Universidad del País Vasco Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

MÁSTER UNIVERSITARIO EN

NAUTICA Y TRANSPORTE MARITIMO

TRABAJO FIN DE MÁSTER

CIBERSEGURIDAD A BORDO DE BUQUES MERCANTES

Estudiante *Blanco, López, Daniel*
Director/Directora *Basterrechea, Iribar, Imanol*
Departamento
Curso académico *2019-2020*

Bilbao, 14, septiembre, 2020

Resumen

En este trabajo se va a realizar un estudio de ciberseguridad relacionada con los equipos que se encuentran a bordo de los buques mercantes.

Se elegirán una serie de equipos y sistemas que su operativa, diseño o posibilidad de sufrir un ataque son interesante. También se darán las consecuencias que se producen al recibir un ataque en estos equipos.

Este trabajo se ha dividido en dos fases principales:

En la primera fase se realiza la presentación técnica de cada equipo. Explicando tanto las partes que componen cada equipo como su funcionamiento y propósito que tiene a bordo.

La segunda parte es identificar en cada equipo los posibles puntos débiles del sistema tanto físicos como del software informático que lo controla.

Durante todo el trabajo se han utilizado la información proveniente de las diferentes ramas de la ingeniería desde la construcción naval pasando por la ingeniería de sistemas informáticos la ingeniería eléctrica.

Palabra clave: Buques mercantes, ciberseguridad, radar, ARPA, AIS, ECDIS, Sistema Integrado de Automatización

Summary

In this work made study about equipment can be found onboard merchant ships related with cyber security.

A series of equipment and systems will be chosen that their operation, design or possibility of suffering an attack are interesting. The consequences will occur when received attack in the equipment will also be given in consideration.

This work has been divided into two main phases:

In the first phase, the technical presentation of each equipment is made. Explaining both the parts that make up each piece of equipment and his operation and purpose on board.

The second part is for identify in each equipment the possible weak points of both the physical system and the computer software that controls it.

Throughout the work, information from the different branches of engineering has been used, from shipbuilding through computer systems engineering to electrical engineering.

Keyword: Merchant ships, cybersecurity, radar, ARPA, AIS, ECDIS, Integrated Automation System

Laburpena

Lan horretan, merkataritza-ontzietan aurkitutako ekipoekin lotutako zibersegurtasun-azterketa egingo da.

Ekipo eta sistema sorta bat aukeratuko da, haien funtzionamendua, diseinua edo eraso bat jasateko aukera interesgarria dela. Taldeetan erasoa jasotzerakoan sortzen diren ondorioak ere emango dira.

Lan hau bi fase nagusitan banatu da:

Lehen fasean, talde bakoitzaren aurkezpen teknikoa egiten da. Bai ekipo bakoitza osatzen duten zatiak, bai funtzionamendua eta xedea taula gainean azalduz.

Bigarren zatia ordenagailu bakoitzean sistema fisikoaren zein kontrolatzen duen softwarearen puntu ahulak identifikatzea da.

Lan guztian zehar ingeniaritzaren adar desberdinetako informazioa erabili da, ontzigintzatik hasi eta sistema informatikoen ingeniaritzatik ingeniaritza elektrikoaraino.

Hitz gakoa: Merkataritza ontziak, zibersegurtasuna, radarra, ARPA, AIS, ECDIS, Automatizazio Sistema Integratua

Índice

Índice Imágenes

Índice Tablas

Índice Graficas

Índice acrónimos

SOLAS		International Convention for the Safety of Life at Sea	Convenio Internacional para la Seguridad de la Vida Humana en el Mar
MARPOL		International Convention for the Prevention of Pollution from Ships	Convenio Internacional para Prevenir la Contaminación por los Buques
STCW		Standards of Training, Certification and Watchkeeping for Seafarers	Convenio Normas de Formación, Titulación y Guardia para la Gente de Mar
PRF		Pulse Repetition Frequency	Frecuencia de Repetición de Pulsos
ARPA		Automatic Radar Plotting Aid	Ayuda Automática al Seguimiento de Blancos
TT		Target Tracking	Seguimiento de Blancos
AIS	SIA	Automatic Identification System	Sistema de Identificación Automática
ECDIS	SIVCE	Electronic Chart Display and Information System	Sistema de Información y Visualización de Cartas Electrónicas
ISM	IGS	International Safety Management Code	Código Internacional de Gestión de la Seguridad
ISPS	PBIP	The International Ship and Port Facility	Código para la Protección de los Buques y de las Instalaciones Portuarias
SSO	OPB	Ship security officer	Oficial de Protección del Buque
CPA		Closest Point of Approach	
TCPA		Time to the Closest Point of Approach	
VHF		Very High Frequency	

GNSS	Global Navigation Satellite System	
GPS	Global Positioning System	
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema	
IRNSS	Indian Regional Navigation Satellite System	
QZSS	Quasi-Zenith Satellite System	
CTS	Custody transfer system	Sistema de Transferencia de Custodia
CMS	Cargo Monitoring System	Sistema Monitorización de la Carga
HSMS	Hull Stress Monitoring System	Sistema de Monitorización de los Esfuerzos del Casco
ESD	Emergency shutdown	Sistema de Parada de Emergencia
IAS	Integrated Automation System	Sistema Integrado de Automatización
SCADA	Supervisory Control and Data Acquisition	
PLC	Programmable Logic Controller	Controlador Lógico Programable

Universidad del País Vasco Euskal Herriko Unibertsitatea

BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

MÁSTER UNIVERSITARIO EN

NAUTICA Y TRANSPORTE MARITIMO

TRABAJO FIN DE MÁSTER

CIBERSEGURIDAD A BORDO DE BUQUES MERCANTES

DOCUMENTO 1- *MEMORIA*

Alumno/Alumna: Blanco López Daniel

Director/Directora (1): Basterrechea Iribar Imanol

Curso: 2019-2020

Fecha: Bilbao, 14 de septiembre 2020

1.MEMORIA

INTRODUCCION

En la actualidad tenemos un gran número de ataques informáticos realizados tanto a infraestructuras como a particulares. La seguridad informática se ha convertido en una prioridad de todas las industrias debido a los daños que se pueden producir (principalmente económicos, así como a los sistemas y equipos industriales). Siendo en el sector marítimo estos daños críticos debido a su funcionamiento particular y características.

El sector marítimo tiene como características un tráfico internacional por todo el mundo lejos de las costas. Se realiza usando buques mercantes, en los cuales la utilización de equipos informáticos a bordo de los mismo está aumentando tanto en número como en la automatización de los sistemas de control.

Actualmente se han desarrollado varias guías cursos y conferencias respecto a la prevención y mitigación de los problemas que pueden ser provocados por ataques informáticos a las infraestructuras alrededor de sector marítimo. El sector marítimo engloba a un gran número de sujetos como son los armadores, seguros, agentes, autoridades portuarias, estados, estibadores, técnicos y un largo etc.

Por último, cabe mencionar el futuro cercano donde habrá una implementación progresiva en las flotas mundiales de los buques autónomos. Buques cuyo funcionamiento estará controlado únicamente con equipos informáticos. Además, se está observando un aumento progresivo de ataques a sistemas tanto en buques como en puertos.

CONTEXTO

Este trabajo esta focalizado en la protección de los equipos informáticos que componen un buque mercante. El objetivo es analizar los fallos y vulnerabilidades de los mismo desde el punto de vista de los usuarios y atacantes. Para ello se ve a realizar una introducción técnica de cada equipo con sus características y funcionamiento.

En el buque nos encontramos con diferentes equipos para este trabajo se van a clasificar en varios grupos dependiendo de su propósito.

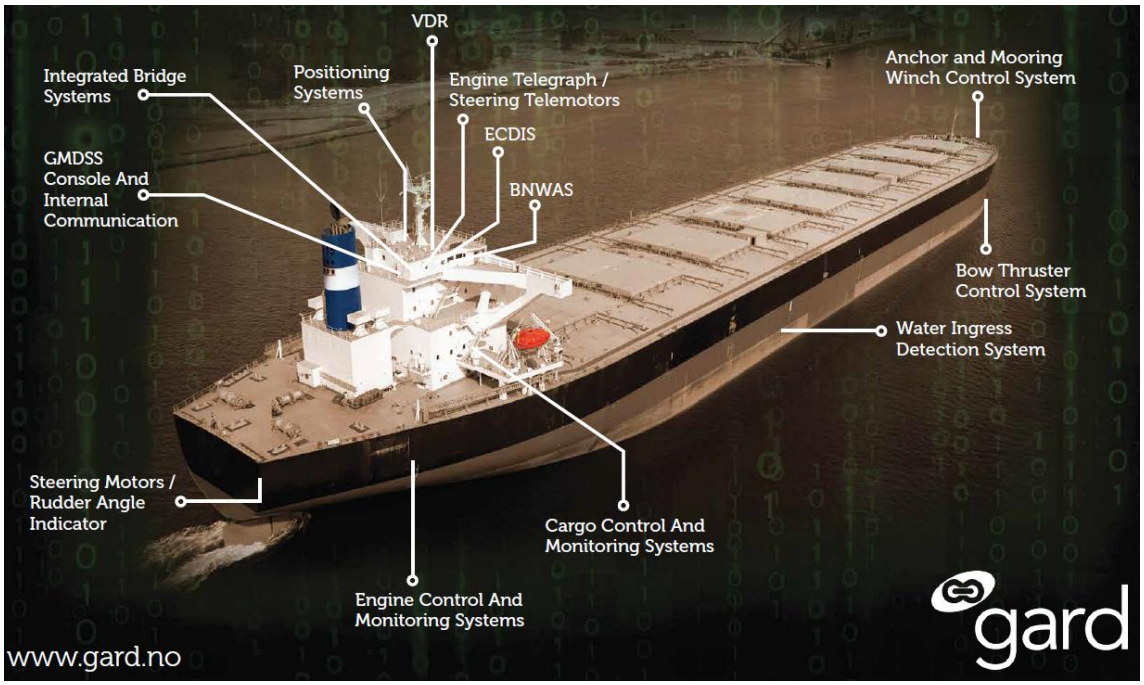

Imagen1. Sistemas de un buque [2]

Los equipos de navegación están destinados a la navegación segura del buque.

Los equipos de control de carga sirven tanto para mantenimiento de las condiciones de la carga como para realizar la operativa de carga – descarga en los puertos. Estos sistemas son exclusivos de los buques tanques diseñados para transporte cargas liquidas y gaseosas.

Los equipos de la sala de máquinas tienen diferentes funcionalidades como son la propulsión del buque, generación de energía eléctrica o mantenimiento de la presión dentro de las líneas hidráulicas y aire a presión del buque o generación agua potable.

Acabando por los equipos ofimáticos y telecomunicaciones donde se encuentran todos los ordenadores tanto los de trabajo como personales, dispositivos móviles y redes wifi.

Una vez quedan especificados los equipos y sistemas que se estudiaran durante el desarrollo de este trabajo definiremos el concepto de seguridad informática. Actualmente la seguridad informática tiene la finalidad de proteger los sistemas, redes y programas de los ataques digitales. Estos ataques generalmente tienen varios objetivos y pueden provenir de diferentes atacantes.

Gráfico1. Vectores de ataque en un ciberataque [2]

Para protegerse de los mismo es necesario la implementación de medidas preventivas y de protección. En los buques mercantes estas medidas tienen una complejidad añadida debido a la especialización de los sistemas a bordo. Actualmente presentan un gran reto tanto para los armadores como los astilleros y los diseñadores de sistemas. Incluso los oficiales se encuentran con dificultades para implementar o revisar el estado de los propios equipos.

El aumento en el número de ataques y objetivos se va aumentando año a año y no solo se ataca a los buques, sino que también a puertos y sectores relacionados con el mundo marítimo. Esto puede implicar sufrir un ataque por un sistema el cual se considera seguro.

En la siguiente fotografía se muestra la cronología de algunos ataques informáticos registrados a infraestructuras del sector marítimo. Tenemos desde ataques a equipos concretos de los buques como a la infraestructura logística en los puertos.

Tabla1. Cronología de algunos incidentes reportados [2]

OBJETIVOS Y ALCANCE DEL TRABAJO

En este trabajo se realiza una identificación de fallos y métodos conocidos de comprometer la seguridad en los equipos informáticos de un buque mercante. Los equipos informáticos se clasificarán por grupos dependiendo su funcionalidad y lugar en el barco.

El objetivo principalmente del trabajo es conocer cuáles son los equipos críticos en los cuales un ataque puede ser más perjudicial o aquellos sistemas que por su diseño o funcionamiento pueden ser más fácilmente manipulables.

Siendo el objetivo secundario de este trabajo dar a conocer los métodos y procedimientos más habituales para atacar los sistemas de un buque. Teniendo en cuenta que muchos de los sistemas del barco están interconectados entre sí. Lo que puede causar que el fallo de seguridad en un equipo comprometa la seguridad de todos los sistemas a bordo.

Se realizará una valoración de los daños que se pueda sufrir dependiendo del tipo de buque. Tanto la filtración de información confidencial como económicas por la paralización de un buque debido a un ataque que inutilice o afecte la operatividad normal del buque.

BENEFICOS QUE APORTA ESTE TRABAJO

Con este trabajo se van a identificar los fallos y problemas más comunes que se encuentra actualmente con los equipos que están presentes en los buques mercantes. La ventaja de un trabajo como este reside en tener un mayor conocimiento tanto de la protección como de la operativa de los sistemas, en mi caso se ha obtenido una visión más completa sobre el buque y cómo actuar en caso de un ataque informático.

ANALISIS DEL ESTADO DEL ARTE

El sector marítimo tiene varios pilares en los cuales queda configurado la protección del buque. Comenzado por las regulaciones internacionales con las cuales se establece los estándares que deben cumplir los buques mercantes. De todas las regulaciones existentes y que se encuentran en vigor en el momento de la realización de este trabajo se van a seleccionar aquellas que contengan una regulación o normativa que esté relacionado con los equipos informáticos que se pueden encontrar a bordo.

Convenio SOLAS

El convenio SOLAS es el convenio más importante teniendo en cuenta todos los tratados internacionales relacionados con la protección de los buques mercantes. La primera versión fue adoptada en 1914, tras el hundimiento del Titanic, la segunda en 1929, la tercera en 1948, y la cuarta en 1960. Y por último la versión de 1974 es la que actualmente se encuentra en vigor, esta versión se actualiza periódicamente gracias al método de aceptación tácita que fue incorporo en este año.[1]

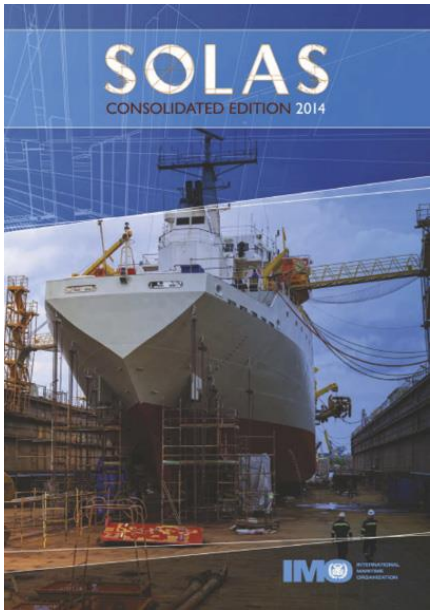

Imagen2. Convenio SOLAS [1]

Actualmente la última versión publicada del código es SOLAS versión consolidada del 2020 que acaba de ser publicada este mes de septiembre.

Durante el desarrollo de este trabajo se ha utilizado la versión anterior la versión consolidad del año 2014.

Se divide en varios capítulos de los cuales son interesante la información contenida en los capítulos que definen el número, tipo y cantidad de equipos electrónicos a bordo y las medidas de seguridad adoptadas para impedir su sabotaje o manipulación.

