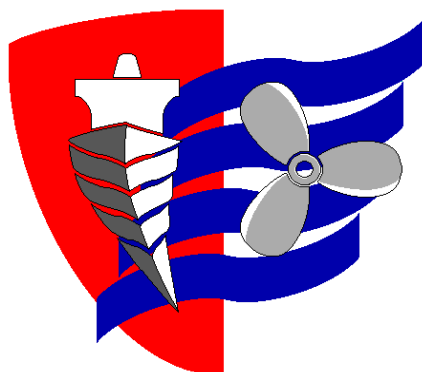


ESCUELA TÉCNICA SUPERIOR DE NÁUTICA

UNIVERSIDAD DE CANTABRIA



Trabajo Fin de Grado

SISTEMA “SECURE AIS”: UNA PROPUESTA DE APLICACIÓN EN OPERACIONES DE ABORDAJES DE BUQUES

**(“Secure AIS” System: A proposal for
application in ships boarding operations)**

Para acceder al Título de Grado en

**INGENIERÍA NAÚTICA Y TRANSPORTE
MARÍTIMO**

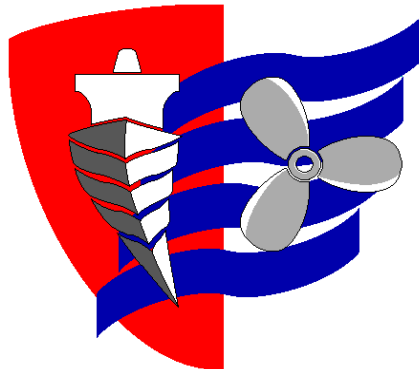
Autor: Jaime Álvarez Velasco

Director: Andrés R. Ortega Piris

Marzo - 2014

ESCUELA TÉCNICA SUPERIOR DE NÁUTICA

UNIVERSIDAD DE CANTABRIA



Trabajo Fin de Grado

SISTEMA “SECURE AIS”: UNA PROPUESTA DE APLICACIÓN EN OPERACIONES DE ABORDAJES DE BUQUES

**(“Secure AIS” System: A proposal for
application in ships boarding operations)**

Para acceder al Título de Grado en

**INGENIERÍA NAÚTICA Y TRANSPORTE
MARÍTIMO**

ÍNDICE:

Resumén.....	5
Palabras clave.....	5
1) INTRODUCCIÓN Y ESTADO DE LA CUESTIÓN.....	6
1.1) IMO: Descripción del organismo	6
1.2) Normativa IMO acerca de AIS	10
1.3) AIS: Características generales, funciones y aplicación	14
2) UNA AMENAZA GLOBAL.....	24
2.1) Las deficiencias del sistema AIS	24
2.2) El uso indebido de la información AIS.....	27
3) SISTEMA AIS SEGURO	33
3.1) Introducción al sistema AIS Seguro	33
3.1.1) Concepto Seguro.....	33
3.1.2) Características del Sistema	34
3.1.3) Comunicación en el canal encriptado	36
3.1.4) Interfaces hacia sistemas externos	36
3.1.5) Modos operacionales	37
3.2) Aplicaciones del equipo a bordo.....	38
3.2.1) General.....	38
3.2.2) Aplicaciones propias.....	38
3.2.3) Opciones para Sistemas AIS Seguros.....	43
3.3) Productos AIS Seguro.....	44

3.3.1) Transpondedores AIS Seguro Marítimo	44
3.3.2) Transpondedores AIS Seguro Aéreo	45
3.3.3) Estación Base	45
3.3.4) Módulo Seguro independiente	46
3.3.5) Servidor Seguro – Red Segura.....	46
3.4) Software generador de claves seguras	47
4) DISCUSIÓN SOBRE LA NUEVA APLICACIÓN DEL AIS SEGURO PARA CASOS DE ABORDAJE.....	49
4.1) Operaciones de abordaje con equipos AIS Seguro: Primeras consideraciones ..	49
4.2) Relevancia del alcance de los equipos AIS	50
4.3) Configuraciones especiales del AIS Seguro	54
4.4) Una ayuda en materia de vigilancia y su función disuasoria.....	59
5) CONCLUSIONES	62
BIBLIOGRAFÍA	64
ÍNDICE DE FIGURAS.....	67
ÍNDICE DE TABLAS	68

Resumen:

En las comunicaciones marítimas e equipos de identificación en el mar, encontramos el sistema AIS, normalizado por IMO, un suborganismo de Naciones Unidas. En mi trabajo estudio una nueva aplicación de este equipo que tendrá como objetivo fomentar el enlace entre ciertas unidades que integren dicho equipo, AIS Seguro. Veremos que aplicaciones tiene y que cuerpos podrían hacer uso de este equipo.

In Maritime Communications and Identification Systems, we are able to manage AIS equipment that is normalized by IMO, an ONU sub organism. In this documnt, I am going to study a new aplication of this system, that is Secure AIS System, which deals with improving communications between some units that integrate this equipment. We will see different kind of applications and who is able to use them.

Palabras clave:

AIS: Automatic Identification System – Sistema de Identificación Automática, equipo que trabajando en frecuencias VHF, trasmite y recepciona información estática y dinámica de los buques que navegan a su alrededor.

Secure AIS: AIS Seguro – Sistema AIS que implementa un tercer canal de comunicaciones por VHF: el enlace encriptado.

Enlace encriptado: enlace VHF del sistema AIS que utiliza un protocolo de información AIS semejante al convencional de forma encriptada.

1) INTRODUCCIÓN Y ESTADO DE LA CUESTIÓN

Las comunicaciones marítimas entrañan una enorme responsabilidad en cuanto a su implantación a bordo de los buques, todas ellas tienen que tener como denominador común el carácter veraz de la información que transmiten, es cierto que la evolución de las comunicaciones ha sufrido una mejora enorme a partir de la revolución de las telecomunicaciones (1998). Desde las comunicaciones por señales de luz, banderas, pasando por el código morse, frecuencias VHF, HF, la llamada selectiva digital hasta las ahora tan en auge comunicaciones satelitales que permiten tener señal de televisión satelital global a bordo (los V-SAT de KVH) o incluso poder acceder a internet por wifi en todo el barco, todo ello con vistas a mejorar la vida en el mar, las relaciones con el exterior y en primera instancia la seguridad de la navegación. En este contexto, la normativa internacional, entre muchas otras funciones, como veremos en el primer apartado regulariza y normaliza el sistema de identificación automática conocido como AIS, un equipo cuyas ventajas para la navegación y especificaciones técnicas estudiaremos en este primer apartado. Seguidamente introduciremos los problemas que acarrearán estas especificaciones técnicas y el uso indebido de este. En tercer lugar, estudiaremos la solución a este problema en las comunicaciones marítimas con la integración de una mejora del equipo AIS. Finalmente, proporcionaremos nuevas aplicaciones y en particular expondré una propuesta pensada a raíz de dicho estudio en la que a mi juicio proporcionaría un mayor control de la flota y del entorno en el que estamos navegando, lidiar en conflictos en el medio marítimo para facilitar operativos, notoriamente de abordajes en este medio tan adverso para los profesionales.

1.1) IMO: Descripción del organismo.

La IMO (International Maritime Organization) en español OMI (Organización Marítima Internacional) es la agencia de las Naciones Unidas especializada en la seguridad y protección (safety & security) del transporte marítimo y la prevención de la contaminación del medio marino cuyo axioma haciendo referencia al documento de la Organización Marítima Internacional “OMI Qué es.” [1]:

“Una navegación segura, protegida y eficiente en mares limpios”

En 1948, se celebra una conferencia de las Naciones Unidas para adoptar el Convenio constitutivo de la Organización Marítima Internacional sentando las bases de este organismo

La OMI es una organización técnica cuyo trabajo lo realiza mayoritariamente distintos comités y subcomités:

El Comité Marítimo de Seguridad (MSC) es uno de los órganos principales junto con la Asamblea (órgano rector de la OMI, constituida por 170 Estados Miembros y tres Estados Asociados que se reúnen una vez cada dos años) y el Consejo(40 Gobiernos Miembros elegidos por la Asamblea que se reúnen entre los periodos de reuniones de la Asamblea y ejercen de órgano rector) es un cuerpo técnico superior de la OMI trabajando sobre cuestiones relacionadas con la seguridad . Está constituido por un número de subcomités:

- Transporte de carga y contenedores
- Proyecto y construcción de buques
- Implantación de los instrumentos de la OMI
- Navegación, comunicaciones y búsqueda y salvamento
- Factor humano: formación y guardia
- Equipos y sistemas de buques
- Prevención y lucha contra la contaminación

El comité de protección del medio marino: se encarga de coordinar las actividades de prevención y contención de la contaminación del medio ambiente por los buques.

Comité jurídico: examina las cuestiones de orden jurídico competencia de la Organización.

Comité de cooperación técnica: coordinación del trabajo de asistencia técnica en particular a los países subdesarrollados.

Comité de facilitación: facilitación del tráfico marítimo internacional, reducir y simplificar formalidades y documentación (salida/entrada de buques en puerto...)

Dichos comités y subcomités trabajan con el fin de mejorar en los siguientes aspectos:

A- Seguridad

La primera tarea que llevó a cabo la OMI en 1959 fue adoptar una nueva versión de la Convención Internacional para la Seguridad de la Vida en la Mar (SOLAS), el tratado más importante relacionado con la seguridad marítima y entró en vigor en 1965.

Cabe destacar entre las medidas tratadas en el SOLAS, la compartimentación y la estabilidad de los buques, instalaciones de máquinas y eléctricas, prevención, detección y extinción de incendios, dispositivos de salvamento, radiotelegrafía y radiotelefonía, transporte de grano y mercancías peligrosas...

La OMI ha desarrollado y adoptado también el Reglamento Internacional para Prevenir los Abordajes en la mar y los estándares globales para la gente de mar (Convenio de formación, titulación y guardia para la gente de mar), así como convenciones internacionales y códigos relacionados con la búsqueda y rescate, la simplicidad del tráfico marítimo, líneas marítimas, el transporte de mercancías peligrosas, bienes y medida de estos, el Convenio internacional sobre líneas de carga, Convenio internacional sobre Arqueo de buques.

En 1976, la OMI adoptó el Convenio Constitutivo de la Organización Internacional de Telecomunicaciones Marítimas por Satélite (INMARSAT) que hoy por hoy se ha convertido en una empresa que da soluciones de comunicaciones satelitales en el sector marítimo.

B- Protección marítima

Como consecuencia del secuestro del crucero Achille Lauro (1985) la OMI adopta una resolución para prevenir actos ilícitos en buques y salvaguardia del pasaje y la tripulación. A partir de los atentados terroristas perpetrados el 11 de septiembre de 2001 y sucesivos ponen de manifiesto la intencionalidad de atacar las infraestructuras de transporte, conlleva a la OMI a adoptar medidas de protección marítima: Código Internacional para la protección de buques y de las instalaciones portuarias (Código PBIP) que estipula la obligatoriedad de los gobiernos para realizar evaluaciones de riesgo de amenaza de los puertos, infraestructuras portuarias, buques e instalaciones

marítimas, y de esta forma nombrar a oficiales de protección y elaborar planes de protección.

Piratería y robos a mano armada perpetrados contra los buques:

A finales 1990 se inicia el proyecto antipiratería de la OMI por medio de la cooperación regional en la zona de Asia (RECAAP). Mientras que en la actualidad frente a la costa de Somalia y el golfo de Adén la situación ha empeorado drásticamente. Fruto de ello la OMI ha elaborado para armadores, propietarios y capitanes actualizaciones y revisiones de las publicaciones de 1990, dando como resultado la contratación de seguridad privada para la protección armada de los buques que navegan sobre todo por la costa de Somalia. Finalmente en 2009, se ha llevado a cabo la firma de un acuerdo regional organizado por la OMI que reconoce el alcance del problema de piratería y robos a mano armada en la zona del Índico y golfo de Adén y los signatarios (regionales) de dicho acuerdo: *Código de conducta relativo a la represión de la piratería y los robos a mano armada contra los buques (Código de conducta de Djibouti)* se comprometían a perseguir este delito y cooperar con la OMI para la investigación de los hechos, detención de los piratas y rescate de los buques y personas objeto de actos de piratería.

C- Prevención de la contaminación

Partiendo del primer convenio que redactó la OMI en 1954: Convenio internacional para prevenir la contaminación de las aguas del mar por hidrocarburos hasta el actual MARPOL 73/78 (Convenio internacional para prevenir la contaminación por los buques, 1973), se han llevado a cabo numerosas revisiones y estudios que dieron lugar al que ahora rige en este aspecto junto con las actualizaciones de 1978. Dicho convenio se ocupa de la contaminación originada por hidrocarburos, productos químicos, y otras sustancias, basuras, aguas sucias, además por el Anexo VI de la contaminación atmosférica y las emisiones procedentes de los buques (especial atención a las emisiones de óxido de azufre y óxido de nitrógeno).

A parte, la OMI elaboró distintos convenios para la cooperación entre organismos y fuerzas del estado frente a emergencias repentinas. Encontramos en el SOLAS la normativa internacional referente al sistema AIS, es decir las reglas, anexos y

circulares formuladas por el comité de seguridad referente a las obligaciones de los buques en cuanto a la instalación de estos equipos sus características técnicas, el modo de funcionamiento, la información que debe procesar etc. El SOLAS procesa esta normativa mediante las reglas que en ciertos casos vienen adjuntadas una circular donde remiten a alguna especificación del asunto que tratan. Dichas circulares están codificadas por las siglas MSC (Maritime Security Commitment).

En el siguiente apartado explicaremos que normas, recogidas en el SOLAS, tiene que cumplir un sistema AIS tipo IMO (Clase A) y sus características técnicas.

1.2) Normativa IMO acerca de AIS

El sistema AIS (Automatic Identification System) es un sistema de información estandarizado de seguridad propuesto en 1997 y adoptado por IMO en 1998 está diseñado para poder proporcionar información del buque a otros buques o estaciones costeras de forma automática en la banda marítima de VHF como un transpondedor. Su implementación a bordo se llevó a cabo en función de las características del buque. La regla 19 del capítulo V del SOLAS establece los requisitos que debe contemplar este equipo. Los siguientes buques deben estar equipados con AIS:

- Buques superiores o iguales a 300 GT que lleven a cabo travesías internacionales
- Buques de carga superiores a 500 GT que no hagan navegaciones internacionales
- Todo buque de pasaje independientemente del tamaño.

Y se equiparán en las siguientes fechas límite:

- 1- Aquellos construidos en o después del 1 de Julio de 2002
- 2- Los que lleven a cabo travesías internacionales construidos antes del 1 de Julio de 2002
- 3- En el caso de buques de pasaje no más tarde del 1 de julio de 2003
- 4- En el caso de buques tanque no más tarde de su primera inspección de seguridad durante o después del 1 de Julio de 2003
- 5- En el caso de todo tipo de barcos salvo tanque o de pasaje de 50 000 GT y superior no más tarde del 1 de Julio de 2004

- 6- En el caso de todo tipo de barcos salvo tanque o de pasaje de entre 300 GT y superior pero no más de 50 000 no más tarde de la primera inspección después del 1 de Julio de 2004 y antes del 31 de Diciembre de 2004
- 7- Los buques que sin hacer viajes internacionales contruidos antes del 1 de Julio 2002 a más tardar el 1 de Julio de 2008.

Dicho requerimiento que aparece reflejado en la regla 19 del capítulo V de SOLAS: Requerimientos de integración de sistemas y equipos de navegación a bordo [2]- “*Chapter V: Safety of navigation - Regulación 19: Carriage requirements for shipborne navigational systems and equipment*” - se hizo efectivo a partir del 31 de Diciembre de 2004.

Con fecha 23 de Abril de 2009 se publicó la *Directiva 2009/17/CE* [3] por parte de la UE en relación al establecimiento de un sistema comunitario de seguimiento y de información sobre el tráfico marítimo, haciendo obligatorio el uso de AIS para buques de pesca, con el siguiente calendario de integración a bordo:

- buques de pesca de eslora total superior o igual a 24 metros e inferior a 45 metros, a más tardar el 31 de mayo de 2012,
- buques de pesca de eslora total superior o igual a 18 metros e inferior a 24 metros, a más tardar el 31 de mayo de 2013,
- buques de pesca de eslora total superior o igual a 15 metros e inferior a 18 metros, a más tardar el 31 de mayo de 2014.

En cuestión de legislación Española a partir del Reglamento por el que se regulan las radiocomunicaciones marítimas a bordo de los buques civiles españoles, el *Real Decreto 1185/2006*, [4] que recoge el BOE el 16 de octubre, marca el comienzo de la implementación de medidas de seguridad del tipo AIS.

Además, como establece la Resolución de la OMI A.917(22) [5]. Hoja de ruta para el uso a bordo del sistema automático de identificación (AIS) - *Guidelines for the onboard operational use of shipborne automatic identification systems (AIS)* - todo buque equipado con sistema AIS debe mantener operativo el equipo salvo en áreas donde bajo acuerdo internacional se establezca la desconexión y no transmisión de

este. Dicha resolución también estipula las siguientes características de cualquier sistema AIS:

Este equipo permite automáticamente compartir información:

- **Dinámica:** posición del buque, rumbo (course over ground), velocidad (speed over ground), rate of turn, estado de navegación (amarrado, fondeado, con máquina avante, sin gobierno, restringido por (calado, faenando, etc.)
- **Estática:** relacionado con los datos del viaje y del buque: Maritime Mobile Service Identity (MMSI), número IMO, distintivo de llamada, nombre del buque, tipo de buque, dimensiones del buque, posición de la antena en el buque.

