como las de recreo o determinadas embarcaciones pesqueras. Estos equipos presentan requisitos técnicos menos exigentes, con potencias de transmisión de 2 W y menores frecuencias de actualización de la información dinámica. A diferencia de los equipos Clase A, que emplean el mecanismo SOTDMA, los transpondedores Clase B utilizan generalmente *Carrier Sense Time Division Multiple Access* (CSTDMA), que busca *slots* libres cada vez para su transmisión, lo que implica una menor prioridad en el acceso al canal [6]. Aun así, se puede dar el caso de que un clase B utilice SOTDMA, con transmisiones del orden de 5 W de potencia. El comportamiento operativo del AIS en escenarios reales se refleja en la coexistencia entre ambas clases.

Estas clases de transpondedores se complementan con la existencia de estaciones base AIS [6], instaladas en tierra por autoridades marítimas para la gestión del tráfico y provisión de servicios de tráfico marítimos (VTS). Se incluye además la ayuda a la navegación (AtoN) [7], empleado en ayudas de navegación físicas, sintéticas o virtuales. Como complemento a las redes AIS terrestres se ha desarrollado el AIS satelital (SAT-AIS), que extiende la cobertura del sistema a zonas oceánicas fuera del alcance de las estaciones costeras.

En función de la estación desde la cual se transmita un mensaje y de las condiciones de esta, la variación en los intervalos de la transmisión se muestra en la Tabla 2-1:

Tipo de estación	Intervalo
Clase A SOG < 3 nudos en estado “Fondeado” o “Amarrado” y Clase B SOG < 2 nudos	3 min
Clase A SOG > 3 nudos en estado “Fondeado” o “Amarrado” y Clase A SOG 0 – 14 nudos	10 seg
Clase A SOG 0 – 14 nudos con cambios de rumbo	3 $^{1}/_{3}$ seg
Clase A SOG 14 – 23 nudos	6 seg
Clase A SOG 14 – 23 nudos con cambios de rumbo	2 seg
Clase A SOG > 23 nudos	2 seg
Clase B SOG > 2 nudos	30 seg
Clase A y Clase B información estática	6 min
AIS-SART, MOB-AIS o EPIRB-AIS	8 mensajes/min

Tabla 2-1 Intervalos de informe AIS (Fuente: [7])

2.1.3 Dependencia del AIS de GNSS

Para funcionar correctamente y generar sus informes correspondientes en forma de mensaje, el AIS requiere de un sensor de posición, además de una referencia temporal (UTC) para mantener la sincronización del enlace TDMA. Es por ello por lo que los transpondedores pueden llevar implementado un receptor del Sistema Global de Navegación por Satélite (GNSS) o recibir una alimentación externa al sistema; de hecho, su uso se contempla en [6] como fuente de datos para posición y disponibilidad de tiempo. La importancia de la fuente GNSS es tal que, en caso de fallo o degradación de esta, la posición que se transmite y la calidad temporal con la que AIS organiza sus transmisiones pueden verse comprometidas.

La posibilidad de que el GNSS sufra degradación, interferencia o manipulación puede dar lugar a la transmisión de posiciones erróneas al recibir *spoofing* directo o indirecto a través del sensor de posición [11]. Como resultado, se aumenta el riesgo operacional de la unidad si se toma tan solo el AIS como única fuente de datos. Se deberán tener en cuenta todos los sistemas instalados en los buques para así corroborar la información recibida a través del AIS, que en muchos casos puede ser errónea o falsa [12].

2.1.4 Extensiones del sistema

Las ampliaciones mencionadas a continuación refuerzan la conciencia situacional, pero mantienen la misma arquitectura abierta, heredando sus vulnerabilidades estructurales:

2.1.4.1 AtoN

Una AtoN no es más que una ayuda externa que complementa al sistema y proporciona mayor seguridad en la navegación y conocimiento del entorno. Facilita datos relevantes necesarios para detectar peligros o incluso establecer rutas seguras [7]. La Asociación Internacional de Autoridades de Ayudas a la Navegación y Faros (IALA) define una AtoN como "un dispositivo o sistema externo a buques designado y operado para mejorar la navegación segura y eficiente de buques y/o tráfico marítimo" [7]. Son faros, marcas o balizas que emiten el mensaje AIS tipo 21 en el que se identifica el MMSI de la AtoN, el tipo, nombre, posición geográfica, estado operativo, características, dimensiones [6] y un indicador que determina si es una AtoN física, virtual o sintética. Una AtoN física es aquella en la que el transmisor está instalado directamente en la plataforma; una sintética existe físicamente y se le añade información digital pese a que su señal lumínica, por ejemplo, no funcione; y la virtual no existe físicamente sino que su posición se transmite desde una estación separada geográficamente [7].

2.1.4.2 SAT-AIS

Las limitaciones existentes en la propagación de VHF descritas en el apartado 2.5.1, con la restricción en la cobertura de estaciones costeras con buques o con otras estaciones, debido a la distancia muestra, uno de los puntos débiles del sistema. Con la necesidad de proveer cobertura AIS global se desarrolló un sistema espacial de recepción de señales, con capacidad de captar de forma simultánea las transmisiones de buques fuera del alcance de estaciones costeras. Uno de los problemas del SAT-AIS es su capacidad de recibir señales de un gran número de buques, a diferencia de las estaciones terrestres. Con superposiciones en *slots* TDMA se producen pérdidas de mensajes en zonas de alta densidad de tráfico. A pesar de ello, en zonas donde no existen estaciones costeras su uso se ha vuelto relevante, complementando al AIS convencional [13].

2.1.4.3 AIS-SART

La función del AIS-SART es la de dispositivo de supervivencia con envío autónomo de mensajes tipo 1 y tipo 14 que contienen la posición GPS de un siniestro [14]. Permite la visualización en las pantallas de navegación de buques y de estaciones costeras y alerta de forma inmediata a los servicios de rescate. Transforma una señal de socorro en un objetivo digital dinámico, facilitando la detección de la posición de naufragio o emergencia para que se vea bajo cualquier tipo de condición meteorológica [7]. Permite tanto a aeronaves de búsqueda y rescate (SAR) como a buques de salvamento identificar con buena precisión la posición de emisor.



Figura 2-2 Radiobaliza AIS-SART

2.1.4.4 EPIRB-AIS

Este tipo de balizas combina una alerta por satélite a centros de coordinación de rescate con la emisión de señales AIS de localización a buques que se encuentren por la zona [15]. De esta manera, se reduce el tiempo de respuesta pues permite comenzar las labores de búsqueda y rescate rápidamente. Mejora la conciencia situacional en este tipo de emergencias, asegurando que la alerta llega tanto a equipos de rescate especializados como a barcos que se encuentren por la zona, cumpliendo así la regla V-33 del Convenio SOLAS.



Figura 2-3 Radiobaliza EPIRB-AIS

2.1.4.5 MOB-AIS

Estos sistemas transmiten una señal de socorro local mediante mensajes AIS de corto alcance [15]. Se diseñan para portarse en chalecos salvavidas y activarse al caerse al agua. Permite que la posición del náufrago se vea en las pantallas de navegación para su seguimiento en caso de pérdida de contacto visual. En muchos casos, los sistemas de los barcos pueden generar una ruta directa al náufrago.



Figura 2-4 Radiobaliza MOB-AIS

2.1.4.6 AIS R

Para lograr mayores alcances a los mencionados en 2.5.2, se utiliza un repetidor AIS. Se suelen situar en estaciones costeras, boyas o balizas [7] para mejorar la recepción más allá de la línea de vista (LoS). No actúa como transpondedor sino como un complemento repetidor cuyo fin es extender la huella de cobertura del sistema. La topografía es uno de los grandes enemigos del VHF. Los repetidores permiten superar los obstáculos topográficos con los que se pueda encontrar una transmisión en su camino y vencer las limitaciones de la propagación.

Se evitan puntos muertos y proporciona caminos alternativos para las señales al añadirse puntos adicionales de transmisión. Da redundancia a la red AIS al minimizar la dependencia de estaciones base, actuando como un refuerzo pasivo frente a pérdidas de cobertura locales.

Aunque muchos son los beneficios, el repetidor también cuenta con limitaciones. Depende por completo de la señal recibida; si esta es de baja calidad, débil o errónea, la retransmisión será la réplica de lo recibido. El sistema es igual de susceptible a *jamming, spoofing* o cualquier tipo de perturbación que un sistema AIS [2], pudiendo amplificar la propagación de información falsa si no existe un protocolo de control adecuado.

2.2 Vulnerabilidades intrínsecas al AIS

Al priorizarse la interoperabilidad global sacrificando mecanismos de seguridad críticos, la exposición a interferencias deliberadas por parte de emisores no autorizados es elevada. Las debilidades estructurales habilitan diversos vectores de ataque, desde la manipulación de datos legítimos hasta denegación de servicio (DoS). Según [8], las vulnerabilidades se pueden clasificar en tres categorías principales: *spoofing, hijacking* y DoS. A estas tres categorías se podría añadir una cuarta: *jamming*. En el presente capítulo se desarrollan las tres y su relación con DoS, ya que de una forma u otra intervienen en el protocolo de pruebas desarrollado en el apartado 3.8.3.

2.2.1 Spoofing

El objetivo de este tipo de amenazas es el engaño a barcos por medio de la creación de trazas ficticias. Se trata de objetivos “fantasma” como describe [16], AtoNs o transpondedores SAR (SART), entre otros, con información estática asignada con el fin de alterar el comportamiento de las unidades que se encuentran por la zona. La falsificación de las AtoNs puede tener consecuencias tales como la desviación de un buque de su canal seguro hacia aguas poco profundas, pudiendo dar lugar a un encallamiento. Por otro lado, la generación falsa de un SART es alarmante ya que los protocolos obligan a buques cercanos a acudir a la supuesta emergencia. Esto último podrían aprovecharlo piratas para dirigir a sus víctimas a espacios marítimos bajo su control. Pero lo más relevante en este TFG es la generación masiva de barcos “fantasma”, que permite medir la resiliencia del receptor frente a este tipo de amenazas.

2.2.2 Jamming

El *jamming* se realiza mediante la emisión de ruido o señales de alta potencia en las frecuencias de funcionamiento de AIS. Al transmitir una señal radio de mayor potencia, las transmisiones se solapan o pueden llegar incluso a anularse. Este tipo de interferencia se puede aplicar tanto directamente sobre la banda VHF como sobre las señales GNSS [11] de las que depende el sistema. En este último caso, el bloqueo de GNSS provoca que el transpondedor pierda la capacidad de reportar la posición real del buque. Existen diversos tipos de *jamming*; sin embargo, para el caso del presente trabajo se emplea ruido blanco gaussiano (AWGN).

2.2.3 Hijacking

El *hijacking* consiste en la modificación de información asociada a estaciones AIS legítimas. Se puede considerar una variante del *spoofing* al alterar la información de objetivos reales y no la generación de entidades ficticias. A nivel radioeléctrico, se puede lograr sobrescribiendo la señal mediante la emisión de una de mayor potencia [8]. Este tipo de ataque guarda una estrecha relación con la prueba de suplantación descritas en el apartado 3.8.3, al introducirse información falsa que puede ser interpretada como legítima por el receptor.

2.2.4 DoS

La capacidad de anular la comunicación AIS se puede llevar a cabo mediante la disrupción de disponibilidad. Destaca el *slot starvation* [8], el cual impide que buques reales puedan emitir datos debido a la reserva fraudulenta de todos los espacios de tiempo de transmisión disponibles. De esta manera se deja a un buque "invisible" o se satura la red. Una generación masiva de trazas ficticias como las que se describen en el apartado 2.2.1 pueden causar *flooding*, con el fin de ocupar todos los recursos del sistema, ya sea a nivel canal o de procesamiento.

En este contexto, el DoS no constituye un mecanismo aislado, sino un efecto que puede lograrse mediante diferentes técnicas. Estas pueden variar desde la inyección de grandes volúmenes de tráfico falso, hasta la degradación de la disponibilidad al corromper información crítica. Aunque los enfoques sean diferentes en su naturaleza – lógico en el caso de *spoofing* y *hijacking* y físico en *jamming* – convergen en un mismo resultado: la pérdida de disponibilidad operativa del AIS.

2.3 Comunicaciones VHF marítimas

La banda de frecuencia muy alta (VHF), comprendida entre 30 y 300 MHz, alberga una parte significativa de las comunicaciones marítimas y los servicios relacionados. Concretamente, la banda VHF 156-174 MHz [17, 18] se dedica principalmente a estas aplicaciones. El Apéndice 18 del reglamento de Radiocomunicaciones de la ITU [19] establece un plan internacional que organiza esta banda en canales específicos como muestra la Figura 2-5:

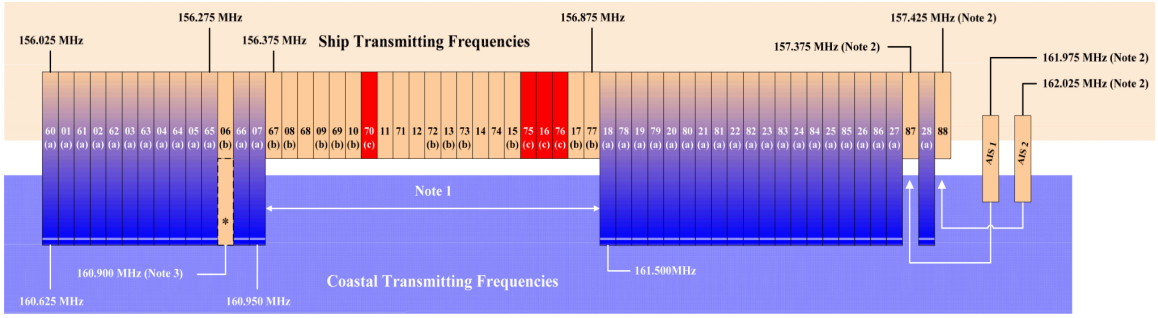


Figura 2-5 Distribución de frecuencias VHF (Fuente: Apéndice 18 UIT)

Las comunicaciones VHF marítimas operan predominantemente en modo simplex, caracterizado por la transmisión y recepción alternadas en la misma frecuencia. No obstante, conforme al plan de

canalización establecido por la ITU, las estaciones costeras emplean canales dúplex para enlaces buque-costa, permitiendo la transmisión y recepción en frecuencias distintas [19]. La mayoría de equipos instalados a bordo admiten una canalización con un espaciado de 25 kHz [20], con modulación en frecuencia de banda estrecha.

La Tabla 2-2 resume los canales VHF más representativos con sus respectivas frecuencias y usos principales:

Canal/Servicio	Frecuencia (MHz)	Uso principal
Canal 16	156,800	Distress, Safety and Calling (voz)
Canal 70	156,525	DSC (Llamada Selectiva Digital)
AIS 1 (87B)	161,975	Canal AIS global designado
AIS 2 (88B)	162,025	Canal AIS global designado
Canal 06	156,300	SAR y seguridad

Tabla 2-2 Canales VHF marítimos más representativos (Fuente: Apéndice 18 ITU)

2.4 Interferencias en la banda VHF marítima y estrategias de mitigación

La propagación en esta banda se caracteriza por un comportamiento en LoS condicionado por diversos factores como el horizonte radioeléctrico, la altura de la antena y otros fenómenos atmosféricos que limitan el alcance efectivo [21]. Esto causa que el sistema sea particularmente sensible a interferencias generadas dentro de su radio de cobertura.

El marco regulador del AIS define parámetros de potencia y modulación, entre otros, pero no contempla mecanismos de protección frente a interferencias en la capa física como puede ser el ruido, tanto intencionado como accidental. El ruido es una de las principales causas de interferencias en sistemas VHF en entornos marítimos [22]. En el presente apartado se describen los productores de interferencias más frecuentes además de técnicas de mitigación y buenas prácticas.

2.4.1 Tipología de interferencias

Las interferencias en la banda VHF se pueden catalogar en tres categorías principales: no intencionadas, derivadas o intencionadas.

En las no intencionadas destacan, sobre todo, aquellas generadas debido a la presencia cercana de diferentes tipos de transmisores, tanto propios como de terceros, que pueden causar una desensibilización del receptor. Dada la alta densidad de antenas en las superestructuras de los barcos y su proximidad física a la antena AIS, se pueden hacer más notables las interferencias. Resaltan más si cabe cuando se encuentra próxima a una estación de VHF operando en canales con frecuencias próximas a las asignadas para AIS. En entornos portuarios o zonas de alta densidad de tráfico, estos factores pueden provocar degradaciones temporales en la recepción de mensajes AIS.

Se debe tener en cuenta también el *"man-made noise"*, un ruido electromagnético artificial generado por los propios equipos eléctricos y electrónicos a bordo de los buques [22]. En instalaciones con aislamientos deficientes, los sistemas de iluminación LED, convertidores de potencia, motores eléctricos, radares y equipos de comunicación, entre otros, pueden introducir emisiones no deseadas en el entorno radioeléctrico. Estas emisiones pueden elevar el nivel de ruido de fondo en la banda VHF, reduciendo la relación señal a ruido (SNR) efectiva de un receptor AIS y disminuyendo su sensibilidad operativa. Resulta especialmente relevante en plataformas navales modernas que integran una alta cantidad de equipos y en entornos portuarios donde confluyen las emisiones tanto de buques como de estaciones costeras.

Como interferencias derivadas cabe destacar la congestión espectral causada por el propio mecanismo de acceso al medio que emplea el AIS descrito en el Anexo III. En escenarios de tráfico intenso, se incrementa la probabilidad de colisión y pérdida de mensajes [8]. Aunque es inherente al diseño del sistema, puede ser explotado deliberadamente.

Finalmente, las interferencias intencionadas consisten en la emisión deliberada de señales en frecuencias AIS con el objetivo de impedir la recepción legítima de mensajes. Se pueden centrar en un único canal AIS o en ambos. Debido a que los transpondedores AIS trabajan en potencias relativamente bajas, un emisor trabajando a una potencia mayor puede interferir fácilmente en el receptor, comprometiendo la operatividad del sistema.

2.4.2 Impacto operacional de las interferencias

Las interferencias en la banda VHF no solo implican la pérdida de mensajes AIS, sino que pueden conllevar efectos operacionales relevantes como la degradación en el cálculo de parámetros de riesgo de colisión como son el punto de aproximación más cercano (CPA) y tiempo al CPA (TCPA). Además, en los radares de puente o ECDIS con entradas AIS, se puede producir la desaparición temporal de la información de los blancos, reduciendo la conciencia situacional del OGP y de centros de vigilancia costera. Estos efectos pueden comprometer la seguridad en la navegación, especialmente en zonas de alta densidad de tráfico o en áreas estratégicas.

Desde el punto de vista de la ciberseguridad, una interferencia sostenida puede simular un ataque de DoS como se menciona en el apartado 2.2.4. Así, este tipo de interferencia se convierte en un vector de amenaza [2, 23] especialmente relevante dentro del análisis de resiliencia del sistema, al dificultar la distinción de una degradación técnica convencional de una deliberada si no se dispone de equipos de monitorización adecuados.

2.4.3 Técnicas de mitigación

Las técnicas de mitigación se pueden agrupar en diferentes niveles: a nivel del plano físico, a nivel del ámbito electrónico, a nivel sistémico y a nivel de escenarios de interferencia deliberada. Ciertas buenas prácticas reducen significativamente la susceptibilidad a interferencias y mejora la relación señal-ruido del sistema AIS.

En el plano físico, una correcta instalación de las antenas es fundamental. La IALA recomienda mantener una separación adecuada entre antenas y fuentes de alta potencia. El cableado de los sistemas empleado deberá ser coaxial con apantallamiento adecuado y la disposición de los conductores ha de buscar minimizar acoplamientos no deseados [7]. Esto, sumado al empleo de filtros pasa-banda específicos, reduce significativamente la susceptibilidad a interferencias a las que se puede ver expuestas una comunicación en VHF.

En el ámbito electrónico, resulta determinante el diseño de un receptor que cuente con filtros y controles de ganancia que optimicen las señales recibidas y minimicen la saturación frente a señales adyacentes [24] de elevada potencia. Un buen diseño del equipamiento hardware supone una de las principales barreras técnicas frente a interferencias tanto accidentales como deliberadas.

A nivel sistémico, se puede lograr un aumento de la resiliencia global del sistema mediante la integración de redundancia proveniente de SAT-AIS, radares o GNSS. De esta manera se reduce la probabilidad de fallo total ante perturbaciones.

Finalmente, frente a escenarios de interferencia deliberada, es clave una monitorización continua del espectro y la detección de anomalías. Un análisis estadístico de pérdida de paquetes puede ayudar a localizar, en caso de existir, el origen de una interferencia. En el desarrollo del presente trabajo se realiza un análisis estadístico de pérdidas de paquetes, como se describe en el apartado 3.8.7, mediante la inyección de mensajes a diferentes frecuencias de envío en distintos tipos de receptores.

2.5 Limitaciones físicas del AIS en banda VHF

2.5.1 Propagación LoS como condicionante estructural

La propagación de la banda VHF marítima se lleva a cabo mediante lo que se conoce como LoS. El alcance en VHF viene determinado principalmente por la geometría del enlace y la altura relativa de las antenas transmisora y receptora.

La causa principal por la cual la cobertura del AIS no depende exclusivamente de la potencia de transmisión, sino de las condiciones físicas del enlace radioeléctrico, es la reducida altura relativa de las antenas respecto a la superficie del mar. Por este motivo, la curvatura de la tierra se convierte en el principal factor limitante del alcance [21]. Esta limitación estructural tiene como consecuencia que cualquier interferencia o emisor malicioso que se encuentre dentro del horizonte radioeléctrico de una unidad, tenga una alta capacidad de afectar a la disponibilidad del sistema, independientemente de la distancia entre plataformas.

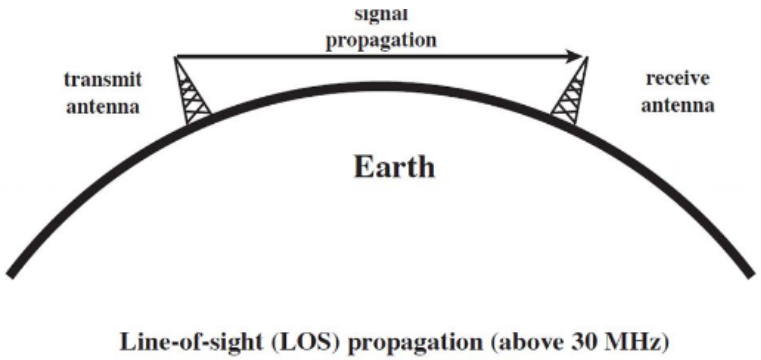


Figura 2-6 Transmisión en línea de vista (Fuente: IN3ECI. Italian Amateur Radio Station)

2.5.2 Horizonte radioeléctrico y alcance operativo real

Al modelarse la Tierra como una esfera de radio *R* y situar una antena a una altura *h*, solo se podrá establecer un enlace directo hasta el punto en el que la línea que une la antena y la superficie es tangente a la misma. De esta forma, la distancia al horizonte puede aproximarse mediante (1):

$$d = \sqrt{2Rh} \tag{1}$$

Se debe tener en cuenta, además, que existe un efecto de refracción troposférica que se introduce mediante un factor *k*, que en condiciones atmosféricas estándar se adopta habitualmente un valor de *k*=4/3, lo que conduce al concepto de radio terrestre efectivo (2) [25]:

$$R_{ef} = k \cdot R \tag{2}$$

Para enlazar de manera efectiva dos antenas se deberá tener en cuenta que ambas tendrán su propio horizonte radioeléctrico. La distancia máxima a la que se podrán conectar tanto transmisora como receptora dependerá de la altura a la que se encuentren; a mayor altura, mayor distancia de enlace. Teniendo en cuenta el radio terrestre efectivo mencionado previamente y suponiendo condiciones atmosféricas normales, el alcance máximo se puede aproximar mediante (3):

$$d_{km} \approx 3{,}57(\sqrt{h_1} + \sqrt{h_2}) \tag{3}$$

Estas expresiones evidencian que el alcance práctico del AIS en enlaces buque-buque o buque-costa es la suma de ambos horizontes radioeléctricos. En consecuencia, pequeñas variaciones en la altura de la instalación de la antena pueden producir diferencias significativas de cobertura. Es por ello por lo que se debe buscar que la instalación de las antenas, tanto de buques como estaciones costeras, tenga lugar en los puntos más elevados posibles [25].

Desde el punto de vista del presente trabajo, esto implica que: cualquier *jammer* situado en una posición elevada puede ampliar su radio de influencia, una estación costera situada correctamente puede extender su capacidad de monitorización y una degradación del sistema puede deberse a una limitación geométrica por una pérdida de LoS. Por tanto, la propagación VHF no es solo un aspecto teórico sino un factor estructural que condiciona la disponibilidad real del AIS en escenarios operativos.

2.5.3 Multitrayecto, reflexiones y pérdida de mensajes AIS

La propagación en el entorno marítimo introduce fenómenos como el multitrayecto, aparte del alcance geométrico, debido a reflexiones en la superficie del mar. Una señal recibida puede estar compuesta por la componente directa y una o varias reflejadas con diferencia de fase. En determinadas condiciones, se pueden generar desvanecimientos de la señal si las componentes interfieren constructiva o destructivamente.

Estos desvanecimientos son típicos en sistemas de voz VHF en los que se produce la pérdida temporal de calidad de audio. Sin embargo, en el caso del AIS, una variación brusca de amplitud puede provocar la pérdida del mensaje [6]. Este aspecto adquiere especial relevancia en escenarios de alta densidad de tráfico, donde la combinación de multitrayecto con la congestión de *slots* TDMA puede incrementar la tasa de pérdida de mensajes.

Todo ello puede dificultar la distinción entre una degradación natural del canal, una saturación estructural del sistema, o una interferencia intencionada. Se introduce así un problema adicional ya que la frontera entre fallo técnico y ataque deliberado no siempre es evidente si no se dispone de mecanismos de monitorización adecuados [2, 8].