Capítulo V: Seguridad de la navegación

En este capítulo se encuentra los aparatos y sistemas náuticos de a bordo, se mencionan varios de los aparatos que estudiaremos más adelante. Los equipos de radar, el sistema de identificación automática (AIS) y el sistema de información y visualización de cartas electrónicas (ECDIS).

Al final de este apartado también se incluye una normativa para los puentes con sistemas integrados. En caso de fallo de este sistema se debería activar una alarma acústica y visual. Además, el fallo no debe afectar a otros subsistemas del buque.

Capítulo IX: Gestión de la seguridad operacional de los buques

Este capítulo está supeditado al código internacional de gestión de la seguridad (ISM Code). Dentro del mismo está descrita la regulación y normativa aplicable tanto a la compañía del buque como a la tripulación y al personal designado en caso de accidente, contaminación o alguna incidencia grave.

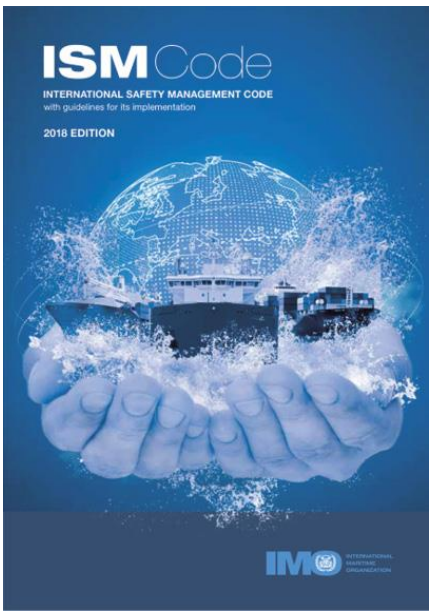

Imagen3. Código ISM [1]

A su vez queda regulado la manera de revisar la seguridad del buque mediante inspecciones tanto del personal de la compañía como de los estados.

Analizando los accidentes, no conformidades y situaciones peligrosas para realizar las oportunas correcciones.

Capitulo XI-2: Medidas especiales para incrementar la protección marítima

Dentro de este capítulo nos encontramos con la implementación del código internacional para la protección de los buques y de las instalaciones portuarias (ISPS Code).

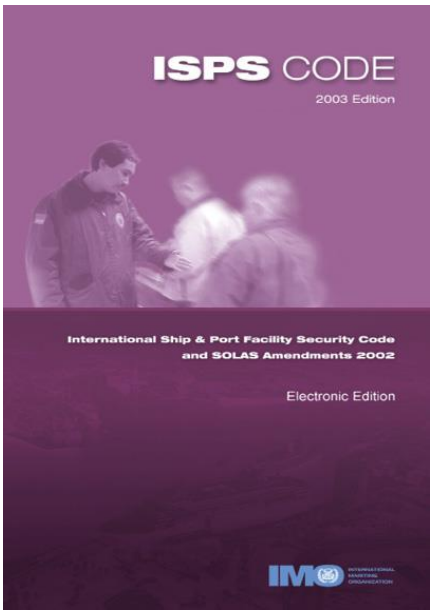

Imagen4. Código ISPS [1]

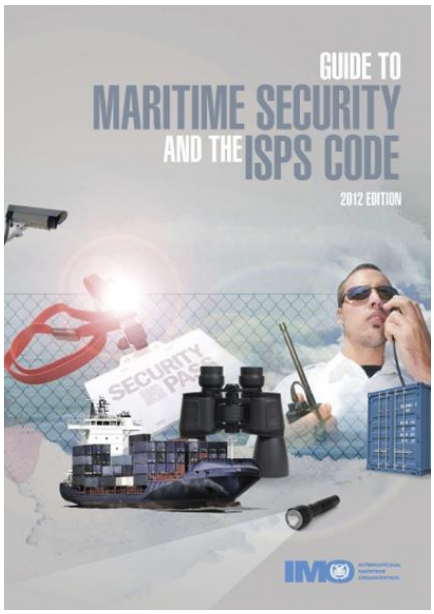

Imagen5. Guía al código ISPS [1]

Convenio STCW

El convenio STCW a diferencia del SOLAS regula la formación y titulación de la gente que trabaja a bordo de los buques mercantes. Dentro del mismo se encuentra definidos las condiciones mínimas de formación necesarias para cada posición a bordo. Tanto los estudios como los cursos pasando por los periodos de prácticas. Siendo STCW 2017 la versión actualmente en vigor durante el desarrollo del trabajo.

Para entender los problemas en la seguridad de los equipos a bordo es necesario entender la formación de las personas que utilizan dichos equipos diariamente. Entendiendo su formación podremos entender como actuaran ante ciertas eventos o situaciones que ocurran en los equipos informáticos.

Al igual que en el SOLAS este convenio esta divido en varias partes. Para este trabajo solo mencionaran las partes relacionadas directamente con la seguridad de los equipos.

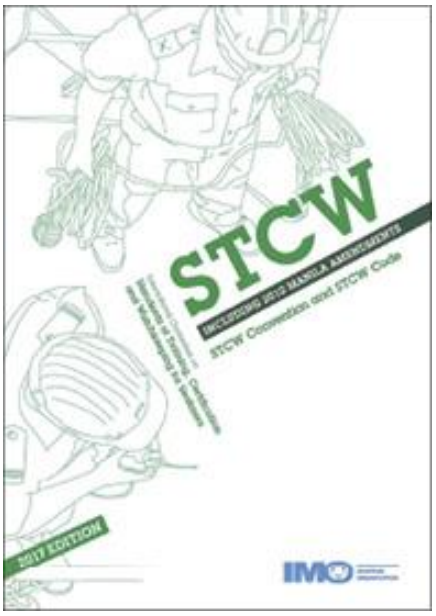

Imagen6. Convenio STCW [1]

Sección A-VI/5

En esta sección quedan definidas todas las competencias que tiene que conocer el oficial de seguridad del buque (SSO). Algunas de ellas están relacionas con la seguridad de los equipos.

Por ejemplo, el oficial de protección de buque se le exige conocer los planes de contingencia y procedimientos de actuación en caso de brechas de seguridad tanto en los equipos como en el buque. También se le exige un conocimiento en lo relativo a la manera de transmitir y recibir información usando los diferentes canales de manera segura.

Sección A-VI/6

En esta sección se definen las competencias en materia de seguridad que deben ser conocidas por todos los miembros de la dotación del buque. Dentro de estas competencias se incluye el entrenamiento que se va recibiendo a bordo. Desde hace varios años se están realizando a bordo de los buques cursos de seguridad informática principalmente informativos. Durante la realización de estos cursos se intenta que todos los miembros de la tripulación entiendan los peligros de la seguridad informática y como pueden ser atacados tanto ellos como los dispositivos del barco.

The guidelines on cyber security onboard ships

Desde hace algunos años varias asociaciones marítimas internacionales han creado una guía sobre seguridad informática a bordo de los buques. En esta guía se explica de manera detallada la forma de identificar y responder a las amenazas cibernéticas. Como resultado de la guía se busca enseñar al personal a bordo la manera de actuar de los atacantes.[6]

Durante el desarrollo de este trabajo se usará esta guía para las partes que componen la identificación de amenazas y procedimientos de actuación. El objetivo de la guía es enseñar a las personas relevantes en la compañía como en el barco los modos de actuación durante un ataque informático.

Imagen7. Guía en ciberseguridad a bordo de buques [6]

Sistemas del buque

En este apartado se van a estudiar algunos sistemas que se encuentra a bordo de los buques mercantes y que por su funcionamiento, diseño o conexión con otros sistemas podría ser objetivo de un ataque. Se crearán varios grupos dependiendo de la funcionalidad del equipo a bordo.

Para cada equipo se hará una explicación técnica para entender el funcionamiento del mismo y sus características técnicas. Los posibles métodos de manipulación junto con los problemas que conlleva la inutilización o funcionamiento erróneo de estos equipos seleccionados.

Sistemas de navegación

El primer grupo se compone de algunos de los sistemas que se encuentran en el puente de los buques. La selección de estos quipos se realiza de acuerdo a su importancia para realizar una navegación segura del buque.

Imagen8. Disposición de los equipos de navegación del buque gasero Bilbao Knutsen

Radar

El primer equipo seleccionado es el radar porque se trata de un equipo para localizar peligros durante la navegación.

La palabra RADAR viene del acrónimo derivado Radio Detección y Alcance. Los radares marinos civiles actualmente son totalmente diferentes en tamaño, aspecto, y diseño de los primeros que aparecieron en la década de 1940. Sin embargo, los datos que muestran como son rango y demora de los blancos continúan estando sin cambios. Para el funcionamiento de los radares en buques necesitamos de varios componentes.

La antena se utiliza de dos formas como emisor para enviar las ondas electromagnética hacia una dirección en el horizonte donde está apuntando en ese momento la antena con un haz concentrado y como receptor para recibir las ondas electromagnéticas que vuelve después de haber rebotado en los blancos. La palabra blanco en los radares hace referencia a cualquier objeto que por su composición refleja la onda del radar y produce un eco en la pantalla del mismo.

La característica esencial de los radares marinos es la de proporcionar una cobertura continua de 360 grados alrededor de ellos. Para conseguir esto la antena tiene que girar a una tasa de rotación entre 24 a 45 revoluciones por minuto. Como resultado se obtiene una rotación completa desde 1.3 a 2.5 s, dependiendo del sistema. [7.2]

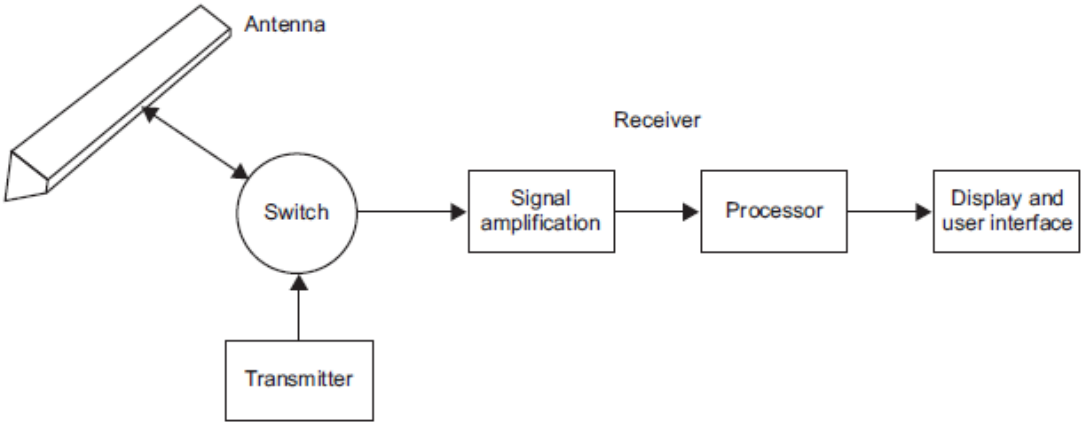

Imagen9. Esquema de los componentes de un radar [7.1]

Generador de ondas sirve para crear los pulsos electromagnética que se va enviar para detectar los blancos en los buques mercantes suelen encontrase el denominado “magnetrón”. Actualmente existen dos bandas electromagnéticas que tienen diferentes características para poder generar una de estos pulsos se necesita un magnetrón único.

Dependiendo de tamaño del buque siguiendo el contenido en SOLAS Capítulo V Seguridad de la navegación Regla19 podemos tener varios equipos radar. Normalmente en buques a partir de 3000 toneladas de registro bruto se suele colocar dos radares uno que trabaja con la banda X con frecuencias que se encuentran entre 9.2 y 9,5 GHz. Estas frecuencias corresponden con una longitud de onda de aproximadamente 3 cm. Se usa para blancos cercanos al buque debido a que da una mejor resolución de los ecos que los equipos con banda S. [7.3]

Y otro radar que trabaja en la banda S trabaja en frecuencias entre 2,9 y 3,1 GHz y corresponde con una longitud de onda de aproximadamente 10 cm durante la navegación sirve para detectar blancos situados a una larga distancias de pendiendo del equipo y las condiciones se pueden detectar ecos que se encuentren a 48 millas náuticas del buque propio. [7.3]

Procesador filtra las ondas electromagnéticas provenientes de los ecos y calcula el tiempo que ha tardado la onda electromagnética en volver después de que esta se haya reflejado con el objeto. El tiempo calculado es una medida de la distancia a la que se encuentra el objeto del radar propio.

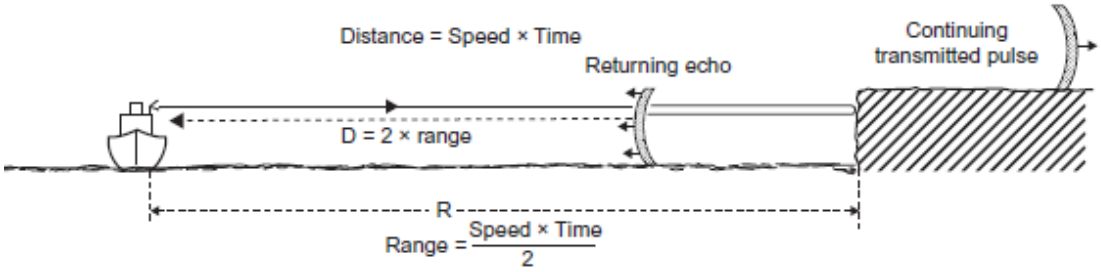

Imagen10. Los principios físicos de funcionamiento en un radar marino [7.1]

Los pulsos se transmiten en intervalos de tiempo lo suficientemente grandes para permiten en función del alcance seleccionado en el radar que los pulsos lleguen a los objetos más alejados y vuelvan antes de emitir el siguiente pulso. Este intervalo se denomina frecuencia de repetición de pulsos (PRF), es el número de pulsos transmitidos en 1s. [7.4]

Monitor y panel de usuario sirve para representar los ecos en una pantalla circular también se encuentran los botones físicos para configurar los parámetros del equipo. Además, en esta pantalla se indican las alarmas y fallos del sistema.

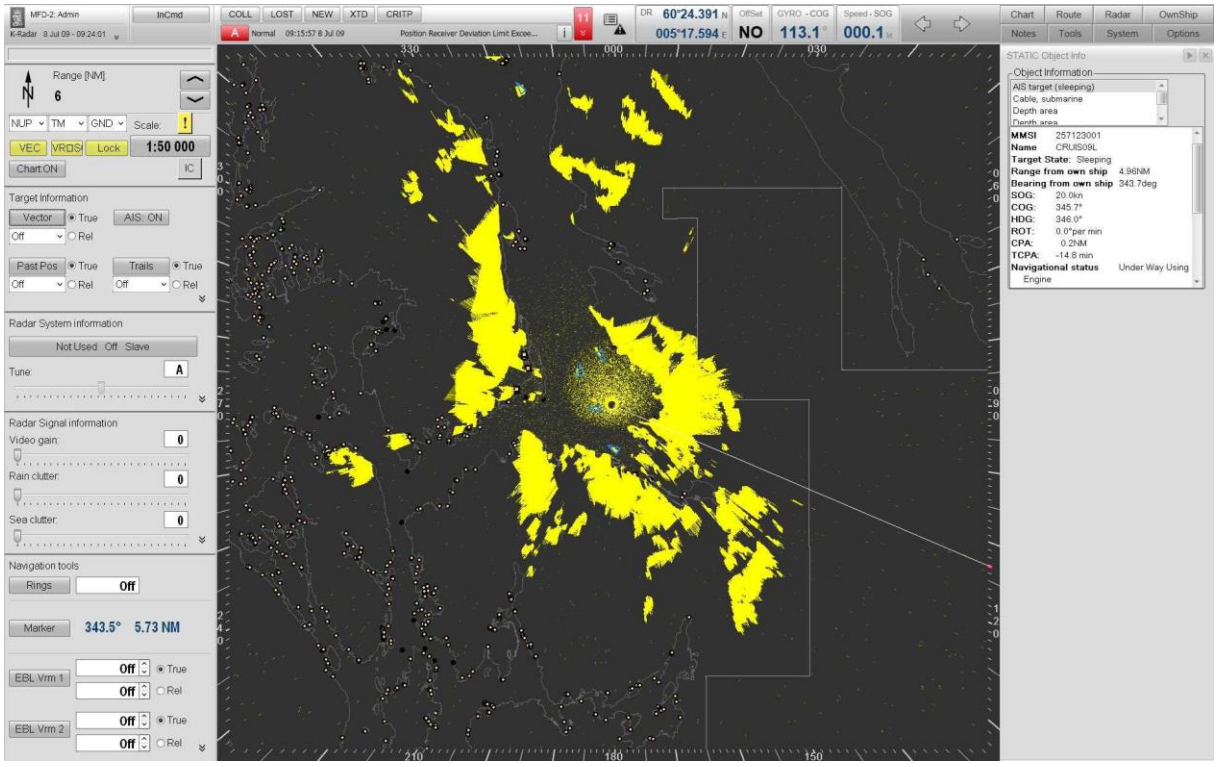

Imagen11. Pantalla de un equipo K-Bridge Radar Kongsberg [12]

Generador de aleatoriedad en la onda sirve para reducir las interferencias con otros radares cercanos. Cada pulso se emite con un patrón aleatorio de tiempo denominado PRF no constante. Este patrón tiene un valor medio el cual sirve para identificar los ecos falsos provenientes de otros radares.

