RECOMENDACIÓN IALA

R0129 (R-129)

VULNERABILIDADES DE GNSS Y MEDIDAS DE MITIGACIÓN

Edición 3.1

Diciembre 2012

urn:mrn:iala:pub:r0129sp

10, rue des Gaudines – 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01 – Fax +33 (0)1 34 51 82 05 – contact@iala-aism.org

www.iala-aism.org

International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

HISTORIAL DEL DOCUMENTO

Las revisiones a este Documento de la IALA deben anotarse en la tabla antes de la emisión de un documento revisado.

Date	Page / Section Revised	Requirement for Revision
Diciembre 2004	Ed.1	
Diciembre 2008	Ed2. Todo el documento	Introduccion de e-Navigation y eLoran
Septiembre 2012	Ed3. Todo el documento	Actualizado para reflejar los cambios en GNSS desde el borrador original.
Septiembre 2020	Ed 3.1 Correcciones editoriales	

DESCARGO DE RESPONSABILIDAD: Este documento es una traducción del original en inglés y es solo para fines informativos. En caso de discrepancia, prevalece el original en inglés. IALA no asume ninguna responsabilidad por errores, omisiones o ambigüedades en la traducción. Cualquier persona o entidad que confíe en el contenido traducido lo hace bajo su propio riesgo. IALA no será responsable de ninguna pérdida causada por la confianza en la precisión, fiabilidad u oportunidad de la información traducida.

EL CONSEJO

TOMANDO NOTA de la función de la IALA con respecto a la seguridad de la navegación, la eficiencia del transporte marítimo y la protección del medio ambiente;

TOMANDO NOTA TAMBIÉN que el Convenio SOLAS de la OMI obliga a las administraciones a proporcionar ayudas a la navegación según lo requiera el nivel de riesgo y la densidad del tráfico lo justifique, pero no especifica el tipo de sistemas que deben proporcionarse;

TOMANDO NOTA ADEMÁS de las resoluciones A.915 (22) de la OMI sobre política marítima para el futuro sistema mundial de navegación por satélite (GNSS), y A.953 (23) sobre el sistema mundial de radionavegación;

RECONOCIENDO la cade vez mayor dependencia de todas las clases de usuarios marítimos de los servicios GNSS y la vulnerabilidad de dichos servicios a la interferencia tanto intencionada como accidental;

RECONOCIENDO TAMBIÉN que GNSS es un elemento clave dentro de la navegación electrónica;

RECONOCIENDO ADEMÁS la existencia de ayudas a la navegación convencionales y VTS como sistemas alternativos terrestres, disponibles para todas las clases de usuarios marítimos;

HABIENDO CONSIDERADO las propuestas formuladas como resultado del estudio que figura en el Anexo a esta recomendación;

RECOMIENDA que:

1 Los Miembros Nacionales y otras Autoridades competentes tienen en cuenta la información del anexo y los demás estudios realizados sobre las opciones de sistemas alternativos

2 Los Miembros Nacionales y otras Autoridades competentes realizan evaluaciones de riesgo, en términos de las diversas etapas de un viaje relevantes a sus áreas geográficas de interés.

3 Los Miembros Nacionales y otras Autoridades competentes mantienen y mejoran el enlace y las asociaciones entre proveedores de GNSS.

4 Los Miembros Nacionales y otras Autoridades competentes monitorean las actividades paralelas sobre mitigación de la vulnerabilidad por parte de otros organismos y otros modos de transporte.

5 Los Miembros Nacionales y otras Autoridades competentes fomentan la transferencia de tecnología de mitigación del ejército para uso civil.

6 En cooperación con la industria, los Miembros Nacionales y otras Autoridades competentes apoyan el desarrollo de estándares mejorados de desempeño del receptor.

7 Los Miembros Nacionales y otras Autoridades competentes fomentan el uso de equipos receptores GNSS que cumplan con los últimos estándares de rendimiento.

8 Los Miembros Nacionales y otras Autoridades competentes sensibilizan a los usuarios sobre la vulnerabilidad del GNSS y la necesidad de mantener las habilidades en el uso de ayudas convencionales.

9 Los Miembros Nacionales y otras Autoridades competentes mantienen y desarrollan ayudas de respaldo y de contingencia a la navegación, que pueden incluir radio ayudas a la navegación y ayudas convencionales a la navegación, apropiadas al nivel de riesgo identificado.

ANEXO

A

LA RECOMENDACION R0129 (R-129)

EN

VULNERABILIDADES DE GNSS Y MEDIDAS DE MITIGACION

CONTENIDO DEL ANEXO

Contenidos

CONTENIDO DEL ANEXO

List of Tables

1 INTRODUCCION

En 2001, el Departamento de Transporte de EE. UU Volpe Center llevó a cabo un estudio de las vulnerabilidades a interferencias intencionales y no intencionales de la infraestructura de transporte de EE. UU que depende de las señales del Sistema de posicionamiento global (GPS) [1]. Se ha realizado un estudio similar para la Agencia de Radiocomunicaciones del Reino Unido [2]. También se han realizado estudios en Europa como preparación para el proyecto Galileo [3] y [4]. Un estudio reciente de la Royal Academy of Engineering ha investigado el nivel de dependencia y las vulnerabilidades de GNSS [5]. Estos estudios indican que los sistemas mundiales de navegación por satélite (GNSS) tienen vulnerabilidades a interferencias intencionales y no intencionales.