2.5.4 Implicaciones de las limitaciones físicas en escenarios de interferencia

Un emisor con mayor potencia que el AIS dentro de su horizonte radioeléctrico puede desensibilizar o saturar un receptor [24] con relativa facilidad como se menciona en 2.4.1. La eficacia de un ataque de *jamming* no depende necesariamente de la potencia absoluta empleada, sino de la posición relativa respecto al blanco y de la geometría del enlace.

Al depender estrictamente de la LoS, la ocultación tras obstáculos naturales o artificiales puede generar lo que se conoce como zonas de sombra. Además, la colocación de repetidores mal protegidos para transmisiones en áreas donde la cobertura AIS es intermitente debido a la topografía puede ampliar involuntariamente el alcance de una señal interferente.

2.6 El AIS en el entorno naval: exposición táctica y resiliencia

2.6.1 Uso del AIS en operaciones de conocimiento del entorno marítimo

Uno de los cometidos principales de la Armada en el entorno estratégico actual es el conocimiento del entorno marítimo (MSA). El concepto trata de recopilar, fusionar y analizar de forma continua la información relativa al tráfico marítimo con el fin de identificar riesgos, amenazas o actividades ilícitas, reflejando así su compromiso con la Estrategia de Seguridad Marítima de la Unión Europea [26].

Operaciones como *Sea Guardian*, desarrollada en el marco de la OTAN y sucesora a la *Active Endeavour* cuyo origen se remonta a la activación del artículo 5 del Tratado de Washington tras los ataques del 11 de septiembre de 2001 contra las Torres Gemelas, tiene como objetivo reforzar el conocimiento del entorno marítimo en el Mediterráneo mediante vigilancia, recopilación de información y, si es necesario, abordaje de buques sospechosos [27].

En este contexto, el AIS constituye una fuente primaria de datos. Permite identificar unidades, verificar la coherencia entre la identidad declarada y comportamiento observado, y realizar lo que se conoce como "*hailings*" para contrastar la información compartida con la declarada por voz. Sin embargo, el empleo del AIS en operaciones navales se puede considerar un arma de doble filo, ya que

la misma herramienta que permite mejorar el conocimiento del entorno puede convertirse en un vector de exposición. Es por lo que las unidades militares están exentas de transmitir en AIS legalmente, para evitar una exposición de información operativa sensible, como se describe en el apartado 2.1.1.

2.6.2 Pattern of Life como herramienta operacional y vector OSINT

El concepto de patrón de vida (PoL) se basa en la identificación y modelado del comportamiento habitual de una unidad con el paso del tiempo, fijando aquellos movimientos que se pueden considerar normales en su comportamiento y, a partir de ahí detectar desviaciones significativas. Esta metodología la aplica la Armada y las diferentes Armadas internacionales en los marcos de operaciones MSA, donde un análisis continuado del tráfico permite conocer zonas de actividad recurrente y las rutinas operativas de diferentes buques.

En el entorno civil, el enfoque del PoL tiende más hacia un análisis de datos de tráfico con fines de seguridad, control y vigilancia. Mientras que desde un punto de vista doctrinal OTAN, el PoL es una herramienta habitual en la inteligencia operacional. El AIS es la principal fuente de datos para la construcción de patrones de comportamiento, debido a su uso obligatorio en buques sujetos al Convenio SOLAS. El patrón operativo habitual de cualquier barco se puede modelar fácilmente gracias a la disponibilidad continua de la información que está obligado a proporcionar.

Plataformas comerciales y de acceso público gratuito como *MarineTraffic* o *VesselFinder,* son herramientas al alcance de todos que permiten generar un PoL correcto y fiable. El enfoque de estas aplicaciones está orientado a la monitorización global con funcionalidades que permiten inferir patrones recurrentes de navegación, rutas habituales y ventanas temporales, elementos claves en la construcción de un PoL. Cabe destacar que estas herramientas no son sistemas de detección de anomalías, pero cuentan con procesos internos de depuración y validación de datos, con el filtrado de, por ejemplo, posiciones duplicadas.

Desde la perspectiva de la inteligencia de fuentes abiertas (OSINT), estas aplicaciones se convierten en vectores de alto valor al facilitar la explotación sistemática de datos marítimos sin necesidad de sensores propios. Se expone así, un doble escenario: por un lado, su uso como instrumento legítimo de vigilancia y seguridad; por otro, pueden ser empleados para el análisis de movimientos de enemigos, identificando los más típicos y aquellos puntos en los que son más vulnerables frente a un ataque.

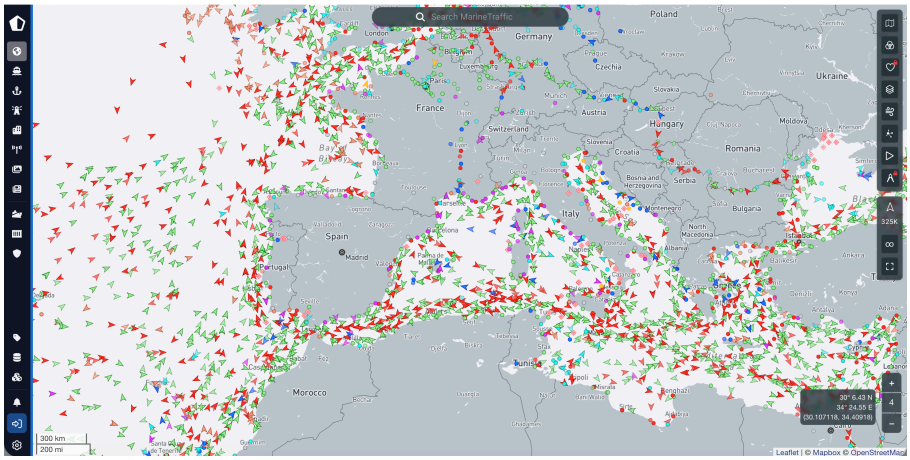


Figura 2-7 Buques en el Mar Mediterráneo (Fuente: Marine Traffic)

2.6.3 Exposición táctica del AIS no cifrado

Al concebirse el AIS como sistema de seguridad en la navegación se priorizó la interoperabilidad y la transparencia, dejando en un segundo plano la confidencialidad. La transmisión sin cifrado ni autenticación criptográfica resulta incompatible con las necesidades de una plataforma militar que debe cumplir unos requisitos operativos específicos para realizar sus cometidos en escenarios conflictivos.

Este diseño, plenamente coherente con un sistema cooperativo civil, resulta incompatible con las necesidades operativas de una plataforma militar en escenarios potencialmente conflictivos.

La información que muestra un AIS – posición, rumbo, velocidad, identidad y destino – supone una exposición táctica evidente. Cualquier actor con capacidad de recepción puede monitorizar los movimientos de una unidad, reconstruir sus trayectorias y analizar su PoL. En este contexto, incluso un pequeño error o transmisión prolongada puede suponer una detección y lo que ello conlleva: un seguimiento sistemático y análisis de patrones de la unidad.

Adicionalmente, al carecer de mecanismos de autenticación criptográfica, se habilitan vectores como los que se exponen en el apartado 2.2. Ante este escenario, en el que la transparencia estructural del sistema puede convertirse en una vulnerabilidad operativa, surge la necesidad de incorporar mecanismos técnicos que mitiguen dicha exposición.

2.6.4 Secure AIS y soluciones técnicas de mitigación

En la actualidad no existe un "AIS militar" estandarizado y universal. Sin embargo, ante las amenazas actuales y las vulnerabilidades evidentes con las que cuenta el sistema han surgido soluciones como el *Secure AIS*, orientado a introducir mecanismos de protección adicionales sobre la arquitectura básica del sistema. Por ello, el fabricante Saab Automobile AB lanzó al mercado el *Saab Secure AIS* que, por ejemplo, incorporará la Guardia Costera Helénica a sus unidades [28].

Estos sistemas incorporan medidas de cifrado, autenticación y control de acceso por medio de un conjunto de doctrinas operativas que usan de forma parcial la estructura AIS. En estos casos, plataformas autorizadas reducen la exposición pública de datos sensibles sin renunciar completamente a la funcionalidad del operativa del sistema. Por lo general, en estos sistemas se tiende a utilizar algoritmos criptográficos simétricos. Debido a que la información acerca de esta encriptación es clasificada, lo único que se conoce es que en el cifrado se utilizan claves centralizadas o distribuidas. De esta manera se impide que un receptor convencional sea capaz de decodificar el contenido y acceder a la información.

En el AIS civil, una de las debilidades más explotadas es la suplantación de identidad. Mediante la integración de la autenticación criptográfica del emisor se elimina la posibilidad de este tipo de *spoofing* directo, al permitir verificar que el mensaje proviene realmente de la unidad que dice ser. Bajo este esquema, incluso el MMSI pasa de ser un dato público a un método de identificación protegido.

El cifrado aporta confidencialidad y la autenticación aporta integridad. Ambas medidas reducen de manera significativa las vulnerabilidades descritas en el apartado 2.2, especialmente aquellos relacionados con suplantaciones de identidad. No obstante, sigue siendo necesario adoptar medidas doctrinales complementarias ya que la resiliencia del AIS en un entorno militar no depende exclusivamente del cifrado, sino de las decisiones operativas que se deben tomar sobre cuándo y en qué condiciones se deberá emitir.

Como materialización práctica del concepto de *Secure AIS*, diversos fabricantes han desarrollado soluciones orientadas específicamente al entorno naval. Entre ellos destaca el sistema R6 Supreme AIS/VDES de Saab AB [29] que integra capacidades de cifrado y autenticación compatibles con acuerdos de estandarización de la OTAN (STANAG) como la STANAG 4668. La STANAG 4668 se nombra en la ficha técnica del sistema, pero debido a su clasificación de seguridad, no está autorizado el acceso. Mantiene la compatibilidad con AIS y VDES estándar, pero restringe la interpretación del contenido transmitido a plataformas autorizadas, esencial en escenarios críticos. De esta manera, se conserva la funcionalidad operativa en redes seguras sin exponer públicamente la información sensible.

Desde el punto de vista técnico, supera en rendimiento a los estándares internacionales, alcanzando una sensibilidad en recepción superior a los -118 dBm, mejorando de manera significativa el rango de cobertura de la señal recibida. Los sistemas AIS convencionales tienen una sensibilidad en recepción de -107 dBm, con receptores de alta sensibilidad que alcanzan los -115 dBm, aún por debajo del R6.

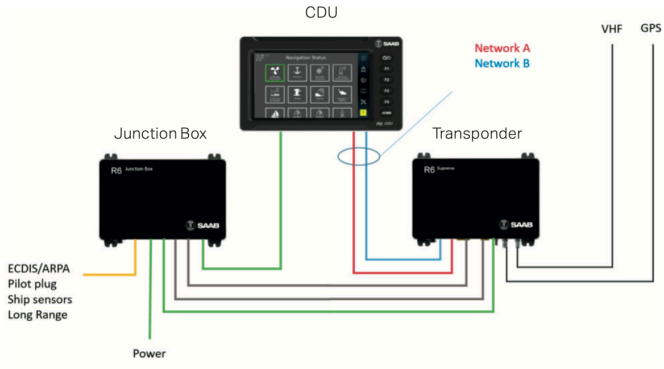


Figura 2-8 Conexiones SAAB R6 Supreme AIS/VDES (Fuente: [29])

Las Armadas que implementan este tipo de soluciones que combinan cifrado, autenticación y mejora de prestaciones radioeléctricas, mitigan riesgos de suplantación de identidad al reducir la obtención de inteligencia por fuentes abiertas, manteniendo al mismo tiempo un uso selectivo del AIS dentro de redes navales seguras, reduciendo la exposición táctica inherente al sistema.

2.6.5 Gestión de emisiones y doctrina EMCON

Más allá de las soluciones técnicas descritas en el apartado anterior, la complejidad de un entorno naval conflictivo hace que la resiliencia del AIS dependa también de decisiones doctrinales relacionadas con la gestión de emisiones. En el ámbito de la guerra electrónica, las emisiones electromagnéticas por parte de diferentes equipos y sistemas de una unidad constituyen un vector primario de detección y explotación. Conocer la banda en la que opera un determinado sistema permite la localización de aquellas unidades que lo integran en momentos de transmisión. En consecuencia, cualquier transmisión VHF, incluida la del AIS, puede ser empleada para detectar y monitorizar una unidad.

En escenarios de tensión estratégica o conflicto, se adoptan medidas de control de emisiones por medio de los planes de control de emisiones (EMCON), cuyo objetivo es reducir la probabilidad de detección. Se desconectan selectivamente sistemas no esenciales o se limitan determinadas transmisiones en función del grado de amenaza al cual la unidad se encuentre expuesta. En este contexto, el uso del AIS se puede limitar a entradas y salidas de puerto o activarse únicamente en escenarios de alta densidad de tráfico donde la seguridad en la navegación lo requiera.

La conciencia situacional del entorno no se pierde al reducirse las emisiones. De hecho, en estos casos se ampara en enlaces de datos militares cifrados que se integran en el sistema de combate del buque, compartiendo información en redes seguras sin exposición pública. De este modo, la gestión de emisiones se convierte en una medida doctrinal complementaria al *Secure AIS*. Tanto la mitigación de vulnerabilidades técnicas por parte del cifrado, como la reducción de la exposición radioeléctrica por la del plan EMCON, forman parte de un enfoque integral de la resiliencia frente a amenazas tanto técnicas como operativas.

2.6.6 El uso del AIS en CEVACO

En las unidades de la Armada es habitual el empleo del AIS para la realización de seguimientos de unidades, tal como se detalla en el apartado 2.6.1. Sin embargo, dada la relativa facilidad con la que se puede interferir con un sistema AIS, no se debe considerar como una herramienta principal de información, sino como un complemento al resto de sistemas. Las unidades militares disponen de diversas fuentes de información y de seguimiento de objetivos, por lo que es fundamental que estas trabajen en conjunto para comparar y contrastar los datos obtenidos.

El Centro de Valoración y Apoyo a la Calificación Operativa para el Combate (CEVACO), en colaboración con el Centro de Operaciones y Vigilancia de Acción Marítima (COVAM), lleva a cabo

ejercicios que exigen a las unidades la elaboración de una imagen marítima común (RMP) completa y precisa de su entorno, utilizando todos los sistemas a su disposición, no únicamente el AIS. Los ejercicios mantienen una estrecha relación con el uso de sistemas AIS con el fin de mantener un alto nivel de adiestramiento de la dotación.

2.7 Casuística documentada de *spoofing* de AIS

2.7.1 Incidentes documentados y tendencias actuales

Los incidentes de manipulación deliberada de señales GNSS y mensajes AIS cada vez son más comunes, impactando de manera directa en la seguridad en la navegación y en la construcción de una imagen marítima fiable. Lejos de tratarse de escenarios hipotéticos, estos eventos han afectado a regiones estratégicas como el Mar Negro, el Estrecho de Ormuz, el puerto de Shanghái o el Mediterráneo oriental, mostradas en la Figura 2-9, donde unidades reales fueron desplazadas, duplicadas o agrupadas en patrones anómalos de forma virtual [30].



Figura 2-9 Hotspots de interferencias GNSS y AIS

La suplantación de identidad, generación de trayectorias ficticias, manipulación de ayudas a la navegación virtuales y la creación masiva de objetivos falsos con el objetivo de saturar el enlace VHF, son algunos de los tipos de ataque que se han documentado [16]. En algunos casos, los buques afectados aparecieron miles de millas alejados de su posición real, mientras que en otros se generaron patrones circulares o nubes de objetivos artificiales, degradando la conciencia situacional marítima.

La tendencia de estos ataques de *spoofing* no se limita al encubrimiento de actividades ilícitas, sino que también se puede vincular a ejercicios de guerra electrónica o a contextos geopolíticos sensibles. La explotación de la naturaleza abierta del AIS y la ausencia de mecanismos de cifrado y autenticación son el elemento común en todos los casos.

En el contexto de tensiones recientes en Oriente Medio [31, 32], se han reportado perturbaciones en sistemas de navegación en el Golfo Pérsico y Estrecho de Ormuz. Estas interferencias posiblemente deliberadas han provocado anomalías tanto en sistemas GNSS como en trazas AIS, incluyendo posiciones erróneas, incluso en tierra firme. Esto sugiere que el empleo de capacidades de guerra electrónica (EW) afectan directa e indirectamente a los sistemas civiles de navegación [30]. Este tipo de incidentes pone de manifiesto la vulnerabilidad actual de los sistemas GNSS y AIS en entornos de conflicto.

2.7.2 Caso de estudio: evento de spoofing en la Isla de Elba (2019)

Uno de los incidentes mejor documentados de manipulación deliberada del AIS tuvo lugar en diciembre de 2019 entre la isla de Elba y Córcega [16]. Durante el evento se detectó una generación masiva de contactos AIS ficticios que aparecieron de forma repentina en las estaciones base de la zona. En total, se registraron 5.241 mensajes AIS que correspondían con 3.741 barcos inexistentes, generados en un área de 11 millas de radio.

El ataque se desarrolló en tres fases diferenciadas, caracterizadas por diferentes volúmenes y tipos de mensajes transmitidos. En la primera se recibieron 2.380 mensajes AIS tipo 1; en la segunda se produjo el mayor volumen de tráfico registrado, con 2.845 mensajes AIS tipo 1 y tipo 5; y finalmente, en la tercera se registraron solo 7 mensajes AIS tipo 1, cerrando el evento. Un aspecto llamativo en el segundo ataque fue la presencia de mensajes tipo 5. Al analizar los datos transmitidos, muchas de las embarcaciones se identificaban como buques de pasaje de 90 metros de eslora sin destino declarado, una característica inusual que facilitaba la identificación de la anomalía. También se detectaron identidades sospechosas, como un MMSI inválido que habitualmente se asocia a unidades militares y otro perteneciente a un buque que había sido desguazado tres años antes. Entre las trazas falsas se identificó un supuesto pesquero que transmitía datos estáticos coherentes, pero navegaba a 40 nudos, situándose directamente en la trayectoria del m/v Credemed, un buque real que se encontraba navegando por las aguas descritas en el momento del ataque. Este tipo de inconsistencias evidenciaba la naturaleza artificial de las señales y el potencial impacto en la toma de decisiones en el puente.

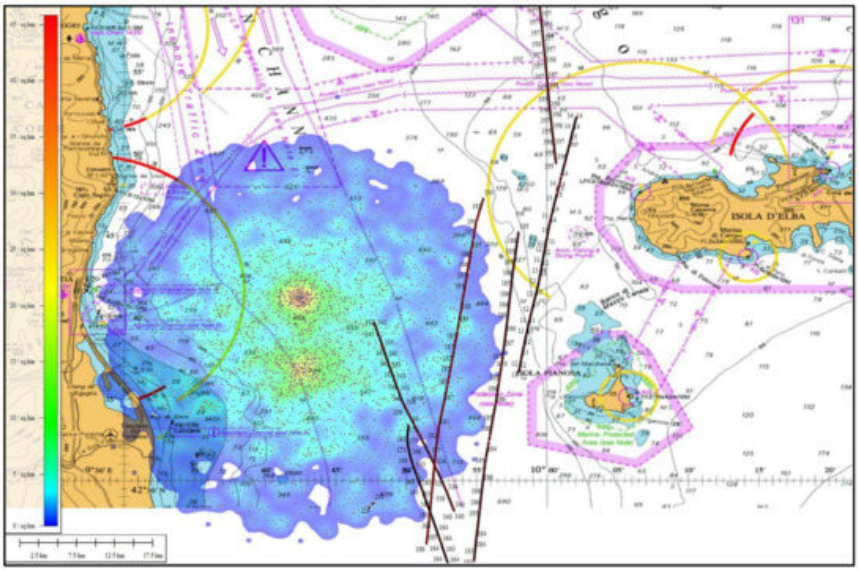


Figura 2-10 AIS *Spoofing* en la isla de Elba, 2019 (Fuente: [16])

El análisis posterior del incidente se realizó utilizando los datos registrados por la estación terrestre situada en Monte Capanne. Los investigadores descubrieron que, durante el ataque, siete barcos reales se vieron envueltos por la nube masiva de trazas generada, lo que permitía evaluar cómo se habría representado la situación en los sistemas de navegación de los presentes en la zona. Para ello, se recreó un escenario en el que se simulaba lo vivido en el puente del m/v Eliana Marino en el momento exacto del ataque. Los resultados obtenidos mostraron que la aparición de miles de contactos AIS provocó una degradación significativa de la imagen marítima mostrada en sistemas ECDIS y VTS, generando múltiples alarmas de CPA y posibles escenarios ficticios de colisión. Al analizar la potencia de la señal, detectaron variaciones que sugieren que la transmisión de las señales falsas pudo haberse realizado desde una plataforma móvil.

Los investigadores concluyeron que el principal riesgo de estos ataques no era únicamente la saturación del enlace AIS, sino la sobrecarga que producen las alarmas continuas en el oficial de guardia,

desviando su atención hacia amenazas ficticias mientras podrían desarrollarse situaciones de riesgo reales en el entorno de navegación.

2.7.3 Evaluación institucional y marco estratégico – Informe RIN 2026

Más allá de los casos concretos estudiados, la vulnerabilidad estructural del AIS dentro del ecosistema de posición, navegación y tiempo (PNT) ha estado en el punto de mira de diversos informes institucionales. El informe RIN 2026 del Royal Institute of Navigation [33] señala que la creciente dependencia de GNSS y sistemas digitales interconectados han ampliado significativamente la superficie de ataque en el ámbito marítimo.

El informe dedica su Anexo A específicamente a las interferencias del AIS. Destaca que la ausencia de mecanismos criptográficos de autenticación e integridad convierte al sistema en un vector susceptible tanto a manipulación como a interferencias accidentales. La confianza del navegante en los sistemas integrados de navegación se ve erosionada por la degradación del posicionamiento y la inyección de información falsa. Por ello, se enfatiza la necesidad de adoptar marcos de resiliencia que combinen mejoras técnicas, validación cruzada multisensor y pruebas sistemáticas frente a escenarios de interferencia y *spoofing*. Se refuerza así la idea de que la vulnerabilidad a la que se ve expuesta el AIS no debe considerarse como un simple problema aislado, sino como parte crítica en la seguridad en la navegación.

2.7.4 Estrategias de detección y mitigación

Los incidentes documentados y los análisis técnicos convergen en la idea de que la manipulación de señales GNSS y AIS son una amenaza real para la seguridad en la navegación y para la fiabilidad de los sistemas de vigilancia marítima. Diferentes organismos han propuesto una serie de estrategias destinadas a mejorar la resiliencia del sistema PNT frente a interferencias, ataques de *spoofing* y manipulación de datos AIS. Las medidas presentadas combinan la detección de inconsistencias con la reducción de la dependencia de una única fuente de posicionamiento.

Una de las recomendaciones con mayor fuerza es la de reforzar la verificación de la información mediante la integración de sensores independientes. Sistemas como el radar permiten contrastar la información proveniente del AIS y GNSS, manteniendo en todo momento una RMP clara. El uso combinado de diferentes fuentes permite detectar discrepancias, algo especialmente relevante en escenarios de *jamming* o *spoofing*.

Otra propuesta es la implementación de sistemas que monitoricen el espectro y que sean capaces de detectar interferencias en los sistemas de posicionamiento y navegación. Esto permitiría advertir a buques de la presencia de anomalías antes de entrar en zonas potencialmente afectadas. Además, se contempla la mejora de la robustez de los receptores con la implementación de algoritmos de detección de *spoofing* y la utilización de antenas especializadas capaces de mitigar interferencias. De esta manera, se reduce la probabilidad de que un receptor sea engañado por señales falsas o interferencias de alta potencia. En conjunto, estas estrategias, entre otras reflejadas en [33], reflejan una tendencia creciente hacia arquitecturas de sistemas de navegación más resilientes, en las que la información tanto AIS como GNSS se validan mediante diversas fuentes independientes.

En este contexto, [33] incluye resultados de una encuesta realizada a 271 profesionales, con el objetivo de analizar cómo se veían afectados los sistemas de navegación de los buques en eventos de interferencias. Un 79% de los participantes afirmaron haber experimentado en algún momento interferencias GNSS o *spoofing* durante sus operaciones. A partir de estas respuestas se analizó, entre otros aspectos, el comportamiento del AIS al abandonar zonas de interferencia como se muestra en la Figura 2-11. Las opciones de voto incluían que el sistema se recuperaba automáticamente; que era necesario un reinicio manual, reajuste o restablecimiento de ajustes; un ciclo completo de encendido; un reemplazo de software o firmware; o que ha sido dañado físicamente y reemplazado.

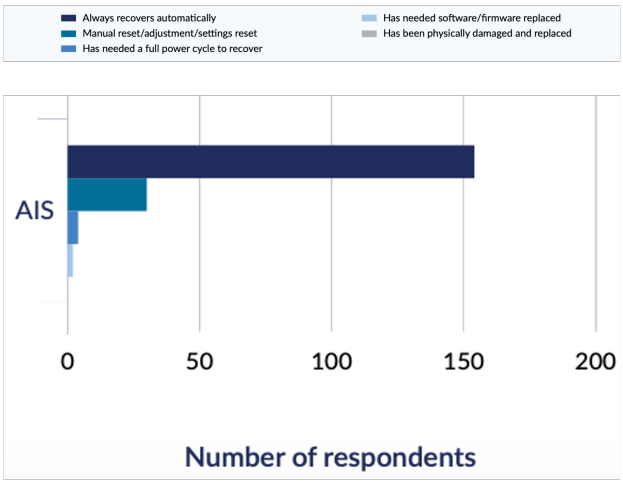


Figura 2-11 Recuperación del AIS tras un episodio de interferencias (Fuente: [33])

Los resultados muestran que el sistema puede requerir reinicios o ajustes manuales para recuperar su funcionamiento normal. En algunos casos, los encuestados indicaron que estos equipos no se reestablecen automáticamente. El comportamiento refleja la posibilidad de que los efectos de un ataque o interferencia persistan incluso después de abandonar una zona afectada por interferencias.