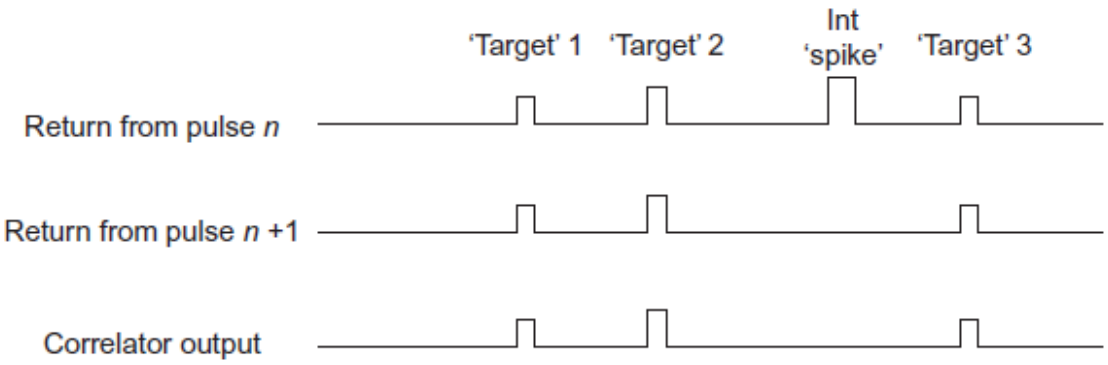

Imagen12. Identificación de ecos proveniente de otro radar [7.5]

Problemas de los radares

Interferencias en la frecuencia de la onda del radar que recibe la antena. Puede ser producida por otros radares cercanos. La solución a este problema fue la creación de unos rangos de banda con el mayor tamaño posible para permitir que diferentes radares puedan operar en diferentes frecuencias dentro de la misma banda, siempre respetando los límites establecidos en las normativas internacionales en las dos bandas (Banda S trabaja entre 2.9 y 3.1 GHz y Banda x que trabaja entre 9.2 y 9.5 GHz. Esto no elimina toda interferencia sino una forma de reducir significativamente el efecto que se producía en la pantalla del radar. [7.3]

Para minimizar estos problemas se desarrolló una aleatoria en la sincronización de cada pulso transmitido, con un valor medio entre todos los pulsos igual al escogido por los diseñadores.

Teniendo en cuenta lo mencionado anteriormente para interferir en el funcionamiento de un radar necesitaríamos conocer cuál es número escogido que genera los pulsos aleatorios y colocar un radar con esas características en las inmediaciones del barco objetivo.

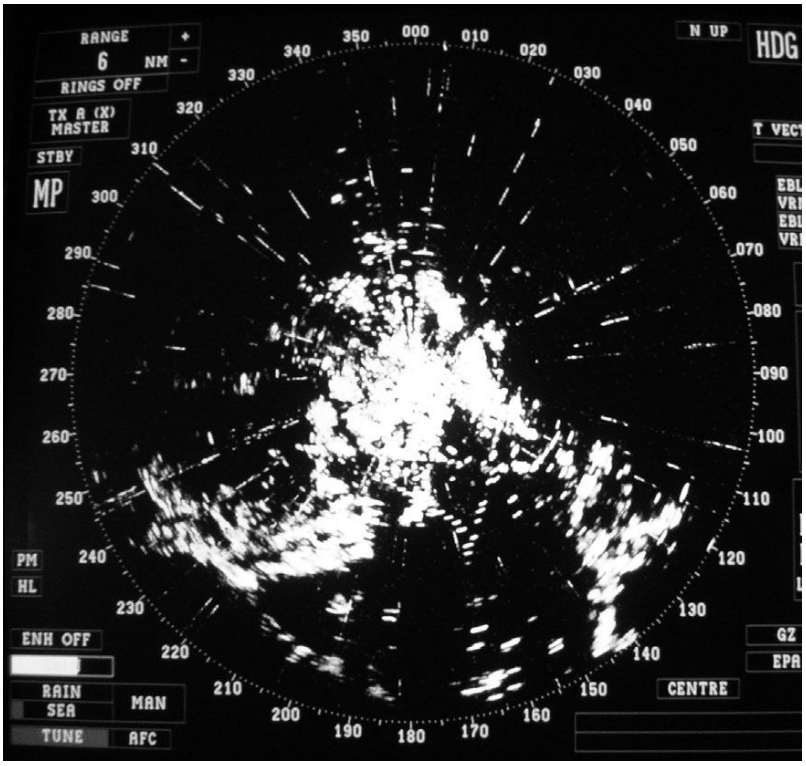

Imagen13. Interferencias generadas en la pantalla de un radar [7.5]

Sin embargo, actualmente existe documentados otro tipo de ataques a los sistemas radares estos ataques producen dentro del software del equipo. Totalmente diferentes a los presentados anteriormente que se centraban en una interferencia en el hardware del equipo.

Un ejemplo documentado por la empresa israelí “Naval Dome” especializada en seguridad informática utilizó un conector de red ethernet local que interconectaba en una red local los equipos del puente: el radar con el ECDIS con el sistema de alerta de puente (BNWAS) y el registrador de datos de viaje (VDR) todos ellos conectados a internet. Los técnicos de esta empresa lograron tener acceso al radar remotamente. Con este acceso podían eliminar ecos del radar en tiempo real de la pantalla del mismo equipo sin hacer saltar ninguna alarma del equipo. Además de poder manipular cualquier parámetro del mismo. [8]

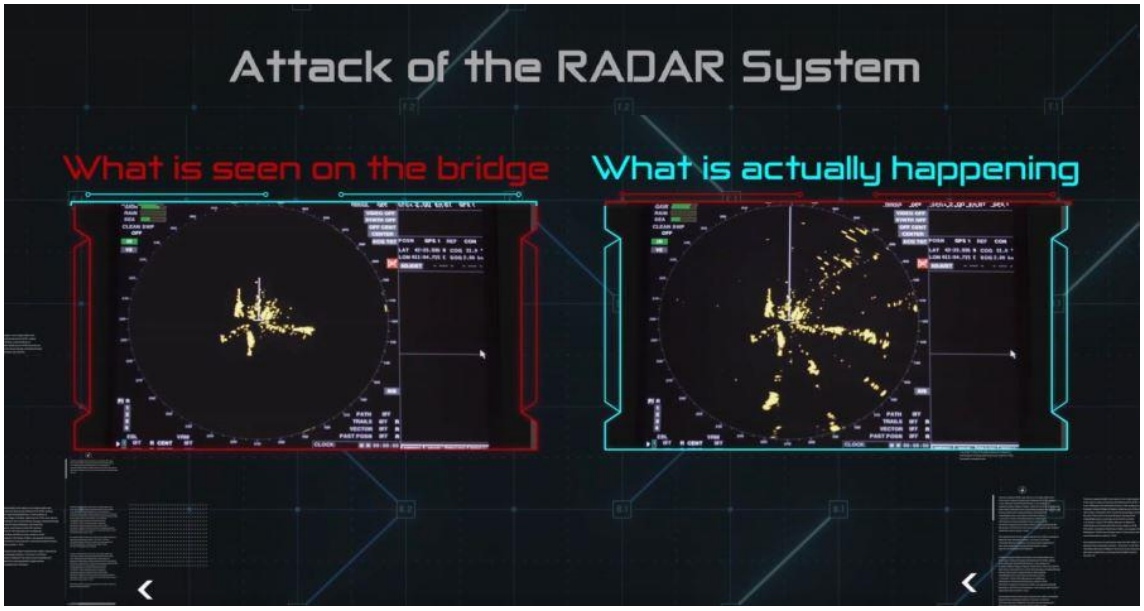

Imagen14. Pantalla de radar que muestra el efecto del ataque informático [8]

Conclusiones en los radares

En los casos de interferencias en las señales recibidas por el radar se mostrará en la pantalla un mayor número de ecos lo que produce y distorsiones en la posición de los mismo. Para el oficial de guardia y el transito seguro del buque se puede aumentar el riesgo de abordaje. Debido a que se empeora la visión alrededor del buque.

Para el caso de hackeo del software del radar el riesgo de producirse un abordaje se aumentaría considerablemente debido a que puede manipular cualquier información que aparece en la pantalla. Como se explicó los atacantes pueden obtener el control total del equipo tanto de los datos de visualización como de los ecos recibidos por el radar. Como parte positiva para poder realizar un ataque de estas características es necesario además de un conocimiento técnico que los equipos estén conectados a una red LAN con acceso a internet para poder realizar esto remotamente.

ARPA

Es un sistema incorporado dentro de los equipos radares para el seguimiento automático del movimiento de los ecos. Estos ecos pueden ser adquiridos para el seguimiento de manera automática o manual. Actualmente no se usa esta terminología y se ha dado paso a TT "target traking" que incorpora además el sistema AIS.

Size of ship/craft	<500 gt	500 gt to <10,000 gt and HSC<10,000 gt	All ships/craft ≥10,000 gt
Minimum operational display area diameter	180 mm	250 mm	320 mm
Minimum display area	195 x 195 mm	270 x 270 mm	340 x 340 mm
Auto acquisition of targets	-	-	Yes
Minimum *acquired* radar target capacity	20	30	40
Minimum *activated* AIS target capacity	20	30	40
Minimum *sleeping* AIS target capacity	100	150	200
Trial Manoeuvre	-	-	Yes

Tabla2. Características técnicas del ARPA en función del tamaño de los buques [1.3]

Para calcular el movimiento de los ecos respecto del buque propio se necesita la información tanto del girocompás como de la corredera que nos da en valor de nuestra velocidad sobre el agua. Con esta información es capaz de calcular tanto la dirección como la velocidad real de los ecos. Y los valores de CPA y TCPA que son la distancia mínima a la que pasara el eco del buque propio y el tiempo que falta para que ocurra esa situación.

Problemas ARPA

Los problemas que podemos tener en los equipos ARPA esta relacionados con los problemas que pueda tener el radar. Para el funcionamiento óptimo del ARPA en lo referido al seguimiento de ecos es necesario que estos blancos sean en primera estancia detectados con nitidez por el radar. Por tanto, en los supuestos de grandes perturbaciones por condiciones climatológicas como son lluvia o gran oleaje que dificulte la discriminación de los ecos.

La otra parte del problema es el fallo o manipulación de la información que obtiene de los sistemas secundarios que necesita el ARPA para realizar los cálculos de seguimiento. Los fallos en la corredera, girocompás o GNSS. Producirán un cálculo erróneo en los valores de CPA y TCPA.

Conclusiones ARPA

El ARPA es un equipo que depende completamente del radar por lo tanto cualquier acción que afecte el funcionamiento del radar produce en el ARPA un funcionamiento erróneo. Para el oficial de guardia en el buque supone un aumento del riesgo de abordaje debido a que unos valores erróneos pueden conllevar una interpretación errónea de una situación de peligro o al contrario una situación segura se pueden interpretar como insegura debido a los cálculos que está realizando el ARPA.

AIS

Es un sistema de que transmite información acerca del barco propio hacia otros barcos o estaciones costeras mediante ondas de radio VHF. El sistema es capaz de trabajar con un gran número de buques al mismo tiempo. Las estaciones costeras mandan automáticamente la información que reciben de cada AIS que detectan a una base de datos en internet en tiempo real. El rango normal de alcance es el habitual de las ondas VHF entre 20 a 30 millas náutica. Siendo este valor mayor en función de la altura a la que este colocada a la antena en el buque. También se puede transmitir esta información a través de los satélites.

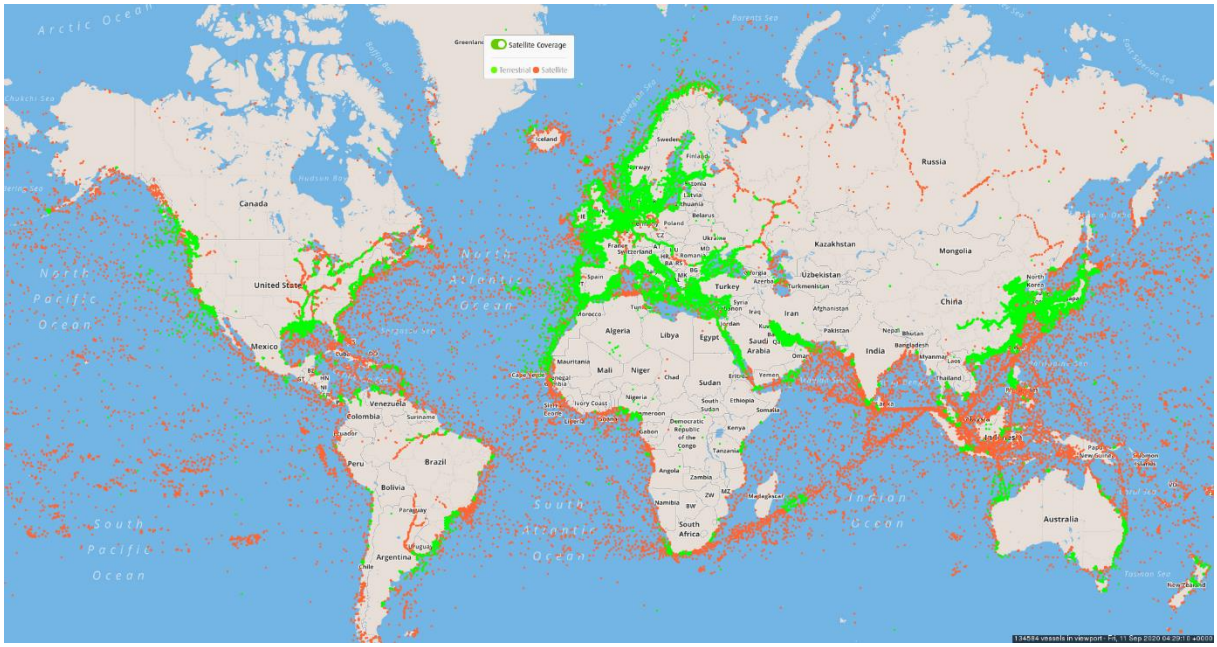

Imagen15. Cobertura mundial del sistema AIS [15]

Puntos verdes son buques que se encuentran en el rango de alcance de una estación costera hasta 30 millas náuticas. El seguimiento de buques que se encuentran cerca de una estación costera es gratuito.