1.1 CONTEXTO

La estrategia de la OMI para la e-Navigation incluye la necesidad de usuario a alto nivel de integridad de los datos y del sistema estableciendo:

> *"Los sistemas de e-Navigation deben ser resilientes y tener en cuenta cuestiones de validez, plausibilidad e integridad de los datos para que el sistema sea robusto, fiable y seguro. Deben tenerse en cuenta los requisitos de redundancia, especialmente en relación con los sistemas de posicionamiento ".*

Al abordar el problema de posicionamiento, se puede definir como señales electrónicas de posición, navegación y sincronización precisas y confiables, con prestaciones a prueba de fallos (probablemente proporcionado a través de redundancia múltiple, por ejemplo, GNSS, transmisores diferenciales, eLoran y receptores predeterminados o dispositivos embarcados de navegación inercial).

La creciente dependencia de GNSS en todos los tipos de determinación de la posición y navegación, incluidos los datos de entrada relativos a posición y tiempo en los sistemas de identificación automática (AIS), subraya la importancia de considerar objetivamente las posibles áreas de vulnerabilidad y la importancia de medidas para reducir o mitigar tales efectos. La necesidad de medidas para contrarrestar la vulnerabilidad se ha vuelto particularmente importante con la eliminación gradual de otros sistemas y debe tenerse en cuenta en la formulación de planes de radionavegación. En el contexto de la aviación, [6] indica que el problema de la vulnerabilidad GNSS es gestionable mediante la conservación de sistemas terrestres existentes (VOR / DME, NDB) como respaldo (backups). Se entiende una consideración similar en el entorno marítimo.

1.2 ALCANCE

Este documento considera todos los tipos de vulnerabilidad de GNSS en el entorno marítimo y las medidas de mitigación que se pueden utilizar para superarlas.

El efecto sobre la navegación marítima de las interrupciones de GNSS será significativo. Cuando los fenómenos naturales, como la meteorología espacial, afecten a la recepción de la señal GNSS, es probable que los efectos se observen en áreas extensas y durante cualquier fase de la navegación. Es más probable que la interferencia provocada por el hombre se produzca dentro de las aguas costeras, ya que es probable que las fuentes de interferencia provocada por el hombre se encuentren en tierra y estén restringidas a la línea de visión. Sin embargo, no se puede descartar la posibilidad de una interferencia deliberada en el barco o en el aire.

Se considera buena práctica la utilización de todas las fuentes de posicionamiento disponibles.

2 DEFINICIONES & ACRONIMOS

Se utilizarán los siguientes acrónimos en el documento:

ASF	Additional Secondary Factors / Factores secundarios adicionales
dBW	decibels relative to One (1) Watt / decibelios por vatio

DME	Distance Measuring Equipment / Equipo de medición de distancia
ECDIS	Electronic Chart Display / Carta electronica
EGNOS	European Geostationary Navigation Overlay System / Sistema europeo de navegación por complemento geoestacionario
ENC	Electronic Navigational Chart / Carta de navegación electrónica
GLONASS	Global Navigation Satellite System / Sistema Global de Navegación Satelital
GMDSS	Global Maritime Distress and Safety System / Sistema mundial de socorro y seguridad marítimos
IEC	International Electro-technical Commission / Comisión Electrotécnica Internacional
IMO	International Maritime Organization / Organización Marítima Internacional
LBS	Location Based Services / Servicios Basados en la Localización
Loran	Long Range Navigation / Navegación de Larga Distancia
NDB	(Aeronautical) Non-Directional Beacon / Baliza no direccional
PNT	Position, Navigation & Timing / Posicionamiento, Navegación, Temporización
SOLAS	Safety of Life at Sea (Convention) / Convención de la Seguridad de la Vida en el Mar
UMTS	Universal Mobile Telecommunications System / Sistema universal de telecomunicaciones móviles
VOR	VHF Omnidirectional Ranging / Alcance Omnidireccional VHF
WAAS	Wide Area Augmentation System / Sistema de Aumentación Basado en Satélites

3 FUENTES DE VULNERABILIDAD

Algunos modos de fallo son comunes a todos los tipos de sistemas de navegación electrónicos. El sistema en sí puede fallar, por ejemplo, debido a daños deliberados o accidentales afectando a la infraestructura terrestre. Dada la naturaleza militar del actual GNSS - GPS y GLONASS, se puede suponer que los niveles de seguridad son altos y que se proporcionan equipos de reserva. La experiencia con el GPS lo confirma y se puede suponer que la avería del sistema es un evento muy raro. Las medidas de seguridad de Galileo son comparables a las del GPS, con la excepción de que los satélites no están reforzados para resistir los pulsos electromagnéticos de las explosiones nucleares. El fallo de los satélites GPS de forma individual no es inusual, aunque el tiempo medio de reparación es inferior a 48 horas.

GNSS es particularmente susceptible a interferencias accidentales o maliciosas debido al nivel extremadamente bajo de la señal en el receptor del usuario. Las fuentes no intencionales de interferencia o interrupción del servicio incluyen la variabilidad ionosférica, los efectos de la actividad solar y también señales fuertes, armónicos o generado por intermodulación de transmisores potentes que operan en otras bandas o proveniente de fuentes cercanas al receptor GNSS. Las causas intencionales de interferencia incluyen la radiación de señales de interferencia deliberadas de banda estrecha o banda ancha. El Informe Volpe también identifica como un peligro el spoofing “suplantación de identidad” en la que se irradia una señal GNSS falsa con la intención de engañar al usuario.

La avería de los equipos electrónicos a bordo de un barco también es frecuente, debido a un fallo en el suministro de energía o un fallo, temporal o permanente, en el receptor o la antena. Las medidas para contrarrestar estos problemas son las mismas que para otros sistemas a bordo: el uso de fuentes de alimentación de reserva (requeridas para embarcaciones SOLAS) y seguir las pautas de instalación y localización de fallos. Aunque el requisito de la OMI es para un solo sistema electrónico de posicionamiento, es bastante común que se instale más de un receptor para que ese sistema proporcione redundancia en caso de falla del equipo.