Para aumentar la capacidad del sistema, la cadencia de refresco de la emisión se efectúa en función de la velocidad del buque y de su evolución: un barco lento en ruta rectilínea refrescará sus datos con una cadencia menor, más espaciada como muestra la siguiente tabla (extraída de la normativa SOLAS OMI [6]):

Tabla 1: Intervalos de información de los equipos móviles a bordo de barcos de la Clase A. **Fuente:** Resolución A.917(22): *Guidelines for the onboard operational use of shipborne automatic identification systems (AIS)* OMI

Type of ship	General reporting interval
Ship at anchor	3 min
Ship 0-14 knots	12 sec
Ship 0-14 knots and changing course	4 sec
Ship 14-23 knots	6 sec
Ship 14-23 knots and changing course	2 sec
Ship >23 knots	3 sec
Ship >23 knots and changing course	2 sec

Se han escogido estos valores para cargar al mínimo los canales de radiocomunicaciones manteniendo al mismo tiempo la conformidad con las normas de calidad de funcionamiento del AIS, de la OMI.

Por otro lado encontramos en la regulación de los estándares AIS normativas de distintos organismos, es el caso de la Unión Internacional de Telecomunicaciones (UIT) que es el organismo especializado de Naciones Unidas responsable de las tecnologías de la información y las comunicaciones. Elaboró una serie de

recomendaciones que contemplaban las características que debían tener los equipos AIS para asegurar el enlace de datos entre estaciones AIS, cabe destacar citando de las recomendaciones de la ITU [7]:

“La estación móvil AIS debe diseñarse para funcionamiento en la banda de ondas métricas del servicio móvil marítimo en canal símplex o dúplex en modo semidúplex, ya sea de 25 kHz o de 12,5 kHz. El sistema debe ser capaz de funcionar en dos canales paralelos de la banda de ondas métricas. Cuando los canales AIS designados no estén disponibles, el sistema deberá seleccionar alternativas mediante métodos de gestión de canales con las mismas características.”

De forma general los canales estándar 1 y 2 de emisión/recepción de datos AIS serán:

- AIS 1 (primer canal por defecto): 161,975 MHz
- AIS 2 (segundo canal por defecto): 162,025 MHz

Con el fin de evitar que dos estaciones transmitan a la vez y se solapen, cada estación AIS se sincroniza con las demás. Las de Clase A tienen un intervalo aleatorio de entre 0 y 8 slots. Cuando una estación cambia de slot, preanuncia el nuevo slot y el timeout que empleará. De ese modo las nuevas estaciones de buques que entren en el rango de alcance de la radio, siempre serán recibidas.

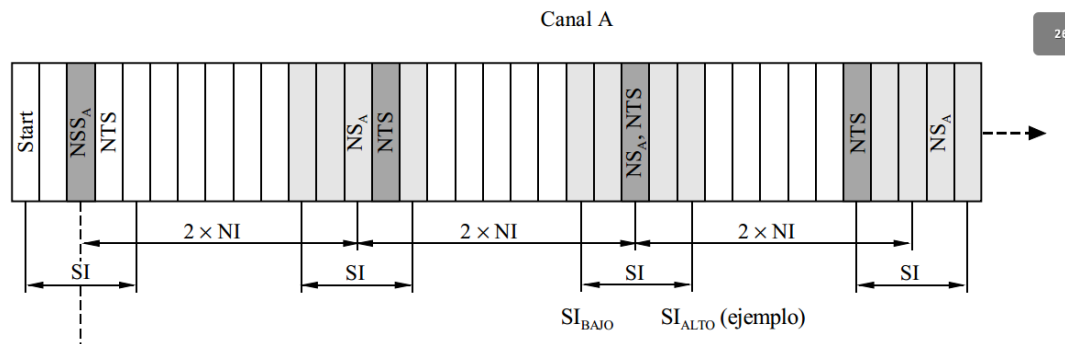


Figura 1: Diagrama de periodicidad de la información. **Fuente:** RECOMENDACIÓN UIT-R M.1371-1* Características técnicas de un sistema de identificación automático universal a bordo de barcos mediante acceso múltiple por división en tiempo en la banda de ondas métricas del servicio móvil marítimo. [7].

Por tanto, gracias al AIS se tiene información objetiva en tiempo real de los barcos, que están equipados con el sistema, antes de ser detectados por el radar y cuando la orografía de canales y puertos crea un obstáculo insalvable para el radar. Se conoce el destino, tamaño, calado de otros barcos, si están en condición de navegación

restringida por su calado, su velocidad, rumbo, etc... Datos importantes para establecer maniobras de paso y evitar colisiones. Se tiene constancia rápidamente de cualquier cambio de rumbo que se realice antes de que lo perciba el ARPA (que necesita al menos dos minutos para detectar un cambio, frente a los tres segundos del AIS). Los datos se pueden representar gráficamente en la carta electrónica EDCIS. Ayuda a identificar objetos y a discriminar ecos falsos del radar, como el oleaje. Todo ello con el objeto de mejorar la seguridad en la navegación por medio de una navegación eficiente de los buques, protección del medio marino y operatividad de las torres de control de tráfico.



Figura 2: Dibujo situación de zonas de sombra. **Fuente:** AIS Transponders, <http://www.imo.org/OurWork/Safety/Navigation/Pages/AIS.aspx>. [8]

1.3) AIS: Características generales, funciones y aplicación.

A.- Descripción:

Un equipo AIS convencional contempla tres partes:

- Transpondedor
- Unidad de control y monitorización (CDU)
- Caja de conexiones

El Transpondedor consiste en una unidad de transmisión de radio, un receptor de 50 canales GPS y una unidad de control. La radio tiene tres receptores, dos receptores TDMA y uno DSC. El transmisor alterna sus transmisiones entre los dos canales TDMA. La unidad de control crea y organiza los paquetes de datos (contenido

dinámico, estático y datos relacionados con el viaje) para transmisiones relacionadas con los requerimientos IMO en la resolución OMI MSC.74 (69) [9].

El CDU es la unidad de monitorización y configuración AIS. Pudiendo marcar la posición de otros barcos (interrogarlos), ayudas a la navegación etc. También puede utilizarse para mandar y recibir mensajes, llevar a cabo configuraciones así como supervisar el estado del transpondedor AIS.

La caja de conexiones permite de forma fácil conectar equipos externos: ECDIS, DGPS, GYRO, Central Alarm Manager, piloto automático...

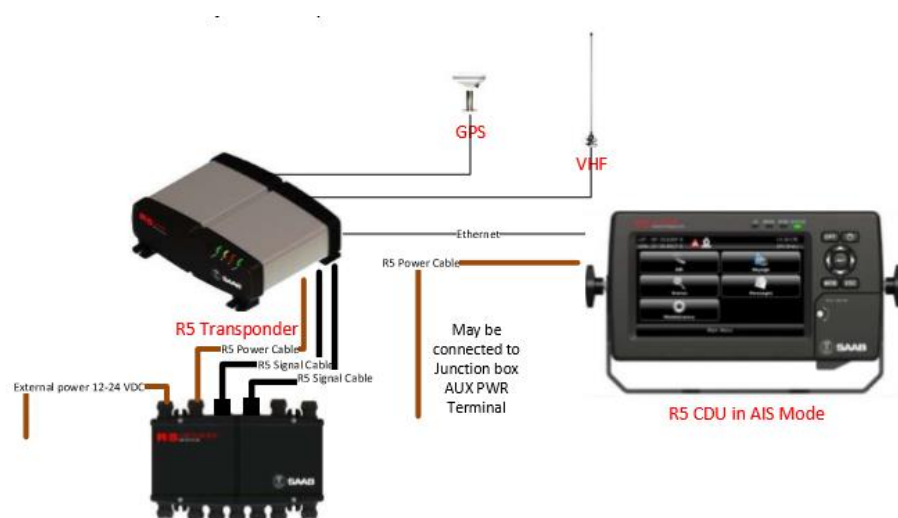


Figura 3: Diagrama de bloques equipo AIS. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]



Figura 4: Imagen CDU. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]



Figura 5: Imagen traspondedor, vista superior. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]



Figura 6: Imagen traspondedor, vista trasera: interfaz con el resto de unidades. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]

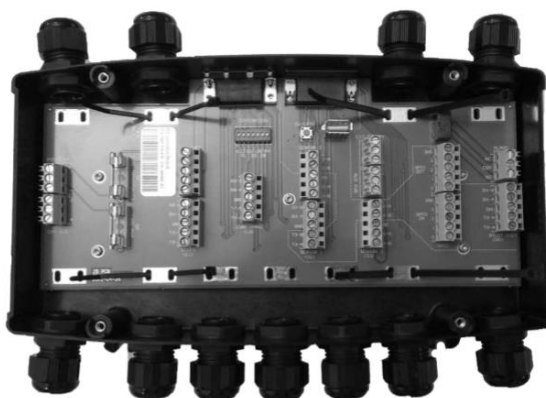


Figura 7: Imagen Junction Box. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]

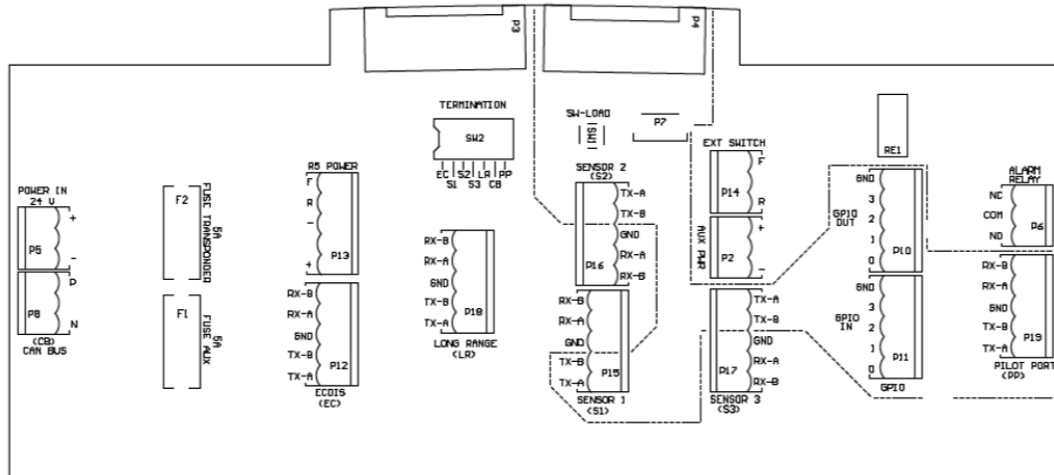


Figura 8: Esquema conexiones Junction Box. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]

B.- Procedimiento de instalación:

Cuando se lleva a cabo una instalación del equipo AIS se recomienda seguir los siguientes pasos, descritos en el manual de instalación del fabricante, en este caso Saab [10]:

1. Montar la CDU en la consola de navegación
2. Montar el transpondedor
3. Montar el relé de alarma
4. Conectar todos los sistemas externos y sensores a la Junction Box
5. Montar la Junction box
6. Conectar el transpondedor y el CDU directamente o por puerto Ethernet
7. Montar la antena VHF
8. Montar la antena GPS
9. Alimentar el sistema y encenderlo
10. Configurar el IP y los ajustes LWE-ID

11. Ajustes otros parámetros

12. Llevar a cabo una prueba de rendimiento

Para el conexionado de los distintos equipos del sistema AIS, en el Anexo I, mostramos en detalle el cableado.

Cuestiones a tener en cuenta sobre la disposición de las antenas:

Cuando conectemos la antena VHF propia del AIS, habrá que prestar especial atención a que su situación en la cubierta de la magistral no sea próxima al resto de antenas para evitar interferencias y aún más atención a aquellas antenas que operan en bandas de frecuencia próximas a las de VHF. El traspondedor AIS utiliza canales simplex en las frecuencias de la parte alta de la banda marina (AIS canal A = 2087, 161.975 MHz, y AIS canal B = 2088, 162.025 MHz). Estos canales están cerca de los canales duplex utilizados para comunicaciones marinas tierra/buque. La antena AIS VHF debe estar lo más separado posible de las instalaciones VHF de voz de las comunicaciones VHF principales y así evitar interferencias.

De igual forma ocurre con la localización de la instalación de la antena GPS, donde buscaremos la mayor eficiencia de ella, evitando zonas de sombra y posibles interferencias con otros equipos: dejar al menos 3 metros de separación con el Radar Banda S ya que los pulsos de transmisión son tan potentes que distorsionan la señal GPS.

C.- Configuración:

Una vez terminada la instalación del equipo, se procederá a la configuración de este y los ajustes de parámetros: datos estáticos del buque, datos del viaje, dimensiones del buque,

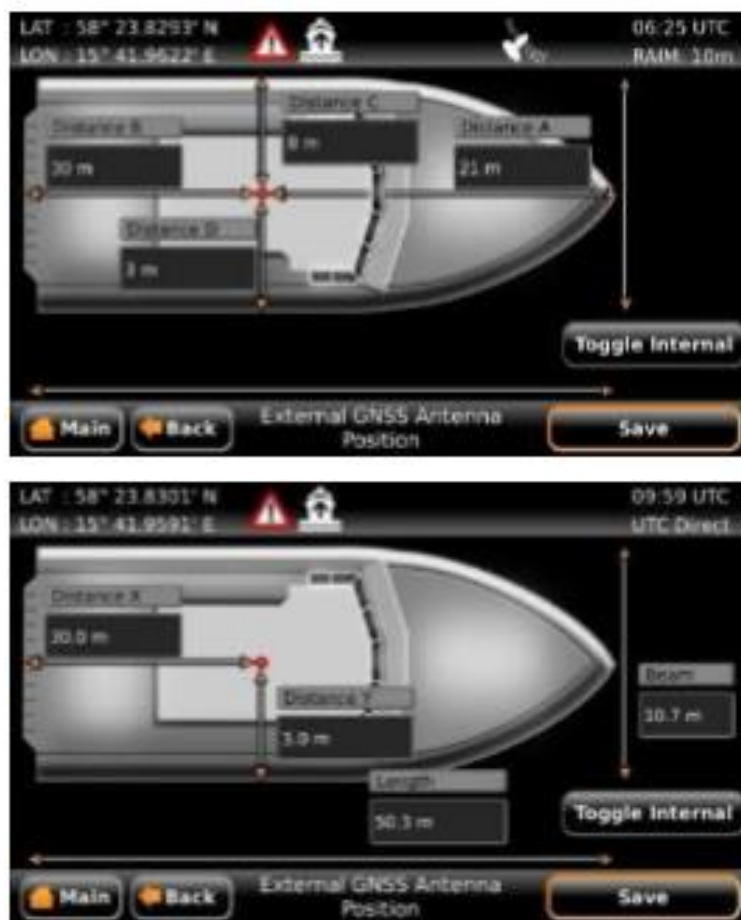


Figura 9: Pantalla de configuración. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. Operaciones con el sistema AIS convencional

En el diagrama de bloques de la página siguiente se muestra el mapa de funciones del equipo y, a continuación, veremos las distintas herramientas útiles para el navegante abordado.

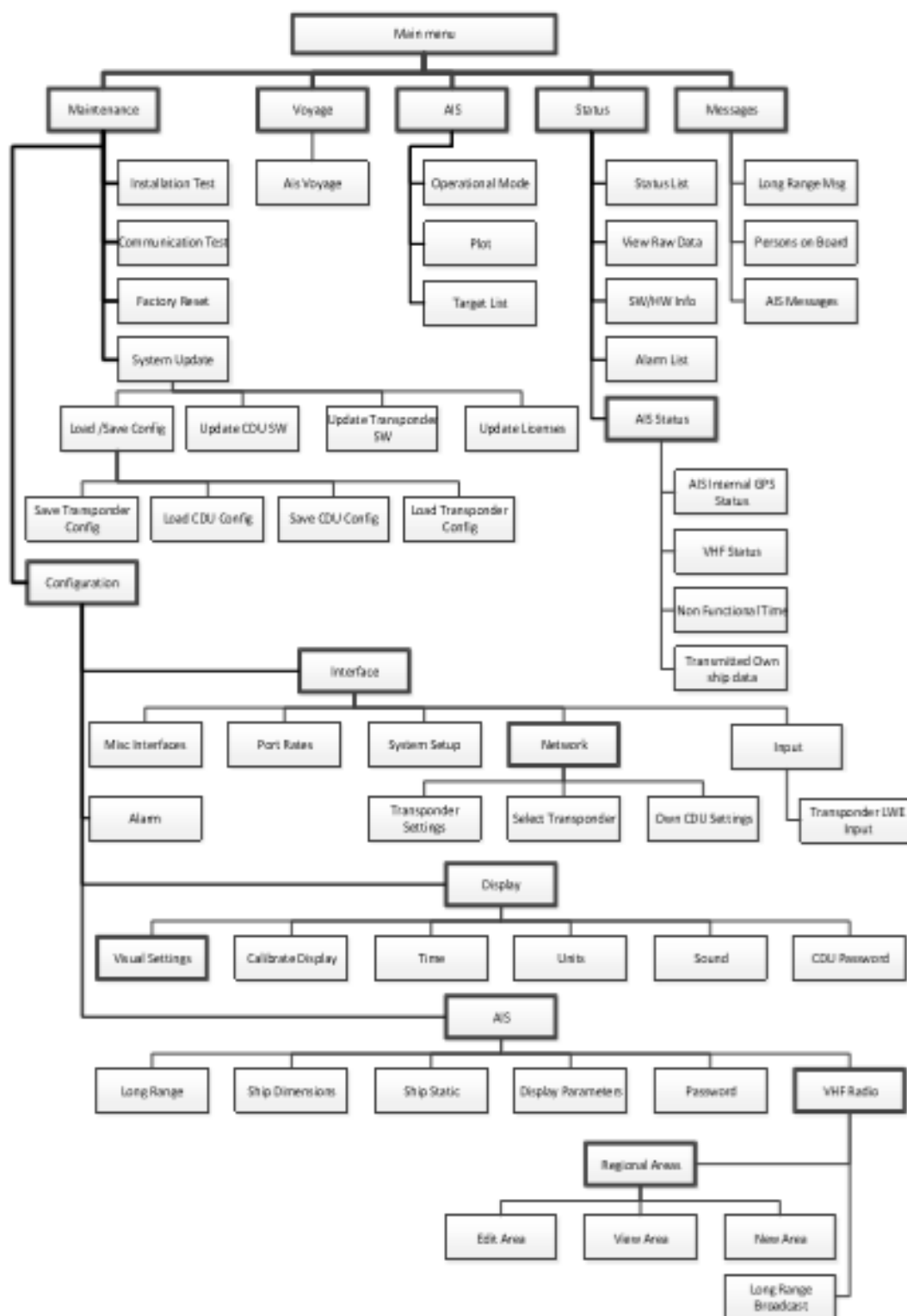


Figura 10: Diagrama de bloques operaciones en el equipo AIS. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]

D.- Funciones con el equipo AIS

A continuación enumeraremos las aplicaciones más importantes y útiles para la navegación:

- Adquisición de ecos: aparecerá en un menu desplegable una lista de ecos AIS recibidos por el enlace VHF que hace referencia a buques con sus respectivos rumbos, demora y distancia, MMSI...