Puntos naranjas son buques que se encuentra navegando fuera del alcance de cualquier estación costera y que el seguimiento se puede hacer mediante los satélites. El seguimiento de los buques mediante el AIS satelital es de pago.

El sistema AIS al igual que el ARPA también realiza los cálculos de CPA y TCPA de cada buque que detecta. Además de ello está conectado tanto al radar como al ECDIS compartiendo toda la información que recibe.

Imagen16. Furuno F150 AIS [16]

La transmisión de información se realiza automáticamente sin intervención del oficial de guardia. Hay tres tipos de información que se transmite simultáneamente.

Información estática es la información que se introducción durante la instalación del equipo en el buque. Tiene la información relativa al buque que no va a variar. Como es el número de Identificación del Servicio Móvil Marítimo, dimensiones, tipo de buque y numero IMO. [1.2]

Information item	**Information generation, type and quality of information**
Static	
MMSI	Set on installation Note that this might need amending if the ship changes ownership
Call sign and name	Set on installation Note that this might need amending if the ship changes ownership
IMO Number	Set on installation
Length and beam	Set on installation or if changed
Type of ship	Select from pre-installed list
Location of electronic position fixing system (EPFS) antenna	Set on installation or may be changed for bi-directional vessels or those fitted with multiple antennas

Tabla3. Información estática del AIS [1.2]

Información dinámica que puede ser modificada en función del tipo de navegación que esté realizando el buque se incluye velocidad sobre fondo, rumbo y tipo de navegación. [1.2]

Dynamic	
Ship's position with accuracy indication and integrity status	Automatically updated from the position sensor connected to AIS The accuracy indication is approximately 10 m.
Position Time stamp in UTC	Automatically updated from ship's main position sensor connected to AIS
Course over ground (COG)	Automatically updated from ship's main position sensor connected to AIS, if that sensor calculates COG This information might not be available
Speed over ground (SOG)	Automatically updated from the position sensor connected to AIS. This information might not be available
Heading	Automatically updated from the ship's heading sensor connected to AIS
Navigational status	Navigational status information has to be manually entered by the OOW and changed as necessary, for example: - underway by engines - at anchor - not under command (NUC) - restricted in ability to manoeuvre (RIATM) - moored - constrained by draught - aground - engaged in fishing - underway by sail In practice, since all these relate to the COLREGs, any change that is needed could be undertaken at the same time that the lights or shapes were changed
Rate of turn (ROT)	Automatically updated from the ship's ROT sensor or derived from the gyro. This information might not be available

Tabla4. Información dinámica del AIS [1.2]

Información del viaje puede ser modificada en función del viaje a realizar. Colocando normalmente el puerto de destino y el día aproximado de llegada. Además, se puede añadir el tipo de mercancía peligrosa y algunos waypoint o punto de ruta. [1.2]

Voyage-related	
Ship's draught	To be manually entered at the start of the voyage using the maximum draft for the voyage and amended as required (e.g. – result of de-ballasting prior to port entry)
Hazardous cargo (type)	To be manually entered at the start of the voyage confirming whether or not hazardous cargo is being carried, namely: - DG (Dangerous goods) - HS (Harmful substances) - MP (Marine pollutants) Indications of quantities are not required
Destination and ETA	To be manually entered at the start of the voyage and kept up to date as necessary
Route plan (waypoints)	To be manually entered at the start of the voyage, at the discretion of the master, and updated when required

Tabla5. Información sobre el viaje en el AIS [1.2]

Información de seguridad puede ser transmitida en formato texto a todos los buques en los alrededores o a una estación costera.

Safety-related	
Short safety-related messages	Free format short text messages would be manually entered, addressed either a specific addressee or broadcast to all ships and shore stations

Tabla6. Información de seguridad del AIS [1.2]

Problemas AIS

Los problemas en los equipos AIS vienen a través de dos vías. A través del proprio software del sistema o a través de las ondas de radio con los mensajes.

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

Tabla7. Listado de amenazas en los sistemas AIS [17]

AtoN spoofing es un método con el cual se interferir con ayudas a la navegación como pueden ser colocar boyas falsas en canales angostos para engañar a los buques hacia zonas de bajos fondos. [17]

SAR spoofing se activa una baliza de hombre al agua en una posición concreta. Para poder realizarlo es necesario tener un transpondedor AIS para generar alertas. Al ser obligatorio la asistencia por cualquier buque en las cercanías puede ser usado en zonas de piratería para acercar buques a una zona concreta del mar. [17]

AIS Hijacking se altera la información del AIS de un buque como la posición velocidad o tipo de cargamento. Hay una variante usando programas que consiste en sobreponerse a la señal que envía el AIS cuando se encuentra en las cercanías de una estación costera con una señal falsa emitida con el equipo del atacante. Modificando los datos del AIS al suplantarlo esta información llega hasta las páginas web de visualización de AIS. [10]

Imagen17. AIS Hijacking [17]

Conclusiones AIS

Es un equipo que actualmente los atacantes tienen muchas posibilidades para interferir en su funcionamiento debido a que es una señal de radio que se emite sin ninguna encriptación y su modelo de funcionamiento. Tanto los ataques usando software informático como los que usan la señal del AIS son de una gran importancia. Los oficiales guardia deberían revisar tanto la configuración del equipo y selección de estaciones. Como también durante las navegaciones control tanto visual como de los datos que recibimos de otros buques.

GNSS

Son la colección de sistemas satelitales de posicionamiento que actualmente hay en funcionamiento sobre la órbita terrestre. En los buques mercantes debido a que realizan viajes por diferentes partes del globo terrestre pueden necesitar trabajar con diferentes tipos de sistemas de posicionamiento.[9]

- El más conocidos es el GPS americano siendo el primer sistema GNSS. GPS lanzo su primer satélite a finales de la década de 1970 por el Departamento de Estados Unidos de defensa. Utiliza una constelación de 27 satélites y brinda cobertura global. [9]

- El siguiente sistema es GLONASS ruso que lo opera el gobierno ruso La constelación GLONASS consiste en 24 satélites y brinda cobertura global. Es usando normalmente en navegaciones cercano a los polos. [9]

- El Galileo es el sistema europeo civil operado por sistemas europeos de satélites de navegación global o Agencia (GSA). Galileo utilizará 27 satélites. La constelación completa estará finalizada en 2020. [9]

- BeiDou es el sistema de navegación por satélite chino. El sistema constará de 35 satélites. Un servicio regional entró en funcionamiento en diciembre de 2012. BeiDou se ampliará para proporcionar cobertura global para fines de 2020. [9]

- El sistema satelital de navegación regional de la India (IRNSS) brinda servicio a India y sus zonas próximas. La constelación completa se compone de siete satélites. está previsto que se implemente en 2015. [9]

- El sistema navegación satelital japones QZSS es un sistema regional que brinda servicio a Japón y la región de Asia-Oceanía. Se planea implementar el sistema QZSS para 2018. [9]

Normalmente en la marina mercarte se tiene variaos receptores de GPS y alguno del sistema GLONASS para navegaciones polares. [1.1]

Imagen18. Furuno GP170 [16]

El receptor recibe la información que transmiten los satélites y calcula el tiempo de propagación de la onda desde el satélite hasta el receptor. Con esta información el receptor es capaz de calcular la hora y un círculo de posición donde se encuentra en función de la información que recibe del satélite. En el caso de la imagen el receptor se encuentra en algún punto del circulo. Para poder calcular una posición exacta es necesario recibir información simultanea de varios satélites.

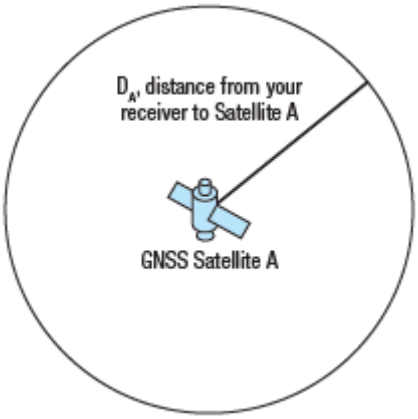

Imagen19. Posición en la superficie terrestre respecto de un satélite [9]

Para poder tener una posición precisa es necesario tener los círculos de posición de varios satélites al mismo tiempo. La posición del receptor estará en el área donde se cruzan todos los círculos de posición. Con tres satélites simultáneos también es posible calcular una posición sin embargo esta posición tiene una precisión menor que con cuatro satélites. La intersección que se forma con tres círculos es un área mayor que la que obtenemos con cuatro satélites.

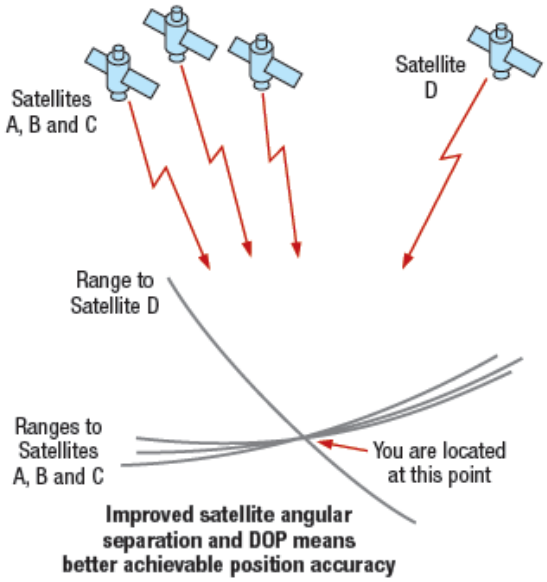

Imagen20. Recepción de cuatro satélites simultanea [9]

Problemas GNSS

Para los sistemas de posicionamiento globales existen varias maneras de interferir en su funcionamiento normal. Algunas de ellas podrían tratarse como ataques informáticos.

El spoofing es el método más habitual de interferir en una señal GNSS es un método con el que se consigue que el receptor calcule de forma errónea el circulo de posición y el tiempo. Debido a que hay algún generador que esta emitido señales falsas o retrasmitiendo una señal anteriormente grabada de un satélite.

Para este problema la solución pasa por la encriptación de la señal GNSS sin embargo esto solo está disponible para algunos usuarios. Además, para poder realizarlo es necesario por parte del atacante tener equipos especializados que imitan las señales. [9]

Conclusiones GNSS

El funcionamiento y el equipo son seguros debido a que el receptor de los sistemas de posicionamiento solo está diseñado para recibir las señales de los satélites. Sin embargo, métodos como el spoofing pueden hacer al equipo calcular una posición errónea. Todos los oficiales de guardia deben conocer estas limitaciones se recomienda contrastar la posición periódicamente mediante observación del sol al mediodía.

Las posiciones que obtiene el receptor serán transmitidas también a los equipos radar, AIS y ECDIS.

ECDIS

La aparición de las cartas electrónicas en la década de 1990 sirvió a los barcos para tener información adicional, como es la información en tiempo real que se podía mostrar en las pantallas de la carta electrónica y los sistemas de información (ECDIS).[1]

La OMI adoptó unos estándares de calidad durante el año de 1990. En 2000, la OMI regula el capítulo V del convenio SOLAS para adaptar los requisitos en los sistemas y equipos de navegación a bordo. Desde ese momento se regula la obligación de llevar a bordo estos equipos, dejando de usar cartas de papel. [1]

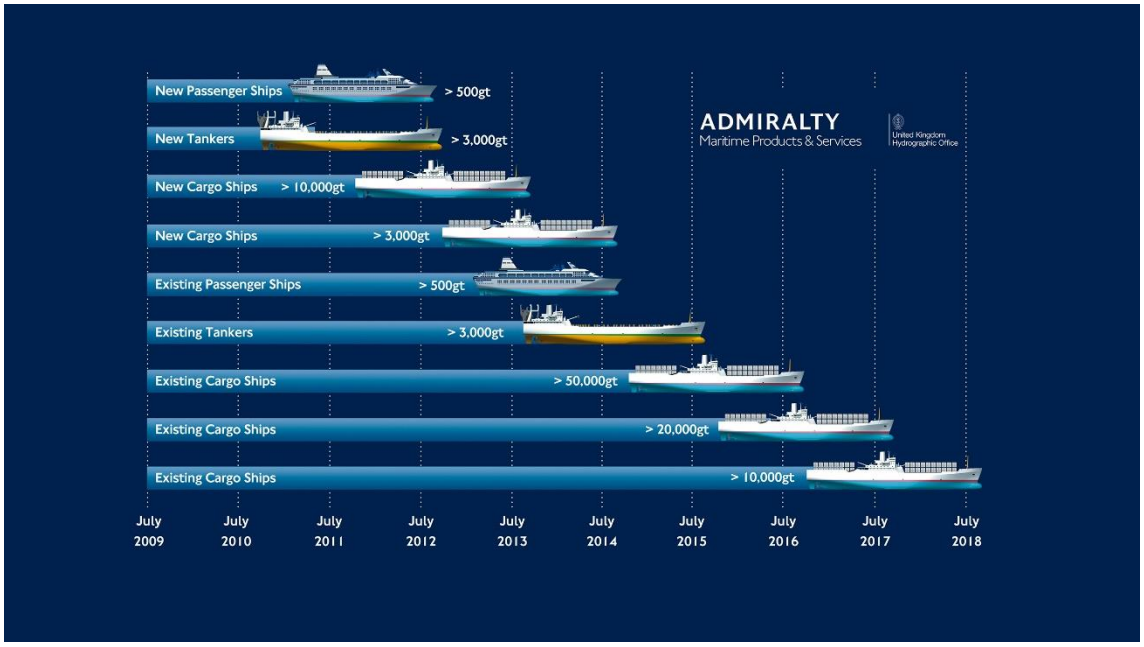

Grafico2. ECDIS cronograma obligatoriedad por tipo de buque [3]

Actualmente el uso de este sistema esta implementado en gran parte de la flota mundial. Las cartas náuticas son emitidas oficialmente por o bajo la autoridad de un gobierno, una oficina hidrográfica autorizada u otras instituciones gubernamental.

En el mundo marítimo existen diferentes distribuidores digitales que ofrecen las cartas electrónicas y sus actualizaciones. Algunos de estos distribuidores usan su propio software para las actualizaciones otros sin embargo siguen usando el correo electrónico para él envió de la información.

Para los casos de actualización a través de internet es necesario meter la información en una memoria USB que luego se insertara en el equipo de ECDIS para realizar la instalación de la misma. En algunos modelos de ECDIS cuando tenemos varios equipos ECDIS interconectados es posible realizar la actualización únicamente en un equipo porque después esta actualización se transmite automáticamente a los demás equipos.

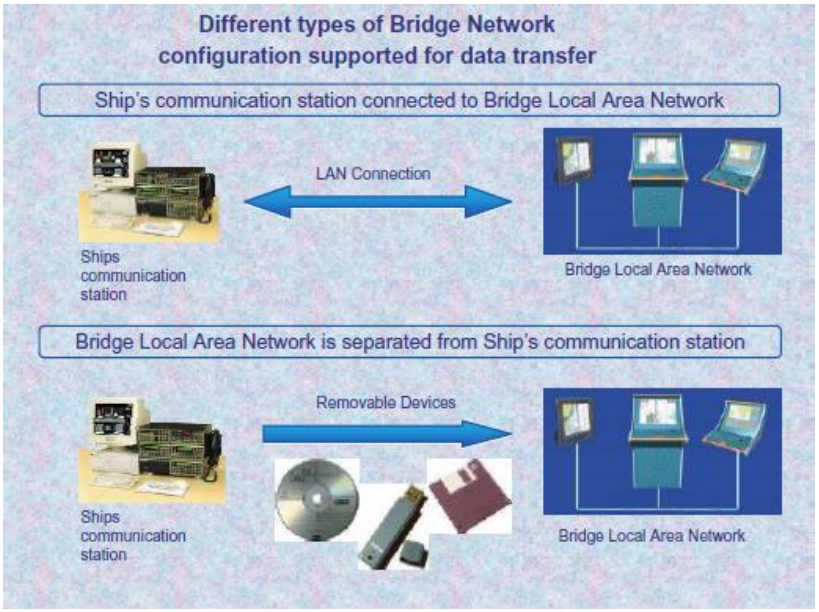

Imagen21. Métodos de actualización de sistemas ECDIS [11.2]

La red LAN de los equipos ECDIS tiene varias funciones como son compartir información con otros equipos además de la información de rutas y actualizaciones. En el caso de las actualizaciones solo es necesario realizarlas en un equipo porque este equipo una actualizado mandara la actualización hacia los demás. Este sistema automático de actualización puede traer problemas en caso de un virus o infección.