Un modo de fallo observado con menos frecuencia es la desactivación permanente o temporal de las antenas del receptor GNSS sometidas a transmisiones de radar de alta potencia, debido a daños por microondas o saturación de los componentes internos [7].

El uso generalizado de GNSS ha dado lugar a una tendencia a depender en gran medida de los sistemas electrónicos - navegación "con la vista hacia abajo" - con una reticencia percibida a utilizar medios alternativos para la verificación de la posición, como recomienda la OMI.

3.1 FUENTES DE INTERFERENCIA

La interferencia involuntaria puede provenir de fuentes naturales o artificiales.

La variabilidad ionosférica y los efectos de la actividad solar en los sistemas de radionavegación han sido objeto de investigación durante muchos años. La referencia [8] informa sobre el efecto del centelleo de las señales GPS. Los efectos de la variabilidad ionosférica repercute en el aumento de los errores en la posición y estos pueden exceder los límites establecidos en la Resolución pertinente de la OMI [9] e incluso pueden hacer que el receptor no compute las señales de los satélites. El sistema de integridad Galileo (y el futuro GPS) debería detectar grandes efectos de perturbación ionosférica y emitir alarmas.

Las fuentes de interferencia causadas por el hombre de forma no intencional en tierra pueden incluir transmisiones de televisión, comunicaciones por microondas, tanto enlaces fijos como enlaces de subida (uplinks) por satélite, y radares VTS. La interferencia de transmisiones de televisión y enlaces fijos de microondas puede ser especialmente grave, ya que podría afectar a todas los buques y embarcaciones dentro de un área significativa o en una vía fluvial en particular.

La interferencia de los equipos a bordo, como los enlaces ascendentes de satélite y los radares, pueden minimizarse mediante prácticas correctas en la instalació. Sin embargo, dicha interferencia puede originarse a bordo de otros buques próximos. En ese caso, se vuelve difícil o imposible hacer algo al respecto. Esto podría ser un serio problema en puertos y aproches portuarios.

Las frecuencias de INMARSAT están próximas a las de GNSS y las instalaciones de antenas GNSS deben tener en cuenta la variación de la elevación de la señal con la latitud cuando se utilizan antenas parabólicas orientables.

También se ha observado interferencias de equipos deficientemente diseñados, como antenas de TV activas en el propio barco u otros barcos en su proximidad [10].

Los planes de compatibilidad electromagnética son un requisito de la OMI para todos los sistemas de los buques SOLAS, pero la minuciosidad con la que se aplican puede variar ya que su implementación puede resultar costosa. La medición y el análisis de las fuentes de interferencia a bordo es un tema muy específico sobre el que hay escasez de conocimientos y formación. Las limitaciones de espacio en los mástiles a menudo dificultan la instalación de la antena ideal para cualquier sistema (no solo GNSS).

3.2 JAMMING & SPOOFING

El jamming (interferencia) de señales GNSS puede lograrse con bastante facilidad y utilizando equipos de coste relativamente bajo. Esto se debe a los niveles de potencia extremadamente bajos de las señales en la superficie terrestre (mínimo -160 dBW para GPS, -154 dBW para Galileo). Las señales de amplio espectro como las del GPS son menos vulnerables a un jammer de frecuencia fija que a uno de banda ancha. Dado que todos los satélites GPS transmiten en una frecuencia, un solo jammer normalmente elimina todos los satélites. Los sistemas de división de frecuencia como GLONASS podrían, en teoría, seguir dando un servicio cuando un jammer de banda estrecha elimina las señales de uno o dos satélites. Por otro lado, es fácil diseñar un jammer que transmita en varias frecuencias simultáneamente, considerando los bajos niveles de potencia requeridos para un bloqueo eficiente. Galileo tendrá la ventaja de disponer de más tiempo para el desarrollo de contramedidas y un equipo de seguridad supervisará asuntos como la interrupción en tiempo de guerra.

El spoofing (suplantación de identidad) es más difícil de lograr, ya que es necesario simular las señales para que el receptor compute las señales falsas. Sin embargo, los simuladores de señales GPS son elementos fácilmente disponibles en los equipos industriales de testeo. Además, las consecuencias del spoofing son mucho más graves que las de la interferencia. Si las señales falsas son indistinguibles de las reales y dan una posición lo suficientemente cercana como para ser creíble, entonces el usuario puede no darse cuenta del

engaño y podría ser llevado a situaciones de peligro. Un servicio de autenticación, como el propuesto para Galileo, podría ser una medida eficaz contra el spoofing.

Dadas las respectivas dificultades de jamming y spoofing, es más probable que se produzcan jamming. Se han registrado eventos de jamming por parte de las autoridades militares. El mundo marítimo es muy vulnerable a dichos eventos en los equipos de navegación, AIS y GMDSS. La provisión de servicios AtoN puede verse afectada con respecto a las luces sincronizadas por DGNSS, VTS y GNSS [11]. Además, se espera que la implementación de e-Navigation resulte en una mayor dependencia de los sistemas de comunicaciones dependientes de la sincronización, pudiendo utilizar GNSS como fuente.

El jamming malicioso de GNSS puede considerarse análogo a atacar ordenadores con un virus, y es probable que atraiga a los mismos tipos de ciber delincuentes. Muchas páginas web proveen detalles sobre cómo lograrlo. El tipo de área que podría verse afectada con un jamming básico no sería un enfoque de puerto único. El servicio GNSS podría interrumpirse en toda una zona de alta densidad de tráfico como el Estrecho de Dover o el Estrecho de Malaca.