3 DESARROLLO DEL TFG

En el presente capítulo se detalla el diseño, implementación e integración del banco de pruebas creado para medir la resiliencia de los receptores AIS. En primer lugar, se describen los elementos de hardware y herramientas de software utilizados para la realización de las pruebas. Se describe el código utilizado para la generación de mensajes AIS tipo 1, 5 y 21. La validación de los ataques se realiza en un entorno controlado en los laboratorios del CUD-ENM. Por último, se pasa del entorno experimental al operativo con la elaboración de un protocolo de pruebas sistemático. Este protocolo evalúa el receptor de un barco permitiendo determinar el grado de resiliencia frente a perturbaciones.

3.1 Caracterización del escenario real

Para que el estudio sea efectivo, las pruebas de inyección de trazas requieren de un escenario en el que exista una continua presencia de buques de distinto tipo.

3.1.1 Ría de Pontevedra

La Ría de Pontevedra, situada en las Rías Baixas, destaca por su alta actividad náutica y comercial. Cuenta con el puerto de Marín, un puerto de alto interés comercial con un volumen masivo de tráfico de mercancías y una importante flota pesquera. Las ensenadas interiores albergan una alta actividad de embarcaciones menores e incluso militares, pertenecientes a la Escuela Naval Militar. La diversidad de unidades que navegan a diario por la ría proporciona un entorno de pruebas real.

3.1.2 Caracterización estadística del tráfico AIS

Para dotar los ataques de un contexto realista se monitorizó la actividad del sistema AIS en el entorno de la ENM gracias al receptor SDR descrito en el apartado 3.2.4. La escucha tuvo lugar desde las 07:45 horas hasta las 16:45 horas del día 13 de febrero de 2026 en la Ría de Pontevedra. En el intervalo mencionado se monitorizó el espectro obteniendo un total de 4.681 mensajes AIS. La Tabla 3-1 muestra el resumen de la fase de escucha descrita:

Tipo de Mensaje	Descripción	N.º de Mensajes	% del Tráfico
Tipo 1	Reporte de posición (Clase A)	2.584	55,2%
Tipo 3	Reporte de posición especial	48	1,0%
Tipo 4	Estación base (MMSI 2242120)	1.956	41,8%
Tipo 5	Datos estáticos y de viaje	32	0,7%
Tipo 11	Respuesta interrogación UTC	12	0,3%
Tipo 18	Reporte de posición (Clase B)	42	0,9%
Tipo 21	Ayudas a la navegación (AtoN)	5	0,1%
Otros	Mensajes de gestión de errores	2	< 0,1%
TOTAL		4.681	100%

Tabla 3-1 Mensajes AIS captados en 9 horas de escucha pasiva en la Ría de Pontevedra

Al analizar los datos se muestra un escenario dominado por dos fuentes principales: reportes de posición de clase A y las transmisiones de una estación base. Llama la atención la alta cantidad de mensajes de tipo 4 recibidos vinculados al MMSI 002242120. Tras consultar los datos en el sistema Maritime mobile Access and Retrieval System (MARS) de la ITU [34] se confirma que se trata de una estación base del Área de Radiocomunicaciones de la Dirección de Marina Mercante perteneciente al Ministerio de Fomento en el puerto de Marín en posición 42°24'01.6"N 8°41'25.2"W.

3.1.3 Justificación de los vectores de ataque

Con más de un 55% del tráfico total de mensajes recibidos en el periodo estudiado, el reporte de posición Clase A es el vector más crítico. También se aprecia la recepción de mensajes de tipo 5 y tipo 21, en menor cantidad, pero no por ello menos importantes. Al buscar la saturación del receptor mediante la inyección de trazas falsas, supone una ventaja al tener un abanico más amplio de ataques posibles.

3.2 Descripción del equipamiento hardware

3.2.1 Receptor QK-A026

Para la validación del código utilizado descrito en el Anexo V, se utiliza el receptor QK-A026 [35] propiedad del CUD-ENM. El equipo es capaz de monitorizar simultáneamente los dos canales AIS, trabajando entre las frecuencias 161,975 MHz y 162,025 MHz, permitiendo la decodificación continua de los mensajes recibidos sin necesidad de conmutación de frecuencia.

Presenta una sensibilidad aproximada de -105 dBm, además de incorporar un receptor GNSS interno que proporciona información de posicionamiento al conectarse a una antena GPS externa. Su característica más relevante es la capacidad de gestionar tres flujos de datos distintos: datos AIS, datos GPS y una entrada NMEA externa.

El dispositivo permite la salida de los mensajes AIS a través de USB, NMEA 0183 o WiFi, lo que facilita su integración con ordenadores o software de visualización como OpenCPN. En el presente trabajo, el receptor se emplea inicialmente para registrar y analizar el tráfico inyectado durante la realización de las pruebas de interferencia o manipulación de señal.

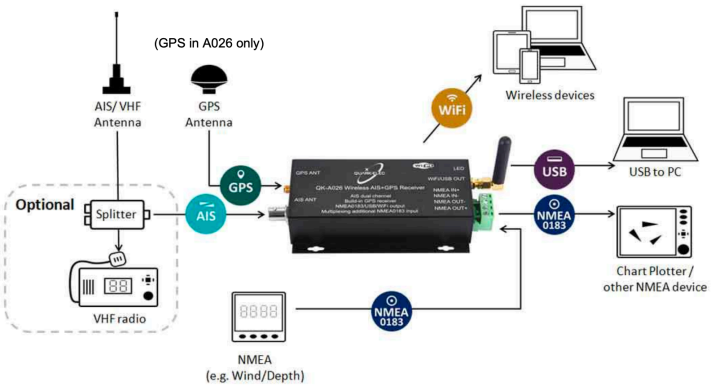


Figura 3-1 Conexiones QK-A026 (Fuente: [35])

3.2.2 Transpondedor SIMRAD V5035

La primera serie de las lanchas de instrucción de la Escuela Naval – GM Barrutia, GM Chereguini, GM Rull y GM Salas – incorporan un transpondedor SIMRAD V5035 [36], utilizado en este TFG para darle realismo a los ataques de *spoofing* y *jamming* al aplicarse el protocolo propuesto.

El dispositivo está diseñado para cumplir con los estándares internacionales aplicables, integrando en una única unidad el transceptor VHF AIS, un receptor GNSS y un módulo de control. Opera entre las frecuencias 156,025 MHz y 162,025 MHz, utilizando modulación GMSK con una velocidad de transmisión de 9.600 bps. El hecho de que el rango inicie en 156,025 MHz y no en 161,975 MHz se debe a que el equipo está diseñado para cubrir las frecuencias descritas en la Tabla 2-2.

La sensibilidad de recepción del equipo es inferior a -107dBm, permitiendo detectar señales AIS de baja potencia. Esto resulta especialmente relevante en el contexto del presente trabajo, ya que es capaz de detectar señales en presencia de interferencias, constituyendo un factor clave en el análisis de resiliencia frente a *jamming*.

La incorporación de un receptor GNSS interno proporciona la información necesaria para la generación de mensajes dinámicos y para la sincronización del acceso al canal mediante el esquema TDMA. Dispone, además, de diferentes interfaces que permiten su integración con otros sensores y sistemas de navegación. Estas interfaces facilitan la extracción y registro de los mensajes AIS recibidos, permitiendo su posterior análisis durante las pruebas experimentales descritas en el Capítulo 4.



Figura 3-2 Transpondedor SIMRAD V5035 de la primera serie de LLII de la ENM

3.2.3 Transpondedor FURUNO FA-170

La segunda serie de las lanchas de instrucción de la Escuela Naval – GM Godínez y GM Herrero – incorporan un transpondedor Furuno FA-170 [37], utilizado en este TFG para aplicar el protocolo propuesto y poder comparar los resultados obtenidos con aquellos de los otros estudiados.

El equipo opera entre las frecuencias 156,025 MHz y 162,025 MHz. El hecho de que el rango inicie en 156,025 MHz y no en 161,975 MHz se debe a que el equipo está diseñado para cubrir las frecuencias descritas en la Tabla 2-2. La arquitectura del sistema incluye un receptor GNSS interno que proporciona posición y referencia temporal UTC para la sincronización con el sistema AIS.

Dispone de múltiples interfaces de comunicación que permiten su integración con sistemas externos que facilitan tanto la visualización de datos como su registro. Esta capacidad resulta relevante en el contexto del presente TFG ya que permite monitorizar el comportamiento del receptor frente a los diferentes escenarios de carga o interferencia. El fabricante no especifica la sensibilidad de recepción pero, según los requisitos establecidos por la ITU, el valor se debe encontrar en torno a los -107 dBm. Esto garantiza la detección de señales de baja potencia.

Además, incorpora dos receptores TDMA en paralelo junto con un transmisor VHF, lo cual permite gestionar simultáneamente la recepción y emisión de mensajes dentro del esquema de acceso al canal. Su funcionamiento interno respeta la recomendación de la ITU utilizando una velocidad de transmisión de 9.600 bps.



Figura 3-3 Interfaz del transpondedor FURUNO FA-170

3.2.4 Dispositivos SDR

Para la validación del protocolo de pruebas propuesto mediante los experimentos descritos en este trabajo, se emplean dispositivos SDR. Estos equipos permiten recibir y transmitir señales personalizadas de radiofrecuencia, posibilitando la reproducción de diferentes escenarios. En el contexto del trabajo, los SDR se utilizan tanto para caracterizar el entorno de tráfico AIS existente en la zona de estudio como para generar señales AIS controladas durante las pruebas experimentales.

Como primer elemento del sistema experimental se utiliza un receptor RTL-SDR, que conectado mediante USB al ordenador permite digitalizar señales de radiofrecuencia y procesarlas posteriormente. Tiene un rango de recepción aproximado de 500 kHz a 1,7 GHz [38], cubriendo con facilidad las frecuencias AIS. Se emplea exclusivamente como receptor pasivo, con el objetivo de realizar un análisis estadístico del tráfico AIS en la Ría de Pontevedra. Mediante la captura continua de mensajes AIS se obtiene información sobre la densidad del tráfico y, especialmente, sobre los tipos de mensajes transmitidos más comunes como se muestra en la Tabla 3-1. Esta caracterización descrita en el apartado 3.1.2, resulta fundamental para comprender las condiciones existentes y establecer una base de referencia para justificar los ataques.



Figura 3-4 Unidad de recepción RTL-SDR

El segundo dispositivo utilizado es el ADALM-PLUTO. A diferencia del RTL-SDR, este equipo funciona como transceptor, permitiendo tanto la recepción como la transmisión de señales de radiofrecuencia [39]. Al igual que el RTL-SDR, se conecta al ordenador mediante USB y puede controlarse desde diferentes entornos software, en este caso GNU Radio. En el contexto de este trabajo, se emplea como generador de señales AIS artificiales, dándole el uso exclusivo de transmisor. Para ello se ejecutan los *scripts* de Python descritos en el Anexo V, los cuales son posteriormente modulados y transmitidos mediante GNU-Radio a través del ADALM-PLUTO.



Figura 3-5 Unidad de transmisión ADALM-PLUTO

Esta capacidad resulta especialmente útil para reproducir comportamientos anómalos en el canal AIS, como la generación masiva de mensajes o la transmisión de identidades o posiciones manipuladas. Por medio de este equipo, los diferentes escenarios se pueden implementar de forma controlada y repetible, permitiendo así analizar la respuesta del receptor y estudiar la resiliencia del sistema frente a los ataques descritos.

3.2.5 Splitter ZX-10-2-20-S+

Para la combinación de señales en las pruebas que requieren superposición de tráfico real y señales generadas artificialmente se emplea el divisor de potencia RF de Mini-Circuits que se muestra en la Figura 3-6. Es un dispositivo pasivo que cuenta con dos vías de entrada y una de salida que operan en el rango de 0,2 a 20 GHz [40]. Esto permite introducir de manera simultánea la señal AIS captada por la antena VHF y la generada por el ADALM-PLUTO, sumándose en el dispositivo e inyectándose directamente a la entrada de antena del receptor. Se trata de un elemento pasivo, por lo que no introduce retardo ni procesamiento sobre la señal. Bien es cierto que puede presentar pérdidas y un aislamiento limitado, por lo que señales de mayor potencia pueden dominar sobre las más débiles.



Figura 3-6 Divisor de potencia RF ZX-10-2-20-S+

3.2.6 HYS Antena Marina VHF

Para llevar a cabo la validación de las pruebas que requieren una señal externa se emplea la HYS Antena Marina VHF. Se trata de una antena VHF marina omnidireccional compatible con sistemas AIS. No existe una ficha técnica de características pública del fabricante pues se comercializa en Amazon, por lo tanto las especificaciones se toman como aproximaciones basadas en la descripción del artículo.

Es una antena de tipo vertical con polarización lineal con una impedancia de 50 Ohmios. Trabaja en un rango de frecuencias de 156 a 164 MHz y posee una ganancia de 2 dBi. El cable de conexión mide 5 metros y cuenta con un conector SO-239.



Figura 3-7 HYS Antena Marina VHF

3.3 Entorno de software y visualización

Para gestionar el flujo de información, el hardware mencionado en 3.2.3 se integra con las siguientes herramientas de software:

3.3.1 AIS-Catcher

En la fase de escucha descrita en 3.1.2 se emplea el software AIS-catcher. Mediante la captura continua de mensajes AIS, permite obtener una visión general del tráfico existente en la zona de estudio, logrando un análisis de la densidad de transmisiones. El programa recibe, analiza y decodifica, aplicando algoritmos de modulación GMSK, las ondas radio captadas por el RTL-SDR. La Figura 3-8 muestra los diferentes barcos y AtoNs captados por el RTL-SDR el día 10 de febrero de 2026 a las 17:30 horas en la Ría de Pontevedra:

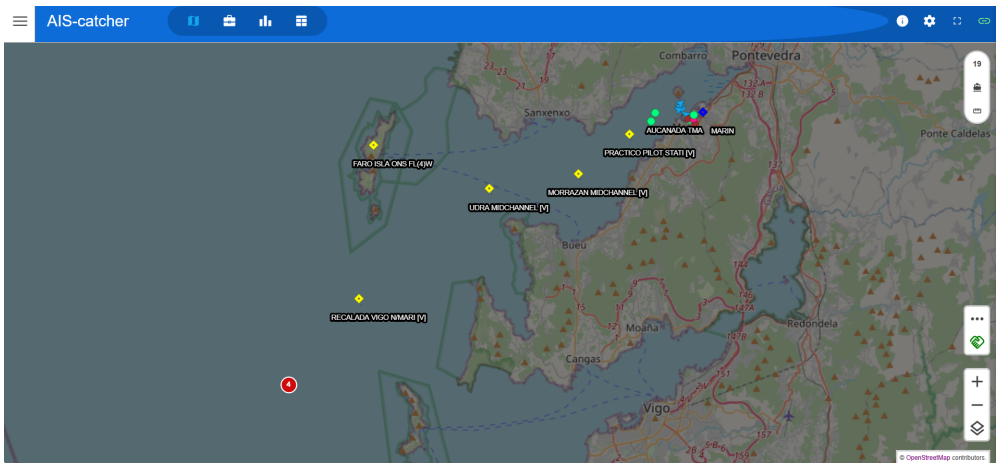


Figura 3-8 Interfaz AIS-catcher (Ría de Pontevedra, 10/02/2026)

3.3.2 OpenCPN

El OpenCPN actúa como interfaz final de visualización de barcos, AtoNs y otras señales, permitiendo ver en tiempo real el impacto de un ataque. Al recibir mensajes AIS decodificados, el software los representa automáticamente sobre la carta náutica, mostrando toda la información correspondiente al envío. En el contexto de este trabajo, se utiliza únicamente como herramienta de visualización. Los datos recibidos que se muestran en la Figura 3-8 se transmiten a la interfaz del OpenCPN para validar el funcionamiento de la aplicación, como se muestra en la Figura 3-9:

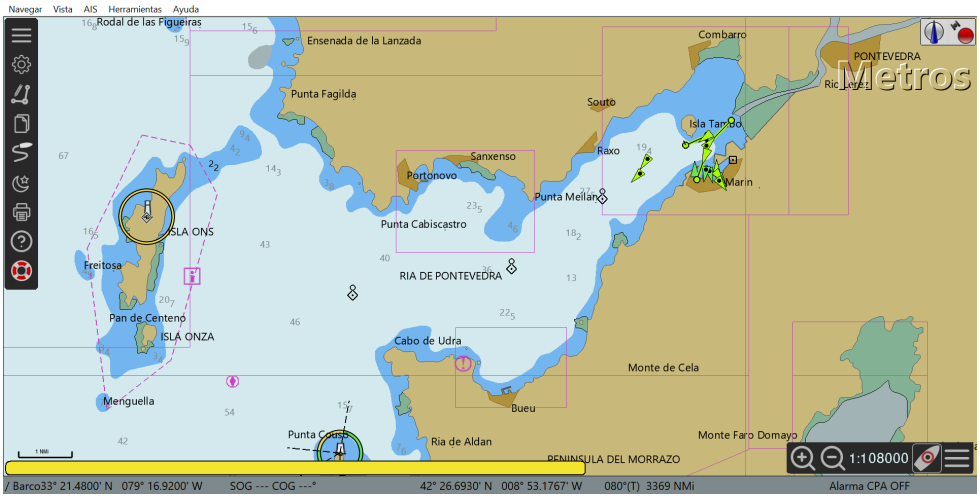


Figura 3-9 Interfaz OpenCPN (Ría de Pontevedra, 10/02/2026 1730)

3.3.3 Arquitectura de interconexión

Para implementar la fase de escucha descrita en el apartado 3.1.2, se utiliza un esquema sencillo, mostrado en la Figura 3-10, que se basa en tres componentes fundamentales. Por un lado, el receptor RTL-SDR, que en modo pasivo recoge los mensajes AIS y los envía por USB al software AIS-Catcher. Los datos procesados se monitorizan vía web por el puerto 8100 (Figura 3-8) y, a su vez, se vuelcan en la interfaz de OpenCPN mediante el puerto UDP 10110 (Figura 3-9). De esta manera se corrobora el correcto funcionamiento en la operatividad del sistema.

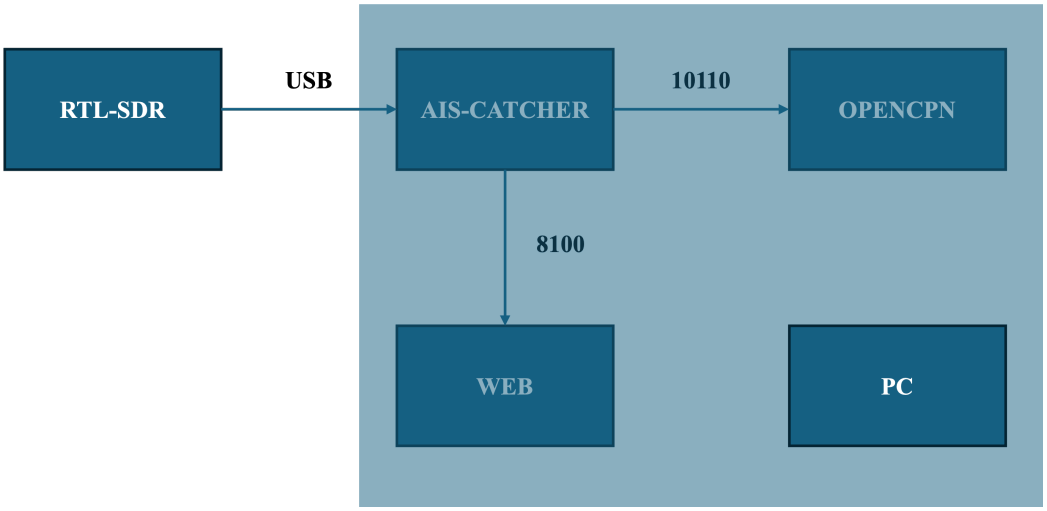


Figura 3-10 Arquitectura de conexión para la fase de escucha

Para validar el funcionamiento de los *scripts* de Python, se ha diseñado un sistema de interconexión que se muestra en la Figura 3-11 donde el código se enlaza con GNU-Radio a través del puerto UDP 52002. En este esquema, el ADALM-PLUTO actúa como emisor, recibiendo la señal vía USB y enviándola por RF hacia el receptor. Dicha señal viaja al receptor QK-A026, entrando por su toma de antena. Finalmente, los datos capturados por el receptor se envían por USB, vía puerto COM9, a la interfaz de OpenCPN para su visualización y análisis, confirmando así la operatividad y correcto funcionamiento de toda la cadena de transmisión, o en su defecto al *log* generado para leer las tramas recibidas que se describe en el Anexo V.

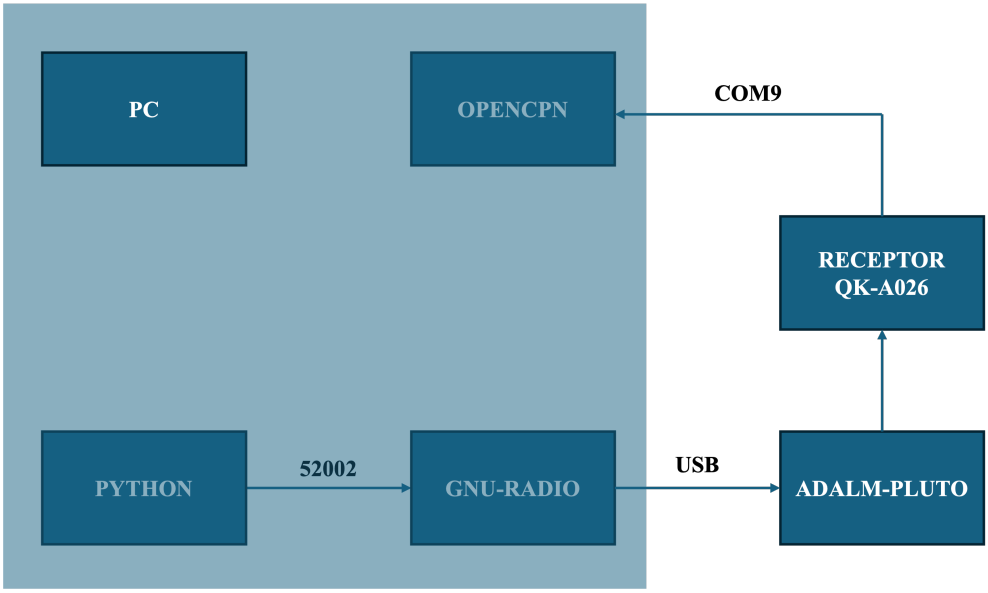


Figura 3-11 Estructura de conexión para validación *scripts*

Para realizar las pruebas de *spoofing* (PS1 y PS2), se aplica una estructura simple y completamente cerrada, de forma que todo el proceso de generación, modulación y recepción queda controlado y aislado de señales externas que puedan alterar los resultados. Lo que se busca con el montaje es que los resultados obtenidos dependan únicamente del comportamiento del sistema y del receptor, sin que puedan intervenir señales de tráfico real. La cadena de funcionamiento comienza en Python, ejecutándose el código encargado de generar los mensajes para cada prueba. Construidas las tramas, se envían a GNU-Radio a través del puerto 52002. GNU-Radio procesa dicha información y la entrega al ADALM-PLUTO que se encarga de transmitir la señal generada. La salida del ADALM-PLUTO se conecta directamente a la toma de antena del receptor o transpondedor, según corresponda. Así, se consigue que la señal siga un camino totalmente guiado y controlado, constituyendo un circuito cerrado. Este esquema permite reproducir de forma estable y repetible las condiciones de ensayo, haciendo posible una evaluación correcta y objetiva de los receptores a estudiar.

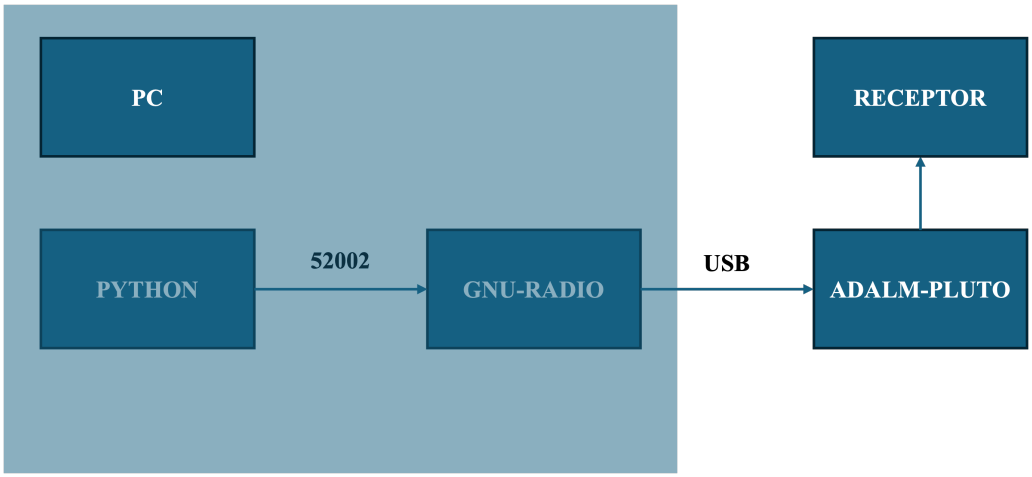


Figura 3-12 Arquitectura de conexión para pruebas de *spoofing* (PS1 y PS2)

Para llevar a cabo la última de las pruebas de *spoofing* (PS3), se desarrolla un montaje que combina señales AIS reales con las generadas artificialmente, permitiendo analizar el comportamiento del receptor frente a escenarios de suplantación o saturación controlada. Se parte de dos fuentes diferenciadas: por un lado la señal AIS real captada por una antena VHF y por otro la señal interferente generada mediante Python siguiendo el mismo ciclo mencionado previamente. Ambas señales se combinan mediante un splitter descrito en el apartado 3.2.5 que permite sumar las dos señales, de forma que el resultado es una señal compuesta que contiene tanto tráfico real como ficticio. La salida del splitter se conecta directamente a la entrada de antena del receptor, de modo que reciba simultáneamente ambas sin poder distinguir su origen físico. Permite evaluar como una señal artificial afecta a la recepción de tráfico real. Se introduce así el escenario más cercano a condiciones reales.