Las partes que componen un equipo ECDIS tienen muchas variaciones dependiendo del tipo de buque lo más común es encontrar con los siguientes partes:

Procesador de datos, software y la red local son los encargados de gestionar la información. Los equipos ECDIS tiene la capacidad también de gestionar la información proveniente de otros equipos de navegación como son AIS, corredera, girocompás, GPS, VDR incluso el radar. [11.1]

Base de datos de cartas es el lugar donde se encuentran los datos de las cartas electrónicas junto con sus actualizaciones. Las cartas electrónicas pueden estar en dos formatos. Formato ráster son cartas electrónicas generadas a partir del escaneo de una carta de papel. Formato vectorial son cartas electrónicas generadas completamente en formato digital. [11.1]

Pantalla del sistema donde se muestran las cartas electrónicas junto con la información del buque y la ruta planificada además de información de los demás sistemas.

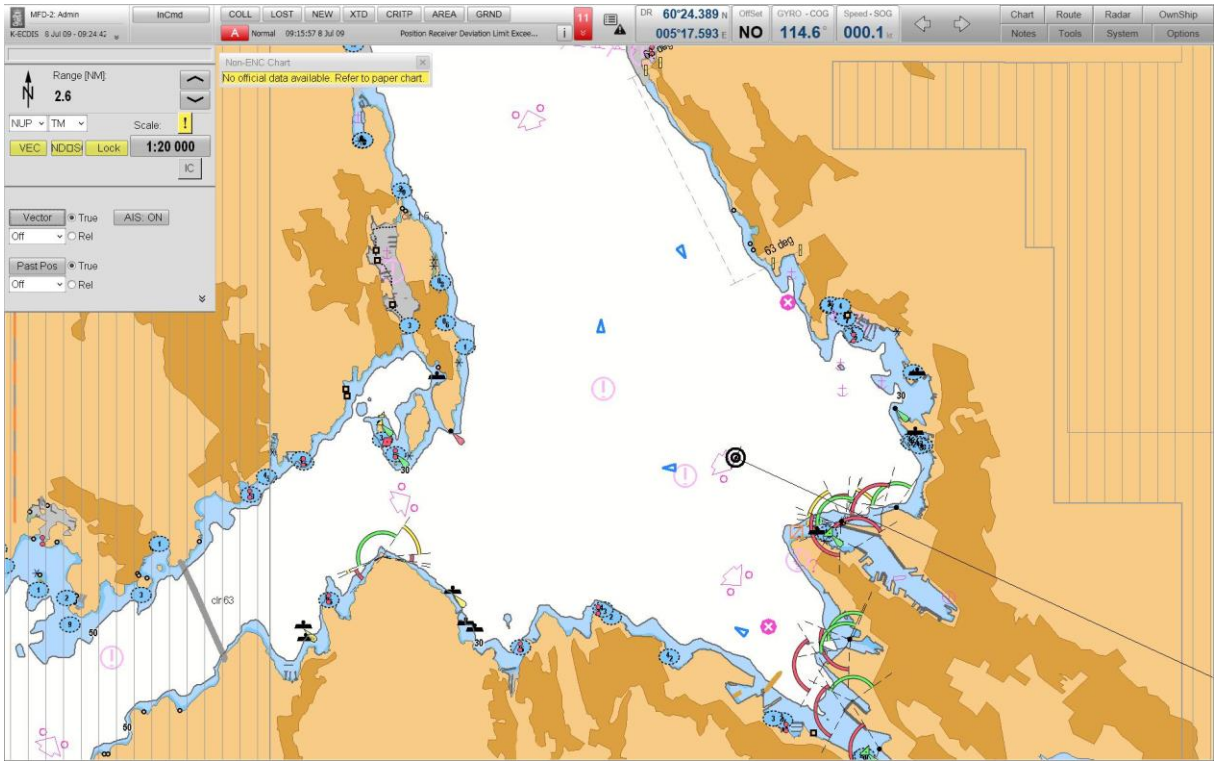

Imagen22. Pantalla de un equipo K-Bridge ECDIS Kongsberg [12]

Hay dos modos de visualización posibles para las pantallas.

Modo relativo, el buque permanece fijo en el centro de la pantalla mientras que la carta electrónica se mueve. Este modo requiere mucha potencia debido a que los datos de la pantalla deben actualizarse y volver a dibujar en cada movimiento del buque. [11.1]

Modo verdadero, la carta electrónica permanece fija mientras el buque se mueve a través de ella. La pantalla puede ser orientada hacia el norte verdadero o hacia el rumbo del barco, según la disponibilidad de datos del sensor de rumbo como como del girocompás. [11.1]

Interfaz de usuario, el oficial de guardia puede configurar los parámetros del equipo introducir nuevos datos y visualizar las luces de errores. [11.1]

Imagen23. Sistema de visualización de cartas electrónicas [12]

Problemas ECDIS

Los sistemas ECDIS normalmente trabajan dentro de sistemas operativos de ordenadores sobremesa usando Windows como sistema base para funcionar el programa específico del ECDIS. Por ello estos sistemas puede ser afectados por virus y vulnerabilidades que afectan a los sistemas Windows.

Por el método que se usa para actualizar mediante memorias USB también tendríamos un posible foco de infección del sistema. Y por supuesto al ser un equipo que esta interconectado con los demás sistemas del puente podría ser el equipo inicial que infecte a los demás equipos del puente, o servir como conexión entre los equipos y un atacante en el exterior.

Todos estos problemas pueden reducirse si se aísla este sistema lo máximo posible con el exterior. Por ejemplo, que el equipo no esté conectado directamente a la red de internet. O que para realizar las actualizaciones se usen equipos preparados únicamente para esta función.

Normalmente las infecciones podrían darse por la memoria USB que está infectada o por la modificado de los archivos de actualización de las cartas electrónicas tanto con programas maliciosos como con la modificación de la información de las cartas. Esto puede ocurrir porque normalmente las actualizaciones de las cartas vienen por correo electrónico y los atacantes podrían generar un correo falso con los archivos infectados.

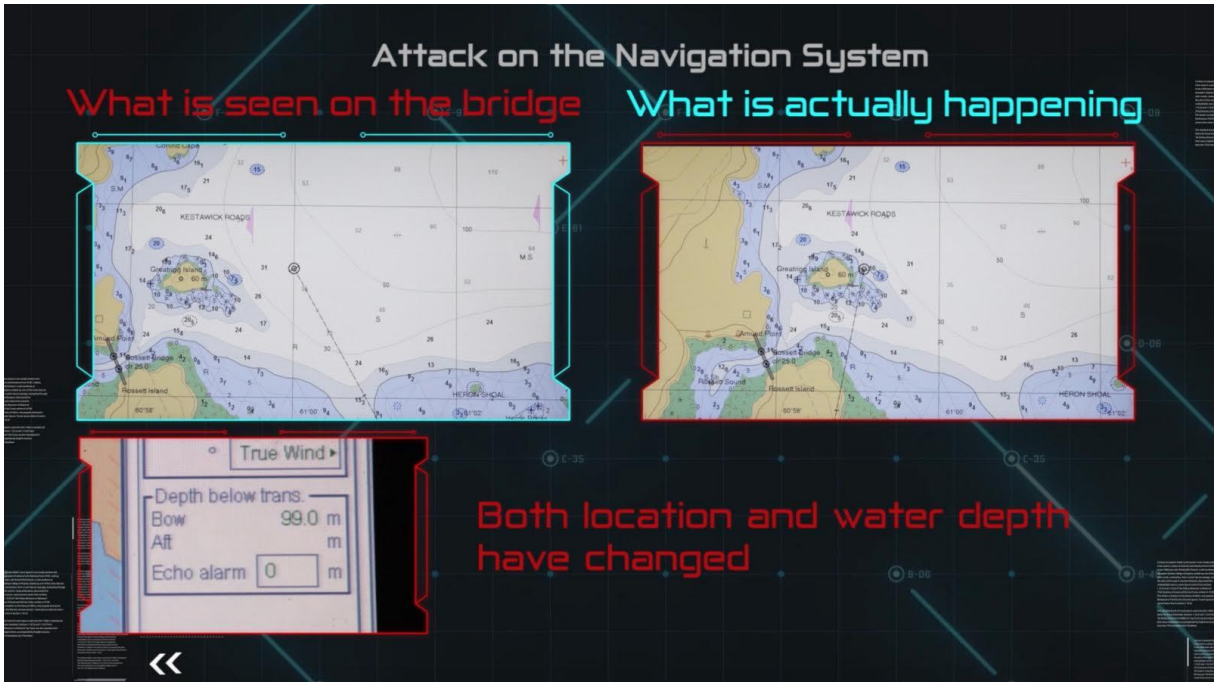

Imagen24. Pantalla del ECDIS muestra el efecto del ataque informático [8]

Al igual que ocurría con el radar la empresa israelí "Naval Dome" especializada en seguridad informática logro modificar parámetros del ECDIS en tiempo real gracias a infectar el equipo con un troyano. Además, después de obtener el acceso remoto al ECDIS pasaron a infectar otros equipos como el radar usando como intermediario al equipo ECDIS. [8]

Conclusiones ECDIS

Los equipos ECDIS puede tener muchas vulnerabilidades debido a su diseño y sus métodos de actualización. Para los oficiales de puente es necesario una supervisión constante del estado del equipo. Especial atención cuando se vayan a realizar las actualizaciones siempre usando equipos y memorias USB únicas para esta función. Por último, se debe prestar atención a los correos electrónicos que se reciben relacionados con las actualizaciones, siempre revisar el remitente y el contenido del mismo antes de introducirlo en el equipo ECDIS.

Los equipos de control de carga

Se trata de equipos que son usados para las operativas de carga y descarga del cargamento a bordo. Este sistema está instalado en los buques tipo tanque que se dedican al transporte de materias a granel liquidas como son los petroleros, quimiqueros y buques gaseros.

Imagen25. Disposición de algunos equipos del control de carga del buque gasero Bilbao Knutsen

CTS o CMS

Uno de los sistemas esenciales en los buques tanque es el sistema de transferencia de custodia o sistema medición de nivel de tanques siendo el equipo encargado del cálculo de la carga a bordo en todo momento. Mediante el sondeo de los tanques de carga, el sistema trabaja con la información de varios equipos entre los que se encuentran el clinómetro, radares de nivel los tanques, sensores de temperatura y sensores de presión.

Este sistema es indispensable en los buques tanque tanto al comienzo como en la finalización de las operaciones de carga o descargas para la comprobación de la mercancía abordo.

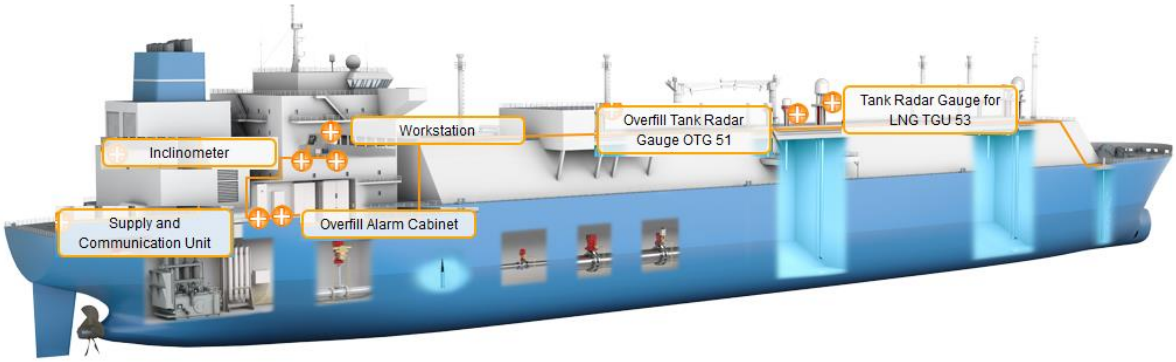

Imagen26. Custody Transfer System Emerson [13]

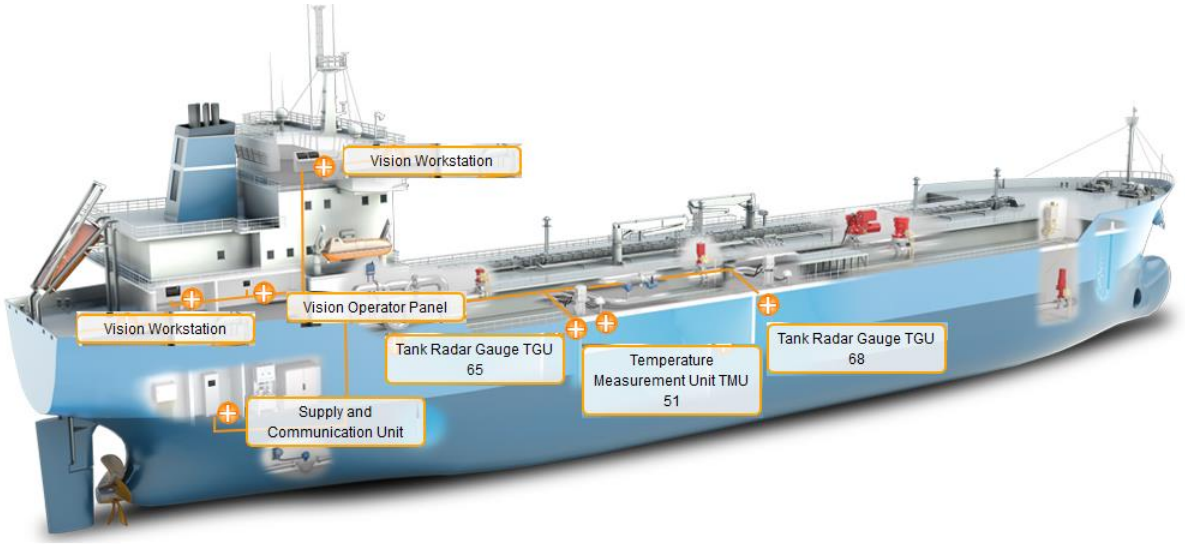

Imagen27. Cargo Monitoring System Emerson [13]

Las partes que componen estos sistemas son una serie de radares repartidos por los tanques para obtener medición de la altura del líquido en los tanques, una unidad de control que procesa las señales analógicas que envían estos radares y por último conectada a esta unidad están los paneles de visualización situados en el control de carga.

Problemas CTS o CMS

Intrínsecamente son equipos muy seguros porque están aislados normalmente de los demás sistemas. Estos equipos utilizan su propia red LAN para transmitir sus datos por el buque. Para poder atacar estos equipos sería necesario tener acceso personal al buque y a los paneles de usuario. Existen ciertos parámetros que si se modifican puede generar un gran error en el cómputo de la carga a bordo. La modificación de parámetros como el coeficiente de dilatación de tanques o el coeficiente de corrección de escora harán a este equipo fallar en el cálculo.

Conclusiones CTS o CMS

En estos equipos las recomendaciones son revisar periódicamente los valores de los ajustes predefinidos. Además de realizar la calibración anual de los equipos para comprobar el correcto funcionamiento de los mismos y su estado.