Las contramedidas de jamming ya están disponibles en forma de antenas direccionales y filtros sintonizables en receptores militares. La interferencia se volverá más difícil a medida que haya más frecuencias disponibles, pero aún será posible. Los niveles de potencia ligeramente más altos de Galileo y GPS III reducirán la vulnerabilidad así como la combinación de múltiples GNSS será preferible antes que un único sistema. Sin embargo, no se puede eliminar la susceptibilidad al jamming.

Una consideración importante es la duración del evento de jamming. Las consecuencias de breves interrupciones son claramente menos graves que una prolongada indisponibilidad del servicio. Las medidas para hacer frente a las interferencias también dependerían de su duración. Proporcionar personal técnico para localizar a los jammers estaría justificado y sería efectivo si se esperaran largos períodos de bloqueos, pero podría ser ineficaz contra los bloqueos de puntual o inesperado . De hecho, muchos países ya tienen equipos y recursos asignados para hacer frente al jamming y las interferencias. Es importante que sean conscientes de la amenaza a los servicios de la seguridad de la vida que representa la posible interrupción del GNSS.

3.3 ANÁLISIS DE RIESGO

Resulta complejo analizar el riesgo debido a la interrupción de GNSS. El usuario puede tener consciencia de que la señal se ha perdido por un período y luego ha regresado, pero no tiene forma de saber la causa, ya sea una interferencia externa o interna, accidental o intencional.

Las consecuencias para las aplicaciones de navegación pueden variar desde la pérdida completa de señal, información de posición falsa o pérdida intermitente hasta la degradación de la precisión. Las consecuencias de las aplicaciones de sincronización pueden incluir fallos debido a la pérdida de sincronización.

La Tabla 1 ofrece evaluaciones subjetivas de los diferentes riesgos en términos de su probabilidad percibida de ocurrencia, consecuencias y dificultad y costo de mitigación. Se enfatiza que se trata de juicios subjetivos, basados en opiniones de expertos. Si es posible, debe realizarse un análisis cuantitativo de riesgos.

Table 1 Evaluación de riesgo

Evento	Probabilidad de ocurrencia	Consecuencias	Dificultad / coste de mitigación
Fallo de servicio GNSS	B	A	A
Fallo de alimentación	M	A	B
Fallo de receptor / antena	M	A	B
Interferencia propia	M	M	B
Interferencia externa	B	A	M
Ionosférico	B	M	M

Jamming	B	A	M
Spoofing	B	A*	A
Malfuncionamiento de receptor radar	B	A	B

A = Alto. Alta probabilidad significa que es probable que suceda más de una vez al año. Consecuencia alta significa pérdida total del uso del sistema. La alta dificultad o coste de la mitigación significa que es poco probable que se logre.

M = Medio. Probabilidad media significa que es probable que tenga lugar menos de una vez al año. Consecuencia media significa que el sistema aún se puede utilizar, pero está degradado. Dificultad o coste medio significa alcanzable a un coste significativo.

B = Bajo. Probabilidad baja significa que es poco probable que ocurra. La baja dificultad o coste significa que se debe lograr la mitigación.

* anote que el spoofing se considera como de impacto más grave (consulte la sección 3.2).

3.4 MITIGACIÓN

Este análisis de riesgo subjetivo ayuda a identificar las amenazas que debe abordar el usuario, particularmente aquellas con alta probabilidad, altas consecuencias y bajo coste de mitigación. El uso de equipos receptores GNSS que cumplan con los últimos estándares de rendimiento reducirá significativamente la susceptibilidad a las interferencias.

El conocimiento del problema y los cambios en el diseño de los sistemas futuros, como una mayor potencia radiada, una mayor sofisticación del receptor y frecuencias operativas adicionales, pueden servir para mitigar el impacto de algunas de las amenazas hasta cierto punto. Sin embargo, la vulnerabilidad del sistema, particularmente a un ataque deliberado, no se puede eliminar por completo. Este mensaje fue claro y se repitió varias veces en el Informe Volpe. La modificación de los sistemas actuales puede reducir el efecto de fuentes de ruido e interferencia naturales e inadvertidas. Los intentos calculados de jammear o denegar a los usuarios los servicios de posicionamiento y temporización de GNSS serán mucho más difíciles de anticipar y combatir. Por tanto, es esencial mantener y desarrollar sistemas alternativos adecuados.

Mediante el uso de un enfoque de PNT integrado como parte del INS, es posible indicar al navegante el nivel de prestaciones disponible (es decir, precisión, integridad, continuidad, etc.). Si los medios primarios y redundantes de PNT no estuvieran disponibles, el sistema podría indicar si los requisitos primarios o de backup son aptos para la navegación.

3.5 SISTEMAS ALTERNATIVOS

Pueden proporcionarse medios alternativos de navegación en varios niveles; Totalmente redundante, respaldo (backup) y contingencia[1].

- Un sistema **redundante** proporciona la misma funcionalidad que el sistema principal, lo que permite una transición sin problemas y sin cambios en los procedimientos.
- Un sistema de **backup** asegura la continuidad de la navegación, pero no necesariamente con la funcionalidad completa del sistema primario y puede requerir algún cambio en los procedimientos por parte del usuario.
- Un sistema de **contingencia** permite completar una maniobra de manera segura, pero puede no ser adecuado para su uso prolongado.

1 Según se define en varios estudios realizados por Booz-Allen & Hamilton en nombre de la Administración Federal de Aviación de EE. UU.