Podremos seleccionar individualmente aquellos ecos que supongan un obstáculo para nuestra navegación y consultar datos más específicos y hacer su seguimiento afín de maniobrar de forma segura.



Ship ID	Bearing	Range	Age
SART ACTIVE: 977115132	199.3 °	3.0 NM	00:30
CATRINA	355.1 °	5.2 NM	00:28
HELI 13	201.0 °	9.0 NM	00:31
HENAB HYBRID	211.7 °	1.0 NM	00:00
HENRIK CLASS B	355.1 °	5.2 NM	00:31
LUDWIG II	128.7 °	5.4 NM	00:28
MMSI: 266125000	100.4 °	0.0 NM	03:57
R40 101 ANI	180.0 °	13.0 NM	00:02
VINGA	135.0 °	13.8 NM	00:30

Figura 11: Pantalla de blancos. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]

- También podremos enviarles un mensaje de texto, al buque seleccionado así evitaremos problemas de idioma y mal interpretaciones de la información que queremos transmitir:



LAT : 58° 23.8304' N
LON : 15° 41.9615' E

07:45 UTC
UTC Direct

NO, WE HAVE THE SITUATION UNDER CONTROL!

Message Type: Addressed Text

Channel: No Preference

MMSI: 555666444

Main Back Send AIS Messages Send Message

Figura 12: Mensaje buque a buque. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab.[10]

- También tenemos la opción de poder enviar y recibir mensajes de rango grande.
- La opción de plotter permit tener una visión de conjunto de todos los buques, equipados con AIS, navegan a nuestro alrededor, esto debe considerarse como una ayuda adicional al radar y a nuestra propia observación visual ya que como hemos visto antes no todos los buques tienen la obligatoriedad de estar equipados con un AIS:



Figura 13: Pantalla AIS para vista de plotter. **Fuente:** R5 Supreme AIS Transponders, System overview, Saab. [10]

Hemos visto en este apartado la obligatoriedad de la implantación a bordo de los equipos AIS por parte de la OMI, las características de estos equipos, la información que transmiten y reciben y su importancia a bordo para llevar de forma segura la guardia.

Destaca por tanto la eficacia del sistema a la hora de manejar información, de forma inmediata y veraz, su simplicidad y el accesible interfaz del software con el oficial de guardia, todo esto otorga a dicha herramienta su carácter cada vez más imprescindible para la navegación.

Sin embargo, basta con acceder a cualquier mapa de localización de buques para ver la cantidad de información que circula en los canales VHF AIS y para también observar que se trata de una red demasiado abierta, en algunos casos puede suponer tanto un problema a nivel de seguridad como de manejo de tal cantidad de información, perdiendo incluso el carácter inmediato de acceso a la información AIS

Sistema “Secure-AIS”: Una propuesta de aplicación en operaciones de abordaje de buques

y su veracidad. La imagen abajo del estrecho de Gibraltar es el resultado de esta concentración de transmisiones por los canales VHF AIS:

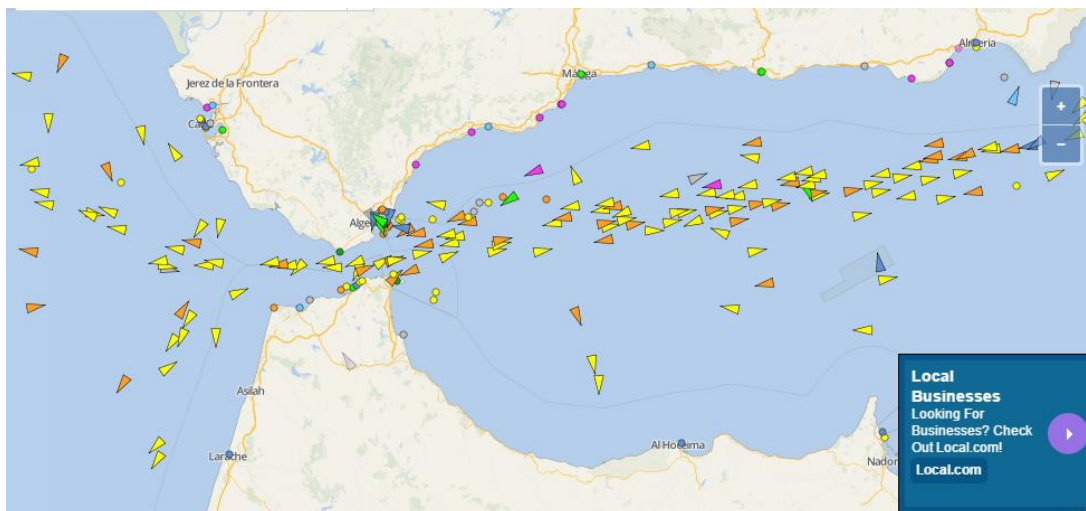


Figura 14: Imagen del tráfico marítimo en el estrecho de Gibraltar. **Fuente:** www.marinetraffic.com [11]

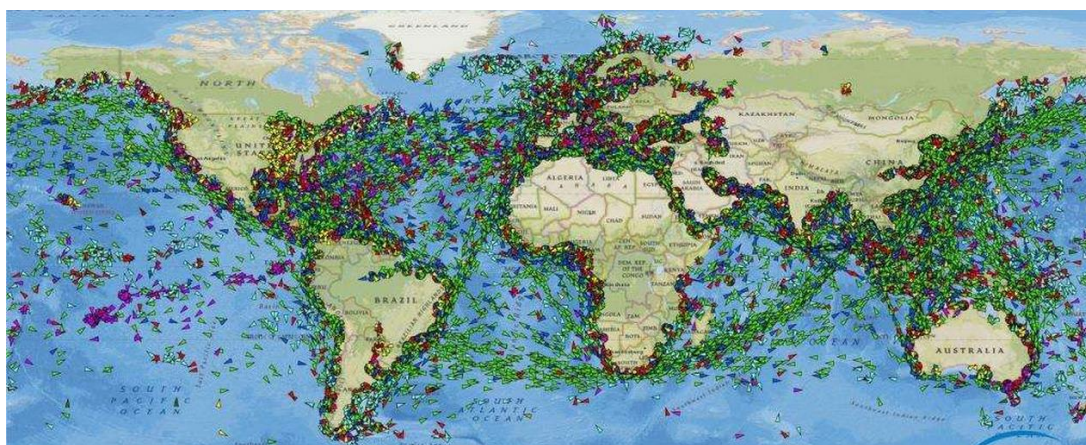


Figura 15: Imagen de la captación satelital de señales de transpondedores AIS. **Fuente:** <http://www.exactearth.com> [12]

2) UNA AMENAZA GLOBAL.

2.1) Las deficiencias del sistema AIS.

El uso de los datos AIS por hackers, piratas y terroristas que puso de manifiesto el estudio resultante de la empresa de seguridad digital Trend Micro escrito por Marco Balduzzi y Kyle Wilhoit y en colaboración con Alessandro Pasta: “*A Security Evaluation of AIS*” el 16 de diciembre de 2014, [13], recalcó las desventajas de este sistema tan accesible y simple en su integración. Su estudio se hizo tanto a nivel de software como del hardware del sistema, identificando en primer lugar las amenazas que podrían afectar durante la implementación y especificación del protocolo de comunicación del equipo AIS: esto incluye la desactivación de las comunicaciones, manipulación de los datos AIS, emisión de alertas SAR para atraer buques a zonas hostiles, simulación de colisiones entre buques...

Hay que destacar que las comunicaciones por los canales VHF AIS no solo se llevan a cabo entre equipos AIS a bordo de buques o estaciones costeras, sino que también se emplea este sistema en las llamadas AtoN (Aids to navigation) que son aquellas boyas, faros etc. que están provistas de transmisores AIS para dar su posición señalando así zonas de navegación restringida, bajos, aguas someras... Por otra parte también vienen equipados los transpondedores SART con transmisores AIS, queda patente la amplia gama de productos equipados bajo este protocolo de comunicación y que pueden ser objeto de ataques de hackers con fines de piratería o terrorismo.

El estudio llevado a cabo por Trend Micro contempla tres tipos de ataques que pueden sufrir los distintos elementos implementados por protocolos de comunicación AIS (Fig.16):

- Spoofing - Falsificación
- Hijacking -Secuestro
- Availability disruption – Disponibilidad interrumpida

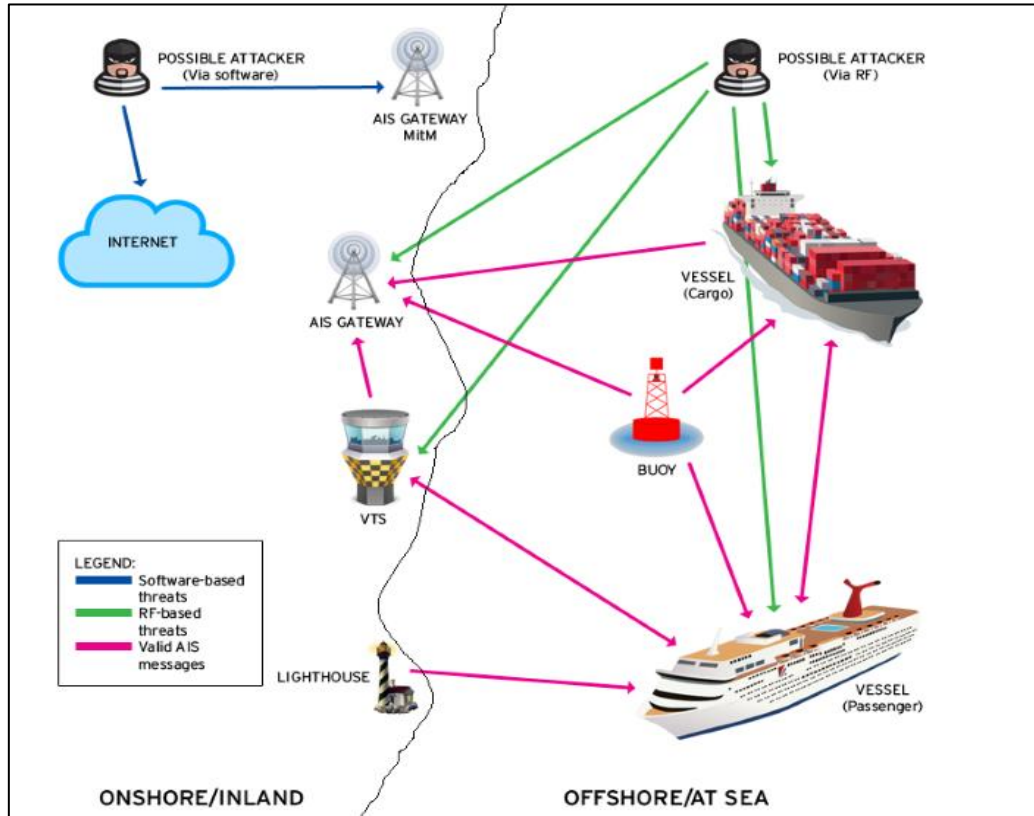


Figura 16: Dibujo de las distintas formas posibles de ataques AIS. Flechas azules: posibles ataques al software AIS; flechas rosas: enlace de datos AIS, flechas verdes: posibles ataques a los distintos transmisores AIS por radio frecuencia. **Fuente:** A Security Evaluation of AIS, Trend Micro.

El spoofing como explican en su estudio Marco Balduzzi y Kyle Wilhoit es la alteración y creación de datos AIS: simular buques falsos y modificar los parámetros de este (posición, rumbo, carga, bandera del país, nombre, MMSI). Además consiguieron también crear y modificar AtoN, aeronaves de búsqueda y salvamento marítimo, señales SART...

El caso de desencadenar alertas SART, a las que todo buque que navegue cerca del lugar de emisión de esta alarma tiene la obligatoriedad de acudir en su auxilio, esto podría permitir a los piratas conducir a los buques a la zona donde quieran atacarlos una vez lancen esta alarma.

En la Tabla 2 se clasifican las amenazas, con su incidencia según el equipo, los datos y las características.

Tabla 2: Sumario de las posibles amenazas en el protocolo y equipo AIS. **Fuente:** A Security Evaluation of AIS, Trend Micro. [13]

TABLE 1 Summary of Identified AIS-Related Threats			
Macrocategory	Threat	Software Based	RF Based
Spoofing	Ship spoofing	Yes	Yes
	AtoN spoofing	Yes	Yes
	SAR spoofing	Yes	Yes
	Closest point of approach (CPA) spoofing	No	Yes
	Distress beacon spoofing	No	Yes
	Faking weather forecasts	No	Yes
Hijacking	Hijacking	Yes	Yes
Availability disruption	Slot starvation	No	Yes
	Frequency hopping	No	Yes
	Timing attacks	No	Yes

Por otra parte, Trend Micro descubrió que los principales portales de seguimiento de información AIS como www.vesseltraffic.com, www.localizatodo.es tienen vulnerabilidades que permiten a un atacante alterar datos AIS reales e inyectar datos AIS falsos (arriba descritos). Tales portales no hacen un reconocimiento de la veracidad de la información que reciben. De esta forma, consiguieron copiar las sentencias AIS (previamente por una búsqueda en internet de ejemplos de sentencias AIS) en el protocolo que utilizan los equipos AIS para transmitir, AIVDM:

```
!AIVDM,1,1,,A,16SteH0P00Jt63hHaa6SagvJ087r,0*42
  MessageType:      1
  MMSI:              440348000
  NavigationStatus:  0
  Speed Over Ground: 0
  Longitude:         -70.7582
  Latitude:          43.08015
  Course Over Ground: 93.4
  TrueHeading:       511

!AIVDM,1,1,,A,H42O55i18tMET00000000000000,2*6D
!AIVDM,1,1,,A,H42O55lti4hhhild3nink000?050,0*40
  MessageType:      24
  MMSI:              271041815
  Name:              PROGUY
  ShipAndCargo:      60
  VendorID:          1D00014
  CallSign:          TC6163
  Dimensions:        15x5
```

Listing 1: Sample AIVDM sentences for position (top) and static (bottom) reports

Figura 17 : Ejemplo de sentencias AIVDM para reportes de posición (arriba) y estáticos (abajo).
Fuente: A Security Evaluation of AIS, Trend Micro [13]

Por otro lado, descendieron un codificador AIVDM: “AIVDM Encoder” para generar sentencias con este protocolo. Crearon un script (algoritmo) que pudiera suplantar una estación AIS describiendo una derrota durante un tiempo. El resultado fue crear un barco siguiendo la derrota de la palabra “PWNED” en el mar Mediterráneo como muestra la imagen abajo:

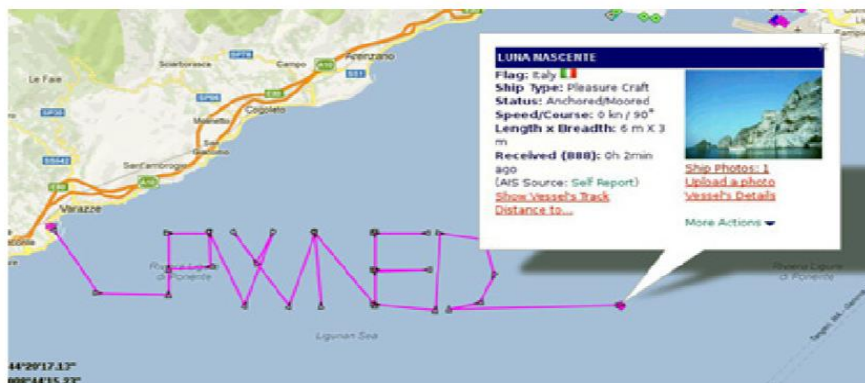


Figura 18: Derrota seguida por el barco ficticio. **Fuente:** A Security Evaluation of AIS, Trend Micro [13].

Pudieron comprobar a la vez que llevaban a cabo el experimento, cómo los portales web de visualización de ecos AIS monitorizaban inmediatamente este Spoofing. Esta vulnerabilidad del sistema se debe a que el protocolo de AIS fue diseñado sin tener en cuenta, aparentemente, consideraciones de seguridad como aparece reflejado en la web de Tren Micro [14]:

1. **Falta de Controles de Validez:** Es posible enviar un mensaje AIS desde cualquier ubicación a un buque en otro lugar. Por ejemplo, es posible enviar un mensaje desde un lugar a otro, y será aceptado sin que se cuestione. **No se llevan a cabo controles de comprobación geográfica.**
2. **Falta de Controles de Calendario:** También es posible reproducir información AIS existente (y que es válida), porque la información sobre las indicaciones no está incluida en el mensaje, por ejemplo, es posible replicar la posición de una embarcación. Es el ejemplo de uno de las pruebas que se hicieron en Texas dónde los autores del estudio replicaron la posición de un buque que navega por la costa de dicho estado y lo duplicaron a un lago cercano.
3. **Falta de Autenticación:** El protocolo AIS no incluye ningún sistema de autenticación. Esto significa que cualquiera que pueda elaborar un paquete AIS puede suplantar a cualquier otro barco en el planeta y todos los buques que lo reciban interpretarán el mensaje como un hecho.
4. **Falta de Comprobaciones de Integridad:** Todos los mensajes AIS se envían sin cifrar lo que los convierte en un objetivo fácil de interceptar y modificar.

Marco Balduzzi y Kyle Wilhoit concluyen como resultado del estudio que [13]:

« Tanto la implementación de AIS y la especificación del protocolo se ven afectadas por varias amenazas, abriendo la puerta para que los agentes maliciosos puedan descubrir y aprovechar las posibilidades de ataque»

2.2) El uso indebido de la información AIS.

A- Estudio de un caso real:

Gracias a los artículos extraídos de la Agencia de comunicaciones Bloomberg, 19 de Octubre de 2014 accesible en <http://www.bloomberg.com/news/articles/2012-10-19/iranian-oil-tankers-said-by-zanzibar-to-be-signaling-wrong-flag> [15; 16] y de la revista especializada en negocio marítimo The Maritime Executive que publicó el artículo: *Iran, Tanzania and Falsifying AIS Signals to Trade with Syria*. [17]. Al igual que en otros artículos de prensa especializada [18; 19], se puso de manifiesto las diversas irregularidades que se llevaban a cabo por parte de buques de ciertos pabellones.

La compañía naviera National Iranian Tanker Company (NITC) que cuenta con 58 buques tiene la reputación de pertenecer al gobierno Iraní por ser una filial de la Compañía Nacional de Crudo Iraní (privatizada en 2009). De acuerdo con el gobierno iraní el NITC es propiedad de un fondo de inversión que también maneja las pensiones de 5 millones de iraníes. La naviera ostenta también el título de ser la compañía de buques tanque más importante de Oriente Medio y la cuarta en el ranking mundial moviendo una capacidad de 11 millones de toneladas de crudo al año y con una perspectiva de crecimiento que contempla la proyección de nuevas construcciones hasta alcanzar el número de 74 buques tanque de diferentes esloras incluido un gran número de VLCCs.

Entre Septiembre y Diciembre de 2012 tiene lugar la denuncia de varios países a Irán y Siria, acusados de transmitir información falsa que se tenga constancia entre los días 24 de Septiembre y 13 de Octubre con el fin de comerciar entre ellos. Y es que debido a los programas nucleares que lleva a cabo Irán y la guerra civil y la violación de los derechos humanos que suceden en Siria, tanto la UE como los Estados Unidos han impuesto una sanción que prohíbe la importación de crudo desde estos países así como la prohibición a cualquier buque de transportar su crudo y la prohibición a cualquier Sociedad de clasificación o aseguradoras marítimas de los 27 miembros de

la UE a registrar dichos buques. Como consecuencia de esto, los buques de la NITC que enarbolaban el pabellón de Zanzíbar, región perteneciente a Tanzania perdieron dicho registro. Sin embargo la naviera ha supuestamente cambiado el nombre y banderas en muchos de sus buques con el fin de obtener financiación y seguros sobre las cargas. La concentración de la industria de seguros marítimos en Europa hace que aproximadamente el 95 por ciento de la flota mundial de buques tanque tengan como Sociedad de clasificación una compañía de la UE. Esto deja a Irán, siendo el segundo mayor productor de la OPEP, más dependiente que nunca de sus propios buques para exportar crudo. Las exportaciones de crudo promediaron aproximadamente 1,2 millones de barriles al día en las fechas donde se puso de manifiesto esta deficiencia, según datos compilados de la agencia Bloomberg [15; 16].

La respuesta de la naviera a estas restricciones para poder navegar y asegurar el transporte de crudo y así sostener el negocio nacional fue la de ir cambiando de estado de bandera: Zanzíbar, Tuvalu, Chipre, Malta etc. El problema se acentúa con las nuevas investigaciones que apuntan a una agencia aseguradora y consignataria con domicilio fiscal en Dubai Philtex Corporation que obtuvo el contrato para gestionar el registro internacional de buques de Tanzania Zanzibar (TZIRS) y que sin un supuesto conocimiento del país en cuestión, registró buques Iraníes bajo la bandera de este.

Por otra parte, y una vez que el recurso de cambio de registro se agotó por las presiones internacionales a estos países, se llevó a cabo la manipulación de la información AIS, esto es, la falsificación de sus transmisiones de datos, la duplicidad de esta en dos puntos distintos y finalmente el corte intencionado de las transmisiones AIS para ocultar sus viajes a otros países y en particular entre Irán y Siria, países aliados y que canjean sus exportaciones ya que los dos, como hemos dicho, están sujetos a restricciones económicas internacionales. Los buques de la naviera NITC transmitían información de otros buques que se encontraban también en navegación con el consiguiente problema que el mismo barco parecía estar en dos lugares distintos a la vez. Fue el caso del buque tanque *Millionaire* que suplantó la información AIS del buque *Lady Rasha*. El *Millionaire* cambió su MMSI, de



572450210 para apropiarse del MMSI del Lady Rasha: 677030700. Dando lugar a dos ecos que emitiendo el mismo MMSI uno navegaba por el Mediterraneo y otro por el Índico. Otro ejemplo similar a este fue la suplantación del MMSI por parte del Pioneer de la naviera NITC al Talavera, buque de carga general registrado en Tanzania. Según fuentes diplomáticas encargadas de supervisar los petroleros iraníes: *“El uso de otro MMSI distinto al suyo sólo puede llevarse a cabo en buques de mismo estado de bandera y tiene que realizarse por uno de los trabajadores de las oficinas de la bandera “*. [19]

Cabe destacar por tanto el uso ya a nivel estatal de la falsificación de datos AIS en beneficio de los intereses nacionales, sin embargo lejos de ser una actividad puntual, y de algunos países con políticas al margen de los tratados y libertades internacionales o en estado de guerra, empieza a ser muy habitual para camuflar actos criminales de muy distinta índole: desde pesca ilegal por parte de pesqueros chinos (40% de los delitos de falsificación de datos AIS según un reciente estudio), descarga de aguas de sentina intencionadas o descarga de fuel accidental, actividades comerciales no permitidas entre países con restricciones internacionales...

Si bien es verdad que antes de 2002, cuando se implantaron los equipos AIS a bordo, no había ningún método de seguimiento de los buques, y por tanto podían cometer las infracciones que quisieran impunemente, la tendencia es tener el control sobre las actividades de estos una vez salen de puerto.

Por otra parte y como señala el SOLAS, la OMI actualizó la norma referente a AIS por medio de la siguiente enmienda: *Amendments to the guidelines for the onboard operational use of shipborne automatic identification systems (AIS) (RESOLUTION A.917(22))* donde recalca [6]:

-“Unless it would further compromise the safety or security, if the ship is operating in a mandatory ship reporting system, the master should report this action and the reason for doing so to the competent authority”-



Esto permite que los capitanes apaguen el equipo AIS en zonas de riesgo de ataque por parte piratas o terroristas.

El sistema AIS es de difusión, por lo que cualquiera puede comprar un equipo y recibir información, sin discriminación. La información AIS que es muy útil para la navegación y para las autoridades, también lo es para organizaciones o estados que se mueven al margen de la legislación. Cabe entonces la necesidad de cubrir esta deficiencia, notoriamente y en primer lugar para organismos y cuerpos de seguridad del Estado: compartir información de forma segura, inmediata y accesible entre aquellos buques, embarcaciones o aeronaves de organismos estatales. En el siguiente apartado, estudiaremos una solución del sistema AIS en lo referente a enlaces de transmisión de datos de forma más restrictiva.

3) SISTEMA AIS SEGURO

Como hemos visto en el apartado anterior, la red de AIS es demasiado abierta y cualquier usuario puede comprar un equipo AIS instalarlo en su casa y empezar a recibir datos AIS. De ahí nacen las páginas web donde tenemos acceso a la visualización de los blancos. Cabe entonces pensar en dar una solución para aquellos organismos que quieren mantener un enlace de datos entre las distintas unidades de forma veraz, segura e inmediata. Dichos organismos como la Armada, Policía, Guardia Civil, Servicios de Vigilancia Aduanera, Salvamento Marítimo, etc. pueden tener la necesidad de intercambiar información encriptada entre sus unidades y poder también recibir información AIS abierta sin transmitir su posición.

3.1) Introducción al Sistema AIS Seguro

3.1.1) Concepto Seguro

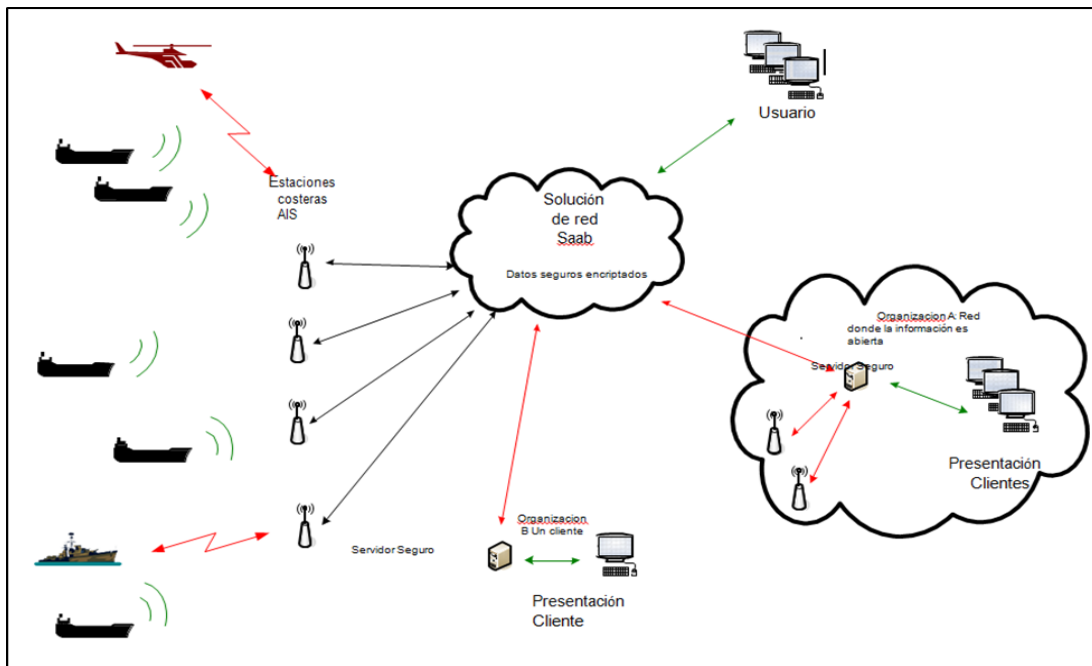


Figura 19: Visión general del Sistema Seguro mostrando datos encriptados y abiertos. Flechas verdes: enlace de datos AIS; flechas rojas: enlace de datos encriptados. **Fuente:** Saab Secure AIS System overview [20]

La función principal del AIS Seguro es proporcionar un enlace de datos encriptados

independientes de los datos de un transpondedor AIS común. Dicha función adicional tiene soporte en todos los productos relacionados AIS incluyendo los transpondedores a bordo, tanto de los buques como de los medios aéreos, estaciones base, redes y sistemas de monitorización. El manual de Instalación y Software de AIS Seguro del fabricante (Saab), nos indica las configuraciones y funciones que presenta este equipo. [20; 21]

3.1.2) Características del sistema

Las principales características del AIS Seguro son:

- 1- Canal dedicado exclusivamente para información encriptada (tercer canal) separado de los canales paralelos, para la función “*channel in parallel with standard AIS operation*”.
- 2- El AIS seguro no necesita un equipamiento externo a bordo.
- 3- Todos los equipos de AIS Seguro que se integren en buques o aeronaves se mantienen invisibles a usuarios estándar de AIS.
- 4- El concepto Seguro utiliza un receptor interno dedicado a la función no-AIS mientras que mantiene todo su rendimiento en los canales AIS 1 & AIS 2.

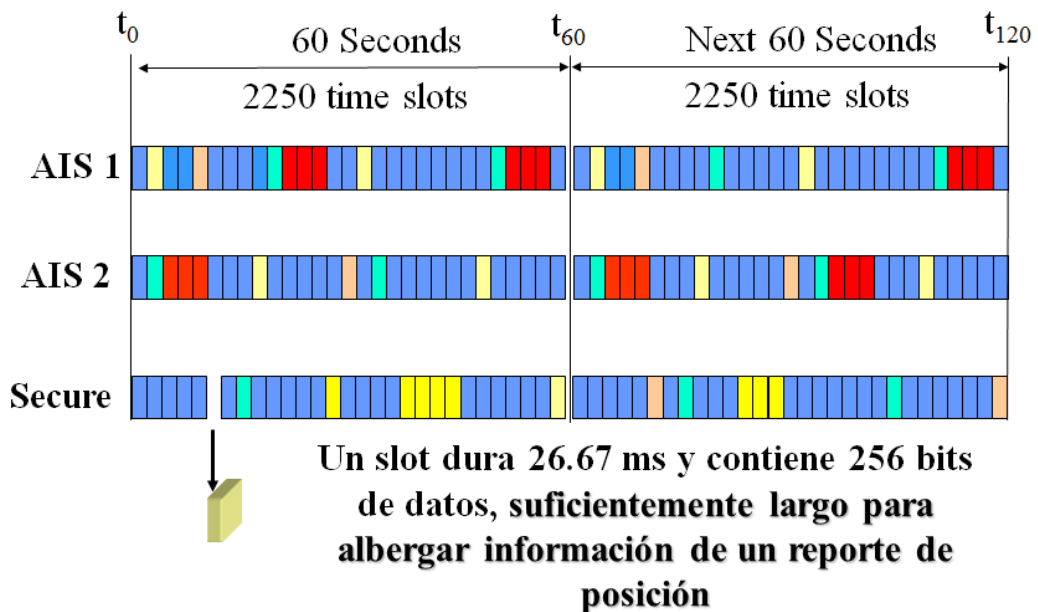


Figura 20: Esquema de transmisión de datos Seguros y convencionales. **Fuente:** Airborne AIS Solution Manual. [22]

A parte de las ya conocidas funciones como la de sistema de posicionamiento automático y envío de mensajes de texto, el tercer canal encriptado puede utilizarse para muchas aplicaciones. Abajo vemos varios ejemplos:

- Compartir vistas de situación
- Coordinación de misiones
- Administración de la flota
- Distribución de puntos y áreas de interés
- Distribución de planos de búsqueda y rescate
- Monitorizar misiones de búsqueda y rescate

La función Segura de AIS proporciona la posibilidad de funcionar en modo AIS convencional como cualquier transpondedor móvil (no encriptado) o en modo Seguro, el cual permite al usuario comunicarse por el enlace encriptado, asegurando así una comunicación protegida entre grupos o unidades móviles definidas. También puede llevarse a cabo la integración de esta función en estaciones base, red de usuarios y sistemas de monitorización. Este sistema permite tener una visión global de la situación mientras permaneces invisible a los usuarios estándar de AIS.

El sistema se basa en el diseño del transmisor utilizado del transpondedor, por medio del tercer canal se puede reconfigurar para funcionamiento seguro. Los tres canales tienen el mismo diseño y rendimiento por lo que al utilizar el modo seguro donde el enlace de datos seguros es totalmente independiente de los otros dos canales convencionales AIS, la carga de datos no baja el rendimiento de transmisión / recepción de la información AIS.

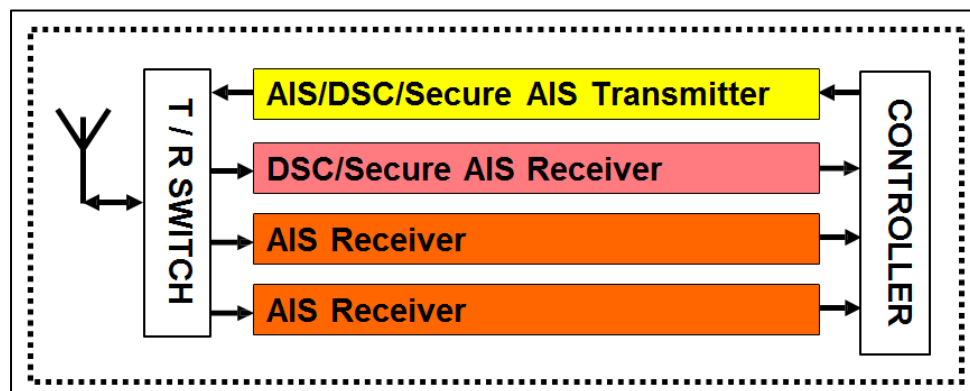


Figura 21: Diagrama de transmisión de datos Seguros. **Fuente:** Saab Secure AIS System overview [20].

El desarrollo de la aplicación segura se empezó a desarrollar considerando la creciente demanda de eliminar comunicaciones inseguras en los canales AIS, por ejemplo por el uso no solicitado de mensajes binarios de transferencia de datos desaconsejado para las autoridades. Por otra parte la cantidad de datos está también limitada de acuerdo con los estándares de los equipos AIS.

En una zona de tráfico marítimo intenso donde operan muchos transpondedores AIS, el sistema Seguro permite que el rendimiento sobre el enlace encriptado no se vea afectado por las transmisiones de AIS convencional. Dicho rendimiento en otro sistema puede reducirse significativamente en condiciones de aumento de tráfico de datos debido a que el ancho de banda de estas redes no es capaz de soportar tales cargas de datos. Sin embargo el hecho de que los datos Seguros viajen en otro canal con un ancho de banda idéntico a los otros dos canales no suponen una carga añadida a los ya saturados enlaces propios de emisión-recepción de datos AIS convencionales, es más, este sistema permite nuevas aplicaciones por parte del usuario desarrolladas en modo Seguro.

3.1.3) Comunicación en el canal encriptado

La estructura del mensaje AIS Seguro es similar al utilizado en las comunicaciones AIS convencionales aunque esta optimizado para transferir datos de forma más eficiente. Los más importantes son:

- Reporte de posición
- Emisión de mensajes de texto
- Emisión de mensajes binarios para aplicaciones externas
- Mensajes de interrogación

3.1.4) Interfaces hacia sistemas externos

La encriptación y desencriptación de datos se lleva a cabo internamente en los

transpondedores móviles, los sistemas externos que admiten estándares AIS (e.g. un ECDIS) deben también trabajar apropiadamente y ser capaces de procesar datos AIS recibidos en el enlace encriptado. Con el fin de distinguir claramente entre los datos AIS convencional y AIS Seguro, se recomienda sin embargo que el sistema externo esté adaptado para compatibilizar las funciones del AIS Seguro. El AIS Seguro permite a las estaciones bases reenviar los datos encriptados a las redes donde se decodificarán gracias a un software dedicado a ello.

3.1.5) Modos operacionales

Las unidades móviles de transpondedores pueden utilizarse en modo Seguro de la siguiente forma:

➤ Normal:

En este modo la unidad actúa como un sistema AIS convencional. La transmisión de los mensajes salientes se efectúa en formato abierto en ambos canales AIS. Los encriptadores no están activados en este momento, por tanto no se recibirá ni mandará ningún mensaje por el enlace encriptado.

➤ Modo Silencio

La unidad no transmitirá ningún mensaje y no responderá a ningún mensaje interrogativo de otras unidades. La unidad solo recibirá datos AIS convencionales, como cualquier transpondedor AIS convencional, y si se ha cargado un decodificador también podrá recibir mensajes encriptados.

➤ Modo táctico

La unidad recibe y procesa mensajes AIS convencionales y Seguros. La unidad automáticamente generará reportes de posición para transmitir en el enlace encriptado, pero no transmitirá ningún mensaje AIS convencional y no responderá a ningún mensaje interrogativo de unidades AIS convencionales. El usuario puede

reducir o incrementar la velocidad de reporte para optimizar la transmisión y controlar la carga de datos en el canal encriptado.

➤ **Modo híbrido**

Este modo puede utilizarse comúnmente antes de cambiar a un modo táctico y después de operar en el modo táctico. El canal encriptado está activado y la unidad recibe tanto mensajes AIS convencionales como Seguros. La unidad puede transmitir en los canales AIS convencionales y en el tercer canal de forma autónoma de acuerdo con su configuración.

3.2) Aplicaciones del equipo a bordo

3.2.1) General

El canal de datos encriptados puede utilizarse para transferencia arbitraria de datos. El número de aplicaciones para dicho canal es ilimitado: mando de misiones, transferencias de puntos de interés, manejo de la flota por medio de sus propias aplicaciones externas...

3.2.2) Aplicaciones propias

A.- Relé de posición

Una función interna de una estación base con software AIS Seguro incorporado es la posibilidad de responder de forma autónoma a preguntas de vistas de situación, desde por ejemplo barcos aeronaves o bases costeras, sin ninguna necesidad de aplicaciones externas.

Sistema “Secure-AIS”: Una propuesta de aplicación en operaciones de abordaje de buques

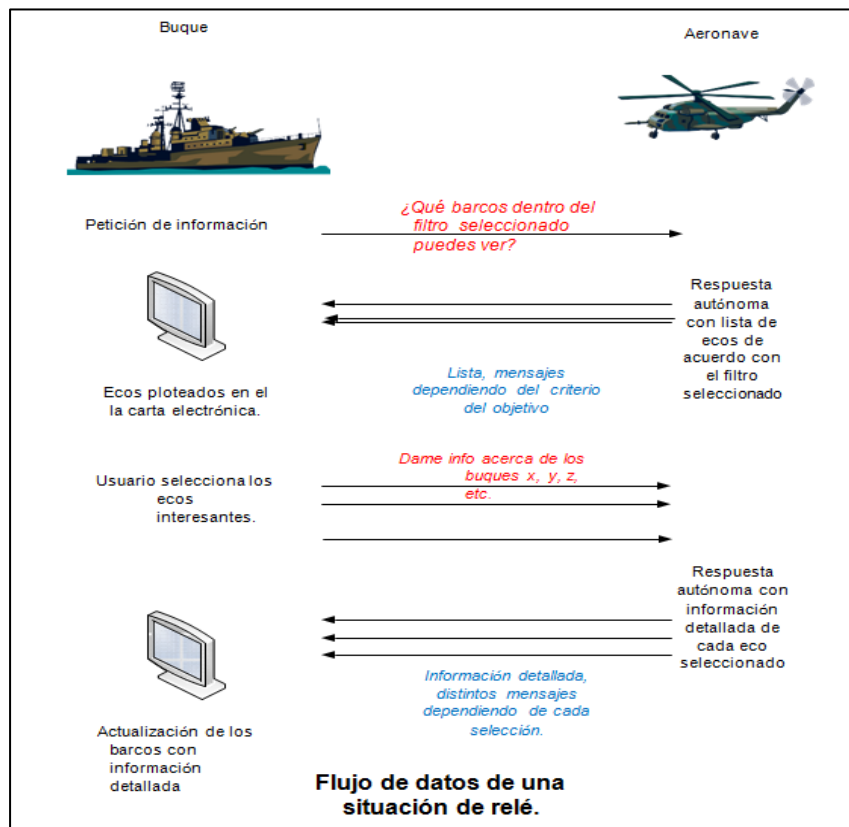


Figura 22: Relé de situación aeronave/buque/estación costera. **Fuente:** Saab Secure AIS System overview [20]

Con el fin de monitorizar una imagen de situación en, por ejemplo, un barco o centro de mando, se requiere un ordenador dedicado a dar soporte a esta función.



Figura 23: Antes y después de una petición de vista de situación. **Fuente:** Saab Secure AIS System overview [20]

B.- Mensajes de texto cortos

Esta es la forma más sencilla de aplicación pero también una de las más flexibles ya que permite tanto mensajes libres como predefinidos. Este tipo de aplicación aparece en todos los sistemas AIS.



The image shows a software interface for sending a message. It is titled 'New Message'. There is a 'To' field containing '999011011'. Below it is a 'Send' button. To the right of the 'Send' button is a large text area containing the text 'This is an example of an message'. Below the text area are three dropdown menus: 'Predef' with 'Example' selected, 'Type' with 'Addressed' selected, and 'Channel' with 'Secure' selected.

Figura 24: Ejemplo de mensaje. **Fuente:** Saab Secure AIS System overview [20]

C.- Misiones de búsqueda y rescate (SAR)

Las misiones SAR requieren de una enorme colaboración entre diferentes cuerpos de búsqueda y rescate SRU (Search and Rescue Unit). Cada SRU tiene que interferir con las demás lo menos posible, pero manteniendo pleno conocimiento del resto. Se busca minimizar la necesidad de comunicaciones de voz vía radios analógicas con la dificultad de escuchar las instrucciones y el riesgo que tiene la malinterpretación de estas. El flujo de datos que ofrece se muestra en el siguiente esquema:

Sistema “Secure-AIS”: Una propuesta de aplicación en operaciones de abordaje de buques

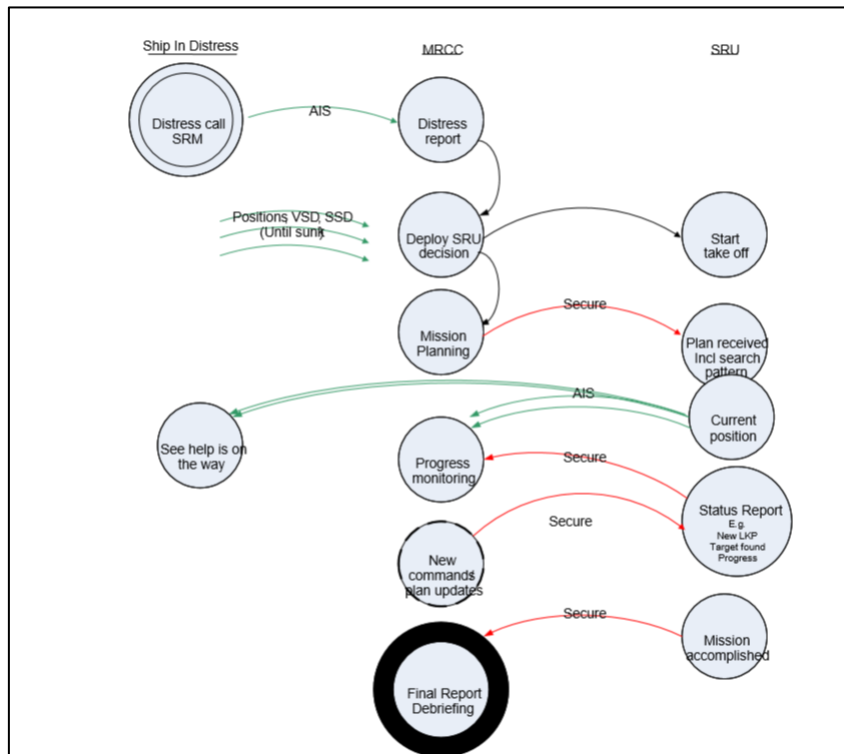


Figura 25: Flujo de datos en misiones SAR. Flechas verdes: datos AIS – Flechas rojas datos encriptados. **Fuente:** Saab Secure AIS System overview [20]

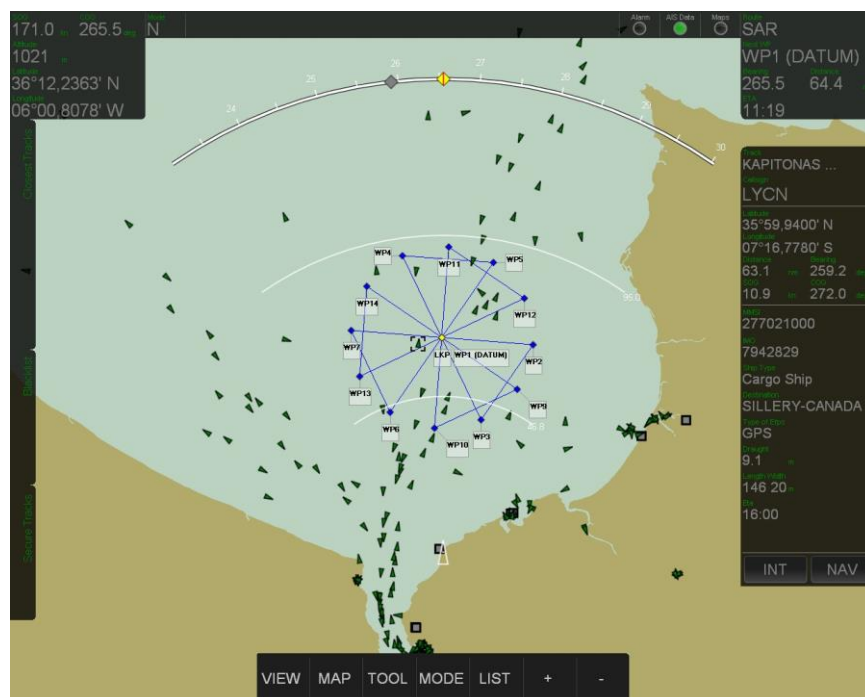


Figura 26: Patrón de búsqueda SAR enviado desde MRCC (estación costera) a aeronave. **Fuente:** Saab Secure AIS System overview Software Coastwatch. [20]

D.- Vigilancia y base de datos de buques

La vigilancia consiste en hacer el seguimiento de algún objetivo. Existen muchas herramientas dentro de una organización que tienen el propósito de visualizar y controlar el tráfico o representar la situación. En cualquier caso necesitan una base de datos de referencia donde poder almacenar toda la información de los buques a la vista. Por ejemplo, una base de datos de una estación costera conectada a un número de unidades móviles de AIS Seguros puede recibir actualizaciones en tiempo real de barcos. Otro ejemplo más, una aeronave de vigilancia puede sobrevolar un buque fuera del alcance de una estación costera, recoger los ecos por inspección visual e información AIS y cotejarlos con su base de datos local. Si se verifican los datos, se puede hacer el informe de reconocimiento a la estación costera, y en el caso de que algo sea incorrecto notificarlo a la estación base.

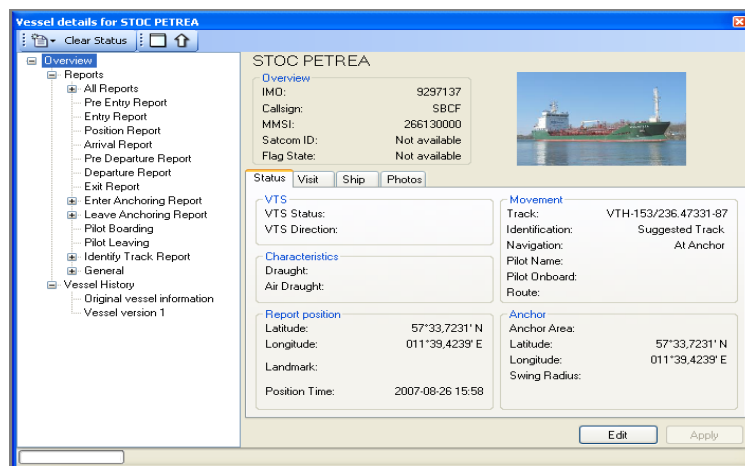


Figura 27: Base de datos de buques de una estación costera. **Fuente:** Saab Secure AIS System overview Software Seawatch. [20]

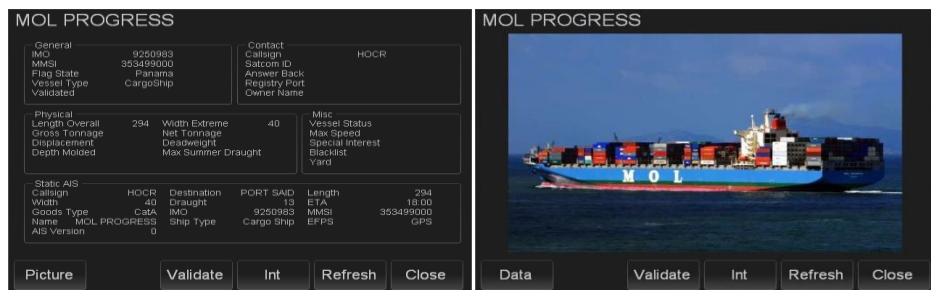


Figura 28: Base de datos software Sea Watch. **Fuente:** Saab Secure AIS System overview Software Seawatch. [20]

E.- POI y rutas

Una función utilizada e incorporada en muchos (W)ECDIS (ECDIS utilizados por las fuerzas armadas) es la posibilidad de mandar información de los puntos de interés: Points Of Interest (POI), áreas o rutas, ej. En misiones militares o vigilancia costera.

El operador de una unidad simple, marca un área o punto y seguidamente manda la información a otra unidad en la que tiene que llevar a cabo una investigación. Los puntos y áreas aparecerán en la pantalla de la unidad receptora.



Figura 29: Imagen de POI y rutas. **Fuente:** Saab Secure AIS System overview Software Seawatch. [20]

Además de las aplicaciones de AIS Seguro, existen algunas funciones opcionales relacionadas ofrecidas a parte. Estas están estrechamente relacionadas con aplicaciones demandadas por las fuerzas armadas en el contexto de estandarización de la OTAN: Warship AIS (WAIS).

3.2.3) Opciones para sistemas AIS Seguro

A.-Warship

La opción Warship para los transponders marítimos AIS Seguro (R4S) incluye

características especiales bajo los requerimientos de los usuarios de las fuerzas militares.

B.-OTAN Warship

La opción OTAN Warship de AIS Seguro permite transmisiones encriptadas: a través de los canales estándar AIS de acuerdo con STANAG 4668 edición 2.

3.3) Productos AIS Seguro

Todos los productos están diseñados para estar interconectados y operar en un amplio sistema AIS Seguro.

3.3.1) Transpondedores AIS Seguro marítimo

El transpondedor AIS Seguro está basado es de Clase A. Esto significa que un sistema Clase A puede actualizarse a cualquier versión AIS Seguro / Warship por medio del software:

- Secure AIS
- Secure y Saab Warship AIS
- Secure y OTAN Warship AIS
- Secure, Warship y OTAN Warship AIS (R4SWN)



Figura 30: Traspondedores marítimos. **Fuente:** Saab Secure AIS System overview

3.3.2) Transpondedor AIS Seguro Aereo



Figura 31: Transpondedores aéreos. **Fuente:** Saab Secure AIS System overview. [20]

Al igual que la versión marítima, puede actualizarse a Seguro por medio del software.

3.3.3) Estación base

La versión Segura para estación base se utiliza para recepción y transmisión en tierra de mensajes y datos Seguros. La estación base AIS R40S puede utilizarse de forma independiente o conectada a una red de infraestructuras. Los mensajes recibidos por el R40S se etiquetarán como mensajes Seguros y enviados vía la red de interfaces. Los mensajes Seguros pueden enviarse en el mismo puerto TCP/IP como mensajes convencionales AIS o pueden configurarse para utilizar su propio número de puerto dependiendo de los requerimientos LAN/WAN del usuario.



Figura 32: Estación base. **Fuente:** Saab Secure AIS System overview. [20]

Hay que decir que el R40S no encripta/desencripta ningún mensaje Seguro, se necesita un software externo (ej. Módulo Seguro) para llevarlo a cabo.

3.3.4) Módulo Seguro independiente

Permite integrar una red para acceder a los datos Seguros. Junto con una estación base (R40S) funciona como un sistema de estación base Segura independiente capaz de codificar y decodificar datos y mensajes Seguros. Como muestra abajo la imagen:

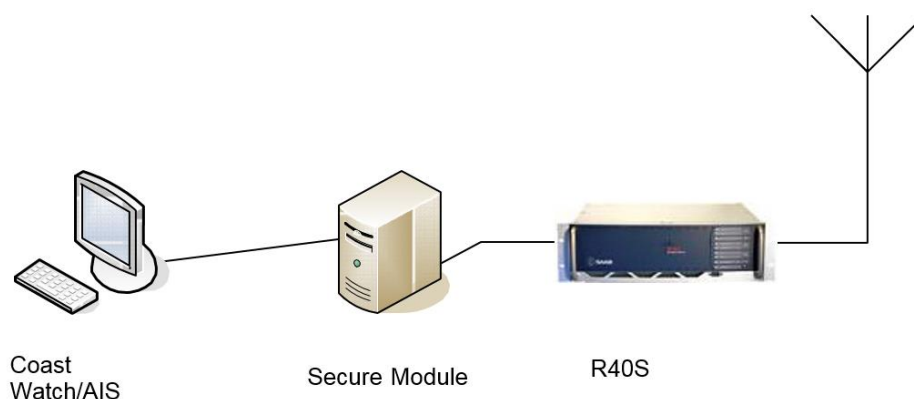


Figura 33: Red segura: Monitor, Módulo Seguro y estación base. **Fuente:** Saab Secure AIS System overview [20]

3.3.5) Servidor Seguro – Red Segura

El Servidor Seguro permite conducir los mensajes Seguros mediante una red AIS. El servidor Seguro lleva a cabo lo siguiente:

- Configurar la estación base
- Enrutar los mensajes Seguros a la estación
- Conexión directa estación y/o redes
- Manejo de la mensajería
- Responsabilidad de interrogación (por ejemplo si distintos clientes quieren plotear un eco específico solo se manda un mensaje por el VDL)

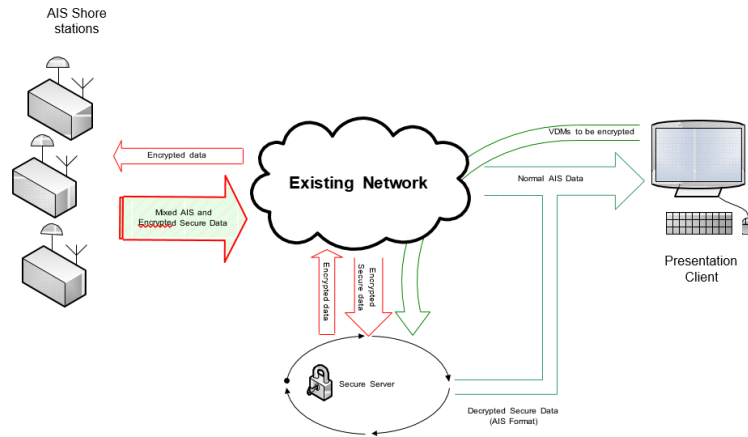


Figura 34: Red segura: estaciones base, servidores seguros, monitores. **Fuente:** Saab Secure AIS System overview. [20].

3.4) Software generador de claves Seguras

Con el fin de llevar a cabo comunicaciones seguras, todas las unidades AIS Seguro que intercambian información están configuradas con la misma llave operativa. Existen distintas formas de generar dichas claves y todas ellas son criptográficamente difíciles, al azar e impredecibles.

El software para generar claves es una aplicación Windows con funcionamiento en cualquier PC equipado con una tarjeta inteligente para acceso y control.

La clave generada por el software Key Generation incluye los siguientes datos:

- Clave de encriptación (128 bits)
- Tiempo de validación (1 a 720 horas o infinito)
- Canal de funcionamiento (cualquier canal de 25 kHz en el rango de 155,00 a 163,00 MHz)
- Ratio de reporte (máximo 1 report/seg)
- Organización ID utilizada una vez que se activa

Dicha clave puede ser electrónica, vía e-mail o mediante un enlace encriptado.

Sistema “Secure-AIS”: Una propuesta de aplicación en operaciones de abordaje de buques

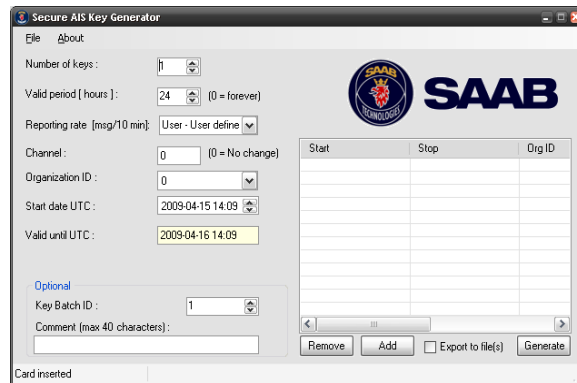


Figura 35: Encriptador. **Fuente:** Saab Secure AIS System overview [20]

4) DISCUSIÓN SOBRE LA NUEVA APLICACIÓN DEL AIS SEGURO PARA CASOS DE ABORDAJE

Por tanto después de tener una visión general del sistema AIS Seguro planteamos los beneficios que pueden aportar su utilización:

- Las aplicaciones de este elemento no tienen la necesidad de equipamiento a bordo, una simple actualización y adaptabilidad del Software al Hardware ya existente es suficiente.
- Permite la monitorización de los buques y aeronaves equipados con sistemas AIS Seguro y AIS convencional mientras que se mantienen invisibles a los usuarios convencionales.
- El sistema AIS Seguro emplea un receptor interno dedicado para una función ajena al AIS convencional de esta forma mantiene el pleno rendimiento en los canales 1 y 2 AIS.
- Permite la transferencia de lista de blancos propia a otras unidades, a través del enlace Seguro, la presentación de listas de blancos AIS recibidas de otras unidades Seguras así como la grabación y reproducción de datos AIS

En vista de los beneficios del sistema, desde aquí hacemos una propuesta para su integración en las embarcaciones de los distintos organismos de fuerzas y cuerpos de seguridad del estado, así como en la armada, para facilitar aquellas operaciones que requieran maniobras de abordaje de otras embarcaciones. Las operaciones se llevarían a cabo como se describe a continuación.

4.1) Operaciones de abordaje con equipos AIS Seguro: Primeras consideraciones

Si bien es verdad que las prestaciones de estos equipos son amplias y muy eficientes, en mi proyecto quiero recalcar la que a mi juicio es la más interesante y es la sinergia entre las distintas unidades AIS en el seno de un mismo operativo de unidades policiales o militares. En este apartado me centraré en llevar acabo abordajes entre buques de forma eficiente y segura entre las unidades que intervienen y el tráfico marítimo existente.

En un primer lugar, debe recalcar que una intervención en el medio marítimo entraña numerosos riesgos por el carácter ya peligroso del mar, esto es, aquellas condiciones meteorológicas que lejos de ayudar al navegante aumentan la incertidumbre del resultado de esta intervención: el oleaje, los golpes de mar, corrientes, viento, humedad, visibilidad etc. Dichos elementos, escapando al control humano, se requiere por tanto de un esfuerzo mayor en la operatividad y eficacia de las unidades, personal, naves y equipos puestos en marcha a la hora de una intervención. De este modo, cobra una gran relevancia la coordinación entre estos agentes.

Es por ello que entiendo el equipo AIS Seguro como un elemento que refuerza la sinergia entre las unidades actuantes en una operación marítima ya que este tercer canal de comunicaciones bajo el protocolo AIS encriptado tiene que servir como una interconexión suplementaria entre las unidades del operativo. De esta forma, encontramos tanto el equipo AIS para uso marítimo, a bordo de buques y en estaciones costeras, así como la serie de equipos AIS para integración en aeronaves.

4.2) Relevancia del alcance de los equipos AIS

Las características de la propagación de la frecuencia VHF: cuya banda de frecuencia es de 30 a 300MHz influye enormemente en el alcance VHF y por tanto en el alcance de transmisión/recepción de los equipos AIS. El mecanismo de propagación dominante en esta banda de frecuencias es el enlace directo punto a punto. Para las comunicaciones terrestres, el alcance depende de las alturas de las antenas transmisoras y receptoras, haremos la demostración de acuerdo con la documentación extraída de la asignatura de Radiocomunicaciones [23]:

El horizonte visual “d” a una altura “h” viene dado por la ecuación [1]:

$$d = \sqrt{2 \cdot a \cdot h} \quad [1]$$

dónde “a” es el radio de la tierra, sin embargo en las radiocomunicaciones se define el radio efectivo de la tierra “a’ ” que tiene en cuenta el efecto de encurvamiento de las ondas:

$$a' = 4/3 \cdot a$$

Teniendo en cuenta el radio efectivo, el horizonte visual d para las radioondas es:

$$d = \sqrt{2 \cdot a' \cdot h} = \sqrt{2 \cdot \frac{4}{3} \cdot a \cdot h} \quad [2]$$

Teniendo en cuenta la figura abajo, el alcance máximo $d(\max)$ se puede calcular de la siguiente forma:

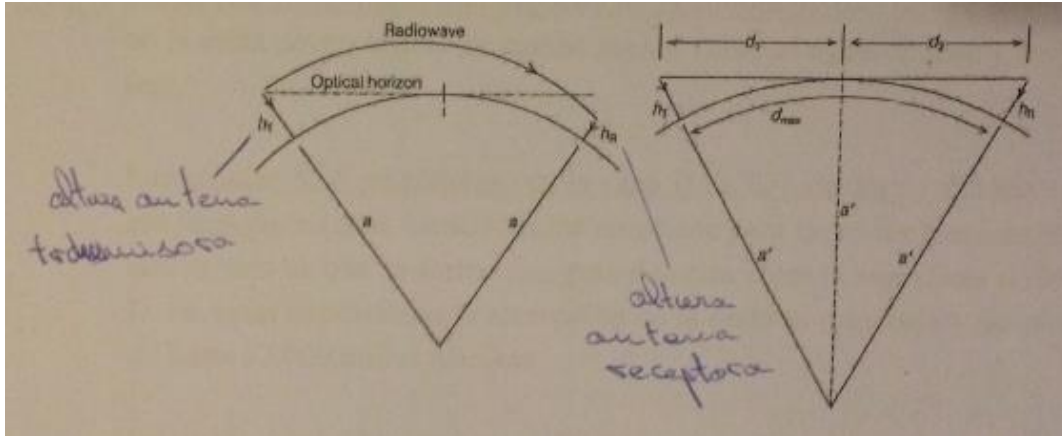


Figura 36: Esquema alcance de señal en función de la altura de la antena. **Fuente:** Espectro electromagnético y propagación de ondas. Apuntes de clase de Julio Barros. Asignatura de Radiocomunicaciones. [23]

$$d(\max) = d_1 + d_2$$

$$d_1^2 = (a' + h_T)^2 - a'^2 = 2 a' h_T + h_T^2 \quad [3]$$

Donde h_T es la altura de la antena transmisora

Teniendo en cuenta que $a' \gg h_T$, esta expresión se puede aproximar por:

$$d_1^2 \approx 2 a' h_T \quad [4]$$

Análogamente, d_2

$$d_2^2 \approx 2 a' h_R \quad [5]$$

Donde h_R es la altura de la antena receptora.

De esta forma la distancia máxima $d(\max)$

$$d(\max) = \sqrt{2 a' h_T} + \sqrt{2 a' h_R} \quad [6]$$

Teniendo en cuenta que el radio ficticio de la tierra es aproximadamente 4/3 del radio verdadero, la distancia máxima se puede expresar en millas o en km de la siguiente forma:

$$d(\max) = \sqrt{(17 h_T)} + \sqrt{(17 h_R)} \quad (\text{altura de la antena en metros}) \quad [7]$$

Esta expresión indica que el alcance en las comunicaciones VHF depende de la altura del transmisor y del receptor. Por tanto al ser una de las características de propagación de las señales en frecuencias VHF, la altura de las antenas, mayor alcance tendrá la antena de recepción de datos integrada en una aeronave que en un buque.

Por otra parte, por el carácter directo de dicha señal VHF, tiene como obstáculo para el alcance de esta, la curvatura de la tierra ya que la propagación de las ondas al ser rectas y no curvas acaban siendo absorbidas por la superficie del mar. La transmisión y recepción de datos se optimiza considerablemente cuando procede de una aeronave, sin ninguna obstrucción del terreno entre emisor y receptor. Como vemos en la figura abajo, el alcance VHF desde el aire es exponencialmente mayor en función de la altitud a la que se sitúe la aeronave.

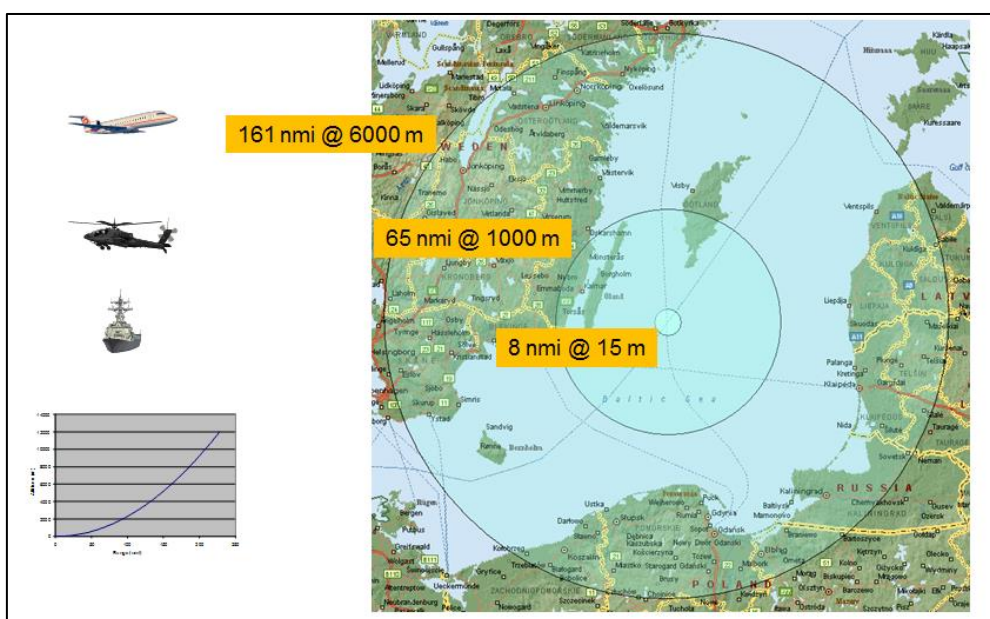


Figura 37: Comparativa entre el alcance de un equipo AIS marinizado, a bordo de un helicóptero y de un avión. **Fuente:** Saab Secure AIS AIRBORNE Systems, System Overview. [22]

Observamos que a mayor altura de la antena AIS, mayor alcance.

El vuelo de prueba con el equipo AIS Aereo: dotado de un receptor AIS acoplado al casco del avión.

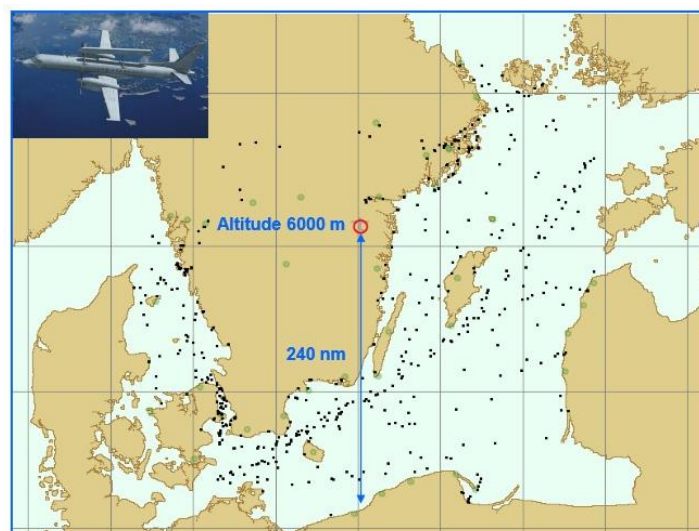


Figura 38: Vuelo del avión de Saab con el sistema Erieye. **Fuente:** Saab Secure AIS AIRBORNE Systems, System Overview. [22]

Vemos por tanto la cantidad de ecos AIS que recoge el receptor del equipo aéreo. Comparando entre un equipo marítimo y otro aéreo, obtenemos la siguiente imagen:



Figura 39: Comparativa entre alcance de ecos AIS recogidos desde un buque A y desde una aeronave B. **Fuente:** Saab Secure AIS AIRBORNE Systems, System Overview. [22]

Queda patente por tanto que el area de control aumenta enormemente con la integración del transpondedor AIS Aereo. Por otra parte, el tercer canal tiene ahora su aplicación en el sentido que proporciona un enlace de datos, independientemente de la carga de datos AIS por los canales 1 y 2 convencionales. De esta forma a través del canal encriptado la unidad aerea es capaz de mandar imágenes de los blancos AIS en tiempo real a las estaciones costeras y buques que forman parte del operativo. El número de blancos al

ser mayor permite la gestión con más anticipación de estos por parte de los centros de control.

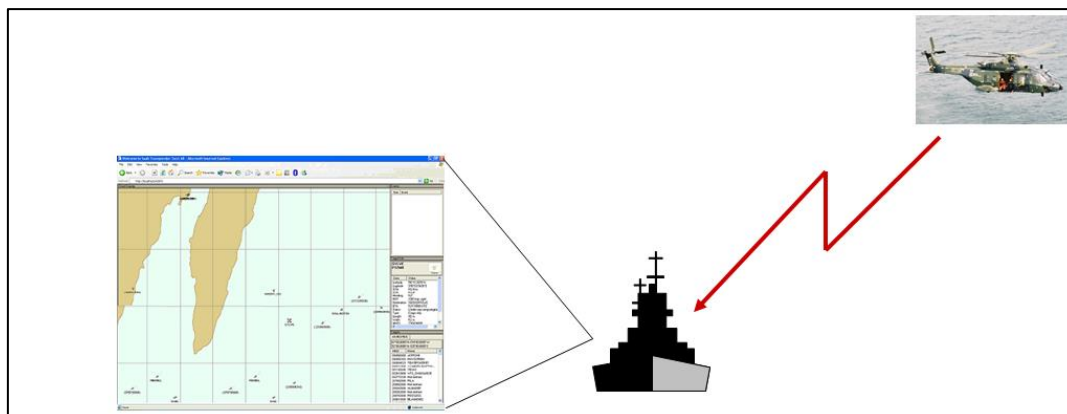


Figura 40: Esquema de transmisión datos AIS Seguros Aeronave/ buque. **Fuente:** Saab Secure AIS AIRBORNE Systems, System Overview. [22]

Se pueden descargar los datos AIS a través del enlace seguro interrogando desde un buque o desde una estación base. Esto proporciona un conocimiento completo e instantáneo del entorno marítimo. Con una velocidad de descarga de 100 kB en 100 s entre imágenes de la carta electrónica con los blancos AIS, radar e incluso video.

Se trata por tanto de anticiparse en las operaciones, de tener una visión en conjunto de la situación, alcanzar un mayor grado de información que no deje espacio a la incertidumbre. Un sistema AIS Seguro en un entorno tan imprevisible permite gestionar con mayor seguridad nuestra flota tanto aérea, marítima y terrestre. Abarcar más información en menos tiempo, que nos permitirá actuar con antelación, una herramienta que por su singularidad solo un cuerpo gubernamental tiene acceso y que se vuelve en la contra de cualquier agente malicioso.

4.3) Configuraciones especiales del AIS Seguro

En el apartado 2, hemos hablado de las deficiencias del protocolo AIS en materia de seguridad por ser un lenguaje demasiado abierto. Se convertía entonces en un equipo fácilmente hackeado en beneficio de actos ilícitos. Sin embargo en la nueva versión de AIS, esta desventaja puede tornarse a favor de los mandos de las operaciones. Y es que dentro de las opciones del equipo, accedemos en el menú de configuración:

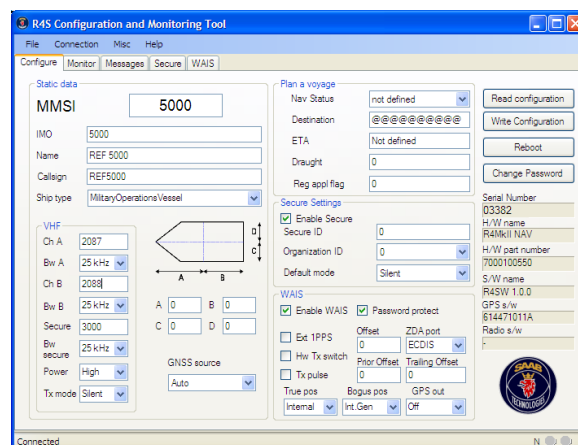


Figura 41: Pestaña de configuración de datos AIS Seguros en el software AIS S. **Fuente:** Software User Manual AIS, System Overview. [21]

Donde podemos acceder a todas las opciones de emisión y recepción de datos AIS, desde los datos estáticos del buque hasta el modo en el que queremos transmitirlos (modo normal, táctico, silencioso...)

Una de las pestañas nos permite acceder a la opción WAIS:

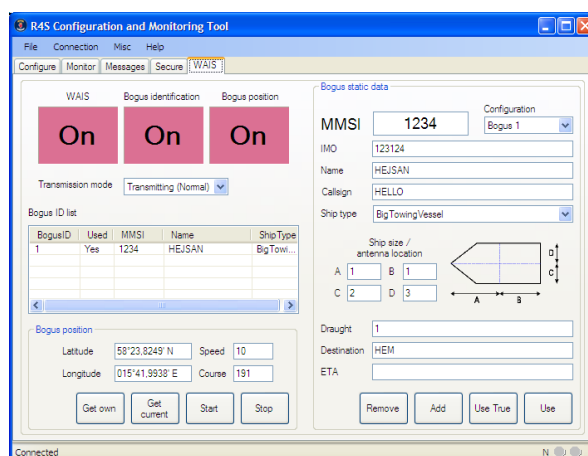


Figura 42: Pestaña de configuración de Spoofings en el software W-AIS S. **Fuente:** Software User Manual AIS, System Overview. [21]

En el que podemos crear lo que se denomina “*Bogus targets*”, como vemos en la pantalla de configuración WAIS, a cada *bogus* puede asignársele un MMSI, un nombre, un distintivo de llamada, el tipo de buque, destino, ETA y sus dimensiones. Para

finalmente crear con estas características un blanco que será transmitido por los canales AIS convencionales:

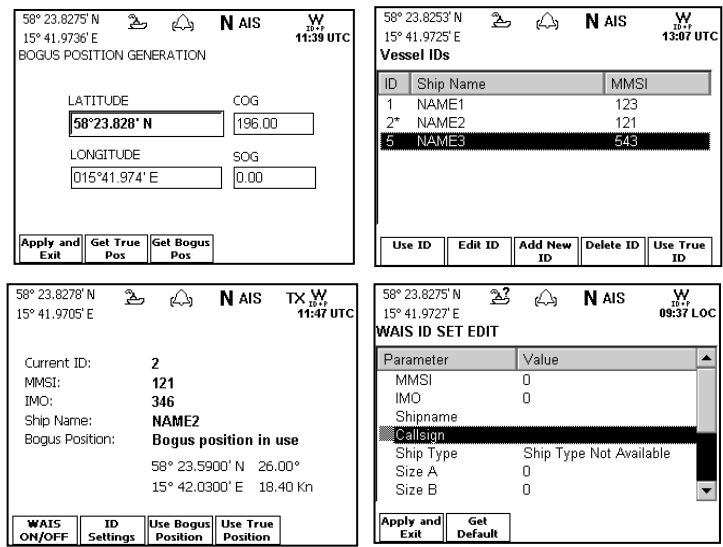


Figura 43: Pantallas del equipo AIS Seguro después de generar los Spoofings. **Fuente:** Software User Manual AIS, System Overview. [21]

En este momento estamos llevando a cabo lo que anteriormente denominábamos Spoofing.

El soporte de los datos dinámicos bogus que se lleva a cabo por el usuario del equipo Seguro, conlleva transmitir información dinámica incorrecta basada en la pre-definición de una posición inicial, rumbo y velocidad. Es posible también utilizar una fuente externa de datos bogus en base a la configuración flexible de las fuentes de posición. Sin embargo, en la práctica no se pone en marcha esta función, ya que el hecho de transmitir información incorrecta conlleva una gran responsabilidad. Si bien hay que decir que con una organización predefinida antes de una operación de abordaje, en una zona libre de tránsito, pueden llevarse a cabo Bogus Targets con el fin de sacar más rendimiento a las operaciones de abordaje a buques sospechosos.

De esta forma, y como resultado final de dicho trabajo, planteo una serie de aplicaciones al configurar Bogus Targets, es decir, crear escenarios favorables para llevar a cabo una operación de abordaje a un buque sospechoso. Esto significa que es posible mandar datos correctos por el enlace encriptado mientras creas falsos ecos por los canales abiertos 1 y 2 de AIS.

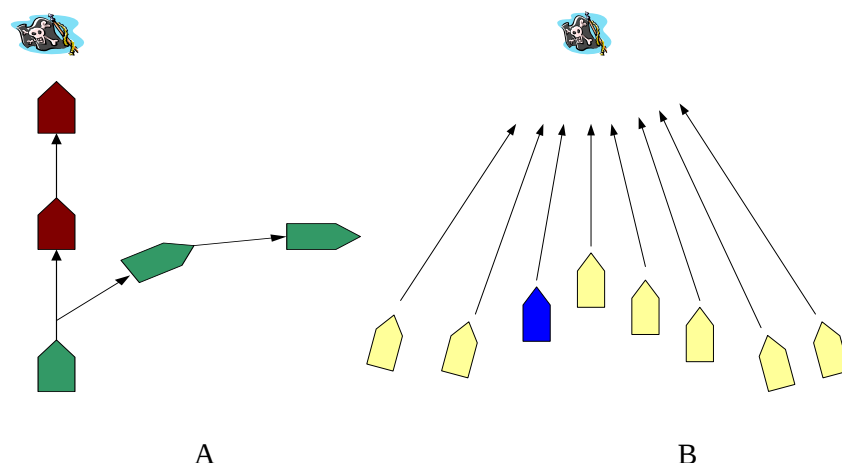


Figura 44: Esquema de organización de un abordaje por Spoofing. A) Posición en rojo: Derrota real de la unidad de intervención. En verde: derrota simulada monitorizada en la pantalla AIS convencional. B) Buque azul: Buque real. Buques amarillos: simulados por Spoofing. **Fuente:** Elaboración propia

La creación de escenarios favorables para el abordaje de buques puede hacerse creando posiciones dinámicas falsas como en el primer dibujo donde el buque a interceptar visualiza en la pantalla de monitorización de blancos AIS como parece que la lancha o buque gubernamental está cambiando su rumbo (blancos en verde) cuando realmente se está acercando al objetivo (en rojo). Por otra parte, la creación de múltiples blancos que intentan abordar al objetivo, provocará el pánico a bordo de la nave perseguida favoreciendo que cometa errores o que tome decisiones radicales provocando que pueda finalmente perder el control de la nave o provoque una avería a bordo, mientras que el operativo de intervención está ahorrando recursos tanto personales como técnicos: menor número de personas que se ponen en riesgo, menor número de unidades desplegadas con el ahorro energético y ahorro de posibles fallos de los equipos.

Existe por tanto una amplia gama para confundir al enemigo:

Tabla 3: Los distintos Spoofings y resultado buscado. **Fuente:** Elaboración propia

Parámetro falsificado	Resultado buscado
Velocidad del buque	Error en el TCPA
Rumbo del buque	Error en el CPA
Tipo de buque	Ignorar el abordaje

Otra opción también interesante para el manejo de la flota es la de crear líneas o posiciones virtuales con el fin de mejorar la organización. Gracias a la opción de transferencia de puntos y áreas de interés podemos llevar a cabo el operativo de forma más organizada, esto es, las unidades de intervención que en un abordaje desarrollan las lanchas pueden seguir el operativo de primera mano. Las ordenes son transferidas de forma clara y concisa, sin acbida a la malinterpretación de la información, y también puede servir de alluda para poner énfasis en los elementos que pueden representar un peligro añadido a la navegación: bajos, zonas de mucha corriente, zona de minas, naufragios, tendido de cable etc.

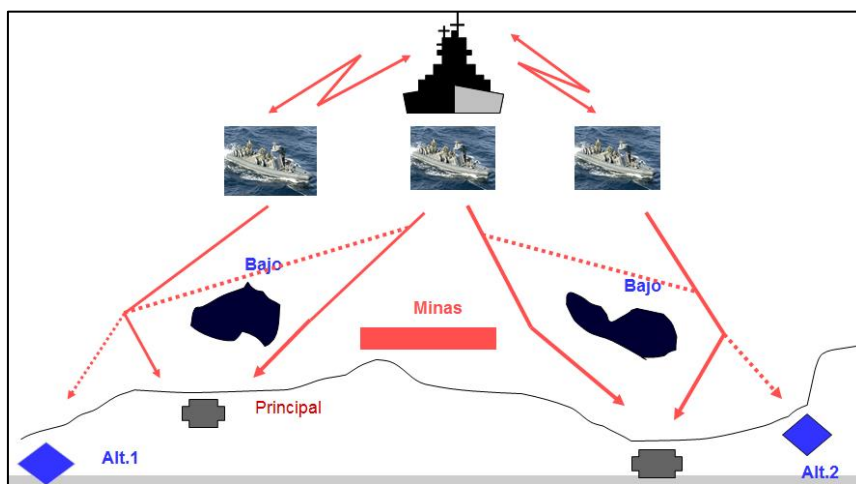


Figura 45: Esquema de organización de un abordaje. Líneas rojas rectas: derrota que deben seguir las lanchas de intervención. Líneas rojas en forma de rayo: transmisión de información por el enlace Seguro.
Fuente: Elaboración propia

Es interesante mencionar el artículo periodístico realizado por Quino Petit en Junio de 2013 “*Abordaje en alta mar*” que hace referencia al Cuerpo de Vigilancia Aduanera, cuyos barcos y aeronaves llevan a cabo abordajes a diario de embarcaciones sospechosas y donde toma real importancia la integración de estos equipos, ya que hasta el momento los sistemas que manejan el Servicio de Vigilancia Aduanera a bordo son radares, cámaras de visión nocturna y cámaras térmicas.



Figura 46: Por Gianfranco Tripodo, abordaje de un velero sospechoso a unas millas de la Isla de Alborán. Lancha de intervención del buque Fulman del Servicio de Vigilancia Aduanera. **Fuente:** El Dominical de El País, 3 de Junio de 2013. [24]

4.4) Una ayuda en materia de vigilancia y su función disuasoria

Es importante poner de manifiesto que los recursos con los que los Estados ponen a disposición de los cuerpos de seguridad y vigilancia pueden llegar a ser muy escasos en las aguas territoriales de cada país y ni que decir queda en aquellas zonas de alta mar o aguas internacionales donde no hay control por parte de ningún gobierno o en aguas interiores de países del tercer mundo donde es el propio gobierno de estos países que da total impunidad a los piratas. El ejemplo del Oceano Índico es claro, zonas como el Estrecho de Malaka entre Indonesia y Malasia o el Golfo de Adén dónde el tráfico marítimo es muy intenso por la aglomeración de buques que provenientes del Mediterraneo, pasan por el Canal de Suez para llegar al Índico, sufren la terrible amenaza de la piratería. En el mapa abajo vemos las zonas con más ataques piratas:

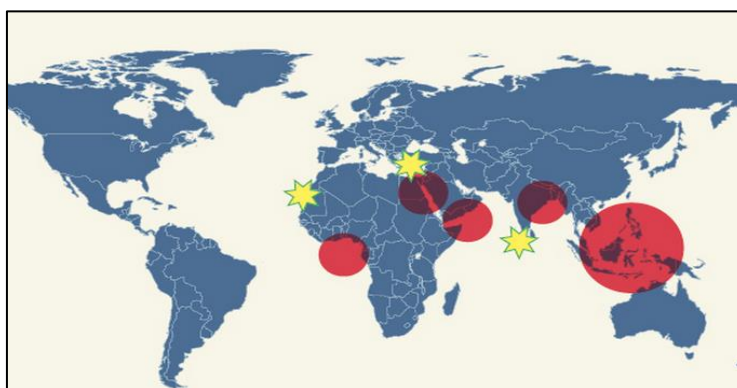


Figura 47: Zonas de piratería. Amarillo: actos aislados de piratería. Rojo: zona de riesgo de ataques piratas. **Fuente:** ICC International Maritime Bureau 2013.[25]

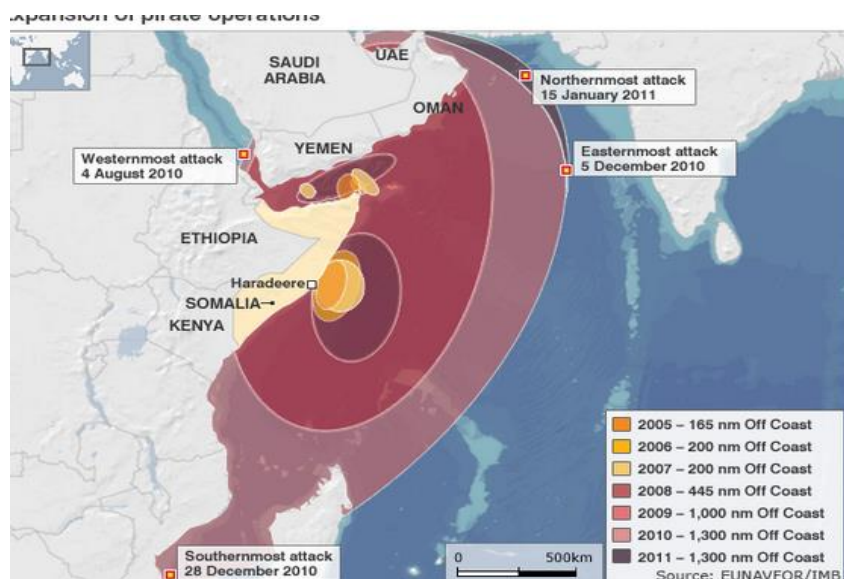


Figura 48: Expansión de las zonas controladas por piratas en el Cuerno de África. **Fuente:** International Maritime Bureau.[25]

La conjunción de las enormes zonas que escapan al control internacional y la tendencia por parte de los piratas a abarcar más territorio, provoca una enorme incertidumbre entre los armadores, compañías navieras y profesionales del mar. Si bien es verdad que la cooperación internacional en las misiones de la OTAN de lucha contra la piratería Ocean Shield en el Océano Índico (OOS) [26] y la Operación Atalanta de la UE, está dando frutos por el descenso de los delitos de piratería, también ha de decirse que supone un esfuerzo muy importante en movilización de la flota y contingente militar, en el caso español, la Armada tiene desplegada:

Un total de 16 buques de superficie, 16 Equipos Operativos de Infantería de Marina, 5 unidades de Guerra Naval Especial y el Centro de Vigilancia de Acción Marítima (COVAM) situado en Cartagena, han estado participando en la Operación Atalanta, según la página web de la Armada Española [27]:

- Fragata "VICTORIA"
- AO "MARQUÉS DE LA ENSENADA"
- FF "NUMANCIA"
- FF "CANARIAS"
- FF "MENDEZ NUÑEZ"
- FF "NAVARRA"
- PA "INFANTA ELENA"
- PA "INFANTA CRISTINA"
- BAA "GALICIA"

- BAC "PATIÑO"
- FF "SANTA MARÍA"
- FF "REINA SOFÍA"
- Unidades de Guerra Naval Especial
- Equipos Operativos de Infantería de Marina<
- Unidades Aéreas Embarcadas

Además de las unidades, la Infantería de Marina también ha proporcionado los Equipos Operativos que forman parte de las dotaciones de abordaje de los buques y proporcionan seguridad a los buques de la Armada. Por lo tanto, significa todo un compendio de profesionales, infraestructuras y naves que deben organizarse para mantener la seguridad en estas zonas. Con el inevitable factor de riesgo para los militares desplegados y el impacto económico en los presupuestos de defensa. Cabe destacar que de los 445 incidentes registrados por el IMO en 2003 se ha pasado, en el año 2008 y 2009, a solo dos ataques cada año según el estudio de Joaquín Castellón Moreno, Capitán de Fragata de la Armada [28].

Puede por tanto imaginarse y es lo que quiero manifestar en mi estudio, otra propuesta propia de aplicación del equipo AIS Seguro para dar respuesta a los problemas que surgen de controlar estas áreas tan extensas de un modo sencillo y económico. La solución que planteo es la de crear spoofings de blancos AIS que envíen datos falsos sobre posiciones de buques de la Armada a modo de elementos disuasorios. No es una solución final que erradique el problema pero puede ayudar a minimizar el impacto de este delito ni mucho menos que sustituya al contingente desplegado en estas zonas pero contribuiría a crear una seguridad ficticia en zonas altamente amenazadas. Se pueden crear escenarios controlados por buques reales que configuran blancos falsos para aumentar el radio de seguridad.

Por otra parte, también es posible crear escenarios donde se simulen buques en navegación alejados de la zona de tránsito segura por donde navegan los buques reales a modo de señuelo para piratas. Esto es, después de avistar una embarcación sospechosa, el centro de mando elaboraría un dispositivo afín de capturar a dichos posibles piratas, junto con la organización de los buques de acción marítima, se procedería a crear un spoofing de un blanco AIS con las características de un mercante o pesquero, que navegando en una zona sin aparente protección y alejado de los demás buques representará un objetivo asequible para los piratas.

En definitiva se trata de una herramienta con una versatilidad enorme, que puede adecuarse a diferentes misiones, ya sean de salvamento y rescate, control de fronteras y tráfico de sustancias ilegales, anti piratería, guerras etc. Los profesionales de los

cuerpos de policía o militares tienen disponible un sin fin de oportunidades para elaborar una operativa de abordaje o de cualquier otra misión, en este documento he plasmado las que a mi entender, pienso que pueden ser las más adecuadas. El manejo de los datos y de la información se vuelve fundamental para crear escenarios favorables en un medio de por sí peligroso.

5) CONCLUSIONES

Hemos visto en este estudio, la obligatoriedad de la instalación de equipos AIS a bordo en cierto tipo de buques de acuerdo con su desplazamiento y actividad, por sus funciones de ayuda a la navegación, fomento de la seguridad gracias al mayor conocimiento instantáneo de los datos de los buques que navegan a nuestro alrededor, así como el favorecimiento de las comunicaciones entre buques y el control por parte de las estaciones costeras.

Sin embargo, las características técnicas de estos en cuanto a su protocolo de comunicación por los canales VHF de AIS refleja en primer lugar que la red AIS está saturada en los canales convencionales de transmisión y recepción de datos (canales 1 y 2) debido al enorme tráfico marítimo concentrado en algunas zonas del mundo (estrechos, canales, ríos, litoral de grandes urbes...) lo que da lugar a una condensación de flujo de datos llegando a perder el carácter inmediato de acceso a la información.

Por otro lado, recientes estudios de seguridad como los llevados a cabo por Trend Micro de las sentencias AIS dan como resultado la facilidad para hackear esta red, creando datos falsos, suplantando información de los buques, de las AtoN y de todo dispositivo que utilice el protocolo AIS para transmitir información. Por tanto se pone de manifiesto el carácter demasiado abierto del procesamiento de la información entre los distintos dispositivos, dando lugar al aprovechamiento por agentes maliciosos, incluso entre los Estados en los que recaen bloqueos internacionales, para llevar a cabo actos ilícitos (como hemos visto en el caso de comercio entre Irán y Siria).

En un contexto, donde las amenazas globales golpean el sector marítimo: terrorismo, piratería, tráfico de personas, narcotráfico, guerras etc. en un medio de por sí tan incierto, peligroso y aún más extenso que es el mar, todo medio técnico parece imprescindible y cobra importancia para contrarrestar estos hándicaps en las manos de profesionales del mar.

Aparece en este escenario, una herramienta cuya implementación a bordo resulta muy sencilla de configurar con los equipos ya presentes, se trata del sistema AIS Seguro.

La integración de un tercer canal de enlace encriptado en el equipo AIS por el que poder transmitir y recibir información AIS amplía las ya existentes aplicaciones del equipo AIS. Esto es, el tercer canal encriptado para uso exclusivamente por parte de los cuerpos de vigilancia y seguridad del Estado, Ejércitos y Administraciones estatales proporciona un enlace de comunicaciones entre estos organismos, al margen de los canales VHF AIS convencionales, encriptados, a los que solo pueden acceder estos organismos. Origina por tanto un intercambio de información que no se ve saturado por las comunicaciones AIS convencionales, donde pueden intercambiarse entre varias unidades, imágenes, mensajes e incluso video de la situación y así tener una imagen global del entorno en donde se está operando.

Pero no solo supone un enlace más de datos sino que puede crearse distintos escenarios favorables para llevar a cabo operaciones conjuntas entre buques, aeronaves y estaciones costeras o de mando. Es más, la implantación de estos equipos AIS en aeronaves motiva el intercambio mayor de información entre las unidades por el incremento de área controlada (en la banda VHF, la propagación de la señal o alcance será mayor cuanto más alta esté situada la antena, en zonas sin obstaculización de la señal la frecuencia VHF tiene muy buen rendimiento).

Es por tanto el conjunto de la implementación de los equipos AIS Seguros en las distintas unidades de un cuerpo u organismo que acrecienta los resultados a la hora de llevar a cabo un operativo de abordaje, y con la ayuda de los spoofings, la gestión de las unidades y la coordinación entre ellas gracias a la transmisión de información secreta, inmediata y en grandes volúmenes creamos escenarios favorables en cualquier diferentes misiones.

No quiero finalizar mi estudio sin poner de manifiesto la importante repercusión económica que subyace en la integración de un sistema AIS Seguro a bordo, ya que ésta implica ahorro de personal, de mandos y otros artefactos. Al cuantificar la inversión en el nuevo sistema veremos que es despreciable si la comparamos con el ahorro que genera.

BIBLIOGRAFÍA

- [1] INTERNATIONAL MARITIME ORGANIZATION [sitio web]. OMI Qué es. [Consulta 28-10-2014]. Disponible en:
http://www.imo.org/About/Documents/What%20it%20is%20Oct%202013_Web.pdf
- [2] LEGISLACIÓN. Internacional. SOLAS Chapter V, Regulation 19.2 --Carriage requirements for shipborne navigational systems and equipment.
- [3] LEGISLACIÓN. Unión Europea. Diario Oficial de la Unión Europea. DIRECTIVA 2009/17/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO Establecimiento de un sistema comunitario de seguimiento y de información sobre el tráfico marítimo. 23 de Abril de 2009.
- [4] LEGISLACIÓN. España. Ministerio de Fomento. BOE núm. 261. REAL DECRETO 1185/2006. Título V. Reglamento por el que se regulan las radiocomunicaciones marítimas a bordo de los buques civiles españoles. 16 de Octubre de 2006.
- [5] LEGISLACIÓN Internacional. SOLAS. SN/Circ.227 Guidelines for the installation of a Shipborne Automatic Identification System (AIS). 6 de Junio de 2003. Ref. T2/8.02.
- [6] LEGISLACIÓN. Internacional. SOLAS Resolution A.917(22) Guidelines for the onboard operational use of shipborne automatic identification systems (AIS). 25 Junio de 2002. 22nd sesión de la Agenda de la Asamblea - Item 9.
- [7] LEGISLACIÓN. Internacional. Unión Internacional de Telecomunicaciones. ONU. Recomendación UIT-R M.1371-1. Características técnicas de un sistema de identificación automático universal a bordo de barcos mediante acceso múltiple por división en tiempo en la banda de ondas métricas del servicio móvil marítimo (cuestión UIT-R 232/8).1998-2001. Anexo 1 – pág.4.
- [8] INTERNATIONAL MARITIME ORGANIZATION [sitio web]. OMI AIS Transpondedores. [Consulta 28-10-2014]. Disponible en:
<http://www.imo.org/OurWork/Safety/Navigation/Pages/AIS.aspx>
- [9] LEGISLACIÓN. Internacional. SOLAS Resolution MSC.74(69) - Recommendation on Performance Standards for Universal Automatic Identification System (AIS). Anexo III. Pág. 13 – 12 Mayo 1998.
- [10] SAAB TRANSPONDERTECH AB, SUECIA. R5 Supreme AIS Transponder System. Operation & Installation Manual. P.N: 7000 118-300, B1.
- [11] Marine Traffic [sitio web]. Live Maps. [Consulta 14-12-2014]. Disponible en:
<http://www.marinetraffic.com>.

- [12] EXACT EARTH [sitio web].2009.Technology Satellite AIS. [Consulta 23-12-2014]. Disponible en: <http://www.exactearth.com/>. También disponible en el canal de youtube: <https://www.youtube.com/watch?v=OLi24D6axTo> .
- [13] MARCO BALDUZZI . KYLE WILHOIT. ALESSANDRO PASTA. E 2014. A Security Evaluation of AIS.Trend Micro.
- [14] A SECURITY EVALUATION OF AIS [sitio web].2001.Trend Micro. [Consulta 29-01-2015]. Disponible en:
<http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais>.
- [15] BLOOMBERG BUSINESS [sitio web]. Iran Oil Tankers Said by Zanzibar to Signal Wrong Flag [Consulta 30-01-2015]. Disponible en:
<http://www.bloomberg.com/news/articles/2012-10-19/iranian-oil-tankers-said-by-zanzibar-to-be-signaling-wrong-flag>.
- [16] BLOOMBERG BUSINESS [sitio web] U.S. Puts Sanctions on Iran Ships as Trade Noose Tightens [Consulta 30-01-2015]. Disponible en:
<http://www.bloomberg.com/news/articles/2012-07-12/u-s-adds-sanctions-on-iran-for-proliferation-oil-trade>
- [17] MARITIME EXECUTIVE [sitio web] Iran, Tanzania and Falsifying AIS Signals to Trade with Syria [Consulta 31-01-2015]. Disponible en: <http://www.maritime-executive.com/article/iran-tanzania-and-falsifying-ais-signals-to-trade-with-syria>
- [18] VEUS E.V.VEREINIGUNG EUROPÄISCHER SCHIFFFAHRTSJOURNALISTEN [sitio web]. International growing trend of AIS data manipulation.02/2015[Consulta 05-02-2015]. Disponible en:
<http://www.veus.de/index.php/de/news/222-international-growing-trend-of-ais-data-manipulation>
- [19] GCAPTAIN [sitio web] Iran Falsifying AIS Data to Conceal Ship Movements [Consulta 31-01-2015]. Disponible en: <http://gcaptain.com/iran-falsifying-ais-data-to-conceal-ship-movements/>
- [20] - SAAB TRANSPONDERTECH AB, SUECIA. Secure AIS System Overview. P.N: PT-09-0044, A1, Secure AIS.
- [21] - SAAB TRANSPONDERTECH AB, SUECIA. E2009. Software User Manual (SUM) Operator Console Coastwatch. P.N: 7000 115-119, Version D.
- [22] - STEFAN KARLSSON. E. December 2009. Airborne AIS Solutions. Saab Group. P.N: 091201.

- [23] JULIO BARROS. Apuntes de clase. Espectro electromagnético y propagación de ondas. Asignatura de Radiocomunicaciones. Escuela Técnica Superior de Náutica. Universidad de Cantabria.
- [24] QUINO PETIT. Abordaje en alta mar 03 Junio 2013 [Reportage sitio web] [Consulta 20-01-2015]. Disponible en:
http://elpais.com/elpais/2013/05/30/eps/1369938370_909022.html
- [25] INTERNATIONAL MARITIME BUREAU [sitio web] ICC Commercial Crime Service (CSS) – IMB Piracy Reporting Centre. [Consulta 06-02-2015]. Disponible en:
<https://icc-ccs.org/>
- [26] MARITIME COMMAND MARCOM OTAN [sitio web] Operation Ocean Shield [Consulta 04-02-2015]. Disponible en: <http://www.mc.nato.int/ops/Pages/OOS.aspx>
- [27] ARMADA ESPAÑOLA [sitio web] Operaciones Antipiratería. Ministerio de Defensa [Consulta 06-02-2015]. Disponible en:
http://www.armada.mde.es/ArmadaPortal/page/Portal/ArmadaEspañola/conocenos_especiales/prefLang_es/05_actividades--98_operaciones_antipirateria
- [28] JOAQUÍN CASTELLÓN MORENO. Capitán de Fragata. Armada. E. 2010. Los flujos de la globalización y su seguridad. Las líneas de comunicación marítima. Ed: Ministerio de Defensa. Revista ejército. N. 837 extraordinario diciembre.

ÍNDICE DE FIGURAS

Figura 1: Diagrama de periodicidad de la información	11
Figura 2: Dibujo situación de zonas de sombra. Fuente: AIS Transponders	12
Figura 3: Diagrama de bloques equipo AIS	13
Figura 4: Imagen CDU	13
Figura 5: Imagen traspondedor, vista superior	14
Figura 6: Imagen traspondedor, vista trasera: interfaz con el resto de unidades.....	14
Figura 7: Imagen Junction Box	14
Figura 8: Esquema conexiones Junction Box.....	15
Figura 9: Pantalla de configuración.....	17
Figura 10: Diagrama de bloques operaciones en el equipo AIS.....	18
Figura 11: Pantalla de blancos.....	19
Figura 12: Mensaje buque a buque.....	19
Figura 13: Pantalla AIS para vista de plotter.....	20
Figura 14: Imagen del tráfico marítimo en el estrecho de Gibraltar	21
Figura 15: Imagen de la captación satelital de señales de transpondedores AIS	21
Figura 16: Dibujo de las distintas formas posibles de ataques AIS.....	23
Figura 17: Ejemplo de sentencias AIVDM para reportes de y estáticos	25
Figura 18: Derrota seguida por el barco ficticio.....	25
Figura 19: Visión general del Sistema Seguro mostrando datos encriptados y abiertos.....	31
Figura 20: Esquema de transmisión de datos Seguros y convencionales.....	32
Figura 21: Diagrama de transmisión de datos Seguros	33
Figura 22: Relé de situación aeronave/buque/estación costera	37
Figura 23: Antes y después de una petición de vista de situación.....	37
Figura 24: Ejemplo de mensaje	38
Figura 25: Flujo de datos en misiones SAR	39
Figura 26: Patrón de búsqueda SAR enviado desde MRCC (estación costera) a aeronave	39
Figura 27: Base de datos de buques de una estación costera.....	40
Figura 28: Base de datos software Sea Watch.....	40
Figura 29: Imagen de POI y rutas.....	41
Figura 30: Traspondedores marítimos	42

Figura 31: Traspondedores aéreos	43
Figura 32: Estación base.....	43
Figura 33: Red segura: Monitor, Módulo Seguro y estación base	44
Figura 34: Red segura: estaciones base, servidores seguros, monitores	45
Figura 35: Encriptador.....	46
Figura 36: Esquema alcance de señal en función de la altura de la antena	49
Figura 37: Comparativa entre el alcance de un equipo AIS marinizado, a bordo de un helicóptero y de un avión.....	50
Figura 38: Vuelo del avión de Saab con el sistema Erieye	51
Figura 39: Comparativa entre alcance de ecos AIS recogidos desde un buque A y desde una aeronave B	51
Figura 40: Esquema de transmisión datos AIS Seguros Aeronave/ buque	52
Figura 41: Pestaña de configuración de datos AIS Seguros en el software AIS S....	53
Figura 42: Pestaña de configuración de Spoofings en el software W-AIS S	53
Figura 43: Pantallas del equipo AIS Seguro después de generar los Spoofings	54
Figura 44: Esquema de organización de un abordaje por Spoofing. A) Posición en rojo: Derrota real de la unidad de intervención.....	55
Figura 45: Esquema de organización de un abordaje	56
Figura 46: Por Gianfranco Tripodo, abordaje de un velero sospechoso a unas millas de la Isla de Alborán. Lancha de intervención del buque Fulman del Servicio de Vigilancia Aduanera	57
Figura 47: Zonas de piratería.....	57
Figura 48: Expansión de las zonas controladas por piratas en el Cuerno de África..	58

ÍNDICE DE TABLAS

Tabla 1: Intervalos de información de los equipos móviles a bordo de barcos de la Clase A	10
Tabla 2: Sumario de las posibles amenazas en el protocolo y equipo AIS	24
Tabla 3: Los distintos Spoofings y resultado buscado	55