Sistemas de alarmas

Se compone de varios sistemas independientes que pueden obligar a detener las operaciones si se sobrepasan ciertos criterios preestablecidos. Algunos de los sistemas de alarmas son el sistema de alto nivel de tanques de carga y lastre, sistema de control de tensión de cabos y el sistema de parada de emergencia (ESD).

El sistema de alto nivel de tanques funciona mediante unas sondas o radares que miden la capacidad del tanque. Y puede activar la parada de emergencia si se llega a ciertos niveles de llenado de los tanques. Dependiendo del tipo de buque tanque existe una diferente normativa. Como normal general en estos buques tienen dos niveles a alarma uno que indica 95% siendo una alarma sonora y visual.[12]

Y el nivel de alarma del 98% que puede llegar a activar el sistema de parada de emergencia. [12]

Sistema de parada de emergencia (ESD)

El sistema ESD es un enlace que une al buque con la terminal. Se puede activar automáticamente al sobrepasar algún valor previamente fijado como son los niveles altos del tanque o la presión máxima en los tanques. Este sistema también puede activarse manualmente mediante los botones ESD que se encuentra repartidos por lugares estratégicos tanto del barco como del a terminal.

Tanto el buque como la terminal puede activar el procedimiento de parada de emergencia. El objetivo del sistema es proteger al buque y a la terminal en los casos que aparecieran condiciones anormales durante las operaciones (derrames, rotura de líneas, sobrepresiones en líneas o tanques). Si el sistema es activado comienza una secuencia predeterminada de detención de las operaciones parando bombas, cerrando válvulas del manifold, deteniendo compresores en el caso de buques gaseros.

El movimiento excesivo del buque a lo largo del muelle o la ruptura de cabos del buque puede provocar la falla de la manguera o del manifold. Por lo tanto, este sistema para detener las operaciones debe considerarse un sistema de seguridad crítico en las operaciones de transferencia de carga.

Ship		Terminal
Transmits ESD trip signal to terminal via SSL.	→	Receives ESD trip signal from ship.
	or	
Receives ESD trip signal from terminal.	←	Transmits ESD trip signal to ship via SSL.
		Stops cargo flow, either by tripping terminal's cargo transfer pumps or by other safe means.
Optional		
Closes ship's manifold valves in a safe manner, taking account of potential surge issues.		Closes terminal's ESD valves in a safe manner, taking account of potential surge issues.

Tabla8. ESD acciones posibles durante operaciones de carga [18]

Ship		Terminal
Transmits ESD trip signal to terminal via SSL.	→	Receives ESD trip signal from ship.
	or	
Receives ESD trip signal from terminal.	←	Transmits ESD trip signal to ship via SSL.
Stops cargo flow by tripping ship's cargo transfer pumps.		
Optional		
Closes ship's manifold valves in a safe manner, taking account of potential surge issues.		Closes terminal's ESD valves in a safe manner, taking account of potential surge issues.

Tabla9. ESD acciones posibles durante operaciones de descarga [18]

Los sistemas ESD están compuestos de varios partes repartidos de forma simétrica entre el buque y la terminal. En cada lado tenemos una unidad de control donde se monitorizan los parámetros de alarma y se configura los modos de funcionamiento.

Una unidad de control en el jetty y otra en el buque son las encargadas de hacer de puente de unión para transmitir las señales eléctricas a través del cable de conexión.

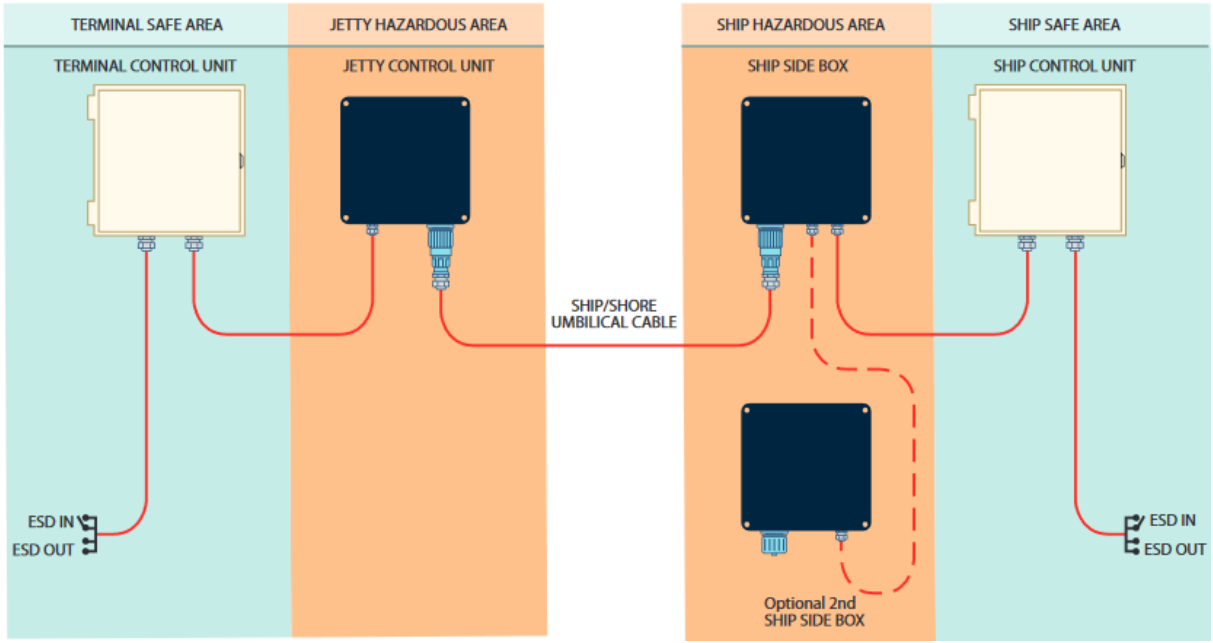

Imagen28. ESD partes del sistema [18]

Problemas con el ESD

Los problemas de los sistemas ESD vienen por el lado de las alarmas y todos los parámetros que hacen poner en funcionamiento este procedimiento de emergencia. Cualquier manipulación que ocurra tanto en el software de los sistemas del buque como en los sistemas SCADA de la terminal pueden producir un funcionamiento erróneo del mismo.

Conclusiones con el ESD

Aunque los sistemas ESD funcionan aislado completamente de los demás sistemas del buque necesitan la información proveniente de otros subsistemas para verificar las condiciones. Tanto los oficiales del buque como los operadores de la terminal deben conocer los parámetros limites que hacen activar este sistema para no activarlo de manera errónea. Además, realizar las pruebas de testeo del sistema antes de la llegada a un lugar donde se vayan a realizar operaciones con la carga para comprobar el funcionamiento del mismo.

Ordenadores de esfuerzos (HSMS)

Es un equipo que monitoriza los esfuerzos a los que se está sometiendo el casco del buque. Estos sistemas son de gran importancia durante las operaciones de carga y descarga de la mercancía en puerto. Porque supervisa que los esfuerzos del acero para proteger de la fatiga y sobreesfuerzos torsionales y de tracción sobre el casco del buque. A su vez estos sistemas sirven para realizar los precálculos de esfuerzos antes de una operación.

Tiene una gran importancia en los buques dedicados al transporte de granel. Debido a que transportan una gran cantidad de mercancía. El sistema se compone de varias partes.

Sensores son los encargados de detectar las deformaciones del casco. Normalmente son del tipo de galga extensométricas situados en lugares estratégicos del buque.

Acelerómetro instalado en la proa para medir la aceleración vertical de la proa.

Unidad de control y monitorización para visualizar y calcular los valores de esfuerzos en el casco.

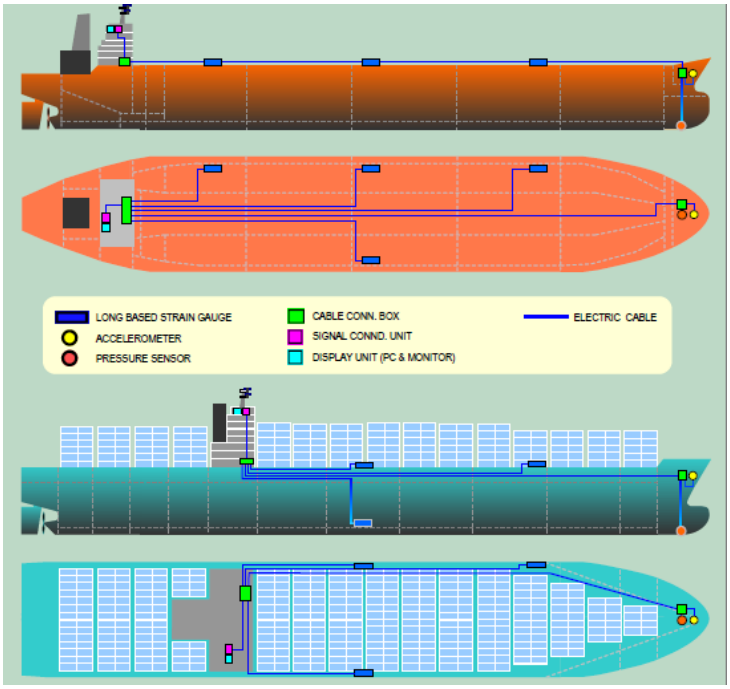

Imagen29. Esquema de un ordenador de esfuerzos [14]

Problemas HSMS

Los problemas en estos sistemas al igual que ocurre con los sistemas CTS que normalmente trabajan aislados de los demás sistemas viene a la hora de calcular los esfuerzos en tiempo real porque necesitan la información precisa del nivel de líquido en los tanques de carga o en el caso de buques a granel el nivel en las bodegas. Si tenemos algún programa malicioso que afecta a la medición de la altura en los tanques que recibe el ordenador de esfuerzos producirá el cálculo erróneo de la situación de esfuerzos del buque.

Conclusiones HSMS

En general es un sistema bastante preciso para medir los esfuerzos del buque dependiendo de las interconexiones que realice con otros equipos será más complicado realizar un ataque sobre el mismo. Para los oficiales se recomienda una supervisión durante las operaciones de carga y descarga. Para los buques dedican al transporte a granel se recomienda una especial atención durante la navegación en condiciones de mal tiempo debido que ha habido un gran número de buques que se han partido al navegar en estas condiciones especialmente cuando se navega en lastre.

Sistemas de tratamiento del agua de lastre

Es un sistema actualmente incorporado en los buques que sirve para la esterilización del agua de lastre con él objetivo de evitar la propagación de organismos acuáticos perjudiciales de una región a otra. El uso de estos sistemas entro en obligatoriedad para todos los buques a partir del año 2017.

Actualmente el convenio que regula esta materia es el convenio internacional para el control y la gestión del agua de lastre y los sedimentos del buque dentro del mismo hay dos tipos de reglas dependiendo el sistema de tratamiento instalado a bordo y como se opere. Para septiembre de 2024 todos los buques deben trabajar con la regulación D-2.

Regulación D-1 es para buques que realizan el cambio de agua de lastre de la forma normal. Para cumplir con esta regulación el buque debe realizar el cambio de agua de lastre con una eficiencia del 95 por ciento del total volumétrico de agua de lastre intercambiada. Para buques que cambian agua de lastre por bombeo será necesario el bombeado de tres veces el volumen total de agua de lastre para cumplir con la normativa.

Regulación D-2 es para buques que realizan el cambio de agua de mejorado. Los buques que realizan este tipo de cambio de lastre deben tener en el agua de los tanques a la hora de vaciarlos menos de 10 organismos viables por metro cúbico menos que 50 micrómetros de un mínimo de dimensión y mayor o igual a 10 micrómetros como mínima dimensión. Durante la descarga no se puede super ninguno de estos valores.

Estos sistemas usan diferentes métodos para tratar el agua de lastre eliminando los microorganismos que puedan contener. Los sistemas tienen desde filtros físicos pasando por desinfección química, usar rayos ultra violetas, también se usan desoxigenación dentro de los tanques de agua de lastre, tratamientos térmicos, acústicos incluso sistemas de vacío.

Problemas de los sistemas de tratamiento de agua de lastre

Los problemas principales vienen relacionados con controlar los parámetros de limpieza del agua cualquier manipulación de esos que produzca que el agua de lastre tratada sobrepase los límites de organismos vivos puede conllevar sanciones al buque. Debido a que en los puertos están obligados a controlar la calidad del tratamiento del agua de lastre.

Conclusiones de los sistemas de tratamiento de agua de lastre

Son sistemas que llevan instalados a bordo muy poco tiempo, su control y supervisión se realizan desde el control de carga. Muchos de estos sistemas funcionan usando sistema operativo Windows por lo que pueden ser objetivo de todas las amenazas que afectan a estos sistemas.

Para los oficiales de guardia se recomienda revisar el funcionamiento concreto del sistema que hayan instalado en su barco para conocer sus singularidades. Además, durante las operaciones de carga y descarga mantener atención a cualquier parámetro que salga del rango normal.

Sistema de control de tensión de cabos

Es un aparato que controla en tiempo real la tensión que ejercen las maquinillas sobre los cabos de amarre para evitar movimientos del buque sobre el jetty y la rotura de cabos. En muchas terminales a lo largo del mundo tiene regulado unas tensiones máximas de trabajo de los cabos. En el caso de los buques gaseros su utilización es obligaría. Sin embargo, para buques petroleros es normal que se use en los de mayor tamaño como son los VLCC y Suexmax.

Hay dos tipos de sistemas para controlar la tensión de los cabos. Un sistema completo puede estar instalado a bordo de los buques. Se compone de sensores en cada maquinilla y de una unidad de control donde se puede configurar los niveles de alarma. En esta unidad también se puede visualizar en tiempo real la tensión de cada maquinilla. Algunos de los parámetros ambientales que también se controlan son la dirección y fuerza del viento y de la corriente de agua.

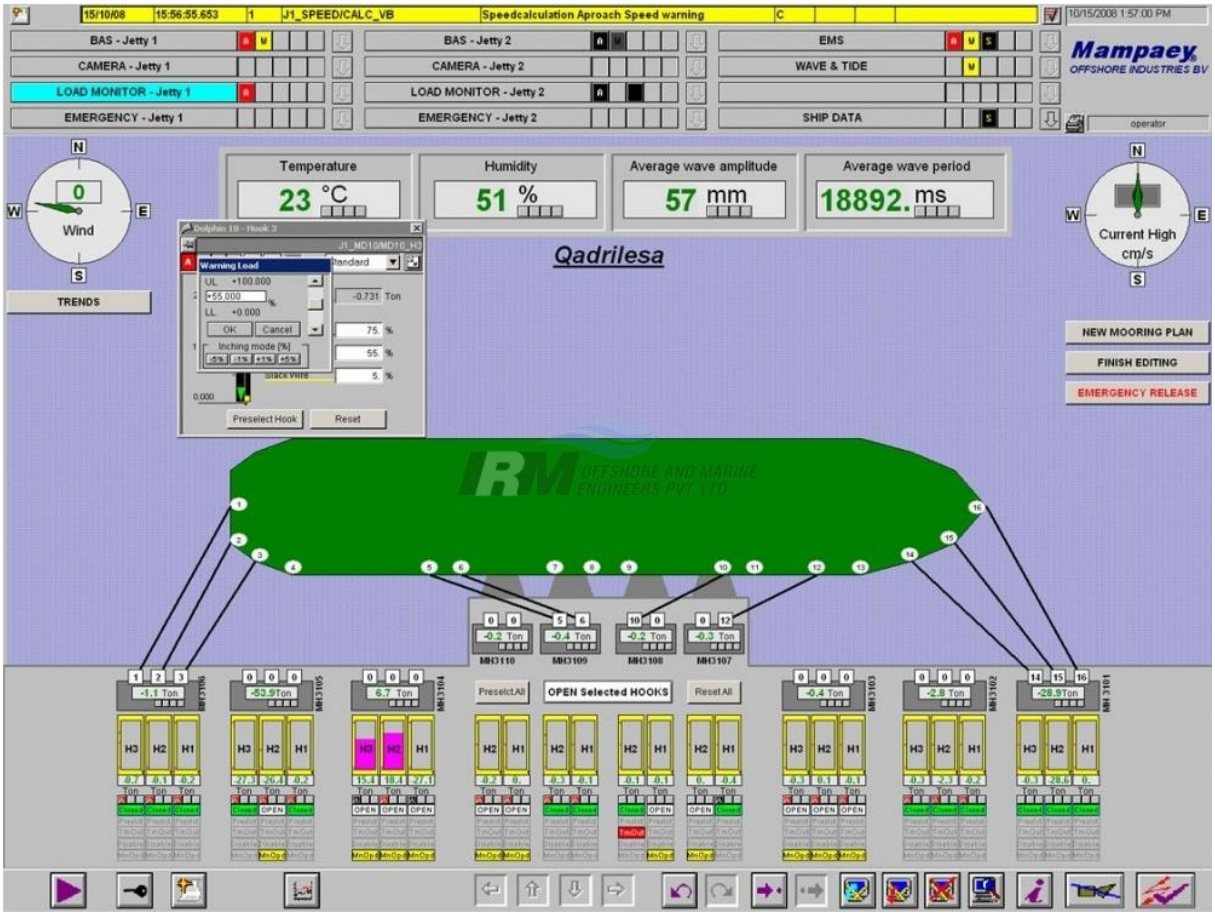

Imagen30. Mooring monitoring system [19]

El otro tipo es el instalado en las terminales de buques gaseros y algunas de grandes buques petroleros tienen instalado en sus jetty unos ganchos de amarre con función de liberación rápida por cada cabo. Cada uno de estos ganchos instalado un sensor de tensión que se monitoriza en tiempo real. La unidad de control está situada en el control de carga de la terminal. Sin embargo, al buque durante operaciones envían un receptor portátil para visualizar desde el buque los valores que tienen en la terminal. Este recetor está conectado al sistema ESD del buque y a su vez mediante ondas de radio VHF se comunica con la unidad de control de la terminal.