3.5.1 Sistema redundante

Los sistemas completamente redundantes deben proporcionar niveles de rendimiento equivalentes en términos de precisión, integridad, disponibilidad y continuidad de posicionamiento y sincronización. GLONASS representa un posible sistema redundante para GPS, con sistemas adicionales como BEIDOU y Galileo que entrarán en pleno funcionamiento en 2020.

También debe tenerse en cuenta que estos sistemas similares pueden tener modos de fallo comunes. Por ejemplo, una fuente de interferencia o jamming podría denegar múltiples servicios GNSS, ya que es muy probable que los dos sistemas utilicen las mismas bandas de frecuencia. También se espera que la mayoría de los receptores empleen ambos sistemas; por tanto, un ataque a uno puede afectar a ambos. Se están desarrollando contramedidas contra el jamming y la interferencia y es probable que sean bastante efectivas cuando Galileo y las generaciones posteriores de GPS entren en funcionamiento.

3.5.2 Sistemas backup

Los sistemas de respaldo pueden incluir sistemas terrestres existentes o planificados, como los siguientes:

- Loran C;
- Enhanced Loran (eLoran);
- Radar y ayudas radar para la navegación;
- Sistemas basados en telefonía móvil;
- Ranging de DGNSS/AIS (R-Mode)[2].

Loran es el único candidato existente como alternativa de radionavegación terrestre y proporciona una sentencia de posición utilizable con cartografía electrónica y otros sistemas a bordo. Loran proporciona posición, navegación y sincronización independientes con modos de fallo diferentes a los de GNSS, sin embargo, la cobertura es limitada. Por ejemplo, en aguas europeas está restringido actualmente a la parte noroeste, mientras que en América del Norte se tomó la decisión de desconectar el servicio en 2010. Los receptores Loran no son de equipamiento e instalación a bordo obligatorio y muy pocos barcos fuera de las aguas norteamericanas los transportan.

eLoran ha demostrado una precisión comparable a GNSS [12]. Para que eLoran se convierta en un sistema redundante o de backup eficaz, es necesario integrar los receptores en los puentes de navegación y hay poca motivación para la instalación voluntaria de receptores como backup siempre que GNSS continúe funcionando bien.

Aunque los receptores para Loran no son un requisito de instalación específico, estarían cubiertos por el requisito del Capítulo V de SOLAS para un Sistema Electrónico de Posicionamiento, adecuado para todo el viaje, en el caso de tráfico regional. Los test de especificaciones actuales de IEC para la aprobación de los receptores Loran se basa en tecnología desactualizada y es posible que deba revisarse.

Loran también tiene vulnerabilidades a fallos de equipos o fuentes de alimentación a bordo, daños a la infraestructura terrestre, pérdida de sincronización debido a la interrupción de los sistemas de comunicación e interferencia por efectos ionosféricos o líneas eléctricas, que pueden transportar señales de datos tanto de corriente alterna de baja frecuencia como de frecuencia más alta. .

El radar se puede utilizar para fijar la posición, pero generalmente no proporciona una entrada compatible a un sistema de cartografía electrónica; por lo tanto, son necesarios diferentes procedimientos para su uso. Sin embargo, la instalación del radar es un requisito necesario en los buques SOLAS y las técnicas de comparación de imágenes radar (referencia de radar) están bien desarrolladas y se utilizan en aguas como los archipiélagos entre Suecia y Finlandia. La limitación más importante del radar como backup se encuentra en zonas costeras de bajo relieve y sin rasgos distintivos, por ejemplo, en Europa, las áreas del norte de

2 During the e-Navigation test bed project ACCSEAS, tests concerning the R-Mode (DGPS/AIS) as an alternative back-up system will be carried out in the North Sea Region. The results of those tests can be expected in early 2015.

Francia, Bélgica y los Países Bajos o la costa este de Inglaterra. Para que el radar sea un equipo de backup universal, tales áreas deberían estar marcadas con suficientes ayudas radar a la navegación.

Este sistema no proporcionaría el mismo nivel de servicio de posicionamiento que Loran, ni una referencia de tiempo alternativa. Sin embargo, dicha opción podría justificar una mayor investigación en regiones donde Loran no es una opción realista. Los radares y las balizas de radar también tienen vulnerabilidades a fallos de equipos o fuentes de alimentación, multipath, lluvia y ecos de mar y efectos de ocultación.

Otro posible backup en el futuro puede ser el posicionamiento mediante el Sistema Universal de Telecomunicaciones Móviles (UMTS). Este es el sistema celular de tercera generación y las primeras redes entraron en funcionamiento en 2002. Una de las principales características de los móviles 3G serán los servicios basados en la ubicación (LBS) en los que la ubicación del usuario se logrará mediante GNSS (vulnerable al mismo fallo como el receptor GNSS del barco) o por sistemas que emplean las propias estaciones base celulares. Dichos sistemas incluyen identificación de celda (cell ID) y triangulación de señales en múltiples estaciones base. Es probable que el despliegue de tales redes comience en las áreas más densamente pobladas y es poco probable que la cobertura de las costas sea una prioridad; sin embargo, es posible utilizar varias técnicas de estaciones base a modo de backup en algunas áreas, como los estuarios. El uso de estos sistemas como alternativa viable aún está por demostrar; la precisión no sería tan alta como con GNSS y es poco probable que dicho equipo sea homologado para su uso en buques SOLAS. Es probable que estos sistemas dependan cada vez más de GNSS para su temporización y sincronización, por lo que podrían verse afectados por cualquier indisponibilidad de GNSS. Las señales de telefonía móvil, radio y televisión también podrían utilizarse dentro de un enfoque de Señales de Oportunidad, en el que las señales proporcionadas para usos alternativos se utilizan para la determinación de distancias. Si bien este enfoque tiene ventajas, es poco probable que se logre el nivel de integridad del servicio requerido para las aplicaciones de navegación, ya que las señales se proporcionan para un propósito diferente y, por lo tanto, pueden alterarse o cesar sin previo aviso.

Otro posible sistema backup futuro es el uso de señales de localización de la infraestructura DGNSS o AIS existente (R-Mode) [13]. Ambos sistemas tienen una disposición generalizada y ya existen estándares marítimos para los equipos a bordo. La nueva funcionalidad del R-Mode es el suministro de información de tiempo desde la costa hasta el barco. El receptor de radio a bordo puede entonces calcular una distancia (alcance) al transmisor. Utilizando varios de estos cálculos de una serie de transmisiones diferentes, el equipo de a bordo puede calcular la posición del barco. Sería necesario investigar las cuestiones de cobertura, geometría e interferencia.

3.5.3 Sistema de contingencia

El sistema de contingencia más obvio, que permite la realización segura de una maniobra, es el sistema de luces y boyas que ya se proporciona en la mayor parte del mundo. Las ayudas visuales tienen dos funciones específicas, advertencia de peligro y fijación de posición. No se despliegan necesariamente de tal manera que permitan una navegación continua, excepto en el caso de los marcadores de canal. Los niveles de precisión dependen de la posición relativa de las ayudas visuales y del alcance de su movimiento en el caso de marcas flotantes, pero se puede esperar que la precisión sea considerablemente inferior a la proporcionada por GNSS. Las ayudas a la navegación visuales (y de radar) proporcionan una alternativa esencial al GNSS, aunque se acepta que ahora son un medio secundario de verificación de la posición relativa. También forman una función de seguridad esencial al marcar físicamente los peligros y al permitir al navegante desarrollar una conciencia espacial y ambiental crítica. Estas funciones deben tenerse en cuenta cuando los usuarios y proveedores de servicios evalúan la necesidad continua de ayudas visuales. Se considera esencial que se mantengan las habilidades en el uso de ayudas convencionales a la navegación. Las luces y boyas tienen visibilidad limitada y lograr altos niveles de confiabilidad representa una carga de mantenimiento significativa. En condiciones de poca visibilidad y en ausencia de Loran o radar, se necesitaría otro sistema.

Un futuro sistema de contingencia podría ser el sistema de navegación inercial. Anteriormente, estas instalaciones eran demasiado caras para embarcaciones no militares, pero ahora están disponibles dispositivos de menor coste con un rendimiento aceptable a corto plazo. Integrado con un receptor GNSS, un sistema de navegación inercial podría proporcionar continuidad de servicio a las cartas electrónicas y los

pilotos automáticos, pero solo durante un período limitado por la velocidad de deriva. Sería muy importante que el usuario conociera las diferencias entre de los datos de entrada de posición GNSS a los de un sistema de navegación inercial y la consiguiente degradación de las prestaciones en cuanto a la precisión de la posición.

La navegación a estima es un método de navegación de contingencia. Se basa en el uso de instrumentos a bordo, principalmente la brújula y el registro, para estimar la velocidad, el rumbo y, por tanto, la posición. La precisión depende de la calidad de la última corrección y se degrada con el tiempo a un ritmo que depende de la precisión del equipo y de las condiciones meteorológicas y del mar.

Otros instrumentos a bordo pueden contribuir a la determinación de la posición, en particular la sonda de profundidad, que es un equipo obligatorio en los buques SOLAS y muy ampliamente transportado por embarcaciones no SOLAS.

El uso de la intervención manual requeriría alarmas adecuadas y las habilidades y experiencia necesarias. Estas habilidades deben incluir capacitación y experiencia para superar la dependencia del sistema primario de otros equipos del puente de navegación.

Cuando se utilizan sistemas electrónicos para contingencias, es probable que los requisitos de rendimiento se encuentren entre los requisitos primarios y de backup; sin embargo, en el caso de los sistemas inerciales o la navegación a estima, solo pueden ser fiables durante un corto período de tiempo debido a la deriva.

El tiempo que un sistema de contingencia sigue siendo adecuado para su uso dependerá de:

- la aplicación de navegación que se está ejecutando;
- las condiciones climáticas;
- el riesgo de colisión o encallamiento (según la situación del tráfico y las restricciones de ubicación);
- el equipamiento del buque.

3.5.4 Sistemas dependientes

Además de proporcionar los datos de navegación primarios, el GNSS en un puente de navegación moderno proporciona entradas de posición, navegación y sincronización a otros sistemas, incluidos AIS, ECDIS y GMDSS. La pérdida de GNSS inutilizaría el AIS para el posicionamiento, sin embargo, no debería inutilizar un ECDIS, ya que debería ser posible introducir marcaciones visuales o de radar. Sería necesario introducir manualmente la posición para el GMDSS. Los sistemas de contingencia no serían de utilidad en este caso: solo un sistema de navegación por satélite similar como Galileo o un sistema de backup compatible como Loran podría proporcionar una entrada de posición directa. Esto se convertirá en un problema cada vez mayor a medida que aumente la dependencia de estos sistemas. AIS se considera una ayuda para la protección (security) además de la seguridad (safety) y, en ese papel, el incentivo para bloquear el sistema que proporciona los datos de posición puede ser mucho mayor.

Las vulnerabilidades de GNSS también se extienden la provisión de AtoN con respecto a las luces sincronizadas por medio de DGNSS, VTS y GNSS. Además, se espera que la implementación de la navegación electrónica dé como resultado una mayor dependencia de los sistemas de comunicaciones a la sincronización basada en GNSS.

3.5.5 Sistemas de integridad

Se proporcionan varios sistemas para monitorear la integridad del GNSS, por ejemplo, el servicio de balizas IALA de GNSS diferencial, que está estandarizado para uso marítimo. Los sistemas de aumentación basados en satélites, como WAAS y EGNOS, llevan mensajes de integridad y el eLoran (enhanced Loran) como Eurofix también realizan esta función, pero no están aprobadas internacionalmente para uso marítimo. Los sistemas de información sobre seguridad marítima para la navegación, como Navtex y Safetynet, también pueden proporcionar alarmas de integridad, pero puede haber demoras en la entrega de dichas mensajes mediante estos sistemas. Cabe señalar que los sistemas de aumentación limentación dependen de GNSS para la indicación de posición y no son servicios autónomos. Por lo tanto, están sujetos a interferencias, jamming y

spoofing de GNSS, pero pueden proporcionar una alarma de mal funcionamiento o degradación de las prestaciones. Los receptores GNSS modernos incorporan la supervisión autónoma de la integridad del receptor (RAIM), que puede proporcionar una alarma de mal funcionamiento.

Puede ser factible utilizar AIS para monitorear anomalías de GNSS analizando los informes de posición y comparándolos con informes anteriores y / u otras fuentes de datos como VTS.

4 PLAN DE ACCION

Para responder a estas inquietudes, se proporciona un plan de acción que incluye la realización de una Evaluación de Riesgos para identificar los requisitos de un sistema backup de navegación y la arquitectura del receptor del usuario que se necesitaría proporcionar.

4.1 EVALUACIÓN DE RIESGO

Las autoridades de ayudas a la navegación deben realizar una evaluación de los riesgos para el tráfico dentro de las áreas de interés. El tipo y nivel de los sistemas de ayuda a la navegación (AtoN) requeridos deben estar determinados por los niveles de riesgo y dependencia de GNSS. Cualquier sistema o procedimiento que se implemente debe considerarse acorde con las diversas etapas de un viaje, es decir, oceánicas, costera, aproches a puerto y aguas restringidas, puerto, vías navegables interiores. Por ejemplo, en el medio del Océano Pacífico, una alternativa adecuada podría consistir en navegación astronómica, navegación a estima y estimación de la posición. El sistema alternativo requerido en áreas críticas como el Estrecho de Dover o el Estrecho de Malaca debe ser significativamente más robusto, ya que muchas embarcaciones pueden estar utilizando sistemas integrados de navegación en las proximidades.

Al evaluar la necesidad de un sistema alternativo, la transición de GNSS a sistemas alternativos también debe considerarse desde un punto de vista práctico y de vigilancia. Las AtoN visuales proporcionan una "verificación de la realidad", sin embargo, la integración de la posición verificad en los sistemas electrónicos existentes no siempre es sencilla e inevitablemente dependerá de una buena formación continua y conocimiento de la situación por parte de los navegantes.

Debe reconocerse que una pérdida de las capacidades operativas actualmente disponibles de GNSS es aceptable siempre que la seguridad del barco no se vea comprometida.

4.2 REQUISITOS PARA UN SISTEMA BACKUP DE NAVEGACIÓN

Cuando la evaluación de riesgos concluya que es necesario un sistema de backup (es decir, un sistema que garantice el funcionamiento continuo, pero no necesariamente con la funcionalidad completa del sistema primario), se sugieren requisitos mínimos para los usuarios marítimos (derivados de la Resolución A.915 (22) de la OMI), se enumeran en el Apéndice 1 los requisitos de prestaciones de dichos sistemas. Sin embargo, puede ser poco práctico esperar que los sistemas de backup logren algunos de estos estándares, como la cobertura global en la fase oceánica de la navegación o la precisión por debajo de un metro en la fase portuaria. En estos casos, podría ser necesario navegar por la fase oceánica a estima o retrasar las maniobras del puerto hasta que se restablezca el sistema de navegación principal. El argumento a favor de un sistema de backup puede depender de la amenaza percibida para el sistema principal y la duración probable de las interrupciones del sistema principal.

4.3 SISTEMA DE ALERTAS DE GNSS

Los proveedores de servicios deben considerar el uso de información de integridad al realizar su evaluación de riesgos. La información sobre integridad se puede proporcionar a través de diferentes medios.

Un fallo de GNSS puede ser de tal naturaleza que el marino lo perciba instantáneamente. Sin embargo, los sistemas a bordo como un sistema integrado de navegación o el uso de RAIM, GBAS o SBAS pueden proporcionar alarmas de integridad.

Los proveedores de servicios que operan la infraestructura IALA-DGPS ya proveen integridad al marino. IALA y otras organizaciones relevantes han mantenido recomendaciones apropiadas para el sistema [14].

4.4 ARQUITECTURA DEL RECEPTOR DE USUARIO

Se considera que existe un equipo de backup apropiado cuando equipos de distintas características (multimodales) integran sus datos en un interfaz común de salida. Dicho sistema presenta ventajas respecto al análisis de interferencias sobre el equipo primario, seleccionando la última traza fiable como origen para el equipo de backup.

Al igual que con los sistemas de navegación primarios existentes, se considera esencial que el usuario sea notificado del estado de los sistemas de navegación tanto primario como de backup por medio de alarmas y mensajes visuales y sonoros entendibles.

Los datos de salida de un sistema de navegación de backup debe estar en un formato electrónico reconocido (es decir, IEC 61162) como datos de entrada en las pantallas de las cartas electrónicas y GMDSS.

5 CONCLUSIONES

Las siguientes conclusiones fueron identificadas a través de estudios realizados sobre Vulnerabilidad GNSS:

1 Es necesario un análisis de riesgo completo para determinar la probabilidad de pérdida o degradación de la señal GNSS, la duración esperada y el área afectada.

2 Una mayor dependencia a GNSS aumentará las consecuencias de su indisponibilidad o degradación.

3 Se espera que los desarrollos actuales de GNSS proporcionen un sistema PNT completamente redundante.

4 Se espera que los futuros GNSS tengan vulnerabilidades similares a las identificadas actualmente para el GPS.

5 La vulnerabilidad del futuro GNSS se reducirá mediante señales (frecuencias) adicionales y mayores potencias de transmisión.

6 eLoran podría considerarse un sistema backup eficaz, pero tiene sus propias vulnerabilidades y la cobertura y la integración a bordo de equipos receptores son limitados.

7 El radar puede proveer un sistema de backup a GNSS limitado, pero no cumple con todos los requisitos de PNT.

8 Los sistemas inerciales de bajo coste pueden proporcionar un sistema de backup a bordo en el futuro.

9 El sistema R-Mode implementado dentro de DGNSS y / o AIS puede proporcionar un sistema de backup en el futuro.

10 Las AtoN visuales y de otro tipo, incluido VTS, son esenciales para complementar GNSS para usuarios marinos.

11 En condiciones de escasa visibilidad, el radar y la navegación a estima son las alternativas actuales, ambas tienen limitaciones.

12 Teniendo en cuenta los resultados de la evaluación de riesgos indicados en (1), puede ser necesario sistema de backup eficaz y compatible con GNSS para dar soporte a los sistemas dependientes (AIS, ECDIS).

6 REFERENCIAS

[1] John A. Volpe National Transportation Systems Center, Vulnerability assessment of the Transportation Infrastructure relying on the Global Positioning System. Final report, August 2001.

[2] S.J.Harding, Study into the impact on capability of UK Commercial and Domestic Services Resulting from the loss of GPS Signals. Qinetiq Report for the UK Radiocommunications Agency, 2001.

[3] GNSS 2 High Level Group 3 on Security and Defence issues, 1999.

[4] The Galileo System Security Board (GSSB) – Galileo Threats and Vulnerabilities, 2001.

[5] Global Navigation Space Systems: reliance and vulnerabilities, The Royal Academy of Engineering, ISBN 1-903496-62-4, March 2011.

[6] ICAO. Draft 11th ANC Secretariat Paper. Task 3. Mitigation of GNSS Vulnerabilities, Oct. 2002.

[7] S.Williams. Commercial GPS Susceptibility. RTCM 2004 Annual Assembly Proceedings.

[8] P.H. Doherty et al. ION GPS-2000, Sept. 2000, p. 662.

[9] International Maritime Organization (IMO), 2003. World-Wide Radionavigation System Resolution A.953(23).

[10] J.R. Clynch, A.A. Parker, R.W. Adler, W.R. Vincent, P. McGill, G. Badger. GPS World, January 2003. The Hunt for RFI – Unjamming a Coast Harbor.

[11] A.Grant, P.Williams, N.Ward & S.Basker, GPS Jamming and the Impact on Marine Navigation. GNSS Vulnerabilities and Solutions Conference, Royal Institute of Navigation. September 2008.

[12] eLoran. Securing Positioning, Navigation and Timing for Europe's Future. European eLoran Forum. April 2008.

[13] German Federal Waterways and Shipping Administration. Contribution to the IALA World Wide Radio Navigation plan, IALA eNAV 4, February 2008.

[14] IALA, Recommendation R0121 (R-121), "The Performance and Monitoring of DGNSS Services in the Frequency Band 283.5 – 325 kHz", Edition 1, 2004.

APPENDIX 1 REQUISITOS MÍNIMOS SUGERIDOS PARA EL USUARIO MARÍTIMO RESPECTO A NAVEGACIÓN GENERAL - SISTEMA DE BACKUP

Table 2 Requisitos mínimos sugeridos para los usuarios marítimos respecto a una navegación general – sistema de backup

	Parámetros a nivel de sistema				Parámetros a nivel de servicio			
	Precisión absoluta	Integridad			Disponibilidad % por 30 días	Continuidad % superior 15 minutes[3]	Cobertura	Intervalo definido (segundos)
	Horizontal (metros)	Límite de alerta (metres)	Tiempo para el disparo de la alarma[2] (segundos)	Riesgo de integridad (por 3 horas)				
Oceánicas	1000	2500	60	10^{-4}	99	N/A[2]	Global	60
Costeras	100	250	30	10^{-4}	99	N/A[2]	Regional	15
Aproches portuarios y aguas restringidas	10	25	10	10^{-4}	99	99.97	Regional	2
Portuarias	1	2.5	10	10^{-4}	99	99.97	Local	1
Vías navegables interiores	10	25	10	10^{-4}	99	99.97	Regional	2

Notes:

1. Tabla obtenida de la Resolución de la OMI A.915(22).
2. La continuidad no es relevante para la navegación costera y oceánica
3. La Resolución A.1046 (27) de la OMI modificó el intervalo de tiempo de continuidad a 15 minutos, en lugar de 3 horas como se requería originalmente en la Resolución A.915 (22) de la OMI.
4. Esta tabla debe leerse junto con los párrafos 2.1 y 2.2. Aunque estos son requisitos mínimos sugeridos, una evaluación de riesgos incluirá muchas variables que pueden alterar los requisitos mínimos. Consulte la Directriz de la IALA sobre la provisión de ayudas a la navegación para diferentes clases de embarcaciones, incluidas los buques de alta velocidad, diciembre de 2003 para obtener más detalles de las variables que acompañan las diferentes vías fluviales, embarcaciones y entornos