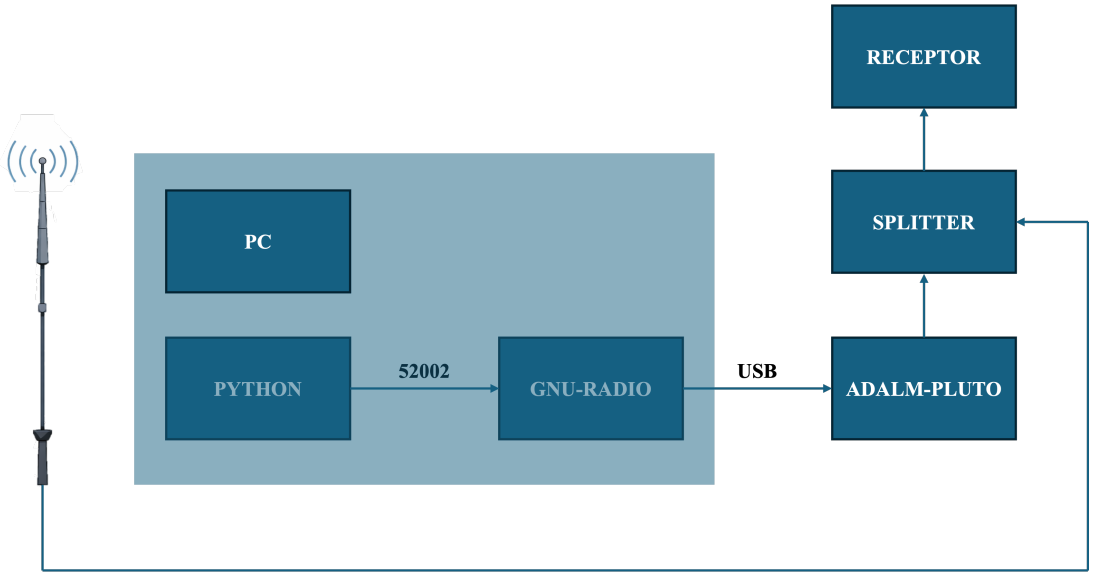


Figura 3-13 Arquitectura de conexión para pruebas de *spoofing* (PS3)

Para llevar a cabo las pruebas de *jamming* descritas en 3.8.3 (PJ1 y PJ2) se utiliza el montaje mostrado en Figura 3-14 que se basa en la superposición de una señal AIS real con una interferente. Una antena VHF recibe el tráfico AIS de la zona y, simultáneamente en el ordenador se ejecuta un flujo de generación de señal mediante GNU-Radio. La señal generada se envía al ADALM-PLUTO que se encarga de convertirla en una señal de radiofrecuencia. Ambas señales, tanto la real como la interferente, se introducen en un combinador RF en el que se mezclan para formar una única señal compuesta. Finalmente, la salida del combinador se conecta a la entrada del receptor AIS, recibiendo la señal final, lo que permite analizar su comportamiento frente a este tipo de escenarios.

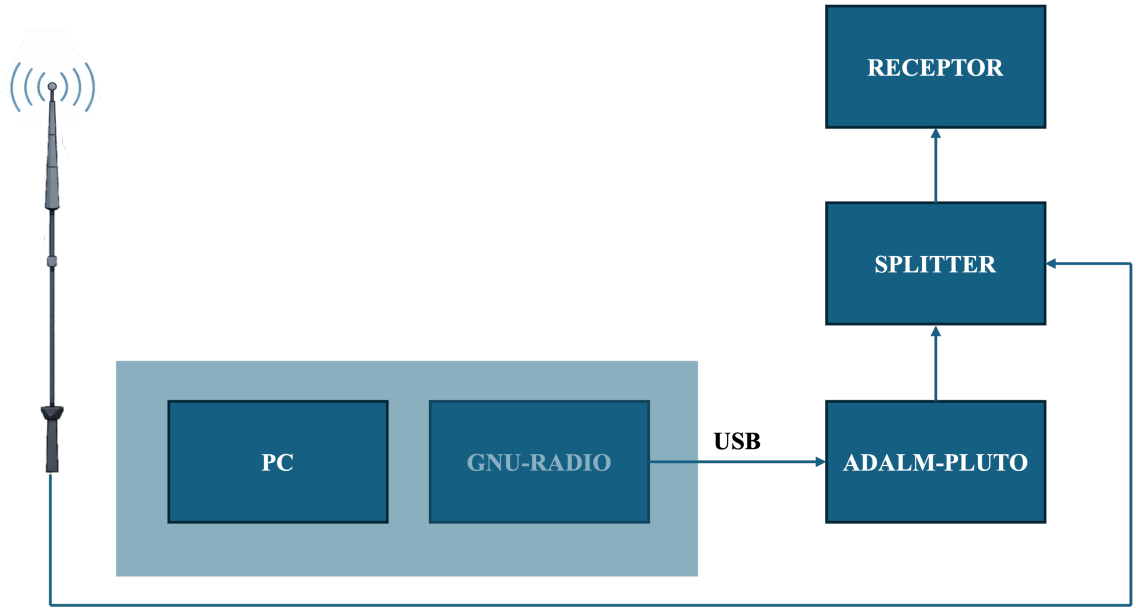


Figura 3-14 Arquitectura de conexión para pruebas de *jamming* (PJ1 y PJ2)

3.4 Implementación lógica de los ataques

Teniendo en cuenta los datos obtenidos en el apartado 3.1.2, se desarrolla un ecosistema en Python capaz de, siguiendo los estándares de la ITU, construir tramas AIS. El código se divide en dos librerías de funciones y tres *scripts* de ejecución de los diferentes escenarios en función del tipo de mensaje. Cabe destacar que el código no es de elaboración propia, sino que fue proporcionado al inicio del TFG. Bien es cierto que muchos aspectos del código proporcionado fueron modificados con ayuda de inteligencia

artificial con el fin de cumplir el objetivo de los ataques, como se describe en el apartado 3.7. La descripción detallada de cada uno de los *scripts* empleados se encuentra recogida en el Anexo V.

3.4.1 Lógica de construcción de tramas

La generación de una señal válida requiere que el software siga una estructura de procesado de datos específica. Se apoya en una serie de pilares que gestionan la integridad y empaquetado de la información, de tal forma que sistemas de recepción comerciales sean capaces de interpretar cada mensaje.

Para la detección de errores, la ITU exige el uso del CRC-16-CCITT. Mediante una fórmula matemática específica con unos valores de inicio, permite que el receptor compruebe si los datos han sufrido alguna alteración o manipulación durante la transmisión debido a interferencias o ruido. Aquellos mensajes que hayan sufrido alguna alteración los descarta de forma automática.

Adicionalmente, se emplea una secuencia de delimitación de trama (*flag*) que permite identificar el inicio y fin de cada mensaje. Con el fin de evitar ambigüedades cuando dicha secuencia aparece en el contenido, se aplica un proceso de *bit stuffing*, mediante el cual se introduce un "0" tras cada secuencia de cinco "1". Se garantiza así la transparencia del *payload* frente al canal y evita interpretaciones erróneas por parte del receptor.

3.4.2 Librería de funciones

La librería inicial proporcionada (Lib_AIS_App), permite generar estructuras de datos conforme al estándar. Sin embargo, durante el desarrollo del TFG se detectaron limitaciones en la codificación de ciertos campos, especialmente en mensajes de tipo 5, por lo que se desarrolló una versión capaz de corregir esas carencias (Lib_AIS_App_v2).

Esta evolución incorpora mejoras en el empaquetado de cadenas de texto y en la adaptación de los campos a sus longitudes binarias correspondientes, lo cual permite una generación de mensajes completamente compatible con los receptores utilizados.

3.4.3 Implementación de los escenarios de ataque

Los diferentes escenarios del protocolo se implementan mediante *scripts* independientes que hacen uso de las librerías de funciones según corresponda. Cada uno está orientado a la generación de un tipo de mensaje AIS concreto con objetivos experimentales específicos del protocolo descritos en el apartado 3.8.3:

- PPv1_PS1: genera múltiples blancos dinámicos con posición, rumbo y velocidad.
- PPv1_PS2: genera una combinación de mensajes dinámicos y estáticos, introduciendo carga adicional al incluir nombre, puerto de destino, ETA, etc.
- PPv1_PS3: genera una transmisión repetitiva de una AtoN, en la que se incluyen todos los datos relevantes acerca de la misma.

Cada *script* permite al usuario definir los parámetros con el fin de adaptar el escenario a las necesidades de la prueba. Todos los *scripts* generan la sentencia NMEA correspondiente a cada mensaje y el *payload* binario que se envía a GNU-Radio para su modulación y posterior transmisión mediante SDR.

3.5 Entorno de modulación y control

3.5.1 Spoofer

El *spoofer* se implementa en GNU-Radio a partir de un diseño base proporcionado, adaptado al entorno de pruebas. El esquema modula y transmite las tramas AIS generadas previamente con los *scripts* de Python. Para que la señal sea indistinguible de una real, se emplea una modulación GMSK con los parámetros propios del estándar AIS. De este modo, las tramas generadas presentan una capa física equivalente a la real.

Tras la modulación, se permite controlar la atenuación de la potencia de salida y la frecuencia de transmisión. Pese a la posibilidad de modificación, estos parámetros no se cambian durante el transcurso de las pruebas. Se establecen valores fijos al inicio.

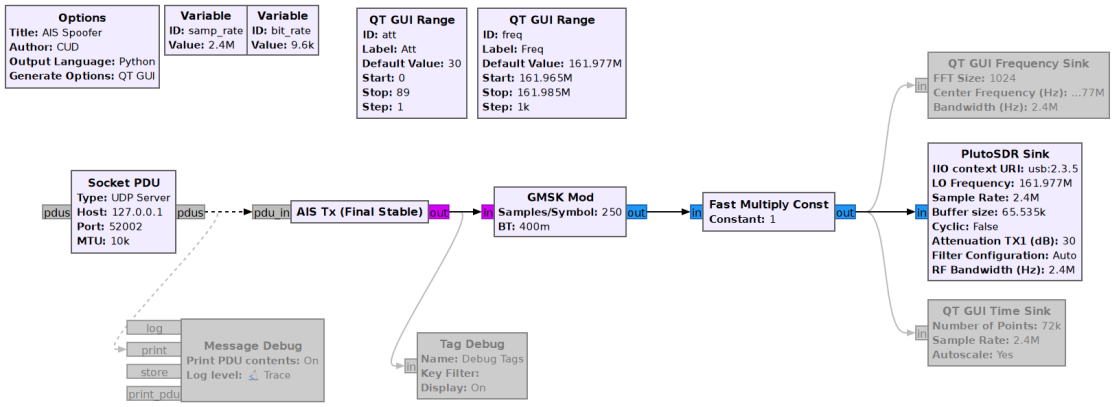


Figura 3-15 Bloques de procesamiento del *spoofer* en GNU-Radio

3.5.2 Jammer

El *jammer* empleado está implementado en GNU-Radio y genera una señal AWGN con un ancho de banda de 50 kHz que se inyecta a demanda del operador en cualquiera de los dos canales empleados o incluso en ambos a la vez. En este caso, se introduce ruido en ambos canales simultáneamente. El ADALM-PLUTO es el encargado de radiar la señal generada directamente sobre la entrada del receptor bajo prueba.

El sistema permite activar o desactivar la interferencia de forma controlada. El parámetro clave que se modifica durante la realización de las pruebas es la atenuación en transmisión. De esta forma, el montaje permite caracterizar de manera directa la sensibilidad del receptor frente a *jamming* sin necesidad de introducir configuraciones complejas.

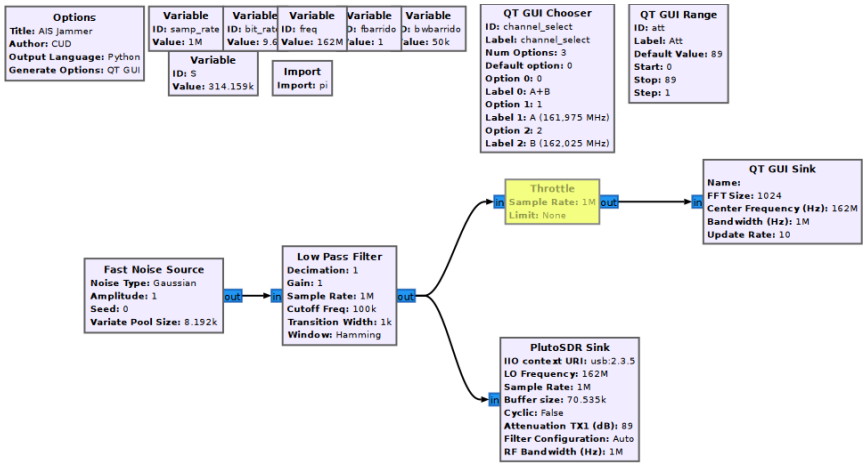


Figura 3-16 Bloques de procesamiento del *jammer* en GNU-Radio

3.6 Conexión del hardware a LLII

Con el fin de conectar el banco de pruebas a las Lanchas de Instrucción de la Escuela Naval Militar para ejecutar el protocolo de pruebas, se llevan a cabo pasos similares.

Para la conexión del banco de pruebas al receptor SIMRAD V5035 instalado en la 1ª serie de Lanchas de Instrucción de la Escuela Naval Militar (A-121 – A-124), se procede en primer lugar a desconectar la antena VHF de la parte trasera del equipo. A continuación, se establece conexión directa

mediante un cable coaxial RG316 por un extremo al ADALM-PLUTO y por otro a un conector SO-239 macho. Este se acopla al conector SO-239 hembra del receptor, de tal forma que se permite la inyección de la señal generada directamente a la entrada del equipo, simulando así una recepción real.

La conexión del banco de pruebas al receptor FURUNO FA-170 instalado en la 2ª serie de lanchas de instrucción (A-127 – A-128) sigue el mismo procedimiento descrito anteriormente, pero requiere de una fase previa de acceso al equipo. Debido a que la interfaz se encuentra empotrada en el cuadro de mandos, es necesario acceder a la unidad del transpondedor desde la parte inferior de la consola. Una vez localizada, se procede de igual forma que en el caso anterior: se desconecta a antena VHF y se conecta el banco de pruebas directamente a la entrada de antena del equipo mediante el cableado correspondiente.

3.7 Validación y puesta a punto del código conforme a los estándares

Con el fin de incorporar los mensajes tipo 1, 5 y 21 al protocolo fue necesario previamente verificar que los códigos de generación y transmisión de mensajes eran capaces de generar correctamente la estructura binaria de los mensajes y que la duración de transmisión se ajustase al número de *slots* TDMA correspondientes definidos en [6]. Además, los códigos tenían que ser capaces de mantener una cadencia temporal estable entre transmisiones que fuera equivalente a la ocupación real de dichos *slots* y garantizar que las posibles pérdidas observadas en el receptor se debiesen al propio receptor y no a posibles limitaciones ligadas al banco de pruebas.

El flujo de generación sigue las siguientes fases:

1. Se genera el *payload* binario mediante Python
2. El *payload* se envía mediante UDP a GNU-Radio
3. El bloque de AIS Tx de GNU-Radio añade el preámbulo, los *flags*, aplica *bit stuffing*, codifica NRZI y empaqueta los bytes listos para el envio
4. El flujo se modula mediante GMSK a 9.600 bit/s
5. La señal generada se transmite por medio del ADALM-PLUTO directamente al receptor

Cabe destacar que el punto de partida no fue un sistema desarrollado desde cero, sino un conjunto de códigos proporcionados que permitían la transmisión de mensajes AIS tipo 1, de forma aparentemente correcta y funcional. Sin embargo, tras analizar detalladamente su funcionamiento, se corroboró que el código era apto solo para trabajar con ese tipo de mensajes, pero requería modificaciones para poder transmitir los otros tipos deseados. Una de las grandes limitaciones provenía del bloque AIS Tx del archivo del *spoofer*. El bloque trabajaba con una longitud fija de 168 bits pues estaba pensado únicamente para mensajes de tipo 1, lo que implicaba que cualquier mensaje que no se ajustase a ese tamaño no se procesaría correctamente. De hecho, tras generar códigos para los tipo 5 y tipo 21, las transmisiones no se decodificaban correctamente y aparecían datos distorsionados.

Para solucionar esto, en una primera modificación se eliminó la longitud fija y se pasó a trabajar con el número de bits efectivos del *payload* antes de ser procesado por el bloque AIS Tx, siendo esta la longitud real del mensaje recibido. Esto permitía al bloque trabajar con el "*raw length*", por lo tanto, aceptaba mensajes de cualquier tamaño sin truncarlos. Este cambio no iba enfocado solo a poder transmitir mensajes de mayor tamaño, sino a evitar un problema: al forzar la longitud fija, el bloque eliminaba bits, lo que terminaba alterando la recepción al provocar duraciones inconsistentes una vez modulada la señal. Con "*raw length*", al trabajar con la longitud real, cada mensaje se procesaba con los bits que le correspondían, manteniendo así la integridad de la trama. De esta manera se permitía que la duración final dependiera del contenido y del procesamiento estándar de AIS.

Pese a la modificación descrita, surgió un nuevo inconveniente: el control temporal. Aunque los mensajes ya no se truncaban, la duración final de la transmisión seguía dependiendo de varios factores internos del AIS Tx, especialmente del *bit stuffing* y de la cola de bytes añadida al final para que los tiempos de transmisión se ajustasen a la duración del número de *slots* TDMA correspondiente. Por este

motivo, el bloque trabaja de forma dinámica con el *payload* recibido, introduciendo en la cola 2 bytes para las transmisiones en los mensajes tipo 1, 3 bytes para los tipo 5, y 22 bytes para los tipo 21, como se describe en 3.7.1, 3.7.2 y 3.7.3.

Otro problema fue la incertidumbre sobre el comportamiento del sistema en términos de flujo de datos. Inicialmente no había forma de asegurar que los mensajes generados en Python se estuviesen transmitiendo inmediatamente, existiendo la posibilidad de que se acumulasen en el ADALM-PLUTO y se enviasen con retardo. Esto ocurrió en un primer instante: los mensajes se transmitían con una cadencia determinada, pero al finalizar la transmisión del script, el receptor QK-A026 con el que se validaron todas las pruebas continuaba recibiendo tramas. Se confirmó de esta forma el hecho de que una vez finalizado el script, el receptor continuaba parpadeando (recibiendo mensajes) hasta que se desconectaba el ADALM-PLUTO del ordenador. Por ello, para descartar que este escenario se repitiese, se incorporaron trazas de diagnóstico que permitían observar lo que ocurría en GNU-Radio. Con las modificaciones pertinentes realizadas sobre el código, las pruebas empezaban a mostrar de forma consistente que el *buffer* permanecía cercano a cero, lo cual indicaba que no existía un almacenamiento intermedio y que el sistema transmitía en tiempo real. Tras varias pruebas con diferentes tamaños de *buffer*, se configuró en un tamaño funcional (0xFFFF). El ajuste no implicaba que se ocupase todo el espacio, sino que evitase limitaciones que pudieran provocar bloqueos o pérdidas, manteniendo un flujo continuo y estable.

Finalmente, un aspecto común y muy relevante que se mencionó previamente fue la influencia directa de la cola de bytes añadida en el bloque AIS Tx. Inicialmente, el valor no estaba ajustado, lo que provocaba que las transmisiones se alargasen más de lo debido y, por ende, invadieran *slots* posteriores. A partir de este punto, la cola de bytes pasó a utilizarse como ajuste fino de la duración de cada mensaje, permitiendo adaptar el mensaje a la estructura TDMA sin modificar el contenido del *payload*.

3.7.1 Tipo 1

El objetivo para la generación de mensajes tipo 1 era garantizar que la duración total de la transmisión se mantuviese dentro del intervalo TDMA correspondiente a un único slot. Como la longitud de este tipo de mensaje es inferior a la de otras tramas, la duración de partida era sensiblemente menor que el intervalo completo del slot, lo que generaba un hueco temporal antes de la siguiente transmisión y rompía el objetivo de buscar una ocupación continua del canal.

Para ajustar la señal a un comportamiento temporal coherente se introdujo la variable correspondiente a la cola artificial de bytes al final de la trama. Se partió de un valor inicial de 6 bytes para aproximar la duración a la correspondiente de un slot. Con esta cola, la duración se incrementaba a 29,17 ms, lo cual superaba el límite de 26,67 ms y causaba la invasión de la siguiente transmisión. Esto resultaba incompatible con el funcionamiento correcto del protocolo TDMA.

Tras varias iteraciones se determinó que una cola de 2 bytes permitía alcanzar una duración total de 26,67 ms, coincidiendo con la duración teórica de un único slot TDMA. Este valor permite ajustar el mensaje al límite del slot sin modificar su contenido ni su estructura interna, garantizando que cada transmisión ocupa exactamente su intervalo correspondiente. Con todo ello, se consigue una ocupación temporal coherente y repetible, evitando tanto huecos como solapamientos entre transmisiones consecutivas.

La Figura 3-17 representa la transmisión de un mensaje AIS tipo 1. Se puede apreciar como la duración completa del mensaje es de aproximadamente 26,67 ms, lo que corresponde a un único slot TDMA. Una vez finalizada la transmisión del primero, se puede apreciar el preámbulo del segundo mensaje transmitido.

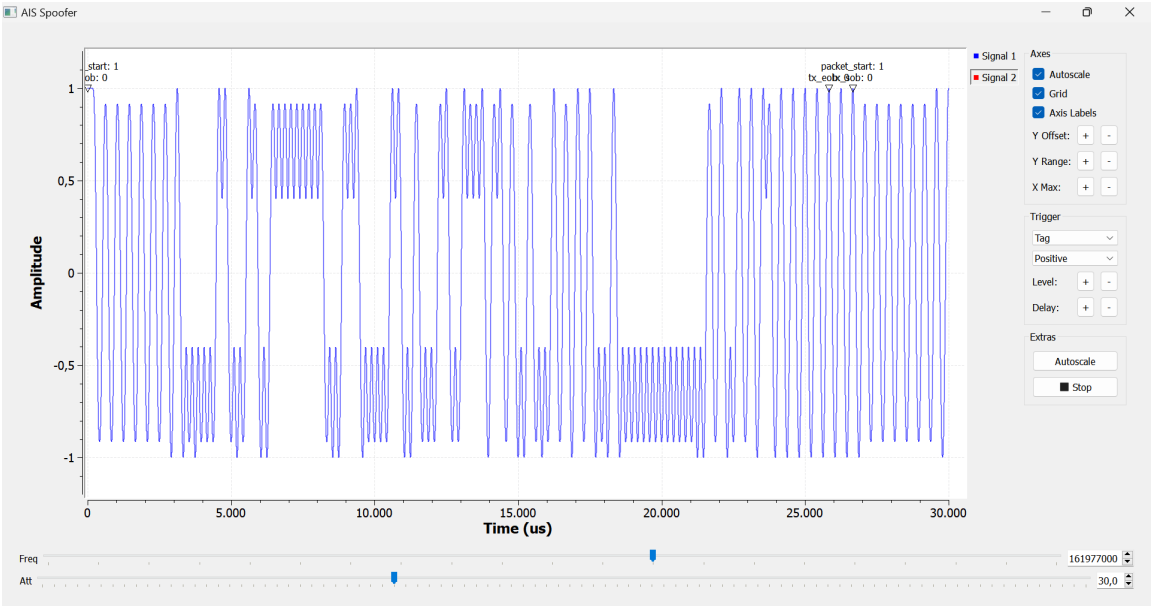


Figura 3-17 Transmisión de mensaje AIS Tipo 1

3.7.2 Tipo 5

El objetivo para la generación del *script* de PS2 era lograr una secuencia compuesta por un tipo 1 seguido de su correspondiente tipo 5. La problemática no era ya la duración individual sino lograr una correcta integración de ambos mensajes en tres *slots* consecutivos. El análisis inicial permitió determinar la duración real de cada mensaje, las cuales eran coherentes y las esperadas.

Pese a que las duraciones individuales eran correctas, la transición entre el tipo 1 y el tipo 5 no estaba completamente controlada. Por ello, se plantearon pequeñas pausas entre ambos mensajes para asegurar la finalización de la transmisión anterior. Sin embargo, este enfoque introducía discontinuidades artificiales en la señal que complicaban la alineación temporal con los *slots*. Fue a raíz de esta problemática que se eliminó el tiempo entre transmisiones del *script* de Python y se establecieron los tamaños fijos de 30 bytes para tipo 1 y 61 bytes para tipo 5, logrando así que la duración fuese ligeramente inferior a los 80 ms correspondientes a tres *slots*.

Tras lograr que los mensajes se enviasen sin solapamientos que pudieran conllevar pérdidas, se realizó el ajusto definitivo actuando nuevamente sobre la cola de bytes del bloque AIS Tx. Manteniendo una cola de 3 bytes se logró una estabilización en la duración total de la secuencia completa, con un tiempo equivalente a los tres *slots* que se buscaban. Esto permitió eliminar cualquier pausa entre mensajes y trabajar con una señal continua, en la que el tipo 1 ocupa el primer *slot* y el tipo 5 los dos siguientes. Cabe destacar que, en transmisiones reales de barcos, un mensaje no tiene por qué preceder a otro. Inicialmente se envía un tipo 1, el sistema escucha para detectar *slots* libres y proceder al envío del tipo 5.

Es importante destacar que en ningún momento se modificó la estructura interna del mensaje ni su tamaño final de 61 bytes, ya que esto alteraría el estándar. El ajuste se realizó únicamente sobre la temporización final de la señal para garantizar una ocupación correcta y total de los *slots*.

Una vez realizados los ajustes y verificados los resultados observando directamente la señal en GNU-Radio, se confirmó que el generador produce de forma consistente la estructura temporal como muestra la Figura 3-18:

- 1.er slot: mensaje AIS tipo 1
- 2.do slot: primera mitad del mensaje AIS tipo 5
- 3.er slot: segunda mitad del mensaje AIS tipo 5

Estas duraciones observadas confirman que la señal generada respeta la ocupación TDMA definida por la ITU. De esta manera se puede utilizar el banco de pruebas para evaluar de forma fiable el comportamiento de los receptores ante la transmisión de mensajes dinámicos y estáticos.

La Figura 3-18 representa la transmisión de un mensaje tipo 1 seguido de un tipo 5. Ambos mensajes van de la mano ya que se complementan. Ocupan conjuntamente tres *slots* TDMA consecutivos, reflejado en la duración aproximada de 80 ms.

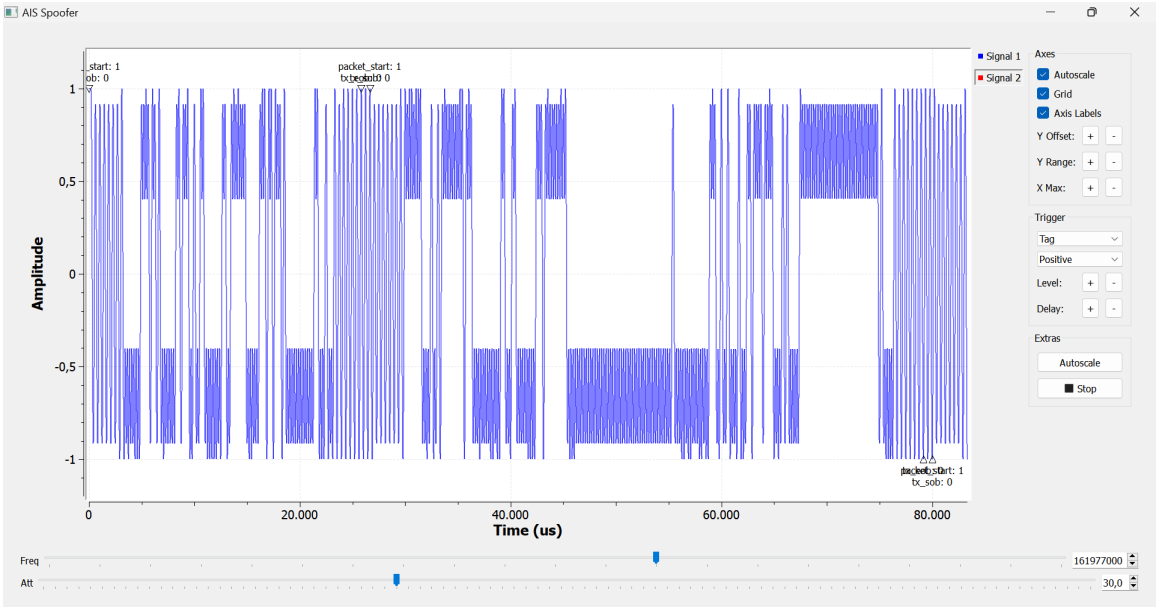


Figura 3-18 Transmisión de mensaje AIS Tipo 1 + Tipo 5

3.7.3 Tipo 21

Inicialmente se verificó el tamaño del mensaje final transmitido teniendo en cuenta que la codificación generaba un *payload* de 272 bits. El estándar establece el rango en 272 – 360 bits, por lo que se cumple con el mínimo requerido. Al transmitir esa cantidad de bits son necesarios dos *slots* TDMA que, considerando la velocidad de 9.600 bits/s, la duración teórica de los dos *slots* es de 53,33 ms. Este valor se utilizó como referencia para el ajuste temporal del sistema.

A diferencia de los otros dos tipos, su longitud de partida es relativamente reducida, lo que implica que su duración natural tras el procesamiento en el bloque AIS Tx queda por debajo de los dos *slots* a ocupar. Al realizar las primeras pruebas se apreciaba claramente que la cola de bytes no estaba ajustada, lo que provocaba duraciones inconsistentes. El receptor nuevamente mostraba actividad pese al cese de la transmisión. Para corregir este problema se ajustó de forma específica la cola de bytes a 22. Así se logró que la duración total de la transmisión fuera equivalente a la correspondiente a dos *slots*, sin necesidad de modificar el contenido del mensaje. El ajuste en este caso es más significativo que en los tipo 1 y tipo 5 ya que existe una gran diferencia entre la duración natural del mensaje y la duración del objetivo, resultando la definición explicita de esta cola en el bloque AIS Tx especialmente importante.

Al interpretar los resultados se puede concluir que el *script* generador produce mensajes de tipo 21 válidos con su correspondiente longitud según el estándar. Además, el bloque AIS Tx encapsula correctamente la trama AIS al completo, permitiendo que el sistema transmita con una cadencia temporal equivalente a dos *slots* TDMA. Por ello, el flujo de GNU-Radio al ADALM-PLUTO no presenta acumulación de *buffers* y el banco de pruebas es capaz de mantener la transmisión durante altos volúmenes de mensajes consecutivos sin una degradación significativa en el temporizado.

El objetivo final de las pruebas realizadas no es tanto medir la cantidad de mensajes que pierde un receptor sino validar el banco de pruebas en transmisiones de mensajes tipo 21. Las mediciones demuestran que el banco de generación mantiene la temporización adecuada, el sistema SDR no

introduce retrasos y los mensajes respetan la estructura AIS. Por tanto, se puede concluir que las posibles pérdidas observadas en el receptor no se deben a limitaciones del generador de tráfico.

La Figura 3-19 representa la transmisión de un mensaje tipo 21, donde se aprecia la ocupación de dos *slots* TDMA consecutivos lo cual corresponde a una duración aproximada de 53,33 ms, siendo apreciable el inicio de la siguiente.

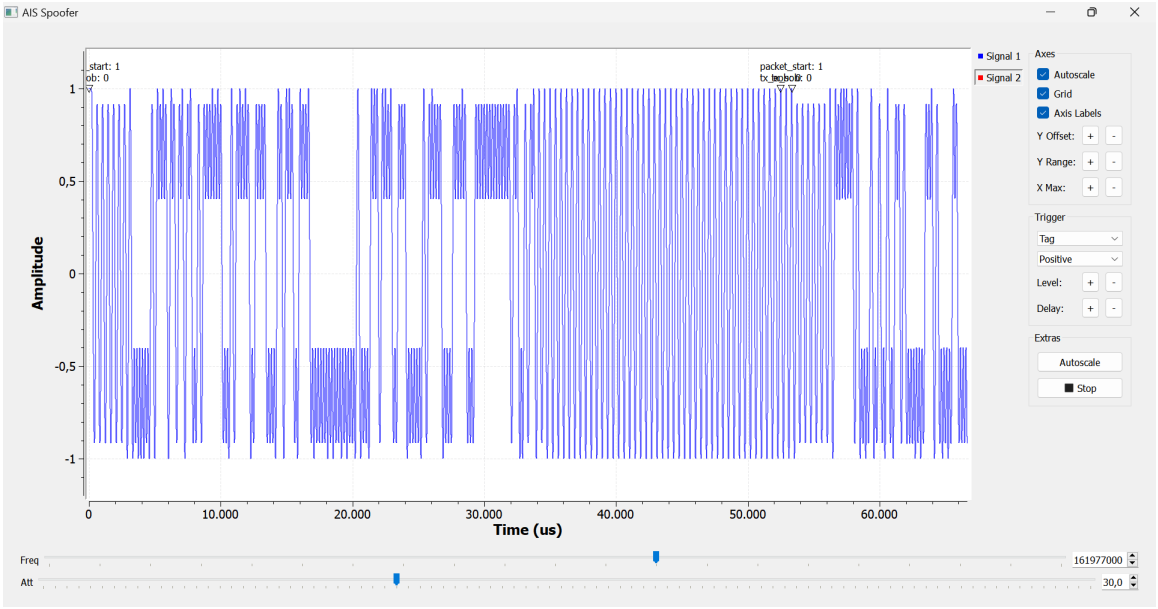


Figura 3-19 Transmisión de mensaje AIS Tipo 21

Una vez realizados todos los ajustes, se procedió a la validación del sistema en condiciones reales de transmisión. Se comprobó que no existían acumulaciones en el sistema, que las duraciones se ajustaban a la estructura TDMA y que la transmisión era estable. Sin embargo, el receptor QK-A026, sobre el que se validaron las pruebas, no fue capaz de decodificar la totalidad de los mensajes tipo 5, obteniéndose de forma consistente un número de mensajes no decodificados.

Este resultado, reproducible entre ejecuciones, permite descartar que las pérdidas estén relacionadas con el banco de pruebas. El sistema genera y transmite las tramas correctamente, respetando tanto la estructura como la temporización del estándar AIS. Por tanto, las limitaciones observadas se deben al propio receptor y no al sistema de generación.

En conjunto, el desarrollo realizado ha permitido pasar de un sistema limitado a mensajes tipo 1 a un banco de pruebas completo, capaz de generar y transmitir mensajes AIS tipo 1, 5 y 21 de forma controlada, sin acumulaciones internas y con una temporización coherente con los *slots* TDMA, lo que permite evaluar de forma fiable el comportamiento de los receptores.

3.8 Metodología de evaluación y criterios de degradación

Es necesario establecer un marco que permita evaluar el comportamiento del receptor una vez definida la arquitectura de la lógica implementada y duración de las transmisiones de cada ataque. Este apartado tiene como objetivo diferenciar los parámetros que se pueden controlar y los efectos observables durante las pruebas.

3.8.1 Variables controladas

Al ejecutar las pruebas se modifican ciertas variables que determinan el nivel de carga o interferencia al que se somete el receptor. Se consigue así simular una diversidad de escenarios, desde una leve inyección de trazas hasta una DoS. Las principales son:

- Frecuencia de generación de mensajes AIS.
- Tipo de mensaje AIS.
- Duración total del escenario de ataque.
- Nivel de ruido AWGN.

Al incrementar cualquiera de estos parámetros individualmente o en conjunto de forma gradual, se puede localizar el punto en el que el receptor comienza a mostrar signos de saturación, detectando el umbral real del sistema.

3.8.2 Variables observables

Para determinar el impacto real de las perturbaciones, existen varios aspectos a monitorizar que indican el comportamiento real del receptor y del software. Se divide en dos niveles diferenciados: a nivel receptor las métricas principales y a nivel visualización las métricas auxiliares.

Nivel receptor:

- Tasa de Error de Paquetes (PER).
- Tiempo de recuperación del flujo una vez finalizado el ataque.

Nivel visualización:

- Número de blancos representados en la interfaz.
- Número de sentencias NMEA correctas recibidas en el *log* de lectura.

3.8.3 Propuesta del protocolo de pruebas

El fin de este Trabajo de Fin de Grado es establecer un protocolo de pruebas sistemático que mida la resiliencia de un sistema AIS frente a perturbaciones. Una vez caracterizado el hardware, software y entorno de pruebas, se establece la siguiente metodología estandarizada que permita evaluar, de forma repetible y objetiva, la robustez de cualquier receptor AIS.

Se busca proporcionar una métrica clara sobre la confianza que se puede depositar en la conciencia situacional que ofrece el AIS en los diferentes entornos de conflicto que se viven en la actualidad. Todos los códigos empleados en la realización de estas pruebas se describen en el Anexo V.

A continuación, se detallan las cinco pruebas principales de las cuales se compone el protocolo, justificando, además, la relevancia de cada una:

1. **Prueba de transmisión de mensajes tipo 1 (PS1):** El objetivo principal de la prueba es determinar la capacidad de absorción de tráfico AIS del receptor al incrementar el volumen de mensajes de tipo 1 recibidos. Se decide utilizar este mensaje al ser el más sencillo y frecuente en el área de pruebas, tal y como describe 3.1.2. Todos los mensajes transmitidos respetan de manera estricta la estructura temporal definida por la ITU, asegurándose que el receptor es evaluado en condiciones equivalentes a las de una red AIS real. El esquema de interconexión tanto para esta prueba como para PS2 se muestra en la Figura 3-12. La prueba se estructura en cuatro series de transmisión compuestas por 50, 100, 200 y 500 mensajes. Durante cada una se registra el número total de mensajes enviados y el número de mensajes que el receptor es capaz de decodificar correctamente, mostrándolos por pantalla. A partir de esta comparación se determina el PER del envío. El resultado de la prueba permite evaluar la robustez básica del receptor frente a flujos continuos de tráfico AIS dinámico, identificando si el equipo presenta pérdidas de decodificación.
2. **Prueba de transmisión de mensajes tipo 5 (PS2):** Esta prueba busca analizar cómo se comporta el receptor ante la recepción de mensajes AIS tipo 5. Estos mensajes contienen información estática y de viaje, y por ello presentan un tamaño considerablemente mayor, requiriendo una ocupación superior del canal TDMA. Todo ello implica una mayor carga de procesamiento para el receptor. Al igual que en PS1, se realizan cuatro transmisiones de 50,

100, 200 y 500 mensajes. Durante cada una se registra el número total de mensajes enviados, mensajes recibidos y mensajes decodificados correctamente. A diferencia de PS1, el parámetro de interés no es solo la pérdida de mensajes, sino también la capacidad que tiene el receptor de procesar correctamente las tramas de mayor tamaño. De esta manera se permite determinar si el equipo mantiene un rendimiento estable con mensajes de mayor tamaño o si aparecen limitaciones asociadas al procesamiento o al manejo interno del *buffer*.

3. **Prueba de suplantación de AtoN (PS3):** Esta prueba tiene como objetivo evaluar el impacto que puede tener una transmisión continua de un AtoN sobre la capacidad del receptor de procesar tráfico legítimo existente. El esquema de interconexión de la prueba se muestra en la Figura 3-13. Para ello se genera en este caso la AtoN del Faro de Ons, situado en la Ría de Pontevedra, con parámetros coherentes que respetan la estructura temporal de TDMA. Así, el blanco generado ocupa de manera continuada los *slots* disponibles del canal con el objetivo de simular un escenario en el que una señal aparentemente válida monopoliza el medio de transmisión, evitando que otros mensajes entren en el canal. A diferencia de PS1 y PS2, este ensayo sí mantiene la recepción de tráfico real precedente de la zona, permitiendo observar el efecto que tiene sobre la capacidad del receptor para mostrar información legitima. Durante el transcurso de la prueba se modifica progresivamente la atenuación de la señal generada, con el objetivo de determinar el punto a partir del cual el receptor comienza nuevamente a mostrar tráfico real. El ensayo permite evaluar la vulnerabilidad del sistema frente a ataques de suplantación de AtoNs, ya que la presencia de una señal falsa pero aparentemente válida puede inducir a errores de interpretación.
4. **Prueba de *jamming* AWGN (PJ1):** Para llevar a cabo esta prueba se utiliza el montaje descrito en la Figura 3-14 que se basa en una señal real con la superposición de una señal interferente. En este caso, la interferencia empleada consiste en AWGN, con el objetivo de analizar el comportamiento del receptor frente a un entorno de ruido aditivo. El procedimiento se desarrolla mediante un barrido progresivo de atenuación partiendo de -89 dB en la señal interferente. A partir de este punto se comienza a reducir de forma controlada el nivel de atenuación de ruido. En cada nivel de atenuación se monitoriza el número de mensajes decodificados (en función del receptor se comprueba *log* o tiempo de refresco del mensaje en interfaz) comprobando por un lado el umbral a partir del cual comienza a apreciarse degradación en la recepción y, por otro, el punto límite en el que el receptor deja de mostrar mensajes válidos. El objetivo final es determinar el nivel de interferencia a partir del cual el receptor pierde su capacidad de mantener una recepción operativa del tráfico AIS real. Es importante destacar que esta prueba se realizará exclusivamente en un entorno controlado, empleando medidas de acoplamiento que evitan emisiones no deseadas fuera del banco de ensayo.
5. **Prueba de recuperación tras *jamming* (PJ2):** Esta prueba está orientada a analizar la capacidad del receptor para recuperar su funcionamiento normal tras un *jamming* deliberado. En este caso se genera una señal de *jamming* partiendo de la atenuación a partir la cual el receptor pierde la capacidad de decodificar tráfico válido (obtenida en PJ1). Al igual que PS3, esta prueba también mantiene el tráfico real precedente de la zona. Finalizada la transmisión interferente se monitoriza el comportamiento del receptor, midiendo el tiempo necesario para que recupere su funcionalidad normal. La funcionalidad normal se entiende como el momento en el que vuelve a decodificar correctamente tráfico AIS válido, mostrándolo por pantalla o por el log, según corresponda. Resulta especialmente relevante ya que un receptor puede verse temporalmente afectado por una interferencia externa, siendo fundamental que recupere su capacidad operativa a la mayor brevedad, tal y como se menciona en el apartado 2.7.4.

El protocolo se presenta como un estándar para plataformas navales, de tal manera que su aplicación sistemática permita clasificar los equipos según lo descrito en la Tabla 3-3.

3.8.4 Indicadores de evaluación del sistema

Una vez definido el protocolo de pruebas, es necesario establecer los indicadores que permiten la correcta evaluación del receptor al verse sometido a cada una de las pruebas descritas en el apartado 3.8.3. Con el fin de garantizar una evaluación homogénea, en cada prueba se analizan un conjunto de métricas específicas que relacionan el tipo de perturbación con el impacto observable en el receptor. La Tabla 3-2 resume las pruebas incluidas en el protocolo, los indicadores utilizados para evaluar el comportamiento y la ponderación asignada a cada una de ellas con el fin de reflejar la relevancia relativa de cada escenario dentro del análisis para el posterior cálculo del índice de resiliencia (I_R) descrito en 3.8.6.

Prueba	Escenario	Métrica principal	Peso	Objetivo
PS1	Saturación tipo 1	PER (%)	0,25	Determinar límite de carga
PS2	Saturación tipo 5	PER (%)	0,15	Determinar límite de carga
PS3	*Spoofing* AtoN	Reducción de tráfico (%)	0,20	Integridad situacional
PJ1	*Jamming* AWGN	Umbral de fallo (dB)	0,25	Robustez RF
PJ2	Recuperación	Tiempo de recuperación (s)	0,15	Persistencia de interferencia

Tabla 3-2 Pruebas del protocolo y métricas de evaluación

La relevancia relativa de cada una de las pruebas la reflejan las ponderaciones asignadas. No todas las pruebas representan el mismo nivel de impacto sobre la capacidad del receptor para permitir al OGP mantener una RMP clara y fiable.

La prueba PS1 recibe una ponderación de 0,25 al evaluar mediante mensajes de tipo 1, que constituyen el tipo de mensaje más frecuente, la capacidad del receptor para sostener cargas elevadas de tráfico AIS. Este escenario trata de simular la cantidad de mensajes que se podrían llegar a perder bajo un ataque real, reproduciendo uno de los vectores de perturbación más accesibles.

La prueba PJ1 se pondera con 0,25 al evaluar la resiliencia del receptor frente a interferencias en la capa física del sistema. Al afectar el *jamming* directamente a la capacidad del receptor para discriminar señales en el canal radioeléctrico, pudiendo provocar la pérdida completa de tráfico AIS en escenarios reales, se le concede el peso descrito.

La prueba PS3 recibe una ponderación de 0,20 al evaluar un escenario directamente relacionado con la seguridad operacional. Recibe ese valor ya que permite analizar cómo afecta la inyección de trazas artificiales aparentemente reales a la pérdida de tráfico legítimo.

Las pruebas PS2 y PJ2 reciben una ponderación de 0,15 al centrarse en aspectos complementarios. En el caso de PS2, al evaluar la capacidad de decodificación, permite identificar limitaciones en el procesamiento interno del sistema sin implicar necesariamente una pérdida de funcionalidad. La prueba PJ2 recibe esta ponderación al tratarse de una prueba complementaria a la prueba PJ1, determinando si los efectos del *jamming* desaparecen de forma inmediata o si, por el contrario, dejan al receptor degradado.

3.8.5 Marco de evaluación y rúbrica de resiliencia

Este apartado establece el nexo entre los datos brutos obtenidos en las pruebas y la capacidad operativa del equipo. Para ello se define una rúbrica de puntuación común de 1 a 5 puntos, en la que 1 representa el mejor comportamiento y 5 el peor. Esta escala permite estandarizar el comportamiento del receptor ante cada vector de ataque:

Puntos	PS1	PS2	PS3	PJ1	PJ2
1	< 1%	< 1%	< 10%	≥ -10 dB	< 1 seg
2	1% – 4,9%	1% – 4,9%	10% – 29,9%	-20 dB – -10 dB	1 – 4,9 seg
3	5 % – 14,9%	5% – 14,9%	30% – 49,9%	-35 dB – -20 dB	5 – 14,9 seg
4	15% – 49,9%	15% – 49,9%	50% – 79,9%	-50 dB – -35 dB	15 – 59,9 seg
5	> 50%	> 50%	> 80%	< -50 dB	> 60 seg

Tabla 3-3 Rúbrica de puntuación de un receptor en base al protocolo

La Tabla 3-3 traduce métricas descriptivas de cada prueba a una escala común de 1 a 5 puntos:

- PS1 y PS2: Evalúa la robustez ante un volumen bruto de recepción de mensajes mediante el PER, cuyo cálculo se describe en el apartado 3.8.7. Un PER inferior al 1% se considera óptimo, mientras que el superar el 50% se considera un fallo completo.
- PS3: La puntuación se asigna en función de la reducción del tráfico legítimo observado durante el ataque respecto al minuto de referencia previo. De esta manera se mide la pérdida real de conciencia situacional causada por una AtoN falsa.
- PJ1: Se toma como métrica principal la atenuación de la interferencia a la que se produce el fallo completo del receptor. A mayor atenuación para anular, menor robustez del equipo.
- PJ2: Se valora el tiempo necesario para recuperar un funcionamiento nominal una vez cesa la interferencia. A mayor tiempo de recuperación, peor puntuación.

En aquellos receptores que, por funcionamiento interno, no sean capaces de representar los mensajes recibidos en cualquiera de las pruebas de *spoofing*, las pruebas se considerarán no aplicables. En ese caso el índice final se calcularán los pesos únicamente sobre las pruebas válidas, manteniendo valores proporcionales, evitando penalizar al equipo por una limitación funcional del ensayo sobre el mismo.

3.8.6 Calificación final del receptor

A continuación, se describe Tabla 3-4 en la que se integran las puntuaciones resultantes de cada una de las pruebas realizadas por parte del usuario que aplica el protocolo:

Escenario de prueba	Métrica principal	Puntuación (1-5)
PS1. Saturación con tipo 1	PER total (%)	A AÑADIR POR USUARIO TRAS PRUEBA
PS2. Saturación con tipo 5	PER total (%)	
PS3. Suplantación de AtoN	Reducción de tráfico (%)	
PJ1. *Jamming* AWGN	Umbral de fallo (dB)	
PJ2. Recuperación	Tiempo de recuperación (s)	
ÍNDICE FINAL	I_R	

Tabla 3-4 Tabla a rellenar por el usuario tras obtener la puntuación de las pruebas

Para obtener un índice de resiliencia objetivo y adecuado al receptor que se evalúa, la Figura 3-20 ubica al evaluador y resume las métricas principales que se deben tener en cuenta y sus pesos descritos previamente en 3.8.4:

Prueba	Métrica principal	Peso (W_i)
PS1	PER total (%)	0,25
PS2	PER total (%)	0,15
PS3	Reducción de tráfico (%)	0,20
PJ1	Umbral de fallo (dB)	0,25
PJ2	Tiempo de recuperación (s)	0,15

Figura 3-20 Resumen de ponderación de cada prueba

Teniendo en cuenta las puntuaciones obtenidas siguiendo la rúbrica descrita en 3.8.5, el Índice de Resiliencia (I_R) mediante (4):

$$I_R = \frac{\sum(P_i \cdot W_i)}{\sum W_i} \tag{4}$$

Donde P_i es la puntuación de 1 a 5 final de cada una de las pruebas (PS1, PS2, PS3, PJ1 y PJ2) y W_i es la ponderación o peso de cada una de ellas. Cuando todas las pruebas son aplicables, el denominador es igual a 1. De lo contrario, si alguna no es aplicable, el denominador pasa a ser la suma de los pesos considerados.

Dependiendo del valor obtenido, el receptor se clasifica en uno de los siguientes cuatro niveles de resiliencia definidos:

1. **Índice $1.0 \leq I_R \leq 1.5$:** Resiliencia Alta. El hardware cuenta con una alta capacidad de proceso, apto para operar en entornos de amenaza sin comprometer la seguridad. En estos niveles, el receptor absorbe las fluctuaciones de carga, permitiendo una correcta toma de decisiones por parte de un oficial de guardia en puente.
2. **Índice $1.6 \leq I_R \leq 2.5$:** Resiliencia Estándar. Comportamiento adecuado para la navegación. Presenta degradaciones leves que no afectan a la conciencia situacional.
3. **Índice $2.6 \leq I_R \leq 3.5$:** Resiliencia Limitada. El sistema muestra debilidades a la hora de gestionar la memoria o priorizar la seguridad. Se genera un estado de incertidumbre en el OGP al no poder corroborar la validez de los blancos mostrados en sus pantallas de navegación.
4. **Índice $3.6 \leq I_R \leq 5.0$:** Vulnerabilidad Crítica. El receptor no es apto para entornos de conflicto. El sistema deja de ser una ayuda y se convierte en un factor de riesgo a causa de desinformación o ausencia total de datos.

3.8.7 Cálculo del Packet Error Rate

Se adopta la variable PER para establecer un punto de partida que permita cuantificar de manera objetiva la degradación del sistema. Permite estimar la fiabilidad del enlace AIS y la capacidad del receptor para procesar correctamente las tramas recibidas bajo diferentes condiciones de carga o perturbación. El PER expresa el porcentaje de mensajes no decodificados por el receptor.

Dada la naturaleza del protocolo en las pruebas PS1 y PS2, el análisis del PER se tiene que abordar desde dos perspectivas diferentes: una para determinar el punto de quiebra del receptor en cada prueba individualmente y otro que busca normalizar los resultados para su posterior traslado a la Tabla 3-3 y clasificación:

1. **PER individual:** Se calcula un porcentaje de error específico para PS1 y PS2 descritas en el apartado 3.8.3. El cálculo se muestra en (5):

$$PER_{IND}(\%) = \frac{Mensajes_{TX} - Mensajes_{RX}}{Mensajes_{TX}} \times 100 \quad (5)$$

donde $Mensajes_{TX}$ indica el total de mensajes enviados y $Mensajes_{RX}$ el número de tramas que el receptor procesa y decodifica correctamente.

2. **PER total:** Para obtener una clasificación final objetiva del receptor estudiado, se suma la totalidad de mensajes transmitidos y perdidos en todas las muestras de la prueba, representado así el comportamiento global del equipo ante la batería completa de mensajes. Se define como el sumatorio total de los mensajes perdidos frente al sumatorio de los mensajes transmitidos en toda la secuencia de la prueba como se muestra en (6):

$$PER_{TOTAL}(\%) = \frac{\sum Mensajes_{TX} - \sum Mensajes_{RX}}{\sum Mensajes_{TX}} \times 100 \quad (6)$$

El PER_{TOTAL} constituye el parámetro que se traslada a su apartado correspondiente en la rúbrica de evaluación reflejada en la Tabla 3-3. A partir de este valor se determina el nivel de degradación del receptor durante cada prueba, asignándole la puntuación correspondiente. De esta manera se obtiene una métrica cuantitativa que permite clasificar de forma objetiva el receptor en las pruebas PS1 y PS2, determinando si es capaz de mantener una recepción fiable o si presenta limitaciones que pudieran comprometer la conciencia situacional.

4 APLICACIÓN Y VALIDACIÓN DEL PROTOCOLO

El presente capítulo describe la aplicación del protocolo de pruebas propuesto sobre los diferentes receptores AIS estudiados. Se detallan los ensayos realizados, permitiendo analizar el comportamiento de cada equipo frente a los diferentes escenarios planteados. De esta manera, se valida el protocolo y su capacidad para caracterizar la resiliencia de los receptores en un entorno controlado.

4.1 Caracterización de la capacidad del receptor QK-A026

Las pruebas parten de un MMSI inicial determinado con incrementos de uno por cada mensaje transmitido para PS1 y PS2. La comprobación de la recepción en todas las pruebas se hace por medio del código descrito en el Anexo V que lee los mensajes que entran al PC por el puerto COM9 al que está conectado el receptor.

Es importante destacar que el *script* empleado en COM9 actúa como registrador pasivo del flujo NMEA. En ningún momento modifica tramas o filtra información, únicamente contabiliza y almacena las sentencias recibidas. Por tanto, las pérdidas medidas se atribuyen a la capacidad del receptor para procesar y volcar información por su salida, no al software de visualización.

4.1.1 PS1 Saturación con mensajes Tipo 1

En el primer ensayo se transmitieron 50 mensajes consecutivos. De ellos, el receptor decodificó 48 correctamente. El PER asociado es:

$$PER_{50}(\%) = \frac{50 - 48}{50} \times 100 = 4\%$$

La secuencia de MMSI recibidos es prácticamente continua, observándose únicamente pérdidas puntuales. Las tramas recibidas no presentaban errores de codificación ni formato, estando todas formadas como sentencias *!AIVDM* de una sola frase.

En el ensayo de 100 mensajes se decodificaron correctamente 98, produciéndose únicamente 2 pérdidas. El PER asociado es:

$$PER_{100}(\%) = \frac{100 - 98}{100} \times 100 = 2\%$$

El resultado mantiene el mismo camino que el anterior, observándose dos pérdidas puntuales y dispersas. No aparece ningún patrón claro ni indicios de saturación. De nuevo, las sentencias recibidas muestran el formato válido.

Al transmitirse 200 mensajes aumentan las pérdidas a 8. El PER asociado es:

$$PER_{200}(\%) = \frac{200 - 192}{200} \times 100 = 4\%$$

En este caso comienzan a apreciarse más pérdidas en la transmisión, lo que indica que el receptor no mantiene una decodificación completa de los mensajes cuando crece la carga. Pese a ello, no se observa ningún error en la sintaxis de las sentencias NMEA recibidas, por lo tanto el código generador hace su trabajo correctamente y se aprecia una pequeña degradación en la capacidad del receptor en decodificar volúmenes de transmisión mayores.

En el último ensayo, de 500 mensajes, se decodificaron correctamente 486. Esto resulta en el siguiente PER asociado:

$$PER_{500}(\%) = \frac{500 - 486}{500} \times 100 = 2{,}8\%$$

Este resultado confirma que las pérdidas persisten para cargas mayores. Pese a que el PER no aumenta respecto a las pruebas anteriores, se observa que la degradación en la decodificación se mantiene y no es capaz de procesar correctamente la totalidad de los mensajes. Al igual que el resto de pruebas, la sintaxis de las sentencias es correcta, lo que refuerza que el problema no está en la construcción de la trama, sino en la capacidad y forma en la que el receptor decodifica los mensajes que recibe.

La Tabla 4-1 muestra un resumen de los mensajes totales enviados, los perdidos y el PER para cada intervalo:

Totales	Perdidos	PER
50	2	4%
100	2	2%
200	8	4%
500	14	2,8%

Tabla 4-1 Resumen de la prueba PS1 para el receptor QK-A026

El análisis de la PS1 muestra que el receptor no decodifica el 100% de los mensajes transmitidos. No se aprecia relación lineal entre el número de mensajes enviados y el PER, por lo que no puede determinarse que la degradación sea progresiva. Cabe destacar que todas las sentencias NMEA que llegan al receptor son válidas, lo cual es especialmente relevante para confirmar que el problema aparece en que no todas las transmitidas terminan siendo decodificadas.

El PER total para la prueba utilizado para la posterior calificación del receptor es el siguiente:

$$PER_{TOTAL}(\%) = \frac{850 - 824}{850} \times 100 = 3\%$$

4.1.2 PS2 Saturación con mensajes Tipo 5

En el primer ensayo, con la transmisión de 50 mensajes, decodificó correctamente 35 mensajes tipo 5. El PER para esta prueba es el siguiente:

$$PER_{50}(\%) = \frac{50 - 35}{50} \times 100 = 30\%$$

La tasa de pérdidas pone de manifiesto una limitación clara en condiciones de carga moderada. Pese a ello, como en PS1, no se detectaron tramas corruptas.

Con la transmisión de 100 mensajes, las pérdidas ascienden a 31, prácticamente el doble que en el ensayo anterior. Su PER asociado es:

$$PER_{100}(\%) = \frac{100 - 69}{100} \times 100 = 31\%$$

Por lo tanto, el PER se mantiene prácticamente constante respecto al caso anterior, lo que indica que no existe una degradación progresiva con el aumento del tráfico.

En el ensayo de transmisión de 200 mensajes, el receptor es capaz de decodificar correctamente 136. Se empieza a apreciar que el sistema entra en un régimen estable donde pierde aproximadamente 1 de cada 3 mensajes de tipo 5. El PER para esta prueba es:

$$PER_{200}(\%) = \frac{200 - 136}{200} \times 100 = 32\%$$

Se observa un ligero incremento y no se identifican errores en las sentencias, descartando problemas de integridad de señal.

En el último ensayo realizado, de las 500 transmisiones es capaz de decodificar 343 mensajes tipo 5. El PER obtenido es:

$$PER_{500}(\%) = \frac{500 - 343}{500} \times 100 = 31{,}4\%$$

A pesar del incremento significativo de la carga, el PER se mantiene constante. El patrón de pérdidas es aproximadamente periódico, con una separación típica de 3 a 4 mensajes entre pérdidas.

La Tabla 4-2 muestra un resumen de los mensajes totales enviados, los perdidos y el PER para cada intervalo:

Totales	No decodificados	PER
50	15	30%
100	31	31%
200	64	32%
500	157	31,4%

Tabla 4-2 Resumen de la prueba PS2 para el receptor QK-A026

El análisis muestra que el PER se mantiene en torno a un 30 – 32%, independientemente del volumen de tráfico generado. Este comportamiento indica que la pérdida no depende directamente de la carga del sistema, sino de la naturaleza de los mensajes de tipo 5. Se concluye que la causa es una limitación en el procesamiento de mensajes compuestos por varias sentencias en condiciones de transmisión continua.

El PER total para la prueba utilizado para la posterior calificación del receptor es el siguiente:

$$PER_{TOTAL}(\%) = \frac{850 - 583}{850} \times 100 = 31{,}4\%$$

4.1.3 PS3 Suplantación de AtoN

La ejecución de la prueba se dividió en dos fases: una primera de observación durante 60 segundos de la cantidad de mensajes que era capaz de decodificar, alcanzando una cifra de 18 mensajes, y la segunda de la transmisión continua del mensaje tipo 21 que suplanta la identidad del Faro de Ons. Al activar la transmisión, con una atenuación de -30 dB (la que se usa para la transmisión de todos los tipos de mensaje en el banco de pruebas), se produjo una reducción significativa en la recepción. El receptor pasó a decodificar únicamente 5 mensajes en el mismo intervalo temporal.

El único tráfico que consiguió mantenerse relativamente estable fue el correspondiente a los mensajes de tipo 1 transmitidos por el pesquero “Sajabi”, atracado en el puerto de Marín, del cual se

monitorizó constantemente su MMSI por medio del log. El buque se encontraba a aproximadamente 0,4 millas náuticas de la antena receptora, una distancia bastante prudente y que en alta mar se respeta entre buques por seguridad. Teniendo en cuenta que la transmisión de este mensaje es cada 10 segundos para buques entre 0 y 14 nudos (Tabla 2-1), cabría esperar 6 mensajes en el minuto transcurrido. No obstante, se recibieron únicamente 5.

Estos resultados ponen de manifiesto que la señal de suplantación de un AtoN puede resultar especialmente peligrosa si se recibe con mayor potencia que la de buques que se encuentren en la zona. Aun operando con una atenuación moderada, es capaz de ocupar el canal prácticamente al completo, reduciendo drásticamente la capacidad del receptor para decodificar tráfico legítimo. Pese a que estos mensajes se reciben cada 3 minutos, si el personal de puente no está atento a sus sistemas de monitorización, puede suponer un problema grave para la seguridad en la navegación.

4.1.4 PJ1 Jamming AWGN

Al igual que en PS3, se tomó como referencia la señal del "Sajabi" ya que era claramente la más estable en la zona. El ensayo se inició con una atenuación de -89 dB, valor mínimo permitido por el *jammer* en GNU-Radio, manteniéndose el comportamiento nominal del receptor. A partir de ese punto, se comenzó a reducir la atenuación en saltos de 10 dB.

No se vieron comportamientos extraños hasta alcanzar el nivel de -20 dB. En este punto, las señales más débiles comenzaban a desaparecer. Sin embargo, la señal de referencia persistía, siendo decodificada correctamente. A raíz de la observación de las primeras pérdidas, los saltos pasaron a ser de 5 dB para poder localizar con exactitud el punto de pérdida. Al alcanzar -5 dB de atenuación, se produjo la pérdida total del buque monitorizado. De esta manera el receptor había alcanzado su límite operativo frente a este tipo de interferencia. A partir de este umbral, deja de ser capaz de decodificar cualquier señal presente en la zona.

Se evidencia un comportamiento escalonado, empeorando la decodificación a mayor ruido interferente. Inicialmente, se produce una degradación de señales más débiles, seguida de la pérdida progresiva de las más fuertes hasta alcanzar el colapso total. De esta manera, se identifican dos umbrales característicos: uno de degradación parcial en torno a -20 dB y otro de fallo completo del sistema en torno a -5 dB.

4.1.5 PJ2 Recuperación del sistema

Una vez colapsado el sistema en PJ1 se procedió directamente a PJ2. Los resultados obtenidos mostraron una recuperación inmediata de la señal y decodificación del receptor. Todas las señales de la zona volvieron a ser decodificadas con normalidad. Esto indica, en este caso, que el efecto del *jamming* AWGN es reversible y no deja efectos persistentes ni apreciables en el funcionamiento del receptor.

4.1.6 Calificación final del receptor QK-A026

Escenario de prueba	Métrica principal	Puntuación (1-5)
PS1. Saturación con tipo 1	PER total	2
PS2. Saturación con tipo 5	PER total	4
PS3. Suplantación de AtoN	Reducción de tráfico legítimo	4
PJ1. *Jamming* AWGN	Atenuación de fallo completo	1
PJ2. Recuperación	Tiempo de recuperación	1
ÍNDICE FINAL	I_R	2,75

Tabla 4-3 Calificación final para el receptor QK-A026

Por lo tanto, como el índice obtenido se encuentra entre $2.6 \leq I_R \leq 3.5$, el nivel del receptor se determina como "Resiliencia Limitada". El sistema muestra debilidades a la hora de gestionar la memoria o priorizar la seguridad. Se genera un estado de incertidumbre en el OGP al no poder corroborar la validez de los blancos mostrados en sus pantallas de navegación.

4.2 Caracterización de la capacidad del transpondedor SIMRAD V5035

Un aspecto para tener en cuenta en esta prueba es que, a diferencia de las pruebas realizadas con el QK-A026, en este caso no se dispone de acceso a logs con las tramas NMEA. Por lo tanto, el análisis se basa en la información mostrada en pantalla por el transpondedor. Aunque el equipo dispone de un puerto USB, el fabricante especifica que está destinado únicamente a tareas de actualización, no permitiendo la extracción de datos. Además, tras la finalización de cada transmisión se deja un tiempo de espera para comprobar la cantidad de mensajes recibidos debido al tiempo de refresco de la interfaz.

Cabe destacar también que para evitar una sobrecarga en el dispositivo SDR utilizado, la función del transpondedor se cambia exclusivamente a recepción, para evitar una transmisión de 12,5 W de potencia no deseada que pueda romper el banco de pruebas.

4.2.1 PS1 Saturación con mensajes Tipo 1

En el primer ensayo, con el envío de 50 mensajes, no se registran pérdidas. El receptor es capaz de representar la totalidad de los blancos generados. Por lo tanto, bajo un nivel de carga bajo, el receptor no muestra ningún tipo de limitación.

$$PER_{50}(\%) = 0\%$$

Al aumentar la transmisión a 100 mensajes, comienzan a aparecer pérdidas muy puntuales y dispersas. El total de mensajes no recibidos es 2. El PER correspondiente es:

$$PER_{100}(\%) = \frac{100 - 98}{100} \times 100 = 2\%$$

El sistema sigue manteniendo un alto nivel de rendimiento, con pérdidas que no siguen ningún patrón aparente.

En la transmisión de 200 mensajes, el número de pérdidas se mantiene constante sin ser las mismas que previamente. En este caso el PER obtenido es:

$$PER_{200}(\%) = \frac{200 - 198}{200} \times 100 = 1\%$$

A pesar de duplicar la carga respecto a la prueba anterior, el número de pérdidas no varía, lo que indica que el transpondedor gestiona correctamente un incremento en el tráfico. Al reducirse el PER, se refuerza la idea de que las pérdidas no están directamente asociadas a la carga, sino al procesamiento interno.

Con la transmisión de 500 mensajes, se observa un ligero incremento en el número de pérdidas. En este caso se pierden 3 mensajes del total. El PER es:

$$PER_{500}(\%) = \frac{500 - 497}{500} \times 100 = 0{,}6\%$$

Nuevamente, disminuye el PER con unas pérdidas mínimas en relación con el volumen total de mensajes. Esto indica que el sistema no entra en un régimen de saturación claro.

La Tabla 4-4 muestra un resumen de los mensajes totales enviados, los perdidos y el PER para cada intervalo:

Totales	Perdidos	PER
50	0	0%
100	2	2%
200	2	1%
500	3	0,6%

Tabla 4-4 Resumen de la prueba PS1 para el receptor SIMRAD V5035

El análisis individual de cada transmisión confirma que las pérdidas aparecen a partir de cierto nivel de carga y se mantienen muy contenidas. No se aprecia relación lineal entre número de mensajes y pérdidas, lo que presenta un comportamiento muy estable y eficiente por parte del receptor.

El PER total para la prueba utilizado para la posterior calificación del receptor es el siguiente:

$$PER_{TOTAL}(\%) = \frac{850 - 843}{850} \times 100 = 0{,}8\%$$

4.2.2 PS2 Saturación con mensajes Tipo 5

En el primer ensayo de 50 mensajes decodificó correctamente 44. El PER obtenido en esta prueba es:

$$PER_{50}(\%) = \frac{50 - 44}{50} \times 100 = 12\%$$

En cargas bajas ya se observa un nivel de pérdidas significativo pero muy inferior a aquel del QK-A026. Pese al tamaño y sensibilidad de los mensajes tipo 5, es un valor aceptable.

Con la transmisión de 100 mensajes, el sistema es capaz de decodificar un total de 91 mensajes. Por lo tanto su PER es:

$$PER_{100}(\%) = \frac{100 - 91}{100} \times 100 = 9\%$$

Se aprecia una mejora relativa con respecto al caso anterior pese al número de pérdidas.

Al aumentar a 200 mensajes la transmisión, el sistema no es capaz de decodificar 20 mensajes. Por lo tanto, su PER en este caso es:

$$PER_{200}(\%) = \frac{200 - 180}{200} \times 100 = 10\%$$

El PER vuelve a aumentar relativamente pero se mantiene cercano a los calculados previamente. Esto indica que el transpondedor se comporta de forma bastante estable.

Con la última transmisión de 500 mensajes el transpondedor decodifica correctamente 459. El PER es:

$$PER_{50}(\%) = \frac{500 - 459}{500} \times 100 = 8{,}2\%$$

Pese a ser el escenario más exigente, el PER se mantiene en torno al 8%, sin degradación significativa respecto a cargas menores.

Totales	No decodificados	PER
50	6	12%
100	9	9%
200	20	10%
500	41	8,2%

Tabla 4-5 Resumen de la prueba PS2 para el receptor SIMRAD V5035

El PER total para la prueba utilizado para la posterior calificación del receptor es el siguiente:

$$PER_{TOTAL}(\%) = \frac{850 - 774}{850} \times 100 = 8{,}9\%$$

Está claro que la estructura de los mensajes de tipo 5 supone una limitación en la decodificación por parte del transpondedor. Pese a ello, el comportamiento es estable y predecible, con un PER aproximadamente constante que varía entre un 8,2% y un 12%. Esto sugiere que existe un cuello de botella en la capacidad del transpondedor para procesar correctamente mensajes de tamaño considerable que ocupan varios *slots*.

4.2.3 PS3 Suplantación de AtoN

Durante la realización de la prueba se observó un comportamiento análogo al descrito en 4.1.3, aunque con una degradación mayor. Durante el primer minuto de observación, se recibieron hasta 6 mensajes procedentes del "Sajabi" situado a una distancia de 0,4 mn, igual que en el apartado 4.1.3. Al iniciar la fase de ataque mediante la transmisión del mensaje tipo 21 correspondiente al Faro de Ons, sin variar los -30 dB de atenuación, se produjo una reducción clara en la capacidad de recepción del sistema. El número de mensajes decodificados final fue de 3, reduciendo a la mitad la cantidad esperada.

El resultado obtenido evidencia que el transpondedor presenta una sensibilidad significativa frente a una ocupación del canal. La disminución observada confirma que, incluso con niveles de potencia moderados y respetando la temporización TDMA, la inyección de una traza fija ficticia que, a primera vista puede resultar legítima, compromete la visibilidad del entorno por parte del sistema.

4.2.4 PJ1 Jamming AWGN

Para realizar la prueba se tomó nuevamente el "Sajabi" debido a que presentaba la señal más fuerte y persistente de la zona. El ensayo comenzó con una atenuación de -89 dB, y a partir de ahí se incrementó la interferencia en saltos de 10 dB. Entre -89 dB y -50 dB no se apreciaron alteraciones significativas en el comportamiento del sistema, mostrando con normalidad el tráfico de la zona.

Al alcanzar una atenuación de -40 dB se empezaron a observar las primeras pérdidas de las señales más débiles. Sin embargo, la señal del pesquero se mantenía visible, confirmando que las transmisiones con mayor nivel recibido seguían siendo decodificadas, lo cual indicaba que todavía no se había llegado al límite del transpondedor. Finalmente, al alcanzar una atenuación de -35 dB, el sistema dejó de recibir señal válida. A partir de ese nivel, la interferencia resultó suficiente para provocar la pérdida completa de la recepción AIS.

Los resultados obtenidos muestran un comportamiento progresivo y coherente frente a *jamming* AWGN. El transpondedor es capaz de mantener una recepción estable mientras la potencia interferente mantiene niveles moderados. Esto refleja que el impacto no es ni inmediato ni uniforme sobre todos los objetivos, sino que elimina del mapa los más débiles en una primera instancia.

4.2.5 PJ2 Recuperación del sistema

Una vez alcanzado el colapso durante PJ1, se procedió de forma inmediata a la ejecución de PJ2. La recuperación fue instantánea tras el cese de la interferencia. Todas las tramas volvieron a ser procesadas con normalidad, restableciéndose el funcionamiento habitual del equipo sin necesidad de reinicio ni intervención adicional, confirmando que el efecto del *jamming* en el Simrad es completamente reversible.

4.2.6 Calificación final del transpondedor SIMRAD V5035

Escenario de prueba	Métrica principal	Puntuación (1-5)
PS1. Saturación con tipo 1	PER total	1
PS2. Saturación con tipo 5	PER total	3
PS3. Suplantación de AtoN	Reducción de tráfico legítimo	4
PJ1. *Jamming* AWGN	Atenuación de fallo completo	3
PJ2. Recuperación	Tiempo de recuperación	1
ÍNDICE FINAL	I_R	2,4

Tabla 4-6 Calificación final para el receptor SIMRAD V5035

Por lo tanto, como el índice obtenido se encuentra entre $1.6 \leq I_R \leq 2.5$, el nivel del receptor se determina como "Resiliencia Estándar". El comportamiento es adecuado para la navegación. Presenta degradaciones leves que no afectan a la conciencia situacional.

4.3 Caracterización de la capacidad del transpondedor FURUNO FA-170

4.3.1 PS1 Saturación con mensajes Tipo 1

En el primer ensayo, con la transmisión de 50 mensajes, se registraron tres pérdidas. El receptor es capaz de decodificar prácticamente la totalidad de los mensajes. El PER es el siguiente:

$$PER_{100}(\%) = \frac{50 - 47}{50} \times 100 = 6\%$$

En la transmisión de 100 mensajes, se registraron 3 pérdidas. El PER correspondiente para este caso es:

$$PER_{100}(\%) = \frac{100 - 97}{100} \times 100 = 3\%$$

Se puede considerar que el comportamiento del receptor es correcto, ya que la degradación es mínima.

En la transmisión de 200 mensajes, el número de pérdidas ascendió a 30. En este caso el PER obtenido es:

$$PER_{200}(\%) = \frac{200 - 170}{200} \times 100 = 15\%$$

Se aprecia un empeoramiento notable respecto a los casos anteriores. El aumento de pérdidas no es lineal, lo que sugiere que entra en una zona de funcionamiento poco estable cuando la secuencia transmitida se prolonga en el tiempo.

Con la transmisión de 500 mensajes, se observaron 44 pérdidas. El PER es:

$$PER_{500}(\%) = \frac{500 - 456}{500} \times 100 = 8{,}8\%$$

El PER obtenido muestra que la degradación en la recepción no muestra una tendencia estrictamente creciente en porcentaje.

La Tabla 4-7muestra un resumen de los mensajes totales enviados, los perdidos y el PER para cada intervalo:

Totales	Perdidos	PER
50	3	6%
100	3	3%
200	30	15%
500	44	8,8%

Tabla 4-7 Resumen de la prueba PS1 para el receptor FURUNO FA-170

Los resultados muestran un comportamiento sólido en transmisiones cortas. Sin embargo, con el aumento de la carga, se alcanza un PER del 15%. Ya que el PER disminuye para una carga superior, no puede hablarse de un deterioro proporcional al volumen transmitido. El transpondedor tolera bien cargas moderadas, pero el rendimiento bajo cargas de mayor volumen no es completamente uniforme. Posiblemente internamente el equipo no sea capaz de gestionar cargas elevadas en una recepción sostenida.

El PER total para la prueba utilizado para la posterior calificación del receptor es el siguiente:

$$PER_{TOTAL}(\%) = \frac{850 - 770}{850} \times 100 = 9{,}4\%$$

4.3.2 PS2 Saturación con mensajes Tipo 5

Los resultados de esta prueba fueron especialmente llamativos. En condiciones de baja carga, el sistema únicamente fue capaz de decodificar 3 mensajes, una cifra claramente inferior a la esperada teniendo en cuenta que el canal no se encontraba saturado pues no recibía señal del exterior. El comportamiento no solo se mantuvo al incrementar la carga, sino que en algunos casos se observó incluso una reducción en el número de mensajes decodificados correctamente. Por este motivo se descartó una relación directa entre el aumento de tráfico y el mayor número de mensajes decodificados.

Al transmitir 500 mensajes, el receptor alcanzó un máximo de 10 mensajes decodificados. Aunque supone una mejora, sigue siendo un rendimiento muy malo en comparación con los otros equipos analizados. Esto sugiere que, internamente, el receptor posiblemente aplique algún tipo de filtrado, priorización o limitación en la gestión de mensajes de mayor tamaño.

A la vista de los resultados, se consideró la posibilidad de que la limitación estuviese asociada al tiempo de refresco de la interfaz de visualización del equipo. Para descartar esta hipótesis y confirmar verdaderamente cuantos mensajes decodificaba se implementó un montaje orientado a la captura de las sentencias NMEA generadas por el equipo. El procedimiento consistió en conectar el portátil mediante Ethernet al transpondedor, empleando un servidor de Signal K capaz de recibir las tramas NMEA 2000 que enviaba el sistema para su posterior conversión a Signal K. Posteriormente, ajustando los parámetros de recepción en OpenCPN se observaban los mensajes recibidos, independientemente de cualquier limitación de la pantalla del receptor. Sin embargo, los resultados obtenidos mediante este método fueron prácticamente idénticos con los observados previamente, confirmando que las pérdidas no estaban asociadas a la visualización, sino al propio proceso interno del transpondedor.

Por tanto, para poder evaluar de manera objetiva y correcta, sería necesario realizar un estudio específico de sus capacidades. Solo a partir de ese análisis sería posible adaptar el protocolo experimental y obtener resultados representativos del rendimiento real del sistema y poder compararlo con el resto.

4.3.3 PS3 Suplantación de AtoN

La realización de esta prueba arrojó unos resultados que siguieron una tendencia muy similar a la obtenida en PS2. El sistema no llegó a decodificar ningún mensaje de tipo 21 en ningún escenario de carga, independientemente de la intensidad de transmisión, separación entre envíos o condiciones del canal. Resulta especialmente significativo ya que se descarta que el problema esté relacionado con la saturación del canal o limitaciones puntuales de procesamiento. Puede resultar que el receptor presente un comportamiento algo más determinista en la recepción de mensajes de tipo 21.

Una posible explicación radica en el propio tamaño y estructura de los mensajes de tipo 21 al ocupar más de un slot TDMA, al igual que los mensajes de tipo 5. No se debe descartar tampoco la posibilidad de que el receptor implemente algún mecanismo de validación o filtrado, aun así, no se puede confirmar.

Por tanto, al igual que en PS2, se refuerza la idea de que el receptor no procesa todos los tipos de mensajes de manera homogénea. Nuevamente, para realizar esta prueba, sería necesario un análisis previo de capacidades del sistema a estudiar.

4.3.4 PJ1 Jamming AWGN

Nuevamente se tomó como referencia la señal del pesquero "Sajabi", situado a 0,4 mn. El procedimiento comenzó en el mismo valor que el resto de PJ1 realizadas. Se apreció que la recepción se mantenía sin cambios especiales hasta alcanzar los -50 dB, cuando la señal del pesquero se perdió por completo.

Para identificar con mayor precisión el nivel a partir del cual comenzaban a desaparecer las señales más débiles de la zona, se fue incrementando la atenuación en saltos de 1 dB. Esa comprobación permitió observa que las primeras pérdidas se producían en torno a los -55 dB. El comportamiento observado muestra una degradación progresiva conforme aumenta la interferencia.

4.3.5 PJ2 Recuperación del sistema

Tras el colapso del sistema en PJ1 se comprueba el tiempo de recuperación del sistema. El transpondedor volvió a su régimen de decodificación normal de forma prácticamente inmediata, sin necesidad de realizar ajustes adicionales ni observarse efectos residuales en el sistema.

4.3.6 Calificación final del transpondedor FURUNO FA-170

Escenario de prueba	Métrica principal	Puntuación (1-5)
PS1. Saturación con tipo 1	PER total	3
PS2. Saturación con tipo 5	PER total	-
PS3. Suplantación de AtoN	Reducción de tráfico legítimo	-
PJ1. *Jamming* AWGN	Atenuación de fallo completo	5
PJ2. Recuperación	Tiempo de recuperación	1
ÍNDICE FINAL	I_R	3,3

Tabla 4-8 Calificación final para el receptor FURUNO FA-170

Por lo tanto, como el índice obtenido se encuentra entre $2.6 \leq I_R \leq 3.5$, el nivel del receptor se determina como "Resiliencia Limitada". El sistema muestra debilidades a la hora de gestionar la

memoria o priorizar la seguridad. Se genera un estado de incertidumbre en el oficial de guardia al no poder corroborar la validez de los blancos mostrados en sus pantallas de navegación.

5 CONCLUSIONES Y LÍNEAS FUTURAS

En este capítulo se recogen las conclusiones derivadas de la puesta a prueba del protocolo propuesto, desarrollando el cumplimiento de los objetivos generales y específicos. Asimismo, se proponen líneas futuras de trabajo orientadas a ampliar el alcance del estudio.

5.1 Conclusiones

El presente Trabajo de Fin de Grado ha permitido desarrollar un entorno experimental basado en SDR capaz de generar tráfico AIS controlado para someter a distintos receptores al protocolo de pruebas propuesto. Las pruebas estaban orientadas a evaluar la resiliencia de equipos AIS frente a *jamming* y *spoofing*, trasladando el análisis de vulnerabilidades a un plano práctico. Este planteamiento es la respuesta directa al objetivo general definido al inicio del trabajo.

En relación con los objetivos específicos, se ha logrado diseñar y validar un banco de pruebas funcional. Se realizaron comprobaciones sobre la generación, temporización y transmisión de mensajes, reproduciendo de forma coherente el comportamiento esperado en TDMA. De esta manera se permite atribuir las pérdidas al receptor estudiado y no al sistema generador. Los resultados mostraron que el comportamiento de los receptores estudiados no es homogéneo.

Asimismo, se ha cumplido el objetivo de definir un protocolo de pruebas capaz de evaluar distintos vectores de ataque: saturación mediante carga, suplantación y *jamming*. La aplicación del protocolo en tres receptores diferentes ha permitido obtener métricas comparables. El comportamiento del Furuno FA-170 frente a los ensayos PS2 y PS3 no sigue un patrón asociado a la carga transmitida, lo que apunta a la posible existencia de mecanismos internos de filtrado u otros factores. Se introduce así una limitación importante: el protocolo no puede aplicarse de forma directa y universal a cualquier receptor sin tener en cuenta su arquitectura interna. En este sentido, se puede afirmar que se han cumplido los objetivos planteados al inicio del trabajo. Se ha definido un protocolo de evaluación orientado a analizar la resiliencia de los receptores, se han establecido métricas de evaluación y se ha validado su aplicación sobre equipos reales.

Por tanto, la principal conclusión del trabajo es que el protocolo debe entenderse como una estructura base, no como una herramienta universal en su forma actual. Para la obtención de resultados representativos de cada unidad estudiada, es imprescindible realizar previamente un estudio de capacidades de cada receptor, identificando sus restricciones internas a partir de su funcionamiento. Solo a partir de la caracterización de cada uno es posible adaptar las pruebas y obtener resultados fiables.

Desde un punto de vista operativo, el trabajo refuerza la idea de que el AIS no debe considerarse una fuente única de información. La posibilidad de degradación en entornos de amenaza mediante

interferencia o suplantación junto con la variabilidad en el comportamiento de los receptores obliga a complementar su uso con otros sistemas e interpretar los datos obtenidos con criterio.

Del análisis global de los resultados se obtiene que las limitaciones más críticas aparecen en escenarios de *spoofing*, donde la carga del sistema e integridad de la información se ven comprometidas. Por el contrario, el *jamming* afecta de manera progresiva en función del nivel de interferencia.

En conjunto, se demuestra que es posible analizar de forma objetiva la resiliencia de receptores AIS mediante tecnología SDR, evidenciando limitaciones relevantes en equipos reales. Por ello es necesario integrar este tipo de protocolos en procesos de validación y adquisición de sistemas en el ámbito naval.

5.2 Líneas futuras

Como continuación del trabajo, se proponen las siguientes líneas futuras:

- Incorporación de una fase de caracterización previa: Trata de analizar individualmente cada receptor para determinar sus capacidades reales antes de la ejecución de las pruebas. De esta manera se podría implementar el protocolo adaptado a cada equipo y garantizar la validez de los resultados.
- Desarrollo de una aplicación automatizada de ejecución del protocolo: Consiste en la creación de una herramienta software que permite analizar el protocolo de forma automatizada. Partiría de una base de datos en la que se recogen las características y limitaciones de cada equipo, incorporando así la fase de caracterización mencionada previamente.
- Ampliación del número de receptores ensayados: Por el tiempo relativamente reducido disponible para la ejecución del protocolo en un número elevado de receptores, se busca extender las pruebas a equipos de otros fabricantes para así identificar patrones comunes, validar la generalidad del enfoque propuesto y detectar posibles tendencias en el diseño de receptores.
- Ampliación del catálogo de ensayos: Busca incorporar nuevos escenarios, como combinaciones de saturación e interferencia, variaciones más finas de potencia o pruebas selectivas por tipo de mensaje, permitiendo así la aproximación del banco de pruebas a condiciones más realistas si cabe.
- Desarrollo de una base de datos global de MMSI: Se plantea la creación de un sistema centralizado donde se registren los MMSI de cada buque que permita el acceso de los receptores a ella para verificar la autenticidad de los mensajes. Podría contribuir a la mitigación de ataques de *spoofing* mediante la validación externa de identidad.
- Integración con otros sistemas: Consiste en el estudio de viabilidad de desarrollar mecanismos de validación cruzada que permitan detectar incoherencias y aumentar la robustez frente a manipulaciones teniendo en cuenta la integración del AIS con otros sistemas de navegación.

6 BIBLIOGRAFÍA

[1] International Maritime Organization, «MSC.1/Circ.1595 - E-navigation Strategy Implementation Plan - Update 1,» Londres, 2018.

[2] European Network and Information Security Agency, «Analysis of cyber security aspects in the maritime sector,» 2011.

[3] Naciones Unidas, «Review of maritime transport 2025,» Nueva York, 2025.

[4] UK Maritime and Coastguard Agency, «MGN 379 (M+F) Amendment 1 - Use of Electronic Navigational Aids,» 2024.

[5] International Maritime Organization, «International Convention for the Safety of Life at Sea (SOLAS),» Londres, 1974.

[6] International Telecommunication Union, «Recommendation ITU-R M.1371-6: Technical characteristics for VHF automatic identification system using time division multiple access in the maritime mobile service,» Ginebra, 2026.

[7] International Association of Marine Aids to Navigation and Lighthouse Authorities, «An overview of AIS,» G1082, 2016.

[8] M. Balduzzi, A. Pasta y K. Wilhoit, «A Security Evaluation of AIS Automated Identification System,» Proceedings of the 30th Annual Computer Security Applications Conference, 2014.

[9] D. Dalaklis y M. Baldauf, «Automatic Identification System: Identifying Potential Security Threats,» World Maritime University, Malmö, 2017.

[10] International Maritime Organization, «Resolution MSC.74(69): Adoption of New and Amended Performance Standards for Navigational Equipment,» Londres, 1998.

[11] UK Hydrographic Office, «Jamming and spoofing,» ADMIRALTY Maritime Safety Information, 11 Agosto 2025. [En línea]. Available: https://www.admiralty.co.uk/news/jamming-and-spoofing. [Último acceso: 9 Marzo 2026].

[12] INTERTANKO, «Jamming and Spoofing of Global Navigation Satellite Systems (GNSS),» 2nd ed., 2025.

[13] S. Mendes, S. Amado, V. Teresa, A. Scorzolini, V. de Perini y A. Sorbo, «Satellite AIS - an End-to-End Simulation Approach,» Noordwijk, 2010.

[14] International Maritime Organization, «Resolution MSC.246(83): Adoption of the Performance Standards for Survival Craft Automatic Identification System Search and Rescue Transmitters (AIS-SART),» Londres, 2007.

[15] International Maritime Organization, «Resolution MSC.471(101): Performance Standards for AIS Locating Devices (AIS-MOB),» Londres, 2019.

[16] A. Androjna, M. Perkovic, I. Pavic y J. Miškovic, «AIS Data Vulnerability Indicated by a Spoofing Case-Study,» Appl. Sci. 2021, 11, 5015, Basilea, 2021.

[17] International Telecommunication Union, «Radio regulations,» 2024.

[18] International Telecommunication Union, «Recommendation ITU-R M.1842-1: Characteristics of VHF maritime mobile band communications,» Ginebra, 2009.

[19] International Telecommunication Union, «Recommendation ITU-R M.2231: Use of Appendix 18 to the Radio Regulations for the maritime mobile service,» Ginebra, 2012.

[20] International Telecommunication Union, «Recommendation ITU-R M.1084-5: Interim solutions for improved spectrum efficiency in the band 156-174 MHz used by the maritime mobile service,» Ginebra, 2012.

[21] International Telecommunication Union, «Recommendation ITU-R P.1546-6: Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 3 000 MHz,» Ginebra, 2019.

[22] International Telecommunication Union, «Recommendation ITU-R P.372-17: Radio noise,» 2021.

[23] Bimco et al., «The Guidelines on Cyber Security Onboard Ships,» Version 5, 2024.

[24] International Electrotechnical Commission, «Maritime navigation and radiocommunication equipment and systems - Automatic identification system (AIS) - Part 2: Class A shipborne equipment,» IEC 61993-2, 2018.

[25] International Telecommunication Union, «Recommendation ITU-R P.526-16: Propagation by diffraction,» Ginebra, 2025.

[26] Council of the European Union, «European Union Maritime Security Strategy,» Bruselas, 2014.

[27] NATO, «Operation Sea Guardian,» NATO, 26 Mayo 2023. [En línea]. Available: https://www.nato.int/en/what-we-do/operations-and-missions/operation-sea-guardian. [Último acceso: 4 Febrero 2026].

[28] SAAB, «La Guardia Costera Helénica elige a Saab para proteger sus fronteras,» 2023. [En línea]. Available: https://www.saab.com/es/markets/spain/press-releases/la-guardia-costera-helenica-elige-a-saab-para-proteger-sus-fronteras. [Último acceso: 13 Febrero 2026].

[29] SAAB, «R6 Supreme AIS/VDES,» Datasheet, Linköping.

[30] Inside GNSS, «Inside GNSS,» 2 Marzo 2026. [En línea]. Available: https://insidegnss.com/gnss-interference-complicates-navigation-as-hormuz-shipping-disruption-deepens/. [Último acceso: 11 Marzo 2026].

[31] BBC, «BBC,» 2 Marzo 2026. [En línea]. Available: https://www.bbc.com/mundo/articles/c86yv180qgxo. [Último acceso: 11 Marzo 2026].

[32] Descifrando la Guerra, «Descifrando la Guerra,» 8 Marzo 2026. [En línea]. Available: https://www.descifrandolaguerra.es/claves-guerra-de-iran/. [Último acceso: 11 Marzo 2026].

[33] Royal Institute of Navigation, «Impacts of GNSS Interference on Maritime Safety,» 2026.

[34] International Telecommunication Union, «Maritime Mobile Service (MARS),» ITU-R, [En línea]. Available: https://www.itu.int/pub/r-soft-mars/es. [Último acceso: 13 Febrero 2026].

[35] Quark-Elec, «A024/26 Manual: Wireless AIS + GPS Receiver with NMEA Multiplexer + WiFi,» 2025.

[36] SIMRAD, «V5035 Class A/Inland AIS,» Operator and Installation Manual, 2013.

[37] Furuno Electric Co., Ltd., «AIS Transponder FA-170 Operator's Manual,» 2015.

[38] «RTL-SDR Blog V4 Datasheet».

[39] Analog Devices, «ADALM-PLUTO SDR Active Learning Module,» Datasheet, Norwood, 2017.

[40] Mini-Circuits, «ZX10-2-20-S+: 2-Way Power Splitter/Combiner, 200 to 2000 MHz, Technical Datasheet,» 2023.

ANEXO I: IMPLICACIONES SOCIALES, Y/O ECONÓMICAS, Y/O AMBIENTALES

Las implicaciones de este TFG trascienden en gran parte en el ámbito técnico, al centrarse en la propuesta de un protocolo de pruebas estandarizado para buques de la Armada. La correcta evaluación del comportamiento de estos equipos frente a perturbaciones contribuye de manera directa a mejorar la fiabilidad de uno de los sistemas fundamentales para la conciencia situacional, pero a su vez uno de los más vulnerables.

Desde el punto de vista social, el AIS supone una herramienta clave para la seguridad, al prevenir colisiones y apoyar la gestión del tráfico y operaciones SAR. Una manipulación deliberada de las señales AIS, la cual pueda degradar el funcionamiento del sistema, puede generar situaciones de riesgo. Con la existencia de protocolos de prueba estandarizados que permitan evaluar la resiliencia de los receptores/transpondedores frente a ese tipo de situaciones mejora la confianza en los equipos instalados, reforzando la seguridad en la navegación.

Con la documentación de numerosos incidentes de manipulación de señales de posicionamiento y tráfico marítimo, en la que buques aparecen desplazados de su posición real o agrupados en patrones anómalos en diferentes regiones estratégicas, se pone de manifiesto la necesidad de estandarizar un protocolo de pruebas para receptores AIS. Los fenómenos se asocian normalmente a interferencias sobre GNSS o la propia generación de mensajes AIS falsos, demostrando que los sistemas actuales son vulnerables, justificando de esta manera la necesidad de desarrollar metodologías que permitan evaluar de forma objetiva cada receptor. Por lo tanto, la propuesta de un protocolo capaz de reproducir escenarios de saturación, manipulación o interferencia permite analizar de forma controlada el comportamiento de los receptores/transpondedores instalados en los buques de la Armada. Con la obtención de métricas objetivas se facilita la comparación entre qué equipos tienen un mayor grado de resiliencia, sirviendo como base para futuras recomendaciones técnicas o procedimientos de certificación.

Desde una perspectiva tecnológica, el establecimiento de procedimientos de prueba permite identificar limitaciones en los equipos actuales instalados en los diferentes barcos. Partiendo de esa base, se puede orientar al desarrollo de futuras generaciones de receptores más avanzados que sean robustos frente a escenarios de *jamming* y *spoofing*.

Desde el punto de vista económico, un funcionamiento correcto y fluido del transporte marítimo depende en gran parte de la integridad del AIS. La manipulación deliberada puede acarrear daños colaterales en la planificación de derrotas o en los sistemas de monitorización que emplean las autoridades marítimas. El hecho de que un mercante se vea obligado a alterar su derrota debido a un evento de *spoofing* masivo puede conllevar grandes pérdidas económicas, ya no solo para la naviera sino a nivel global.

Aunque el impacto ambiental en el contexto de este TFG es indirecto, una mejora en la fiabilidad de los sistemas de vigilancia instalados a bordo contribuye a la prevención de accidentes que puedan derivar en daños al medio marino. Con una reducción o menor probabilidad de colisiones o encallamientos, entre otros, se obtiene un efecto positivo en la protección del entorno marítimo, especialmente en áreas protegidas o en proximidades de estructuras costeras.

En conjunto, el desarrollo de metodologías que permitan evaluar de manera objetiva la resiliencia de los sistemas AIS frente a perturbaciones intencionadas provenientes de terceros, constituye una contribución relevante tanto técnicamente como en una perspectiva más amplia de seguridad marítima, eficiencia operativa y protección del entorno.

ANEXO II: REFLEXIONES ÉTICAS Y SOCIALES

El presente anexo describe las reflexiones éticas y sociales derivadas del TFG que se vinculan de manera directa al uso fiable de sistemas de navegación y vigilancia marítima.

El trabajo desarrolla un protocolo de pruebas que implica manejar datos de posicionamiento, generación de mensajes y simulación de escenarios que podrían emplearse con fines maliciosos. Por ello, en todo momento, el trabajo se orienta hacia la mejora de seguridad y prueba de robustez de los sistemas evitando comprometer la integridad del tráfico marítimo, realizando las pruebas en entornos controlados.

Éticamente resulta especialmente relevante considerar las tecnologías empleadas para el desarrollo del trabajo. Los sistemas SDR o las herramientas de generación de señales RF, junto con los códigos generadores de mensajes AIS, pueden utilizarse tanto con fines de investigación como perjudiciales. Por ello, el uso de estos medios se ha realizado exclusivamente en entornos controlados, tanto en los laboratorios del Centro Universitario de la Defensa como en las lanchas de instrucción de la Escuela Naval Militar, evitando en todo momento cualquier interferencia con sistemas reales de operación.

Socialmente se pone de manifiesto la importancia del papel de los profesionales en el diseño y validación de los equipos. Los desarrolladores de estas tecnologías deberán comprender las debilidades de un sistema para identificar puntos de mejora y orientar el desarrollo de soluciones más robustas. Por ello, el estudio que se realiza en este TFG no debe interpretarse como una forma de explotar debilidades, sino como un paso para mejorar los sistemas de navegación en los que se apoyan los marinos de hoy en día. Esto no exime al encargado de la navegación de supervisar de manera efectiva sus equipos ya que la confianza excesiva en este tipo de sistemas automatizados puede generar una falsa sensación de seguridad, por ello se deberá mantener siempre una actitud crítica frente a las limitaciones de las herramientas utilizadas.

En conjunto, el presente trabajo trata de evidenciar la necesidad de abordar el desarrollo tecnológico y el uso de los equipos de apoyo desde una perspectiva ética y responsable. Por ello el análisis de vulnerabilidades y evaluaciones experimentales a sistemas como el AIS deben orientarse hacia la mejora de su fiabilidad y seguridad, contribuyendo a un uso responsable de las herramientas disponibles en el ámbito marítimo.

ANEXO III: TDMA

El presente anexo describe el mecanismo empleado por el sistema AIS de acceso múltiple por división en el tiempo. Esto permite que múltiples estaciones compartan el canal VHF sin interferirse entre sí. No es necesaria una entidad central de control pues el acceso se realiza de forma autoorganizada.

El funcionamiento se divide de la siguiente manera: una trama completa tiene una duración de un minuto, dividiéndose esta en 2.250 intervalos (conocidos como *slots*). Por lo tanto, cada slot tiene una duración de 26,67 ms y, cada transmisión, ocupa por defecto un único slot. Para que el sistema función, es necesario que las estaciones estén sincronizadas temporalmente. Por ello, sistemas incorporan receptores GNNS que proporcionan la referencia de tipo UTC.

Cada slot contiene información necesaria para una transmisión completa, con una estructura típica de preámbulo para sincronización, una bandera de inicio, el campo de datos, CRC, bandera de fin y un margen temporal destinado a compensar retardos y posibles errores de sincronización. El acceso a los *slots* es dinámico pues cada estación cuenta con un mapa interno del estado del canal, identificando qué intervalos están libres, ocupados o reservados.

Al iniciarse, una estación escucha el canal durante un minuto aproximadamente para identificar la actividad existente. A partir de ahí selecciona sus *slots* de transmisión y anuncia sus futuras ocupaciones para permitir una correcta coordinación. TDMA permite que un gran número de estaciones AIS compartan el canal VHF de forma eficiente mediante una organización temporal basada en una sincronización común.

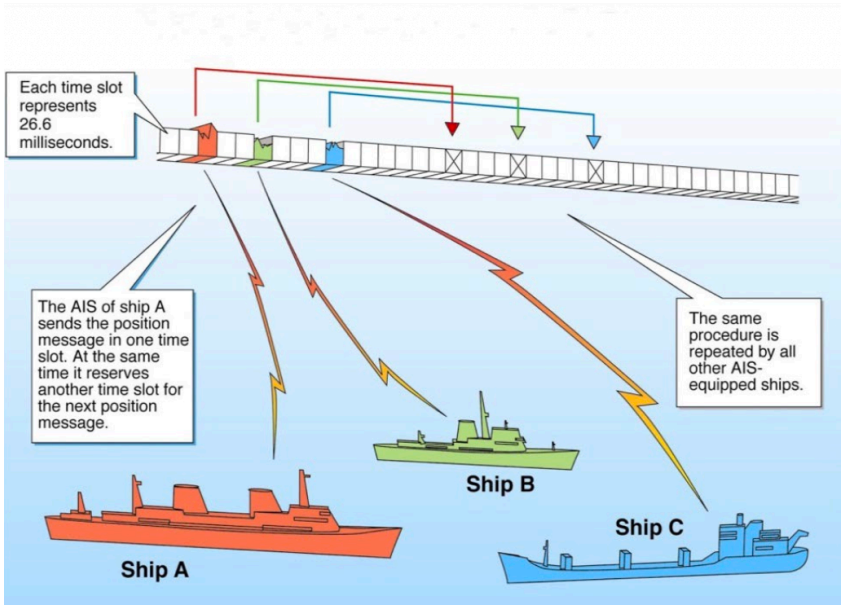


Figura A3-1 Protocolo de transmisión de mensajes AIS (Fuente: [7])

ANEXO IV: FICHAS TÉCNICAS DE LOS RECEPTORES

Receptor QK-A026

1. Introduction

1.1. What is AIS?

The marine Automatic Identification System (AIS) is a location and vessel information reporting system. It allows vessels equipped with AIS to automatically and dynamically share and regularly update their position, speed, course and other information such as vessel identity with similarly equipped vessels. Position is derived from the Global Positioning System (GPS) and communication between vessels is by Very High Frequency (VHF) digital transmissions. There are a number of types of AIS device, like Class A transceivers, Class B transceivers/transponders, AIS base stations, Aids to Navigation (AtoN) and AIS receivers.

1.2. The A024/26

The A024/26 is a compact dual channel, marine AIS receiver which can receive information from both AIS frequencies simultaneously.

A024/26 is aimed at the small-commercial, leisure, fishing boat and vessel monitoring markets. Connected to an on-board PC running compatible software, or a chart plotter, AIS data transmitted from ships within range will be displayed on the screen enabling the skipper or navigator to visualize the traffic within VHF range. Using A024/26 can enhance safety at sea by providing proximity, size and directional information from other vessels, improve safety and efficiency in navigation and help protect the marine environment.

It also combines one external NMEA 0183 data source with the AIS and GPS (GPS-A026 only) messages. This single data stream is then transmitted synchronously via NMEA 0183, USB and WiFi. The A026 model includes an integrated GPS module, this provides GPS data to all outputs when it is connected to a GPS antenna (SMA connection type).

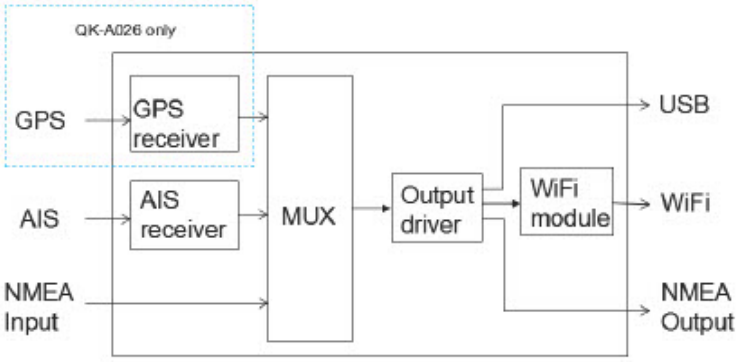


Figure 1: A024/26 Function diagram

1.3. Products covered by this manual

Part No	Description
A024	WiFi Dual channel AIS receiver
A026	WiFi Dual channel AIS receiver with built-in GPS receiver

The only difference between A024 and A026, is that the A026 includes a GPS module (while the A024 does not). All references to GPS throughout the manual refer to the A026. All other specifications and functionality apply to both the A024 and A026.

2. Connections

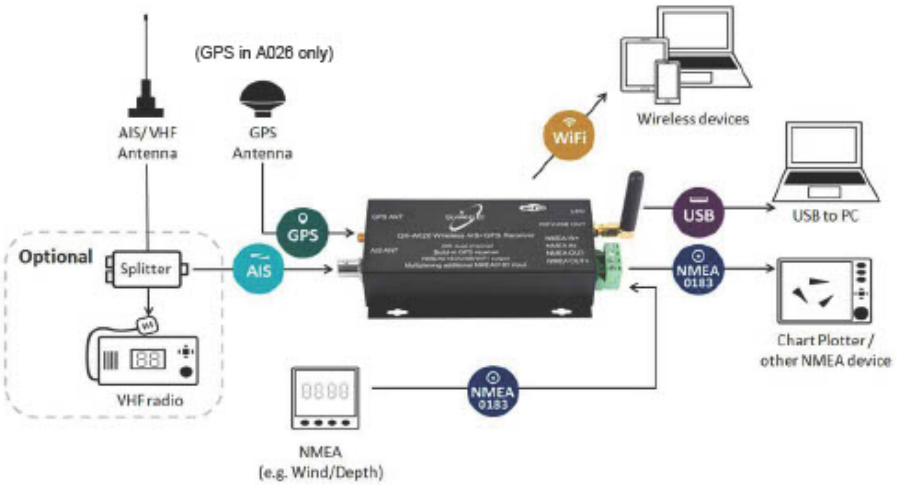


Figure 2: Typical system connection

The A024/26 multiplexer has the following options for connection to inputs, outputs and host devices.

- **AIS antenna connector.** Standard BNC female 50 Ohm connector. An active VHF antenna splitter is required if one VHF antenna is shared by A024/26 and VHF voice radio. (We recommend separate antennas ideally.)
- **GPS connector (A026 only).** Standard SMA female 50 Ohm connector for GPS antenna. An integrated GPS module supplies positional data provided a GPS antenna is connected. GPS information can be output via WiFi, USB or NMEA.
- **NMEA 0183 input/output connectors**. A024/26 can be connected to other AIS compatible equipment, like wind/depth or heading sensors, via the NMEA inputs. The NMEA 0183 messages from these devices can be multiplexed with A024/26 AIS+GPS messages and then sent out through NMEA 0183 to a chartplotter or other NMEA device.
- **USB connector.** A micro USB (type C) connector supplies power to the unit and also outputs the NMEA messages. It can also be used for adjusting parameters using the Configuration software.
- **WiFi.** Connectivity in both Ad-hoc and Station Modes on 802.11 b/g/n provides WiFi output of all messages.
- **LED lights**. A024/26 features three LEDs which indicate power, AIS and GPS status respectively. Three LEDs turn on and then off after initialization. When operating, these LEDs flash. See LED section for more LED information.

Transpondedor SIMRAD V5035

5 Technical specifications

Applicable standards

IMO Resolution A694(17)	IEC 61993-2 Ed. 2.0, 2012
IMO Resolution MSC.74(69) Annex 3	IEC 61108-1 Ed. 2.0, 2003
IMO Resolution MSC. 191(79)	IEC 60945 Ed. 4.0, 2002 incl. Corr. 1 2008
ITU-R M 1371-4 (Class A), 2010	IEC 61162-1 Ed. 4.0, 2010
ITU-R M 825-3, 1998	IEC 61162-2 Ed. 1.0, 1998
ITU-R M 1084-5, 2012	IEC 62288 Ed. 2.0, 2014
CCNR test standard for Inland AIS, edition 2.0 (October 2012)	

VHF transceiver

Frequency Range	156.025 MHz ~ 162.025 MHz
Channel Bandwidth	25 KHz
Modulation	GMSK / FM
Data Rate	9,600 bps
Number of AIS Transmitter	1
Number of AIS Receiver	2
Number of DSC Receiver	1
AIS Channel 1	CH 87B (161.975 MHz)
AIS Channel 2	CH 88B (162.025 MHz)
Tx Power Output	1/12.5 Watt (30/41 dBm ± 1.5 dB)
Rx Sensitivity	< -107 dBm @ 20% PER

DSC receiver

Frequency	156.525 MHz
Modulation	FSK
Channel Bandwidth	25 KHz
Sensitivity	< -107 dBm @ BER < 10-2
Spurious Response Rejection	≧ 70 dB for signal @ -104 dBm; BER ≦ 1 %

Blocking	≧ 84 dB for signal @ -104 dBm; BER ≦ 1 %

GPS receiver (internal)

Receiving Channels	50 channels
Tracking & Navigation Sensitivity	≧-159 dBm
Reacquisition Sensitivity	≧ -159 dBm
Horizontal Position	< 2.5 m Autonomous < 2.0 m SBAS
Receiver Type	SBAS: WAAS, EGNOS,MSAS, GAGAN

Power supply

Supply Voltage	12V / 24 V DC
Power Consumption	Less than 9 W average @ 12 V DC; Less than 65 W peak power @ 12 V DC

LCD display

Screen Size	3.5" color TFT
Pixel Number (Resolution)	320 x 240
Viewing Mode	Basic coastline map/ Radar View/ Alphanumeric views /Satellite View
Dimmer Control	Step-less Setting

Keypad & Knob

6 Keypads with Backlight	1 for SRM, 1 for Menu, 1 for Dimmer, 1 for ESC, 1 for Display, 1 for Nav. Status
Knob	Multi-Function

Connection interface

GPS Antenna Connector	TNC (Female)
VHF Antenna Connector	SO-239 (Female)
Sensor Interfaces 1 to 3	IEC 61162-1 or -2
Pilot / Auxiliary	IEC 61162-2
External Display	IEC 61162-2

Long-range	IEC 61162-2
DGNSS correction input	RTCM-SC-104
Alarm relay	Normally closed
USB	Mini type B USB interface
NMEA2000	IEC61162-3
Alarm Output	Relay contact

Environmental

Operating Conditions	IEC 60945 "protected" category
Operating Temperature	-15°C ~ 55°C
Operating Humidity	95% RH at 40°C
Waterproof	IPX2

Physical

Width	205 mm (8.07 inch)
Height	85 mm (3.34 inch)
Depth (include connectors)	160 mm (6.30 inch)
Weight	≦ 1.16 kg

Pilot plug

Cable length	2 m
Connector type	Std. Sex 206486-2

NMEA 2000 PGN information

The following table is a list of the NMEA 2000 messages supported by the V5035 unit.

The "Transmit" PGNs information includes "Own ship" + "Received AIS information from other ships". This is the reason the NMEA2000 PGN list covers both Class A and Class B related information.

Transmit	
PGN	**Description**
59392	ISO Acknowledgment
59904	ISO Request
60928	ISO Address Claim

Transpondedor FURUNO FA-170

FURUNO FA-170

ESPECIFICACIONES DEL TRANSPONDEDOR U-AIS FA-170

1	**UNIDAD DEL TRANSPONDEDOR**	
1.1	Frecuencia TX/RX	De 156,025 MHz a 162,025 MHz
1.2	Potencia de salida	1 W o 12,5 W seleccionables
1.3	Impedancia	50 ohms
1.4	Receptor DCS	CH70 fijo, 156,525 MHz
1.5	Ancho de banda	25 kHz
2	**UNIDAD DE MONITOR**	
2.1	Pantalla	LCD en color de 4,3 pulgadas, 480 x 272 puntos (WQVGA)
2.2	Control de brillo	18 niveles
2.3	Distancia visible	0,7 m nominal
2.4	Volumen del zumbador	De 75 a 85 dB (A)
3	**RECEPTOR GPS**	
3.1	Frecuencia de recepción	1575,42 MHz
3.2	Código de seguimiento	Código C/A
3.3	Número de canal	12 canales en paralelo, 12 satélites
3.4	Precisión (dependiente de la actividad ionosférica y multirruta)	
	GPS	13 m máx. (2drms、HDOP < 4)
	DGPS	5 m máx. (2drms、HDOP < 4)
3.5	Velocidad de seguimiento	1000 kn
3.6	Tiempo de fijación de la posición	Arranque en caliente: 12 s, Arranque en frío: 90 s
3.7	Intervalo de actualización de la posición	1 segundo normalmente
3.8	Recepción de datos DGPS	RTCM SC-104 ver-2.1
4	**INTERFAZ**	
4.1	Número de puertos	
	Serie	6 puertos, IEC61162-1 Ed.4 o IEC61162-2 Ed.1
	Entrada del sensor	3 puertos, IEC61162-1 Ed.4, 4800 bps
	Alarma E/S	1 puerto, cierre de contacto (cierre o apertura normal)
	LAN	1 puerto, Ethernet, 100Base-TX, conector RJ45, Auto MDI/MDIX para IEC61162-450 Ed.1
	Entrada BLUESIGN	1 puerto, contacto de relé

4.2	Instrucciones de datos	IEC61162-1/2/450
	Entrada	ABM, ACA, ACK, ACM, ACN, AIQ, AIR, BBM, DTM, EPV, GBS, GGA, GLL, GNS, HBT, HDT, LRF, LRI, OSD, PIWWIVD, PIWWSPW, PIWWSSD, PIWWVSD, RMC, ROT, SPW, SSD, THS, VBW, VSD, VTG
	Salida	ABK, ACA, ACS, ALC, ALF, ALR, ARC, EPV, HBT, LR1, LR2, LR3, LRF, LRI, NAK, PIWWIVD, PIWWSPR, PIWWSSD, PIWWVSD, SSD, TRL, TXT, VER, VDM, VDO, VSD
4.3	Sentencias patentadas (solo salida)	
	PFEC	LBK, AIcmd, idatr, ident, idfnc, pidat, pireq
4.4	Grupo de transmisión IEC61162-450	
	Input	MISC, TGTD, SATD, NAVD, PROP
	Output	Arbitrario (opción predeterminada: TGTD)
4.5	Función de red (excepto IEC61162-450)	
	Formato de datos	SNMP, HTTP, Syslog, Protocolo de gestión de Furuno (FMP)
	Data sentences	las mismas que 4.2

5 ALIMENTACIÓN

3.1	Unidad del transpondedor	12-24 VCC: 6-3 A
3.2	Unidad de monitor	12 VCC: 0,3 A máx. (suministrado con la unidad del transpondedor)
3.3	Unidad de alimentación CA/CC (PR-240, opcional)	
		100-115/200-230 VCA, monofásico, 50/60 Hz

6 CONDICIONES AMBIENTALES

6.1	Temperatura ambiente	
	Antena GPS/VHF	De -30 °C a +70 °C (almacenamiento: de -30 ºC a +85 °C)
	Otras unidades	De -15 ºC a +55 ºC
6.2	Humedad relativa	93 % o menos de +40 °C
6.3	Grado de protección	
	GPS/VHF antenna	IP56
	Transponder unit	IP20, IP22 (montaje para mamparos)
	Monitor unit	IP22, IP35 (opcional)
	Unidad de conector del piloto	IP22 (panel frontal), IPX0 (chasis)
6.4	Vibración	IEC 60945 Ed. 4

7 COLOR DE LA UNIDAD

7.1	GPS/VHF antenna	N9.5
7.2	Unidad del transpondedor/monitor	N2.5
7.3	Pilot plug unit	N2.5

ANEXO V: CÓDIGOS

En el presente anexo se detallan los códigos utilizados para llevar a cabo los ensayos de transmisiones de mensajes a los receptores estudiados. Cabe destacar que todos parten de una base común de un generador de mensajes de tipo 1 proporcionado previamente. Por lo tanto, estos códigos no son elaboración propia, sino modificaciones realizadas con inteligencia artificial de un *script* base que se adaptan a las necesidades específicas de cada una de las pruebas. Asimismo, se han introducido mecanismos de control temporal, generación de escenarios especiales y parametrización proporcionada por el usuario, con el fin de reproducir condiciones de carga y comportamientos según los requisitos del usuario. El código fuente se encuentra en un repositorio privado de *Github* por razones de seguridad. Se facilitará el acceso al tribunal previa petición.

PPv1_PS1 – Versión 1 del protocolo. Prueba PS1.

Este *script* implementa la generación y transmisión continua de mensajes AIS tipo 1. El funcionamiento parte de una configuración inicial en la que el usuario tiene libertad de fijar la latitud y longitud de referencia, el número de objetivos a generar y el número de ciclos completos que se desea transmitir.

Durante la ejecución del protocolo, se realizaron únicamente ciclos individuales, en ningún momento se repitieron los mismos mensajes pues invalidaría las pruebas, dándole al receptor una segunda oportunidad de decodificar los mensajes que no había logrado decodificar previamente. A partir de la posición de referencia, cada uno de los MMSI ficticios que parten de uno base introducido por el usuario incrementan de uno en uno, se genera una posición aleatoria dentro de un área definida. El *script* realiza cálculos en función de la latitud y longitud de referencia y el valor introducido por el usuario en "radio de ataque" . Para el caso de implementación del protocolo realizado, se genera una especie de caja de ±20 km^2 aproximadamente con un valor introducido de 0,05. De esta manera se simula una concentración de tráfico AIS en una zona concreta.

Calculada la posición, el *script* determina el rumbo del blanco. Se permite, a elección del usuario, los modos "convergente" y "aleatorio". En modo "convergente" se calcula el rumbo desde la posición generada hacia el punto de referencia, lo que conlleva que todos los blancos apunten al mismo sitio, simulando así que tienen rumbo a la unidad. En modo "aleatorio" el *script* le proporciona un rumbo entre 0 y 359 grados a cada uno de los blancos. Se le asigna también a cada traza una velocidad aleatoria dentro de un intervalo fijo de 10 a 25 nudos. Se tienen en cuenta también el estado de navegación del buque (*status*), la precisión de la posición GNSS (*accuracy*) y la velocidad de giro (*tope*). Son campos de información adicional que se fijan en ciertos valores y no se han de modificar durante la ejecución de las pruebas.

A continuación, el *script* genera la sentencia en formato AIVDM y el *payload* binario (teniendo en cuenta la librería seleccionada) que se envía a GNU-Radio para su posterior modulación y transmisión. El envío se realiza dentro de dos bucles, uno exterior y otro interior. El exterior controla el número de ciclos (aunque como se mencionó previamente se mantiene en un único ciclo) y el interior recorre todos los objetivos definidos.

Los parámetros que puede modificar el usuario son los siguientes:

- MY_LAT y MY_LON: fijan el centro del escenario.
- TOTAL_OBJETIVOS: define la cantidad de buques que se quieren generar.
- TOTAL_CICLOS: define la cantidad de ciclos de envío.
- MODO_ATAQUE: modo "convergente" o "aleatorio".
- RADIO_ATAQUE: dispersión respecto al punto central.
- DURACION_SLOT: establecida en 26,67 ms para respetar la duración de un slot pero modificable por el usuario al valor deseado.
- MMSI_BASE: establece el primer MMSI de la serie generada.

Pueden modificarse también, si se desea, las direcciones y puertos UDP empleados para OpenCPN y GNU-Radio.

PPv1_PS2 – Versión 1 del protocolo. Prueba PS2.

Este *script* implementa la generación y transmisión continua de mensajes AIS tipo 5. A diferencia del *script* anterior, este construye una pareja de mensaje tipo 1 y tipo 5 para cada MMSI, por lo tanto incluye información ampliada del buque como nombre, distintivo de llamada, destino, ETA y dimensiones. Se incluyen campos como previamente de posición de escenario, número de objetivos, etc. Además, permite decidir si los mensajes se envían a OpenCPN, a RF como tipo 1 y a RF como tipo 5. Incluye también parámetros temporales que permiten al usuario modificar el tiempo de envío entre mensajes consecutivos. A diferencia de PPv1_PS1, en este caso sí que se genera un radio de dispersión y no una "caja".

El código incorpora listas predefinidas de nombres de barcos y puertos de destino modificables también según los requisitos del usuario. Se emplean funciones auxiliares para limpiar el texto en caso de que se incluyan acentos o caracteres incompatible con las restricciones del estándar. Se incluyen también funciones de cálculo de rumbo, generación de posiciones y conversión de sentencias AIVDM en secuencias binarias, al igual que el generador de tipo 1.

Cada objetivo recibe un MMSI distinto, IMO y distintivo de llamada secuenciales para que resulte sencillo detectar qué mensajes faltan. Además del nombre, destino, posición, rumbo y velocidad que no se recalculan continuamente en cada transmisión, sino que se crean una sola vez para que cada MMSI mantenga una identidad propia y coherente a lo largo de la prueba. Para cada objetivo se generan dos estructuras diferenciadas en la que se incluye la información de un tipo 1 y tipo 5 respectivamente, lo cual permite que el receptor no solo detecte el blanco, sino que también procese su información estática y de viaje. El envío se divide en dos bloques que se pueden activar o desactivar bajo demanda. Esto se hizo para comprobar que la información generada se presentaba correctamente en OpenCPN previo a su envío a GNU-Radio para su posterior conversión en RF.

En cada iteración, se construyen los dos mensajes del objetivo, se transmiten y se muestran por pantalla que muestra el contador, MMSI, nombre, puerto y ETA. El *script* se queda en ejecución hasta completar el número total de blancos introducido.

Los parámetros que puede modificar el usuario son los mencionados anteriormente además de los siguientes:

- MY_LAT y MY_LON: fijan el centro del escenario.
- TOTAL_OBJETIVOS: define la cantidad de buques que se quieren generar.
- TOTAL_CICLOS: define la cantidad de ciclos de envío.
- MODO_RUMBO: modo "unidad" o "aleatorio".
- RADIO_ATAQUE: dispersión respecto al punto central.
- TIEMPO_ENTRE_OBJETIVOS: establecida en 80 ms para respetar la duración de tres *slots* pero modificable por el usuario al valor deseado.
- MMSI_BASE: establece el primer MMSI de la serie generada.
- SOG: velocidad sobre fondo asignada.
- PAUSA_T1_A_T5: introducido para dar tiempo de procesamiento al receptor entre mensajes, pero establecido finalmente en 0 ms para cumplir con la duración de los *slots*.
- REPETICIONES_T1 y REPETICIONES_T5: introducidos para darle la oportunidad al receptor de leer correctamente cada mensaje pero finalmente se establecen ambos a 1 para el desarrollo de las pruebas.
- ENVIAR_OPENCPN: envía directamente los mensajes a OpenCPN. Se desactiva para el desarrollo de las pruebas, se introdujo únicamente para validar el funcionamiento del código.
- ENVIAR_T1_RF y ENVIAR_T5_RF: envío activado a GNU-Radio.

Otros campos que se pueden modificar pero mantienen valores predeterminados:

- IMO.
- Distintivo de llamada.
- Nombre del buque. Se cuenta con una lista de nombres.
- Tipo de buque. Se permite introducir el tipo pero se mantendrá fijo en todos los casos.
- Dimensiones (A, B, C, D). Se permite introducir las dimensiones pero se mantendrán fijas en todos los casos.
- Sistema de posicionamiento (GPS, GLONASS, Galileo, etc.)
- Fecha estimada de llegada (mes, día, hora, minuto).
- Calado.
- Puerto de destino.
- EPFD. Sistema de posicionamiento. Fijo en 1, que equivale a GPS.
- Estado DTE (0 correcto / 1 sin datos). Fijo en 0 para la realización de las pruebas.

PPv1_PS3 – Versión 1 del protocolo. Prueba PS3.

Este *script* implementa la generación y transmisión continua de mensajes AIS tipo 21. A diferencia de los mencionados previamente, se trabaja con un único emisor transmitido muchas veces de manera consecutiva. La configuración de la AtoN incluye parámetros como: MMSI, nombre, indicador de si es virtual o no, posición, dimensiones e indicadores de estado (estado físico, integridad de posicionamiento y modo de TX).

Para adaptar el mensaje al estándar, se limita el texto a 20 caracteres para evitar problemas de codificación, asegurando que el nombre se pueda empaquetar dentro del mensaje. Se construye el *payload* binario completo con los parámetros deseados y se envía a GNU-Radio para su posterior transmisión por SDR. El *script* compara continuamente el tiempo actual con el instante programado de envío y ajusta la espera para mantener una cadencia lo más estable posible, consiguiendo una temporización más precisa en secuencias largas.

Durante la ejecución, el *script* transmite el mismo mensaje tantas veces como se haya definido por el usuario en el campo correspondiente. Además, el usuario puede modificar los siguientes parámetros:

- ATON_TYPE: tipo de AtoN en función de lo que se quiera representar.
- VIRTUAL_ATON: indica si se trata de una AtoN virtual o no.
- LAT y LON: indican posición de la AtoN
- DIM_BOW/STERN/PORT/STARBOARD: indican las dimensiones de la AtoN.
- OFF_POSITION/RAIM/ASSIGNED: indican si la ayuda a la navegación se encuentra fuera de su posición nominal, si el sistema dispone de un mecanismo de control de integridad de la señal GNSS y el modo de transmisión de mensajes respectivamente. Los valores para introducir son 0 y 1.
- TIEMPO_ENTRE_TX: tiempo entre cada envío del mensaje. En el caso de este TFG se ajusta a la duración de dos *slots* TDMA para mantener el canal saturado.

Lib_AIS_App – Librería de generación.

Esta librería se proporcionó al inicio del TFG y constituye la base sobre la que se desarrolla el *script* de PS1. Proporciona las herramientas necesarias para construir manualmente el *payload* binario de distintos tipos de mensajes. La idea general es disponer de un conjunto mínimo de utilidades capaz de generar mensajes de tipo 1 y tipo 21. Cuenta además con capacidad de crear rutas a partir de puntos geográficos que no se aplican en el presente trabajo.

La librería incluye una función cuya finalidad es calcular el rumbo entre dos coordenadas geográficas (*calculate_bearing*). Transforma latitudes y longitudes a radianes, calculando la diferencia de longitud para la posterior obtención de un ángulo mediante relaciones trigonométricas. Permite

asignar. A un blanco un rumbo coherente entre 0 y 359 grados. Se calcula también la distancia entre dos puntos sobre la superficie terrestre mediante la función *calculate_distance*, que nuevamente, no se aplica en el presente trabajo pero puede ser de utilidad para ensayos futuros. La función *compute_long_lat* tiene como cometido principal la adaptación de las coordenadas geográficas al formato correspondiente en el cual longitud y latitud se multiplican por 600000 para su posterior codificación en longitudes binarias de 28 bits para longitud y 27 bits para latitud.

La función *encode_AIS_type1* implementa la construcción de mensajes de tipo 1. A partir de los parámetros recibidos construye uno por uno los distintos campos del mensaje para, finalmente, concatenar esos campos y devolver una cadena binaria. La función *encode_AIS_type5* aparece también en la librería pero no es de aplicación debido a sus limitaciones.

La función *extract_data* toma una secuencia de información ya preparada y sirve como interfaz intermedia entre estructuras de datos generados y la codificación final del mensaje. Existen también funciones como *process_gpx_routes* y *process_gpx_waypoints* que no se aplican pues no se le introducen rutas a seguir a los blancos. Si se quisiera, se podría implementar la creación de blancos con derrotas determinadas gracias a estas funciones. Requeriría la introducción manual de los puntos de la derrota.

Se incorpora también la implementación de *encode_AIS_type21*, la cual se encarga de la generación de AtoNs. Construye un *payload* binario a partir de los datos introducidos, con el nombre adaptado a un máximo de 20 caracteres y cuya codificación se realiza campo a campo en formato AIS de 6 bits.

Lib_AIS_App_v2 – 2ª versión de la librería de generación.

Esta librería es una evolución de la anterior, desarrollada específicamente para solventar problemas detectados en la generación de mensajes de tipo 5, manteniendo las funciones descritas anteriormente con la misma finalidad. La primera versión presentaba limitaciones en la codificación de cadenas de texto y empaquetado que resultaban incompatibles con una correcta transmisión.

Se incorpora la función *_ais6_char* que implementa una tabla de conversión entre caracteres convencionales y su representación AIS de 6 bits. Incluye todo tipo de caracteres, desde mayúsculas hasta signos básicos. En caso de recibir un carácter no conocido lo sustituye por un espacio. Se construye sobre esa función *_encode_ais_string* que recibe texto, lo recorta o rellena con espacios hasta alcanzar la longitud exigida para la posterior conversión de cada carácter mediante *_ais6_char.* Esto resulta en una cadena binaria válida, resolviendo una de las principales limitaciones de la librería original.

Otra función que se incorpora es *_encode_dimensions* cuyo objetivo es permitir dimensiones del buque flexibles. Puede recibir una lista de cuatro valores, la cual interpreta que se trata de distancias a proa, popa, babor y estribor, o recibir directamente un entero que adapta a 30 bits, considerando que se trata de un valor empaquetado.

Log_COM9_v3 – 3ª versión del *log* para leer datos procedentes del QK-A026

Este *script* fue desarrollado específicamente para la fase de validación experimental cuyo objetivo era analizar las sentencias NMEA recibidas por el QK-A026. Su finalidad es detectar pérdidas, errores y comportamientos anómalos en la recepción.

Al finalizar la ejecución, ya sea de forma manual o por un error, el *script* guarda automáticamente dos ficheros: uno con los eventos procesados y otro con todas las líneas NMEA recibidas.