Imagen31. Mooring monitoring system portátil [19]

Problemas de los sistemas de control tensión de cabos

Los problemas principales que pueden tener estoy sistemas a la hora de tener un funcionamiento correcto fuera de la intromisión de un atacante. Normalmente el sistema que se encuentra instalado en los buques está totalmente aislado de los demás por lo tanto es de difícil acceso para realizar un ataque sobre él. Sin embargo, el sistema instalado en los jetty tiene un punto débil y son los dispositivos portátiles que usan la radio VHF para comunicarse con la terminal.

Asu vez los dispositivos que se encuentran en el buque y que dan la información de viento y corriente podrían ser atacados y los datos que transmiten a este dispositivo ser erróneos.

Conclusiones con los sistemas de control tensión de cabos

Es otro sistema complementario para mejor la seguridad de los buques tanques durante las operaciones tiene algunos puntos débiles en cuanto a su funcionamiento que podrían ser objeto de ataque. Durante las operaciones el oficial deberá controlar tanto los parámetros ambientales como la tensión que se está ejerciendo en todas las maquinillas. Manteniendo todos los cabos fuera de la tensión limite que marque la terminal.

Sistema Integrado de Automatización (IAS)

Son un conjunto de sistemas de control que funciona como interconexión de sistemas más simples que hay repartidos por el buque. Siendo desde este sistema sobre el que se actúa para el control y monitorización de los sistemas más simples. Dependiendo el tipo de buque y el astillero donde se fabricó. Tenemos diferentes niveles de automatización y conexión entre los sistemas.

Estos sistemas integran todos los equipos en un único programa informático. Desde el punto de vista de la operativa tiene muchas mejoras debido a que se pueden controlar una gran variedad de equipos al mismo tiempo y remotamente sin necesidad de estar físicamente donde se encuentra cada equipo. Los sistemas que componen la maquinaria de un buque actualmente tienen una gran automatización debido a varios factores como son el sistema implementado de guardias de los oficiales de máquinas junto con el tamaño y complejidad de los sistemas instalados.

Especialmente durante las horas nocturnas y la navegación el control de máquinas se queda monitorizando todos los parámetros de manera automática. En caso de que algún parámetro salga del rango normal de funcionamiento. El sistema enviara una alarma a los oficiales asignados a la guardia en ese momento para que la verifique.

Los sistemas integrados de automatización están configurados en varios grupos por una parte están los sistemas SCADA. Son programas informáticos que normalmente funcionan en ordenadores con sistemas operativos de servidor. Dentro del programa está programado toda la lógica de control para los equipos que componen el buque. Estos ordenadores están situados en lugares estratégicos como son el control de máquinas, el control de carga y el puente. Estos sistemas funcionan a través de una red local que interconectan todos los ordenadores de control.

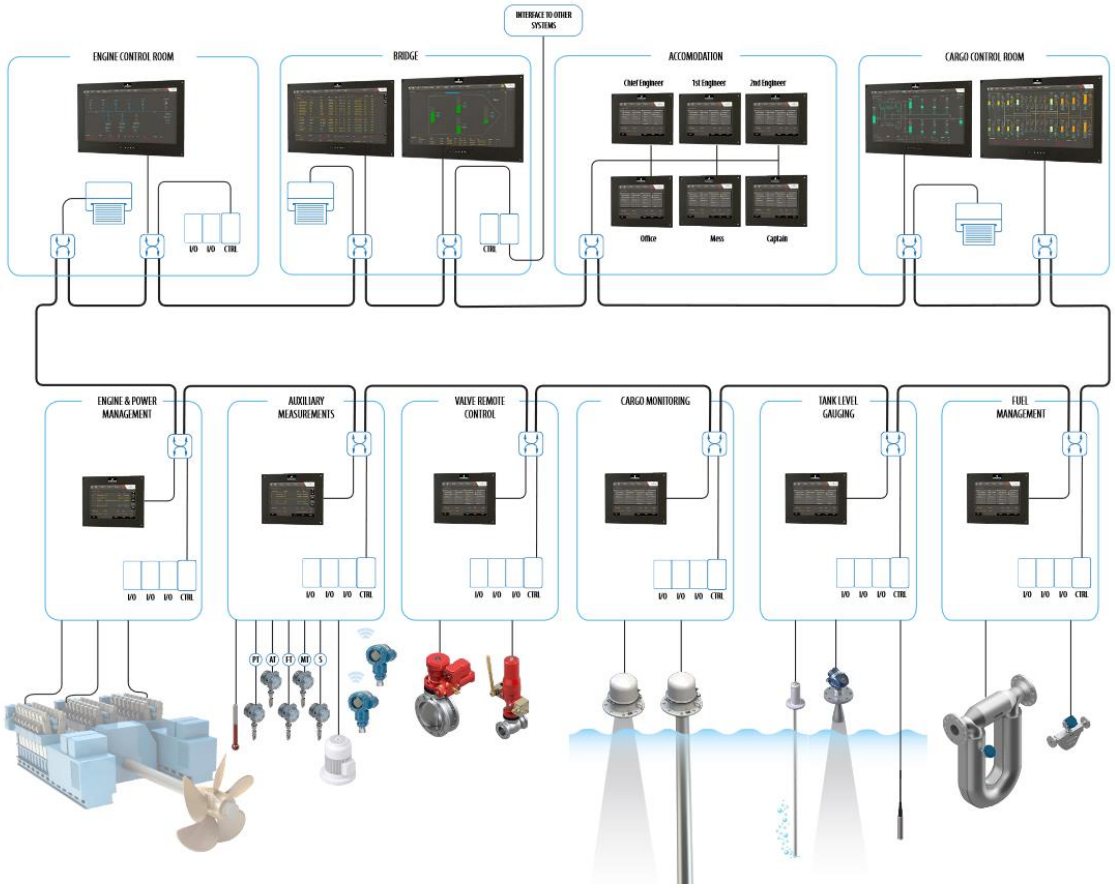

Imagen32. Sistema de control integrado Emerson [13]

Otro gran grupo están los PLC son los equipos encargados del control en el lugar del equipo. Son pequeños ordenadores diseñados para automatizar los equipos. Desde los cuales se controlan las señales analógicas de los componentes internos de los equipos y se envían a los sistemas integrados las señales digitales para su procesamiento y supervisión. Estos sistemas se encuentran ubicados por cada máquina y en cuartos eléctricos especialmente diseñados con ventilación.

Actualmente con los PLC se puede controlar y programar casi cualquier maquina lo que los hace muy versátiles.

Problemas IAS

Como ocurría con otros sistemas mencionados anteriormente estos sistemas trabajan con sistemas operativos de servidor los cuales no se suelen actualizar debido a los problemas que puedan generarse por un mal funcionamiento. A su vez el software de estos sistemas integrado suele ser muy complicado actualizar o modificar por la complejidad de sistema interconectados.

Desde el punto de vista de un atacante si consigue tener acceso remoto a alguno de las terminales podría ser relativamente sencillo conseguir el control del sistema completo.

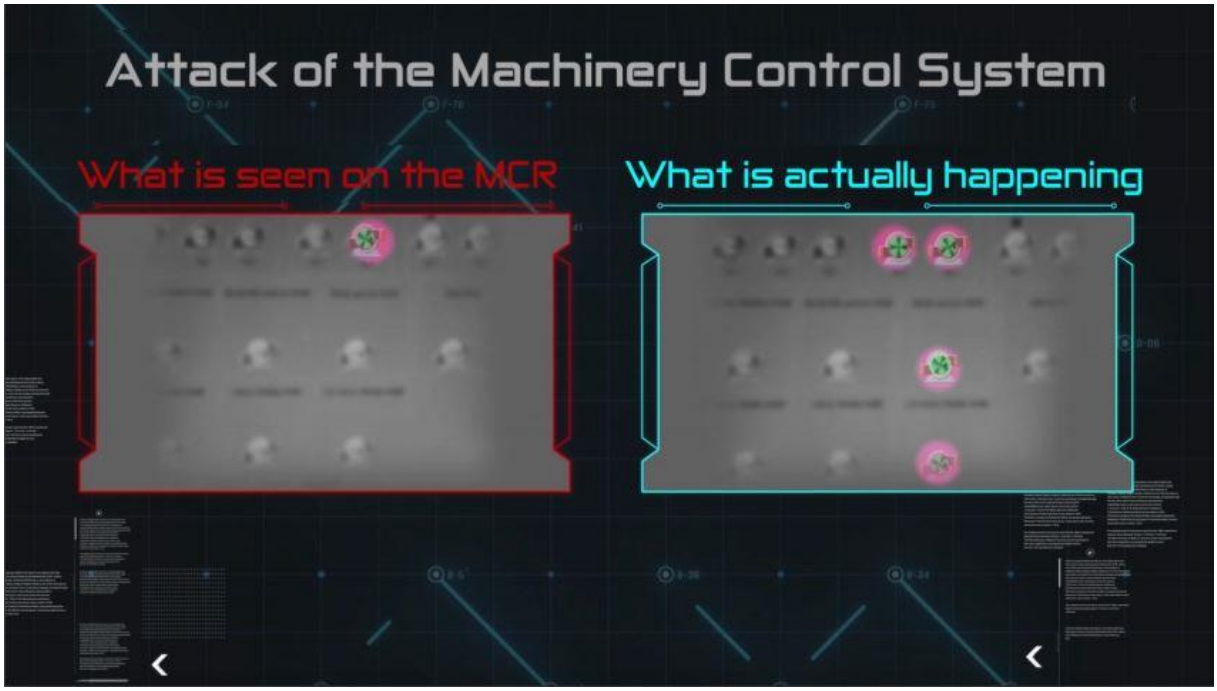

Imagen33. Pantalla de un sistema IAS muestra el efecto de un ataque informático [8]

Conclusiones IAS

Son sistemas seguros siempre que estén aislados del exterior. Son sistemas que su versión de software no suele actualizarse con el tiempo lo que puede ocasionar que se puedan usar exploit y software malicioso antiguo. Los oficiales que operan con estos sistemas se recomendar observar siempre cualquier funcionamiento errático o anormal del sistema. Además de realizar las pertinentes revisiones anuales del sistema para controlar que todos los sistemas están en buenas condiciones.

Conexión satelital

Actualmente los buques necesitan cada vez de una mayor conexión con el exterior debido al aumento del uso de internet para la operativa diaria del buque. Desde el correo electrónico, llamas telefónicas pasando por los sistemas de gestión del buque, monitorización del buque en tiempo real hasta para el uso recreativo de la tripulación.

Todos estos factores han obligado en muchas compañías y buques la instalación y contratación de sistema de comunicación satelital de mayor capacidad y calidad en lo referido a las conexiones de datos.

Por ejemplo, actualmente en muchos buques los técnicos de sistemas pueden realizar algunos de los mantenimientos de los equipos informáticos remotamente. Eliminando la necesidad de que tenga que moverse hasta el buque para solucionar los problemas.

Sin embargo, todas estas ventajas traen consigo algunas desventajas como son un mayor coste para el armador o fletador del buque debido al coste de la banda de datos usada. Además de un aumento en el riesgo de sufrir un ataque remotamente usando esta conexión de internet.

Algunas de las compañías que ofrecen los servicios de internet satelital ofrecen además diferentes métodos para proteger las comunicaciones mediante tecnologías de cifrado, incluidas VPN y OpenVPN. Además, permiten la personalizar del firewall para permitir solo el tráfico hacia páginas con una IP seleccionada o bloqueo de páginas web por contenido.

Equipos ofimáticos

En los buques que componen la flota mundial es normal tener en todos los equipos ofimáticos instalado un sistema operativo Windows. En algunas empresas este sistema tiene configurado algún tipo de máquina virtual con lo cual se aumenta en la seguridad. Además, algunos de estos equipos pueden tener asistencia remota en caso de fallos problemas en el funcionamiento.

En los casos de máquinas virtuales normalmente tienen un servidor el cual almacena los datos de todos los usuarios. El servidor está conectado con todos los equipos que tengan configurado la máquina virtual permitiendo a cualquier usuario entran en su cuenta en cualquier equipo. Es una gran ventaja frente a los equipos normales debido a que no tienes que usar memorias o discos duros para mover la información de un ordenador a otro. Simplemente con iniciar la sesión ya tienes todos los archivos.

En estos equipos instalados en los buques al igual que las empresas en tierra suele usar un correo corporativo con el cual se mejora la seguridad y se puede administrar mejor la base de datos del correo electrónico. Debido al gran número de correos que se envían y reciben de diferentes organizaciones.

Dentro del aparatado de equipo ofimáticos también se encuentran la impresoras teléfonos y demás material que trabaje dentro de la misma red LAN.

ANALISIS DE RIESGOS

Tipos de amenazas

Las compañías deben revisar todos los aspectos específicos de sus operaciones que pueda aumentar su vulnerabilidad a incidentes cibernéticos.

A diferencia de otras áreas de seguridad, donde la evidencia histórica está disponible, la gestión del riesgo cibernético se hace más desafiante por la ausencia de información definitiva sobre incidentes y su impacto.

La administración pública y el transporte aéreo han demostrado que los ataques cibernéticos exitosos pueden resultar en una pérdida significativa de servicios. Hay motivos para que organizaciones e individuos exploten vulnerabilidades cibernéticas.[6]

Group	Motivation	Objective
Activists (including disgruntled employees)	■ reputational damage ■ disruption of operations	■ destruction of data ■ publication of sensitive data ■ media attention ■ denial of access to the service or system targeted
Criminals	■ financial gain ■ commercial espionage ■ industrial espionage	■ selling stolen data ■ ransoming stolen data ■ ransoming system operability ■ arranging fraudulent transportation of cargo ■ gathering intelligence for more sophisticated crime, exact cargo location, ship transportation and handling plans etc
Opportunists	■ the challenge	■ getting through cyber security defences ■ financial gain
States **State sponsored organisations** **Terrorists**	■ political gain ■ espionage	■ gaining knowledge ■ disruption to economies and critical national infrastructure

Tabla10. Motivaciones de los atacantes [6]

Tipos de ciberataques

Los ciberataques que ocurren en el ámbito marítimo pueden ser de dos tipos:

Ataques no dirigidos son aquellos donde el objetivo del ataque no está predeterminado hacia la empresa o los sistemas y datos de un barco en concreto.

Estos ataques suelen usar herramientas y técnicas disponibles en Internet. Además, pueden localizar, buscar y explotar vulnerabilidades generalizadas que también pueden existir en una empresa y a bordo de un buque.

Algunos ejemplos concretos

En primer lugar, está el malware que son software malicioso diseñado para acceder o dañar un ordenador sin conocimiento previos del propietario. Existen varios tipos de malware, incluidos troyanos, ransomware, spyware, virus y gusanos. El malware también puede explotar deficiencias y problemas conocidos en programas desactualizados o software sin parches de seguridad.

El ransomware es un software que cifra los datos en los sistemas que infecta mediante un algoritmo el cual solo se entrega previo pago de dinero. (Fue el caso de la empresa Maersk en el año 2017)

El término "exploit" generalmente se refiere al uso de un software o código, que está diseñado para aprovechar y manipular una vulnerabilidad en otro software o hardware de un ordenador. Estos problemas pueden ser un error en el código fuente, vulnerabilidad del sistema, diseño incorrecto, hardware con un mal funcionamiento o error en la implementación de un protocolo. Estas vulnerabilidades pueden ser explotadas de forma remota o activadas localmente. A nivel local, el usuario puede ejecutar un fragmento del código malicioso, a veces a través de enlaces distribuidos en archivos adjuntos del correo electrónico o a través de sitios web maliciosos.

Phishing se trata de una técnica de envío de correos electrónicos a un gran número de objetivos potenciales donde se solicitan cierta información confidencial. También puede darse la solicitud de visitar un sitio web falso utilizando un hipervínculo que está incluido en el correo electrónico.

Water holing es una técnica con la que se crea un sitio web falso o comprometer un sitio web intentando imitar alguno que los atacantes usen con frecuencia. Por ejemplo, crear una copia de la web que usa una naviera para colocar las nóminas de los empleados).

Scanning o escaneo sirve para atacar grandes partes de internet al azar escaneándolas también se puede usar páginas web como https://www.shodan.io donde se puede buscar por modelos concretos de fabricantes de sistemas SCADA.

La segunda parte se encuentran los ataques dirigidos pueden ser más sofisticados y utilizar herramientas y técnicas creadas específicamente para la infraestructura informática de una empresa o buque.

La ingeniería social es técnica utilizada por posibles ciber atacantes para manipular individuos internos de la compañía para que rompan los procedimientos de seguridad, normalmente a través de interacción a través de las redes sociales.

Ataques de fuerza bruta son ataques de prueba de muchas contraseñas con el fin de encontrar una contraseña operativa. Los el atacante comprueba todas las combinaciones posibles hasta que se encuentre la correcta.

Denegación de servicio (DoS) es una técnica con la que se niega el acceso a los usuarios legítimos y autorizados a la información, para lo que se satura la red con datos.

Existe una variante que es la denegación de servicio distribuido (DDoS) funciona tomando el control de múltiples ordenadores y servidores para satura una red concreta.

Spear-phishing es similar al phishing, pero las personas que son objetivos de están técnicas reciben correos electrónicos diseñados especialmente para ellos, normalmente tienen software malicioso o enlaces de descarga automática de software malicioso.

Ataque a la cadena de suministro consiste en atacar a la empresa o barco comprometiendo sus equipos, software o servicios de apoyo que se encargan del suministro de los suministros.

Escalado de privilegios es un ataque con el cual el atacante obtiene acceso a los recursos que están protegidos en un ordenador o sistema por una contraseña o un usuario.

0-day son ataques a un dispositivo usando tecnología o métodos que no son conocidos por el fabricante del dispositivo.

Spoofing es una técnica con la que se suplanta a una persona o software copiado sus características o información.

Universidad del País Vasco Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

MÁSTER UNIVERSITARIO EN

NAUTICA Y TRANSPORTE MARITIMO

TRABAJO FIN DE MÁSTER

CIBERSEGURIDAD A BORDO DE BUQUES MERCANTES

DOCUMENTO 2- *METODOLOGIA SEGUIDA EN EL DESARROLLO DEL TRABAJO*

Alumno/Alumna: Blanco López Daniel

Director/Directora (1): Basterrechea Iribar Imanol

Curso: 2019-2020

Fecha: Bilbao, 14 de septiembre 2020

2.METODOLOGÍA SEGUIDA EN EL DESARROLLO DEL TRABAJO

DESCRIPCION DE LAS FASES

Este trabajo se ha desarrollado en dos fases principales durante las mismas se han seleccionado algunos de los equipos que son necesario para la operativa de los buques. La primera fase del trabajo ha consistido en explicar el funcionamiento técnico de cada equipo escogido.

La segunda fase se ha realizado estudiando individualmente los sistemas para localizar los fallos de seguridad que tenga debido a su diseño o funcionamiento y que puedan ser utilizados por un atacante. También se explica en varios sistemas algunas de las técnicas conocidas para infectar o modificar los parámetros de funcionamiento de estos equipos. Para cada equipo se ha intentado dar algunas recomendaciones de uso y control para minimizar los riesgos.

Durante el desarrollo de este se ha usado la información proveniente tanto de organizaciones internacionales como de los propios fabricantes de los sistemas. Para algunos ejemplos se ha optado por colocar imágenes para mejorar la compresión de algunos de los ataques.

DIAGRAMA DE GANTT

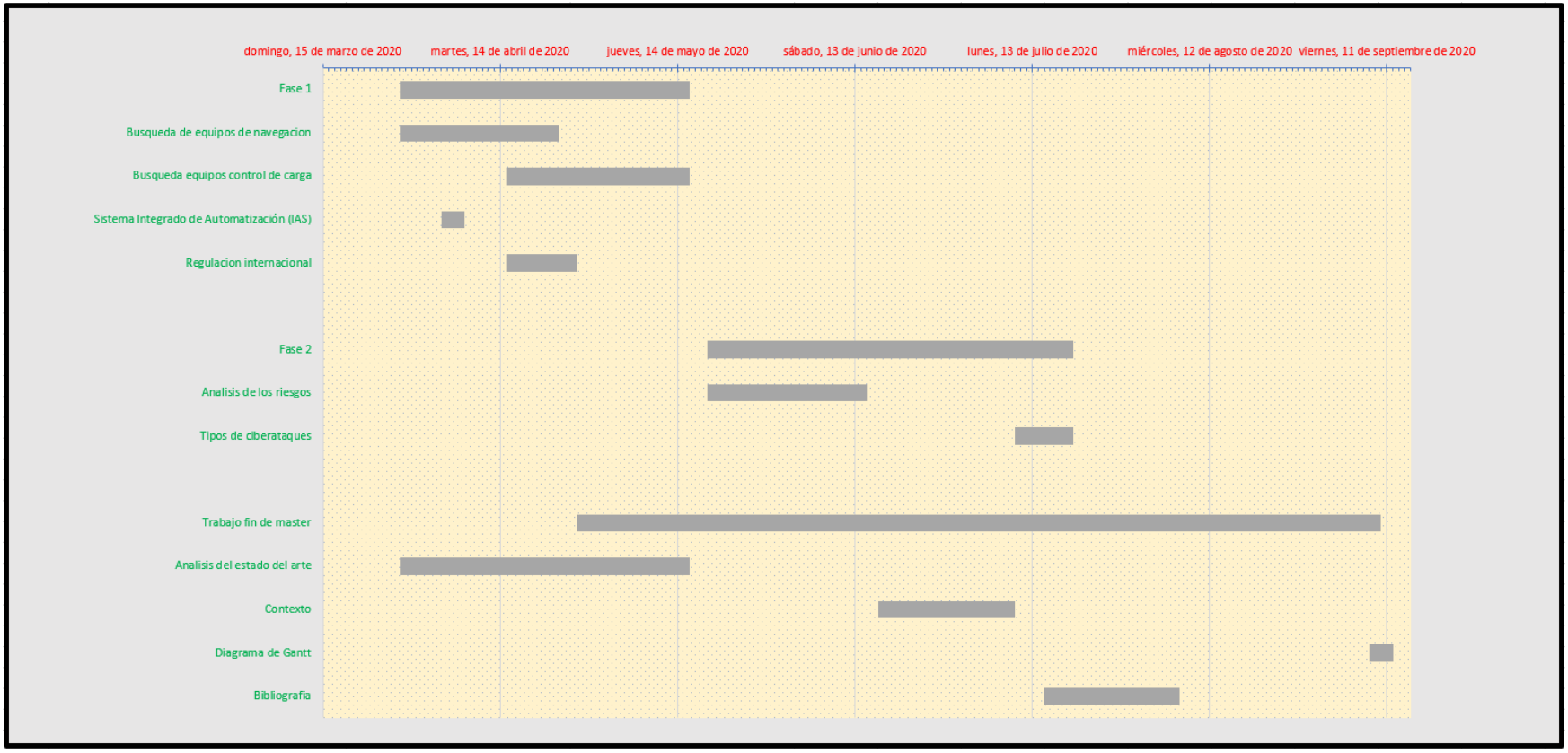

Imagen34. Diagrama de Gantt

DESCRIPCION DE LOS RESULTADOS

Durante este trabajo se ha comprobado que no hay ningún equipo o sistema que sea totalmente seguro frente a un ataque informático. Sin embargo, tomando medidas de prevención y manteniendo los equipos aislados de una conexión a internet se hace muy difícil poder atacar estos sistemas.

En los casos presentados donde se han realizado pruebas exitosas para penetrar en los sistemas del buque se debió a la infección con existo producida gracias al envió de un correo electrónico que contenía un malware el cual una vez infecto el ordenador consiguió transportarse a una memoria USB que el usuario conecto en el equipo ECDIS.

Actualmente los ataques informáticos van a venir principalmente por la conexión a internet siendo la manipulación física de los equipos de una gran dificultad por los protocoles actuales de seguridad que se siguen en puerto.

Para poder realizar algunos de estos ataques es necesario tener un gran conocimiento del mundo marítimo y la operativa de los buques por lo que algunos de los ataques explicados durante este trabajo pueden ser de gran dificultad poder llevarlos a cabo. Además, para la realización de alguno de los ataques es necesario uso de software y equipo concretamente diseñado para realizar ese ataque.

Universidad del País Vasco Euskal Herriko Unibertsitatea

BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

MÁSTER UNIVERSITARIO EN

NAUTICA Y TRANSPORTE MARITIMO

TRABAJO FIN DE MÁSTER

CIBERSEGURIDAD A BORDO DE BUQUES MERCANTES

DOCUMENTO 3- *CONCLUSIONES*

Alumno/Alumna: Blanco López Daniel

Director/Directora (1): Basterrechea Iribar Imanol

Curso: 2019-2020

Fecha: Bilbao, 14 de septiembre 2020

3.CONCLUSION

Actualmente ha habido un aumento significativo en el número de ataques informáticos que tenían como objetivo buques o industrias relacionadas con el sector marítimo. Las asociaciones internacionales junto con las empresas han comenzado a ejecutar protocolos de seguridad diseñados específicamente para evitar o mitigar los efectos que puedan sufrir al recibir un ataque informático.

Durante el desarrollo del trabajo se ha podido comprobar que dependiendo el tipo de equipo se puede atacar usando diferentes métodos. Teniendo en cuenta también la interconexión que existe entre algunos equipos que comparten información o trabajan juntos. Las conclusiones parciales para cada equipo se incluyen en la memoria.

Como trabajos futuros relacionados con la ciberseguridad el enfoque podría ser el estudio a detalle del software malicioso y explicaciones técnicas más detalladas sobre funcionamiento de los equipos y sus señales eléctricas.

Universidad del País Vasco Euskal Herriko Unibertsitatea

BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

MÁSTER UNIVERSITARIO EN

NAUTICA Y TRANSPORTE MARITIMO

TRABAJO FIN DE MÁSTER

CIBERSEGURIDAD A BORDO DE BUQUES MERCANTES

DOCUMENTO 4- *BIBLIOGRAFIA*

Alumno/Alumna: Blanco López Daniel

Director/Directora (1): Basterrechea Iribar Imanol

Curso: 2019-2020

Fecha: Bilbao, 14 de septiembre 2020

4.BIBLIOGRAFIA

[1] Imo.org. 2020. *International Maritime Organization*. [online] Available at: <http://www.imo.org> [Accessed 3 June 2020].

[1.1] *MSC.74(69)*.

[1.2] *A.1106(29).*

[1.3] *MSC.192(79).*

[2] Gard.no. 2020. *Gard.No - GARD*. [online] Available at: <http://www.gard.no> [Accessed 2 June 2020].

[3] Admiralty.co.uk. 2020. *ADMIRALTY Maritime Data Solutions*. [online] Available at: <https://www.admiralty.co.uk> [Accessed 2 May 2020].

[4] 2014. *Solas: Consolidated Edition 2014. Consolidated Tekst Of the International Convention of The Safety of Life at Sea 1974, And Its Protocol Of 1988 Articles, Annexes and Cerfiticates: Incorporating All Amendments in Effect From 1 July 2014*. London.

[5] 2011. *STCW Convention and STCW Code: Including 2010 Manila Amendments + Supplement April 2017*. London: IMO.

[6] n.d. BIMCO. *The Guidelines on Cyber Security Onboard Ships*. 3rd ed.

[7] Bole, A., Wall, A. and Norris, A., 2014. *Radar and ARPA Manual [Recurso Electrónico]*. Estados Unidos: Elsevier Ltda.

[7.1]1.2 Principles of range and bearing measurement

[7.2]1.2.3 Directional Transmission and Reception

[7.3]2.3.2 Choice of Frequency

[7.4]2.3.3.2 Pulse Repetition Frequency

[7.5]2.6.5 Radar Interference

[8] Navaldome.com. 2020. *Naval Dome | The Threat*. [online] Available at: <https://navaldome.com/threat.html> [Accessed 3 June 2020].

[9] Jeffrey, C., 2010. *An Introduction To GNSS*. Calgary: NovAtel.

[10] n.d. Deloitte, *Cyber Security in the shipping industry*

[11] Weintrit, A., 2009. *The Electronic Chart Display and Information System (ECDIS)*. Boca Raton [Fla.]: CRC Press.

[11.1]2.1. Characteristics of electronic chart systems and their different solutions

[11.2]8 Data Updating System

[12] Kongsberg.com. 2020. *KONGSBERG*. [online] Available at: <https://www.kongsberg.com> [Accessed 16 July 2020].

[13] Emerson.com. 2020. *Emerson Global | Emerson*. [online] Available at: <https://www.emerson.com> [Accessed 20 July 2020].

[14] Gmeng.com. 2020. *GME*. [online] Available at: <http://gmeng.com> [Accessed 22 August 2020].

[15] FleetMon.com. 2020. *Live AIS Vessel Tracker with Ship and Port Database*. [online] Available at: <https://www.fleetmon.com> [Accessed 11 September 2020].

[16] Furunousa.com. 2020. *Home*. [online] Available at: <https://www.furunousa.com> [Accessed 11 September 2020].

[17] n.d. *A Trend Micro Research Paper, A Security Evaluation of AIS*

[18] n.d. OCIMF, *Linked Ship Shore Emergency Shutdown Systems for Oil and Chemical Transfers*

[19] Irmome.com. 2020. *Marine and Boat Fenders | IRM Offshore and Marine Engineers*. [online] Available at: <https://www.irmome.com> [Accessed 11 September 2020].

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO