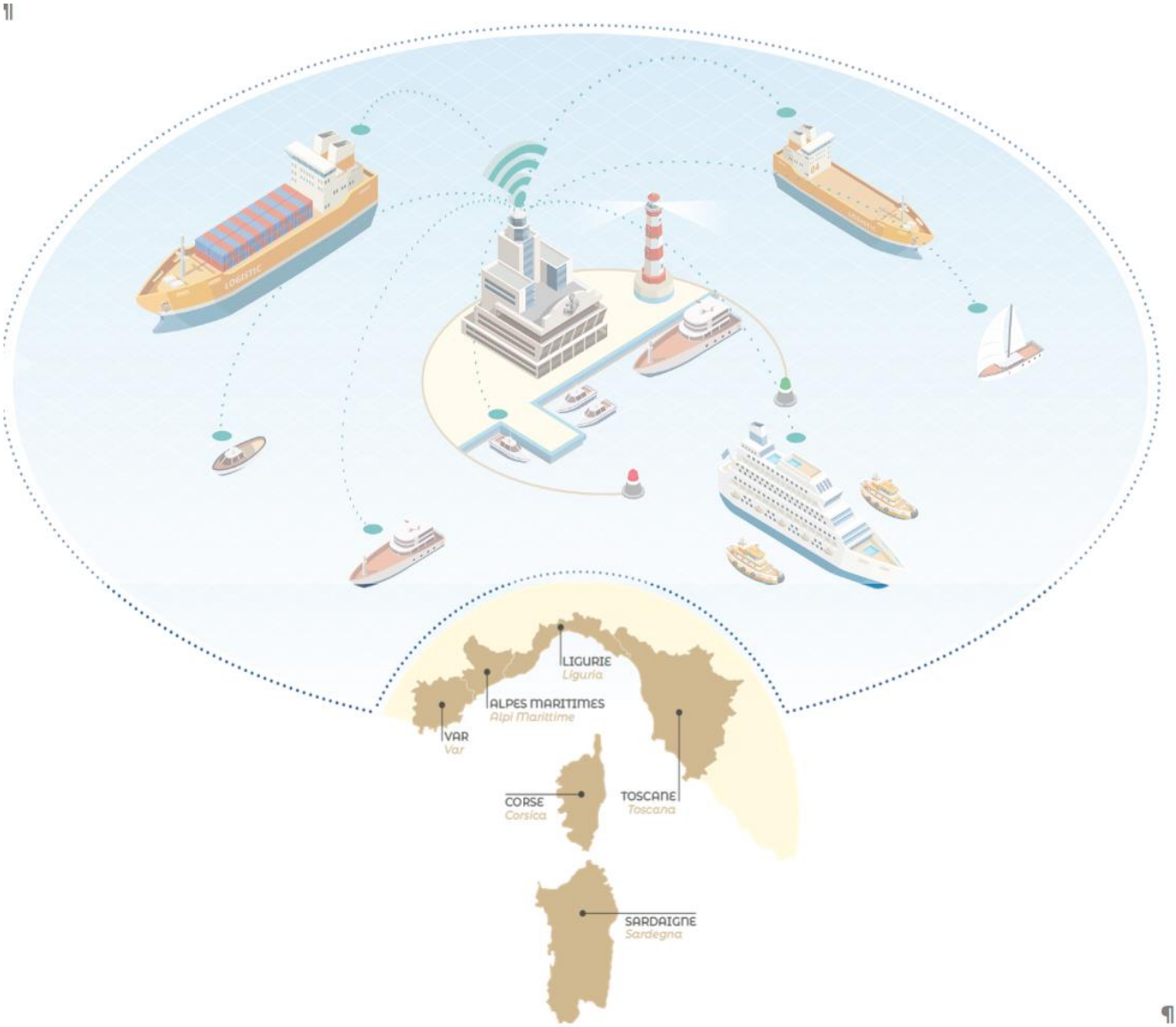
LIVRABLE T 1.1.3 - ISIDE

RECENSEMENT DES INSTRUMENTS DE COMMUNICATION ACTUELLEMENT EN SERVICE



N° G3S PELAGOS/2020/04/004 du 14 avril 2020

Sommaire

GLOSSAIRE

AIS/SIA : Système d'Identification Automatique
AMRDS : Autonomous Maritime Radio Devices
ASN : Appel Sélectif Numérique (DSC)
COSPAS : COSMICHESKAYA SISTYEMA POISKIA AVARIYNICH SUDOW
CROSS : Centre de Recherche et d'Organisation du Secours et Sauvetage (MRCC)
DSC : Digital Selective Calling
EPIRB/RLS : Emergency Position Indicating Radio Beacon
GMDSS/SMDSM : Système Mondial de Détresse et de Sécurité Maritime
HF : High Frequency
IHO : Organisation Hydrographique Internationale
IMO/OMI : Organisation Maritime Internationale
IMSO : Organisation Internationale des Satellites Mobiles
INMARSAT : INternational MARitime SATellite organisation
IoT : Internet of Things = Internet des Objets
ITSO : Organisation internationale de télécommunications mobiles par satellite
LRIT : Long Range Identification and Trafic
MF : Medium Frequency
MMSI : Maritime Mobile Service Identity
MRCC : Maritime search and Rescue Coordination Center (voir CROSS)
MSC : Maritime Security Comitee
NAVTEX : Navigational Text
NCSR : (sub comitee) Navigation, Communications, Search & Rescue
OACI : Organisation de l'Aviation Civile Internationale
PNT : Positioning, Navigation, Timing
RLS : Radiobalise de Localisation des Sinistres
SAR : Search And Rescue
SARSAT : SEARCH AND RESCUE SATELLITE AIDED TRACKING
SART : Search And Rescue radar Transponder
SOLAS : Safety Of Life At Sea
SSAS : Ship Security Alert System
STCW : Convention on Standards of Training, Certification and Watchkeeping for Seafarers = Convention internationale sur les normes de formation des gens de mer, de délivrance des brevets et de veille
UIT : Union Internationale des Télécommunications
VDES : VHF Data Exchange System
VHF : Very High Frequency
VTS : Vessel Trafic Services

1. CADRE GENERAL

1.1. Objet de la mission

L'enjeu de ISIDE est celui d'améliorer la **sécurité en mer** contre les risques de la navigation, grâce au développement et à l'application de modèles de communication innovants qui utilisent les TIC - technologies de l'information et de la communication, afin de contribuer à améliorer la sécurité de navigation commerciale et de plaisance. A cet effet, ISIDE met au point des modèles et des protocoles partagés de théorie de l'information, vocaux et audiovisuels, qui serviront de base aux systèmes de communication utilisant les TIC entre la terre ferme et les navires, visant à optimiser les différents types de signaux et compositions textuelles des messages pour **réduire les risques** pouvant dériver d'une interprétation incorrecte ou ambigüe de la communication en situation d'urgence ou à risque, ceci particulièrement pendant les manœuvres et les conditions météo-climatiques à risque, en navigation et en phase d'accès/départ du port ou d'amarrage aux quais. L'objectif général est de créer une infrastructure de communication TIC à haute disponibilité, essentielle pour la sécurité de la navigation, qui facilite **l'activité de prévention et de gestion des situations à risque** en mer effectuée par la capitainerie du port.

La mission permettra l'élaboration de trois livrables :

- Livrable n°1 : Faire un état de la réglementation nationale, européenne et internationale qui régit le domaine de la sécurité maritime en relation avec l'utilisation d'instruments de communication terre mer.

- Livrable n°2 : Recenser des accidents survenus à cause de mauvaises communication.

- Livrable n°3 : Recenser des instruments de communication actuellement en service avec analyse technologique fonctionnelle, de coût et de gestion d'entretien.

1.2. Livrable n° 3 - Recensement des instruments de communication actuellement en service

Il s'agit de recenser les instruments de communication actuellement en service (avec analyse technologique, fonctionnelle, de coût et de gestion/entretien).
Ce recensement prendra en compte les systèmes de surveillance des approches maritime actuels et quels pourraient être les systèmes du futur (exemple imagerie laser…)

1.3. Methodologie

- Consultation des bases de données IMO, ARIA, CEDRE, BEA MER…
- Retours d'expériences
- Mise en perspective des incidents avec l'évolution de la réglementation
- Archives ouvertes : C.LEBOEUF et A.GENICOT

2. SYSTEMES DE COMMUNICATION NAVIRE - TERRE

2.1. Une organisation Internationale des radiocommunications

- **Perspective historique générale**

Un navire en mer peut paraître isolé : il effectue de longues traversées et parcourt d'immenses distances entre les ports, souvent pendant des semaines. Ce n'est plus le cas aujourd'hui. Grâce à la radiocommunication, les navires modernes sont en réalité presque toujours « sur le réseau». L'aptitude du navire à communiquer de manière instantanée et fiable avec les stations côtières et ses bases a terre est devenue un outil de gestion clé pour un secteur dont dépend l'ensemble de l'économie mondiale.

La marine marchande utilise généralement le spectre radioélectrique pour la navigation, les communications de détresse et de sécurité, les communications à bord et pour que les membres de l'équipage partis en mer puissent communiquer avec leurs familles et amis à terre. En qualité d'institution spécialisée des Nations Unies chargée d'assurer la sécurité et la sûreté des transports maritimes, dans le respect de l'environnement, l'OMI porte un intérêt particulier à la tenue de la Conférence mondiale des radiocommunications 2015 (CMR-15).

Depuis sa création en 1959, l'OMI et ses gouvernements membres, en étroite coopération avec l'Union internationale des télécommunications (UIT) et d'autres organisations internationales, notamment l'Organisation météorologique mondiale (OMM), l'Organisation hydrographique internationale (IHO), l'Organisation internationale des satellites mobiles (IMSO) et les partenaires de Cospas-Sarsat, se sont efforcés d'améliorer les radiocommunications maritimes en matière de détresse et de sécurité, ainsi que les radiocommunications générales.

- **Et l'avènement du GMDSS.**

Les radiocommunications navales sont entrées dans une nouvelle ère le 1er février 1999 avec la mise en œuvre complète du Système mondial de détresse et de sécurité maritime (GMDSS); un système de communication intégré utilisant des systèmes de radiocommunication par satellite et terrestres.

Dans le cadre du GMDSS, tous les navires à passagers et tous les cargos de plus de 300 tonnes brutes lors de voyages internationaux doivent transporter des équipements de radiocommunications terrestres et satellitaires spécifiés pour l'envoi et la réception d'alertes de détresse et d'informations sur la sécurité maritime, ainsi que pour les communications générales. Les règlements régissant le GMDSS sont contenus dans le chapitre IV de la Convention internationale pour la sécurité de la vie en mer (SOLAS), 1974.

Le 'GMDSS Manual, 2009' de l'OMI Publication fournit des informations plus détaillées.

Examen des éléments et des procédures du GMDSS

Le Sous-comité de la sécurité de la navigation, de la communication et de la recherche et du sauvetage (NCSR) entreprend actuellement un exercice de détermination de la portée afin d'établir la nécessité d'examiner les éléments et les procédures du GMDSS.

Examen de tous les documents d'information sur la sécurité maritime

Un groupe de travail du Sous-comité du Service mondial d'alerte à la navigation de l'IHO examine actuellement tous les documents d'information sur la sécurité maritime de haut en bas. Il a tout d'abord préparé des révisions aux résolutions de l'OMI A.705(17), "Promulgation of Maritime Safety Information" et A.706(17), "World-Wide Navigational Warning Service", qui ont été approuvées par le Comité de la sécurité maritime lors de sa quatrième session (MSC 85) en novembre/décembre 2008.

En conséquence, le Groupe de travail a préparé le Manuel conjoint de l'OMI/IHO/OMM révisé sur l'information sur la sécurité maritime, approuvé par le MSC 86 en mai/juin 2009 et la révision du Manuel international safetyNET, approuvé par le MSC 87 en mai 2010.

Conformément aux instructions qu'il reçoit directement du Comité de la sécurité maritime (MSC) et aux demandes qui peuvent lui être adressées par le Comité de la protection du milieu marin (MEPC), le Sous-comité de la navigation, des communications et de la recherche et du sauvetage (Sous-comité NCSR) examine les questions se rapportant aux sujets listés ci-après :

- les normes de performance, les prescriptions en matière d'entretien et les procédures applicables au matériel de radiocommunication et aux communications opérationnelles liées à la sécurité ou à la sûreté maritimes, et notamment le Système mondial de détresse et de sécurité en mer (SMDSM) ;
- la coopération avec l'Union internationale des télécommunications (UIT) concernant les questions liées aux radiocommunications maritimes mobiles ;

- le Plan-cadre de l'OMI relatif aux installations et services à terre dans le SMDSM ;
- les mesures et recommandations techniques et opérationnelles sur la mise en œuvre à l'échelle mondiale des règles de recherche et de sauvetage en mer, et notamment la maintenance du Manuel international de recherche et de sauvetage aéronautiques et maritimes (Manuel IAMSAR) ;
- la coopération avec l'Organisation de l'aviation civile internationale (OACI) concernant les questions communes liées à la recherche et au sauvetage maritimes et aéronautiques ; et
- le plan mondial de recherche et de sauvetage.

- **Jusqu'aux communications satellitaires**

Les navires ont d'abord largement utilisé les bandes des ondes décamétriques, puis celles des ondes hectométriques et des ondes métriques, au moyen de la télégraphie Morse, du service radio télex et de la radiotéléphonie. Plus récemment, la communication par satellite est devenue une composante à part entière des radiocommunications maritimes.

En particulier, le Système mondial de détresse et de sécurité en mer (SMDSM) est un système de communication intégré utilisant, entre autres, les systèmes de radiocommunication de Terre et de radiocommunication par satellite, ce qui permet de ne plus dépendre de la télégraphie Morse dans les domaines cruciaux que sont la communication de détresse et de sécurité.
Conformément au SMDSM, tous les navires transportant des passagers et tous les cargos de plus de 300 tonnes effectuant des voyages internationaux doivent s'équiper des systèmes spécifiés de radiocommunication de Terre et de radiocommunication par satellite, afin de pouvoir émettre et recevoir des alertes de détresse et des informations sur la sécurité maritime, ainsi que pour les communications d'ordre général.

Les navires se servent également de la radiocommunication aux fins de la navigation. L'utilisation des radars, à bord comme à terre, la fourniture de services de radionavigation par satellite, les aides à la navigation et le système d'identification automatique (SIA) sont cruciaux à cet égard. Plus d'un million de radars maritimes fonctionnent dans la bande 9200–9500 MHz.

3. REVUE DES PRINCIPAUX SYSTEMES EN SERVICE

3.1. SMDSM / GMDSS

Le SMDSM (GMDSS) utilise toutes les gammes de fréquences radiomaritimes (VHF, HF, MF et le système ASN) selon la zone de navigation.

Le **S**ystème **M**ondial de **D**étresse et de **S**écurité en **M**er (SOLAS chapitre IV) est conçu pour qu'à tout moment un navire soit capable de rentrer rapidement en contact avec les centres de coordination de sauvetage en mer (Maritime Rescue Coordination Centre - MRCC, en France le CROSS). Les **MRCC** (Maritime search and Rescue Coordination Center) sont chargés de coordonner les opérations de recherche et de sauvetage dans leur zone de responsabilité SAR (SRR).

Depuis 1999, les navires sont obligatoirement munis, selon leur zone de navigation, d'appareils capables d'émettre et de recevoir des alertes et des messages de détresse qui seront reçus par des stations terrestres. Les appareils émetteurs-récepteurs gardent en mémoire les messages émis et reçus. Les messages sont émis sur des fréquences définies.

Le SMDSM permet des Appels Sélectifs Numériques ASN ou DSC (*Digital Selective Call*) par les émetteurs-récepteurs en VHF et par les émetteurs-récepteurs MF/HF pourvus de l'ASN.

Les transmetteurs VHF et MF/HF sont couplés à des systèmes de positionnement par satellite permettant de transmettre la position du navire dans le corps du texte du message.

Chaque navire possède un numéro **MMSI** (Maritime Mobile Service Identity) de neuf chiffres, les 3 premiers correspondant à la nationalité ou la région géographique du navire A la mer, ces émetteurs-récepteurs doivent être en service H24

Les 9 fonctions du SMDSM-GMDSS :

- Émettre des alertes de détresse dans le sens navire-station côtière par au moins deux moyens distincts et indépendants
- Recevoir des alertes de détresse dans le sens station côtière-navire
- Émettre et recevoir des alertes de détresse dans le sens navire-navire
- Émettre et recevoir des communications pour la coordination des opérations SAR
- Émettre et recevoir des communication sur site
- Émettre et recevoir des signaux destinés au repérage
- Émettre et recevoir des renseignements sur la sécurité maritime
- Émettre et recevoir des radiocommunications d'ordre général et en provenance et à destination de réseaux de terre
- Émettre et recevoir des communications navire-navire

Les moyens de communication Radioélectriques suivants seront utilisés selon la zone géographique où se trouvera le navire :

- **VHF** de 156 à 174 Mhz
- **HF** de 4 à 27,5 Mhz
- **MF-HF** de 1605 à 4000 Khz

puis de 415 à 526.5 Khz pour des informations sur la Sécurité Maritime

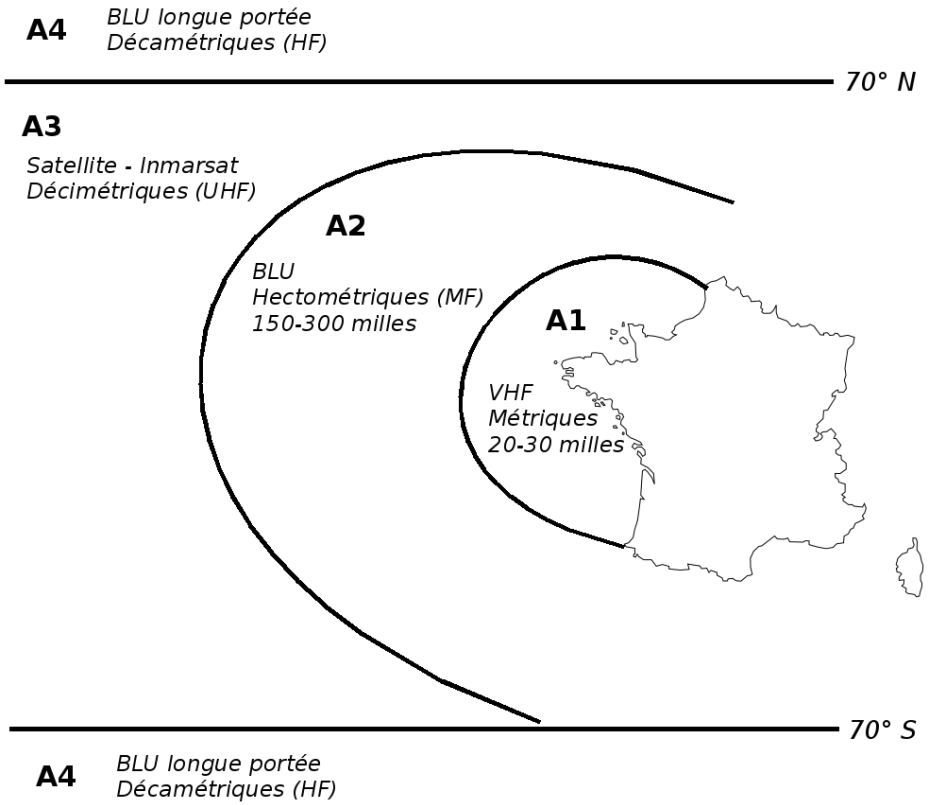
Des zones maritimes ont été définies, L'alerte doit pouvoir être donnée à tout moment dans toutes les zones.

Zone A1 (zone côtière) : zones couverte par au moins une station côtière travaillant en bandes métriques (VHF) utilisant l'ASN ;

Zone A2 (zone large) : zone couverte par au moins une station côtière travaillant en bandes hectométriques (MF) utilisant l'ASN hors zone A1;

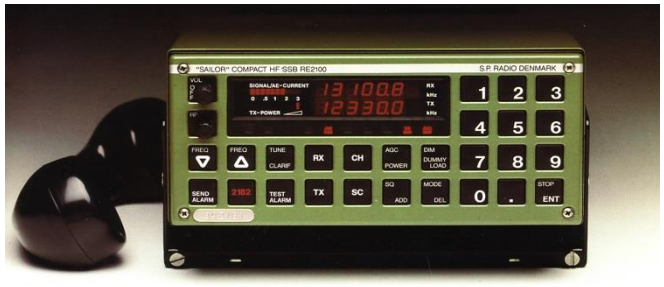
Zone A3 (zone grand large) : zone sous couverture d'un satellite géostationnaire d'Inmarsat hors zone A1 et A2 ;

Zone A4 (zones polaires) : zone couverte par la HF avec l'ASN, hors zones A1, A2, A3.



La Veille de l'Appel sélectif numérique ASN, (DSC en anglais : Digital Selective calling) est obligatoire en :

- ✓ VHF Canal 70, 156.525 Mhz
- ✓ MF-HF fréquence 2187.5 Khz
- ✓ HF fréquence 8414.5 Khz



C'est un système **automatique** de communication télégraphique **sans voie de retour.**

Il permet d'envoyer un message de **détresse** formaté de manière automatique par un simple appui sur le bouton. Le message comprend :

- le numéro MMSI
- la position du navire
- l'heure d'envoi.

Si l'opérateur en a la possibilité, il pourra ajouter la nature de la détresse par sélection dans un menu déroulant (préformaté).

MMSI navire RIF = 635

MMSI navire métropole = 226, 227, 228

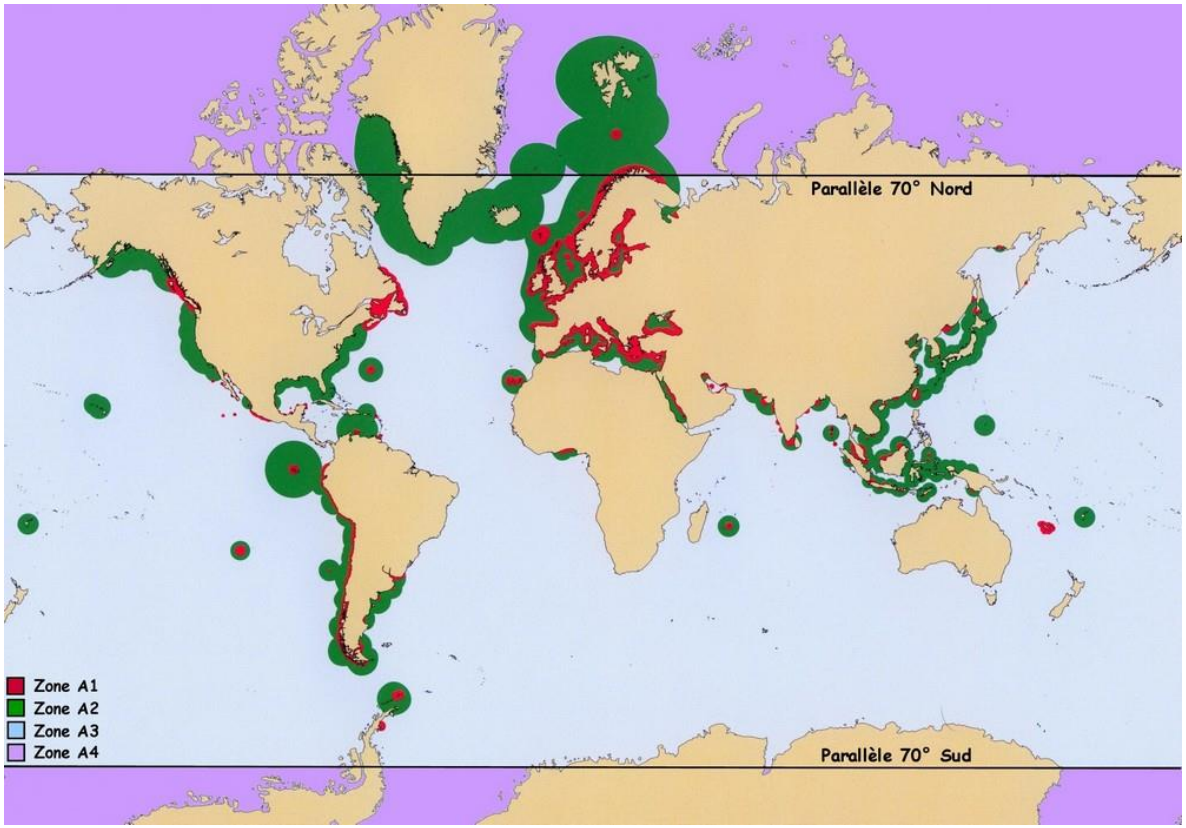
Tous les navires doivent posséder les systèmes ci-après :

- une RLS (Radiobalise de Localisation des Sinistres) ou EPIRB (Emergency Position Indicating Radio Beacon)
- un NAVTEX (Navigational Text)
- un SART (Search And Rescue radar Transponder)
- une VHF portative

Et selon la zone de navigation :

- Zone A1 : VHF ASN (25W)
- Zone A2 : VHF ASN + MF ASN (150W)
- Zone A3 : VHF ASN + MF ASN + HF ASN ou INMARSAT
- Zone A4 : VHF + MF ASN + HF ASN (de plus de 400W)

Remarque : En zone A3, si le navire dispose de l'INMARSAT, la puissance de l'émetteur HF peut être limitée à 250W. S'il n'y a pas d'INMARSAT, la puissance de l'émetteur HF doit être de 400W.



Les 4 « zones » SMDSM

La zone A1 :

En zone A1, l'État s'impose une couverture radioélectrique d'au moins une station côtière travaillant en ondes métriques et utilisant la technique d'appel sélectif numérique (ASN) en VHF sur la fréquence 156,525 MHz (voie 70 des ondes métriques) en permanence (24h/24h).

La zone A2 :

En zone A2, l'État s'impose une couverture totale en ondes hectométriques avec appel sélectif numérique (ASN) cela par la couverture radioélectrique d'au moins une station côtière travaillant en ondes hectométriques et utilisant la technique d'appel sélectif numérique sur la fréquence 2187,5 kHz (ASN).

Les territoires dans la zone A2 : Les stations côtières des États qui ne participent pas au SMDSM de 1999 donc en VHF sont dispensées d'avoir une couverture radioélectrique en appel sélectif numérique sur le canal 70. La couverture radioélectrique est en ondes hectométriques sur le canal 2187,5 kHz en veille automatique par l'appel sélectif numérique, et proche de la côte en ondes métriques sur le canal 16 en radiotéléphonie.

La zone A3 :

En zone A3, l'État est dispensé d'avoir une couverture radioélectrique en ondes métriques et en ondes hectométriques en appel sélectif numérique. (Donc sans la technique d'appel sélectif numérique sur les fréquences 2 187,5 kHz (ASN) et 156,525 MHz (ASN) de la voie 70).

La zone A3 est limitée à la couverture radioélectrique assurée par le service Inmarsat (Fleet 77, fleetBroadband et service Inmarsat C (International maritime satellite), entre les 76°N et 76°S ; ou également dans la portée d'une station côtière HF. La fréquence d'appel sélectif numérique en HF est 8414,5 kHz (portée < 3000 km de jour et le monde dans la nuit). À côté de la fréquence d'appel sélectif numérique 8414,5 kHz, on veille sur une deuxième fréquence décamétrique d'appel sélectif numérique : 4 207,5 kHz, 6 312 kHz, 12 557 kHz ou 16 804,5 kHz.

Exemple : Les DOM-TOM « département et région d'outre-mer » et « territoire d'outre-mer », sont classés en zone A3. La veille en radiotéléphonie des stations côtières y est assurée dans le système antérieur de détresse et de sécurité en mer dans la portée d'une station radio côtière VHF sur le Canal 16 fréquence 156,8 MHz, et dans la portée d'une station côtière (onde hectométrique) sur la fréquence 2 182 kHz. La couverture radio en appel sélectif numérique est alors assurée par les satellites Inmarsat ; les Renseignements sur la Sécurité Maritime (RSM) étant diffusés par l'intermédiaire de ses satellites (SafetyNet).

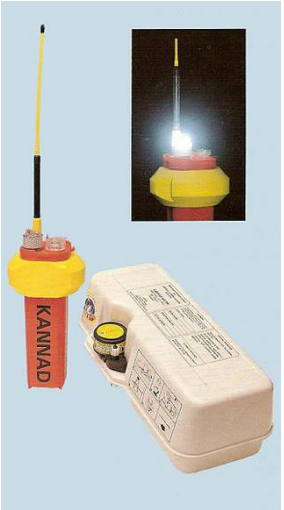
La zone A4 :

La zone A4 est la zone hors A1, A2 et A3, soit au-delà des 76° Nord et 76° Sud, c'est-à-dire l'Arctique et l'Antarctique (zone polaire).

Couverte uniquement en HF 8414,5 kHz (onde décamétrique). Portée < 3000 km de jour et le monde dans la nuit.

À côté de la fréquence (ASN) 8414,5 kHz, on veille sur une deuxième fréquence décamétrique d'appel sélectif numérique : 4 207,5 kHz, 6 312 kHz, 12 557 kHz ou 16 804,5 kHz.

3.2. La balise RLS ou EPIRB



Transmetteur émettant sur la fréquence 406 Mhz en numérique dans les situations de détresse, d'urgence pour donner l'emplacement d'un navire en détresse.

Ce signal est reçu par un des satellites du réseau Cospas-Sarsat

qui localisent le navire et transmettent les coordonnées au MRCC le plus proche.

L'autonomie est de 100 H à +20° et de 40 H à -40°.

Une radiobalise a une puissance comprise entre 3 W et 7 W sur la bande 406 à 406,1 MHz en transmission digitale codée du MMSI d'une durée de 440 ms tous les 50 s.

La radiobalise est placée dans les parties hautes du navire, dans un conteneur muni d'un largueur hydrostatique conçu pour la libérer automatiquement par détection de pression équivalente à une immersion à une profondeur de 3 à 4 mètres lorsque le navire coule

3.3. Le NAVTEX

Système à moyenne portée travaillant sur une fréquence fixe de **518** kHz. Le Navtex est un simple récepteur doublé d'une imprimante ou/et d'un écran. Il permet de recevoir les informations émises par des stations émettrices préprogrammées. Les messages sont enregistrés ou/et imprimés sans intervention. Une alarme est prévue pour attirer l'attention du personnel de quart en cas de message à caractère urgent.

Exemple de message type :

ZCZC

$B^1B^2B^3B^4$, selon le code suivant : B^1 : Station émettrice ; B^2 : type de message ; B^3B^4 : numérotation.

Texte du message

NNNN

3.4. Le SART (Search And Rescue Transponder)

Transpondeur Radar utilisé par les personnes en détresse en mer, embarqué dans les embarcations de sauvetage.

C'est un récepteur-émetteur, mis en veille manuellement. S'il reçoit un signal radar, il renvoie un signal qui le localise sur l'écran du radar qui l'a déclenché. Cela se concrétise sur l'écran des intervenants SAR par 12 traits dans la direction du transpondeur 'SART'.

Le SART émet un signal sonore et/ou visuel quand il est localisé par un radar de 3 cm de longueur d'onde. Il doit être placé à au moins 1,50 m au-dessus du niveau de la mer pour pouvoir être déclenché par un radar dont l'antenne est située à 15 m de hauteur, à une distance de 5 miles.

Plus le radar est haut, plus la portée est grande.

Fréquence **: 9,2-9,5 GHz**.

Un transpondeur SART devra pouvoir assurer une veille de 96 heures et une durée d'émission de 8 heures

Le tableau de la page suivante donne un récapitulatif des différents moyens disponibles pour gérer détresse et SAR.

Tableau récapitulatif des types de communications détresse et SAR

Type de message	N° Fct	Sens	Type	Intervenants	Materiel
Moyens d'émettre et recevoir des alertes de détresse	1	Navire → RCC	Emettre des alertes de détresse par au moins 2 moyens distincts et indépendants	-Navire en détrese -RCC	-ASN (VHF-MF-HF) -INMARSAT -RLS / EPIRB
	2	RCC → Navire RCC → Navires sur zone	Recevoir des alertes de détresse (accusé de réception et relais de détresse)	-RCC -Navire en détresse -Navires sur zone	-ASN (VHF-MF-HF) -INMARSAT
	3	Navire → Navires sur zone	Emettre et recevoir des alertes de détresse directement	-Navire en détresse -Navires sur zone	-ASN (VHF-MF)
Moyens de communication sur site et SAR	4	RCC ⇆ OSC ou RCC ⇆ CSS	Emettre et recevoir des communications ayant trait à la coordination des opérations SAR.	-RCC -OCS ou CSS (hélicoptère, navire…)	
	5	OSC ⇆ Détresse OSC ⇆ Navires Navire ⇆ Navires	Emettre et recevoir des communications sur site	-OSC ou CSS -Navire en détresse -Navires sur zone	-VHF et/ou MF -VHF portable
	6	Naufragé → OSC Naufragé → Navires sur zone	Emettre et recevoir des signaux destinés au repérage final par goniométrie	-Navire en détresse -OSC ou CSS -Navires sur zone	-Transpondeur radar (9,2 à 9,5 Ghz) -RLS/EPIRB (121,5 MHz)

3.5. Le réseau INMARSAT

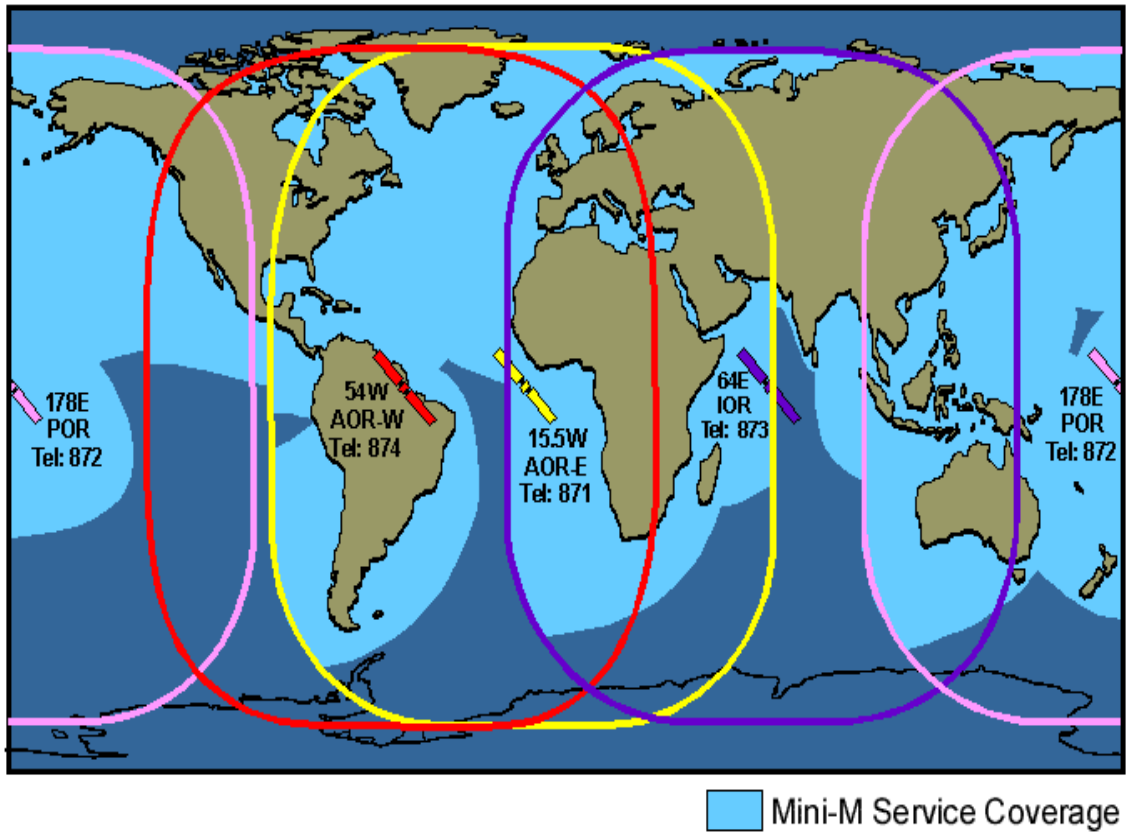
Organisation Internationale de Télécommunications Maritimes par satellite (INMARSAT) créée par l'OMI en 1976 et privatisée en 1999.

Pour mémoire, les principaux Systèmes de satellites utilisés :

- Sat A (Voix, Fax) supprimé en 2007
- Sat B (Voix, Fax, Data), compatible SMDSM
- Sat C (Data, Fax) compatible SMDSM + Positionnement
- Sat D (Data), Positionnement SSAR
- Sat M (Voix, Data) faible débit
- Fleet Fxx

Nouvelle génération d'appareils, entièrement adaptés à tous les besoins en matière de Détresse, Urgence, Sûreté.

Autorise l'Internet illimité (Vsat).



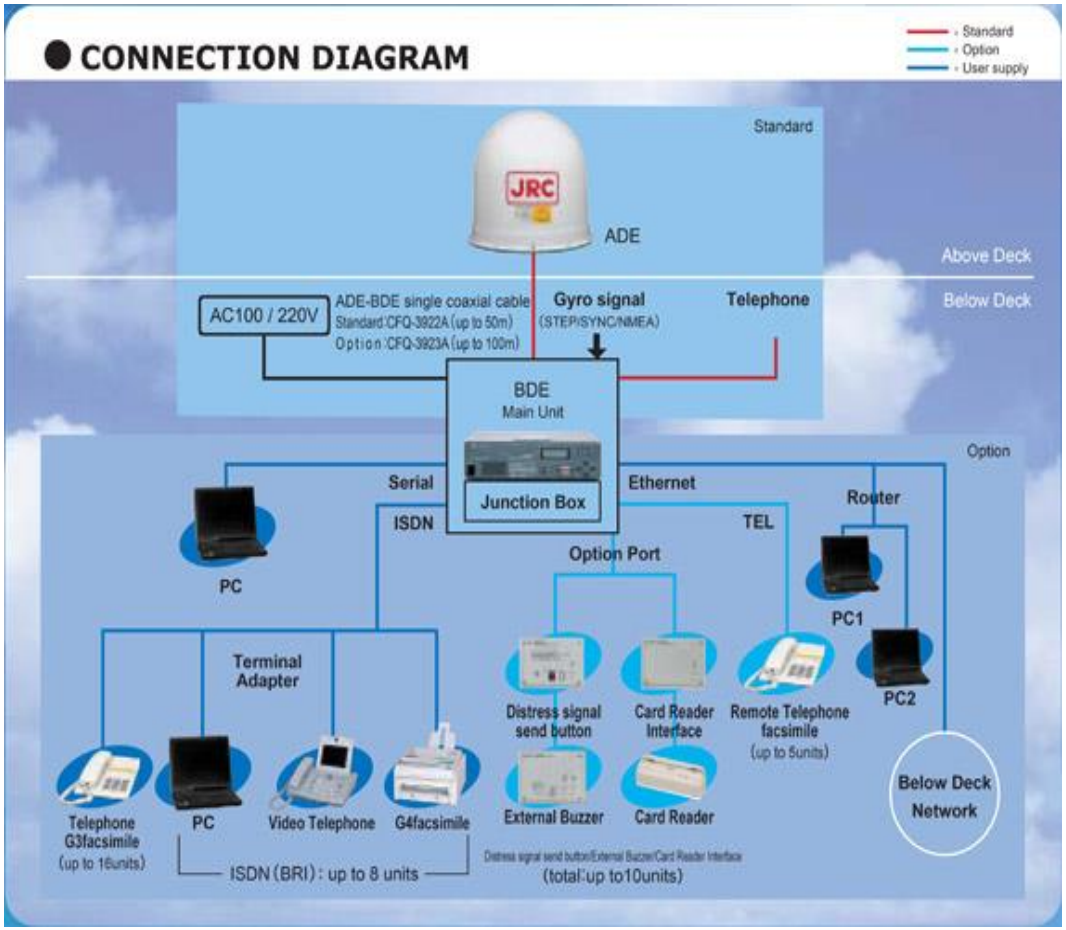
- **AOR-W** : ATLANTIC OCEAN REGION WEST **871**
- **AOR-E** : ATLANTIC OCEAN REGION EAST **874**
- **IOR** : INDIAN OCEAN REGION **873**
- **POR** : PACIFIC OCEAN REGION **872**

INMARSAT Fleet F77, système intégré

Inmarsat Fleet 77 est un service de communication par satellite entièrement intégré intégrant des applications voix et données

Inmarsat Fleet 77 offre la voix et le choix du RNIS mobile jusqu'à 64 kbps ou des services de données par paquets mobiles (MPDS) toujours actifs pour des communications mondiales économiques.
Le Fleet 77 répond également aux spécifications de détresse et de sécurité du SMDSM pour la communication vocale. Grâce à la préemption et à la priorisation de la voix en quatre étapes, le service prend en charge l'accréditation des systèmes des navires et garantit que les besoins de détresse et de sécurité hautement prioritaires sont satisfaits.

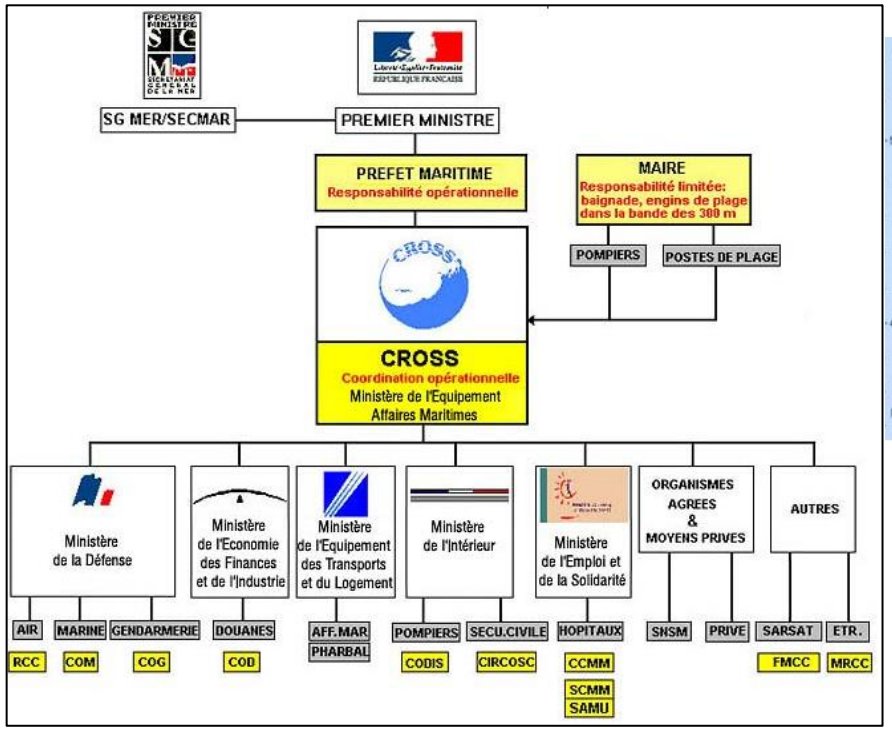
Ce système intégré déjà ancien préfigure les TIC modernes, il sera fermé le 1er décembre 2020 et remplacé par des systèmes a l'intégration encore plus aboutie, allant même jusqu'à prendre en compte les cartes marines (ECDIS).

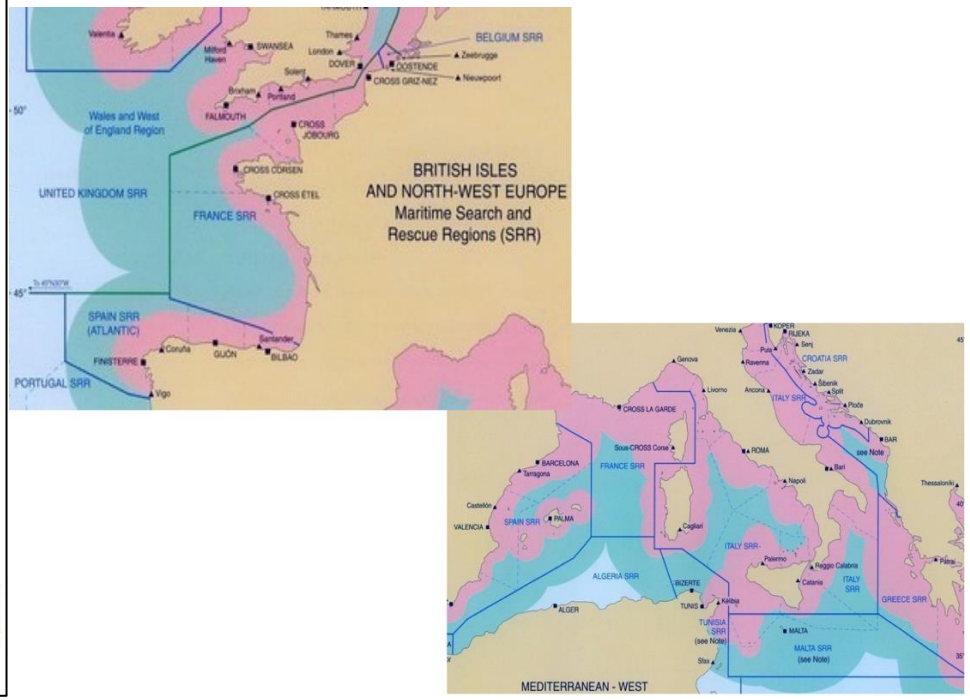


3.6. SEARCH and RESCUE (SAR)

Le SAR définit l'ensemble de l'organisation et des opérations de localisation et de secours aux personnes en situation de détresse.
En adhérant à la Convention SAR un État doit :

- définir une région de recherche et de sauvetage appelée *zone de responsabilité SAR* (SRR) ;
- mettre en place un ou plusieurs centres de coordination de sauvetage (en France les CROSS) ;
- donner des moyens (vedettes, canots, personnel, etc.) à ces CROSS ;
- créer éventuellement des centres secondaires ;
- conclure des accords avec d'autres États voisins afin d'éviter le gaspillage de (moyens) ressources





Organisation du SAR en France

3.7. Le système SARSAT-COSPAS

Le programme **SARSAT-COSPAS** est un système mondial d'aide à la recherche et au sauvetage par satellite.

- **SARSAT= S**EARCH **A**ND **R**ESCUE **S**ATELLITE **A**IDED **T**RACKING
  Développement conjoint par la France, Les USA et le Canada
- **COSPAS= C**OSMICHESKAYA **S**ISTYEMA **P**OISKIA **A**VARIYNICH **S**UDOW
  Développement par l'URSS.

Les deux systèmes ont fusionné le 1er janvier 1988.

L'ensemble fonctionne par la combinaison de 6 satellites en orbite basse et de 5 satellites en orbite géostationnaire.

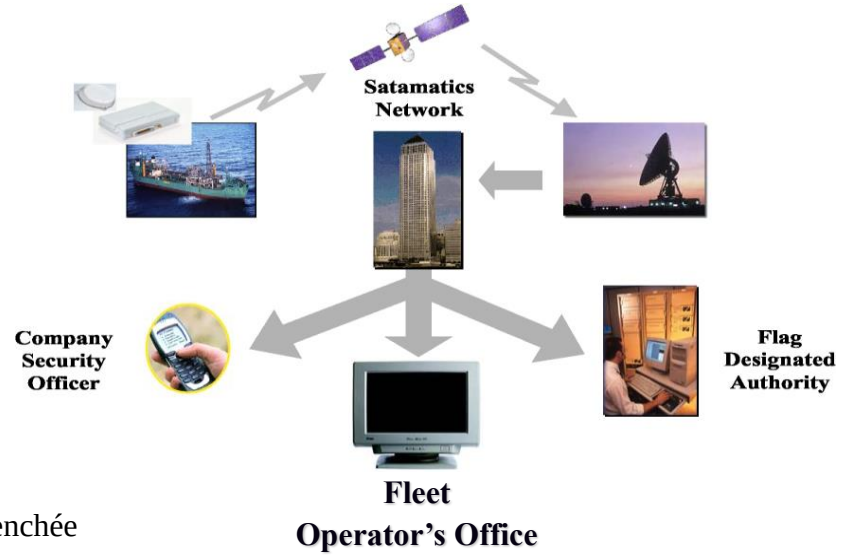
Ces satellites reçoivent un signal sur la bande de détresse internationale de 406 à 406,1 MHz

3.8. Communications de sûreté

Le système SSAS

Avec la mise en application du code ISPS, tous les navires doivent être pourvus d'un système d'alerte de sûreté. En cas d'activation, le SSAS :

- Doit déclencher et transmettre à une autorité compétente (y compris la compagnie), une **alerte de sûreté** navire-terre identifiant le navire et sa position et signalant que la sûreté du navire est menacée ou qu'elle a été compromise
- Ne doit pas donner l'alarme à bord du navire
- Ne doit pas envoyer l'alerte de sûreté à d'autres navires
- Doit continuer l'alerte de sûreté jusqu'à ce qu'elle soit désactivée et/ou réenclenchée



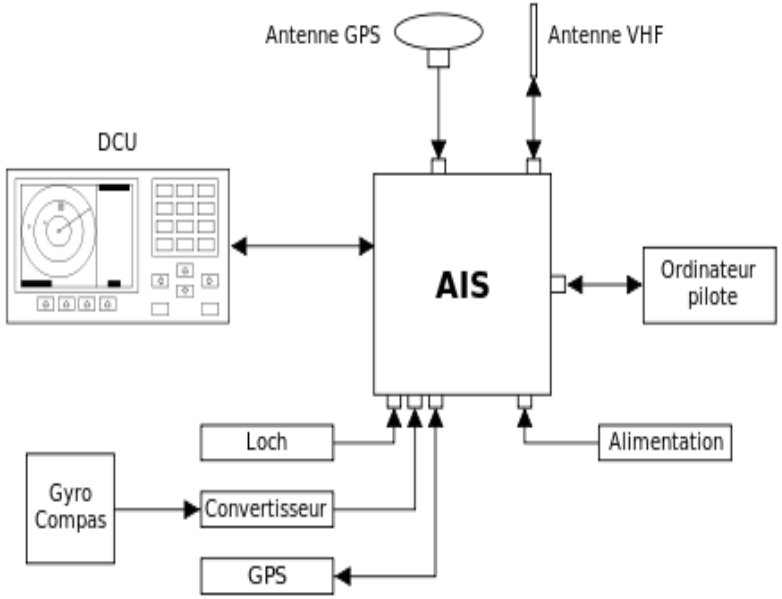
3.9. Système d'identification automatique ou Automatic Identification System (AIS)

Système d'échanges automatisés de messages entre navires qui permet aux navires et aux systèmes de surveillance de trafic (CROSS en France) de connaître l'identité, le statut, la position et la route des navires se situant dans la zone de navigation.

L'AIS permet d'identifier les navires lorsque la reconnaissance visuelle ou radar n'est plus possible (nuit, temps de brume, faible échos radars).

Des systèmes AIS sont installés sur des marques flottantes (bouées) ou fixes (phares) afin de pouvoir les identifier plus rapidement.

L'AIS peut être utile pour éviter les collisions mais il convient toujours de vérifier l es informations par d'autres moyens. Il ne doit pas être assimilé à un **instrument de navigation**



D'autres utilisations sont envisagées comme la transmission aux navires par les stations terrestres des positions des obstructions (épaves, écueils).

L'AIS doit faciliter la coordination des opérations de sauvetage en permettant aux stations terrestres (sémaphores, CROSS) d'identifier les navires les plus à même de se porter sur les lieux d'un sinistre.

L'efficacité de l'AIS dans ce domaine est toutefois limitée par la portée de la radio VHF (30 à 50 milles).

L'AIS permet la transmission de messages adressés à tous, ou à une cible particulière identifiée à portée.

Deux types de transpondeurs AIS, de classe A ou B, ont été développés conformément aux législations pertinentes. Le matériel de classe A correspond aux exigences des résolutions de l'OMI relatives aux *Performance Standards* , applicables aux navires visés par la Convention SOLAS. L'Union Internationale des Télécommunications (UIT) édicte des normes techniques reprises par les législations internationales,

régionales et nationales. Ainsi par exemple, la Recommandation UIT-RM.1371-1 a normalisé la longueur des messages AIS ou encore les intervalles d'émissions des données par les navires. La normalisation technique internationale a ainsi donné lieu à la distinction de deux classes de transpondeurs AIS. La classe B diffère significativement de la classe A. L'intervalle de signalement (*reporting rate)* a une vitesse inférieure à 14 nœuds et de 10 sec. pour la classe A et de 30 sec. pour la classe B. Par ailleurs, la classe B ne transmet pas.

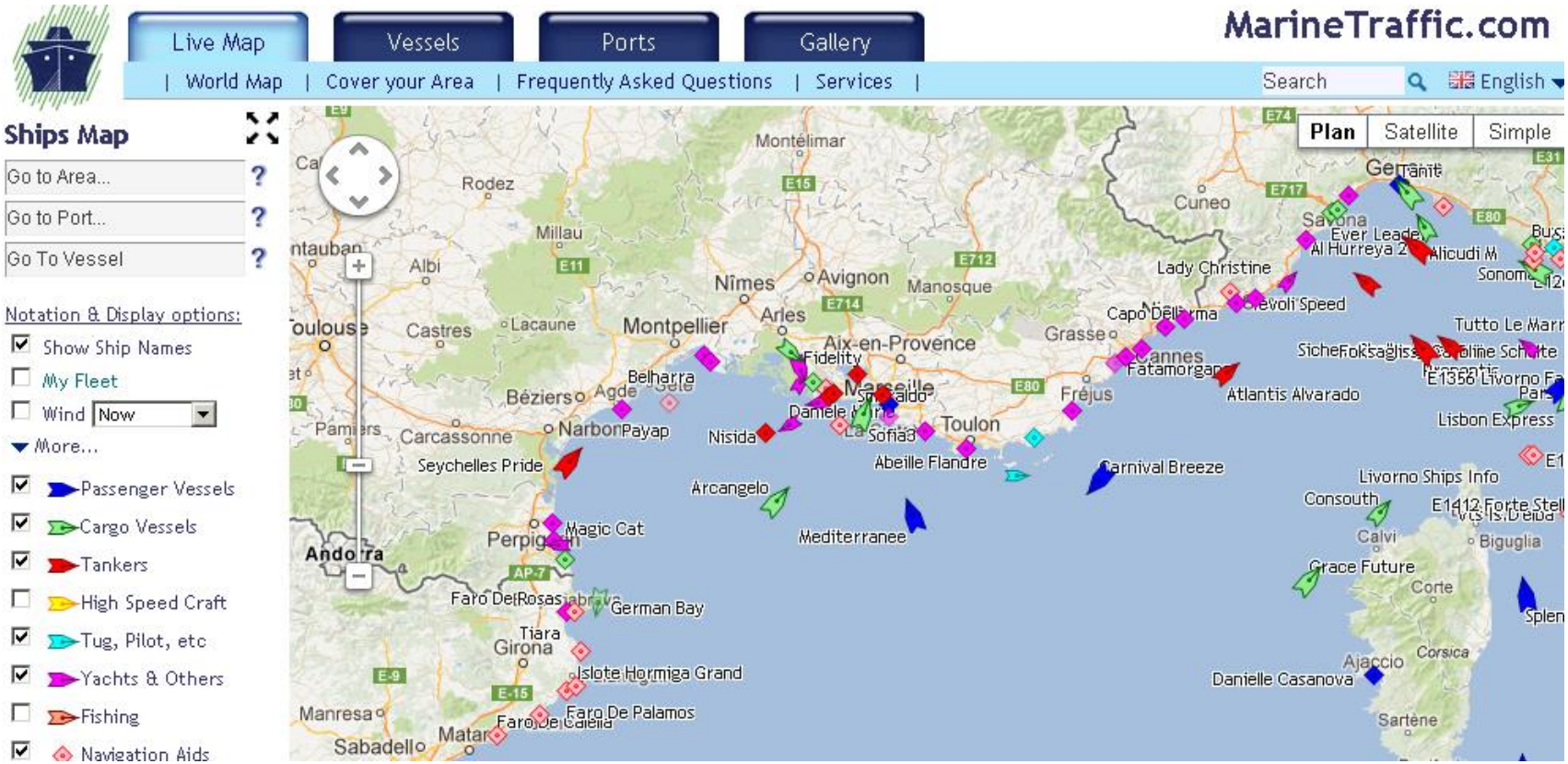
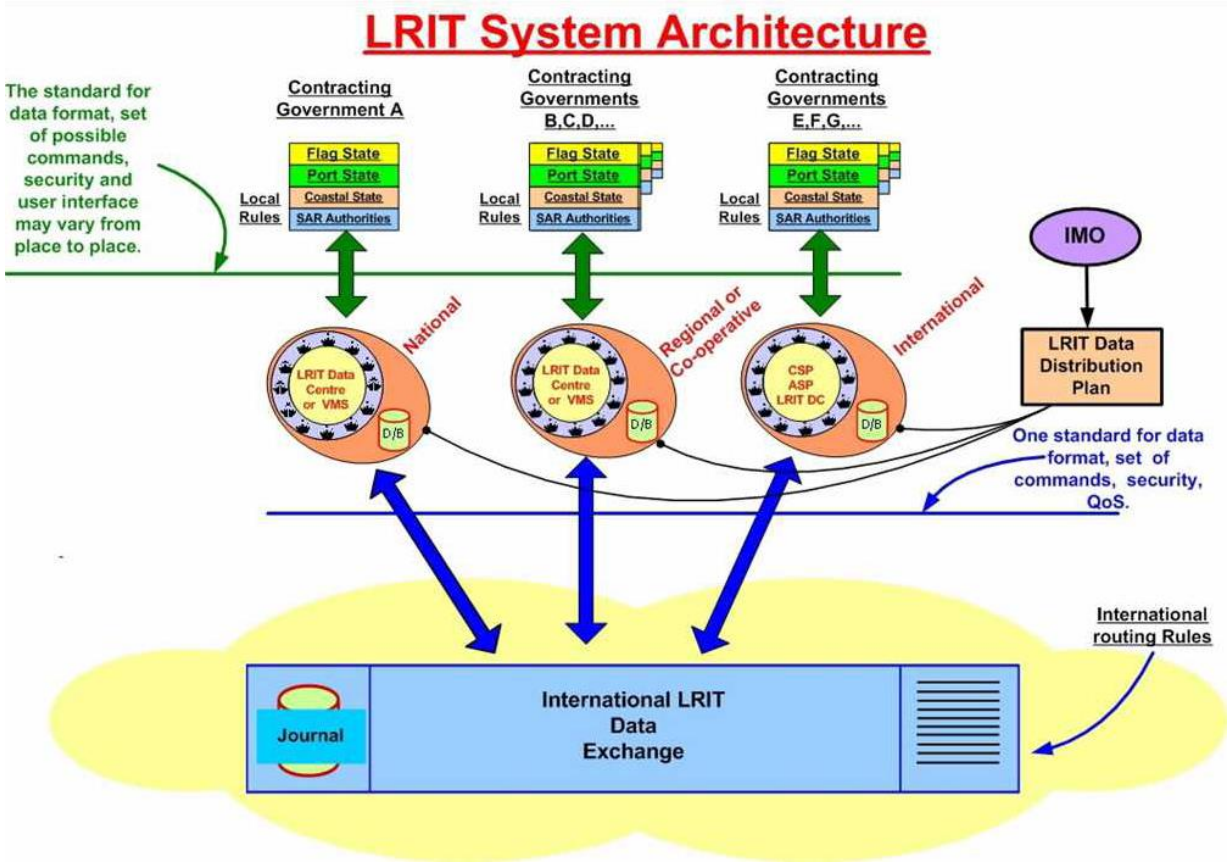


Image type AIS en Méditerranée

3.10. Long Range Identification and Trafic (LRIT)

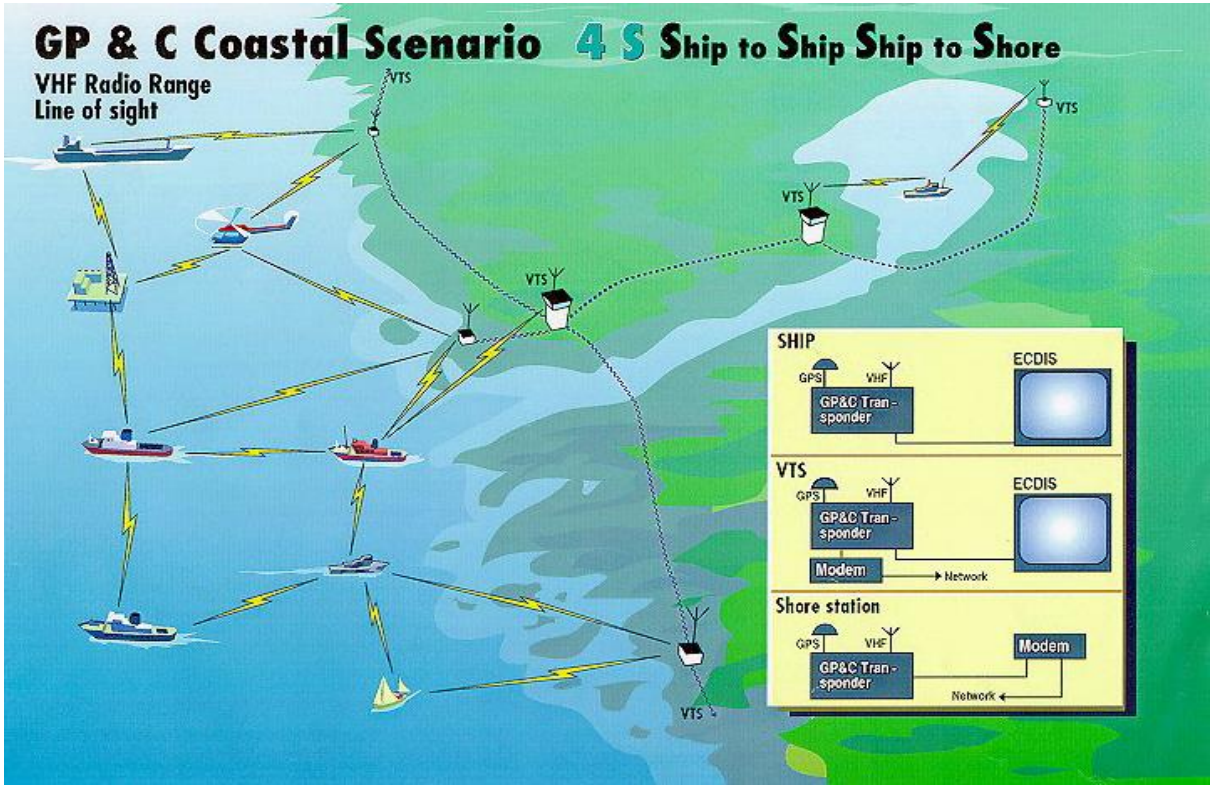
Le LRIT est un système comparable à l'AIS mais avec des transmissions Longue Distance.



Ce système se prête particulièrement aux évolutions des TIC en termes de globalisation et d'intégration des systèmes

3.11. Vessel Trafic Services (VTS)

Le VTS est conçu pour améliorer la sécurité et l'efficacité de la navigation, la sécurité de la vie humaine en mer et la protection du milieu marin. VTS est régi par la Convention SOLAS chapitre V règlement 12 ainsi que par les directives de l'OMI (résolution OMI A.857(20) adoptées le 27 novembre 1997.



3.12. Tableau récapitulatif des différents systèmes en service

Système	Type de technologie	Portée	Observations
SMDSM	Toutes fréquences radiomaritimes Ondes Radioélectriques (ou Hertziennes)	mondiale	Utilise VHF/HF et intègre l'ASN Nature des équipements obligatoires différent selon la zone
VHF	Ondes Radioélectriques de 156 à 174 Mhz	horizon	156,8 Mhz = Canal 16
MF	Ondes Radioélectriques de 1,6 à 4 Mhz	Inf 60 Nq	
HF	Ondes Radioélectriques de 4 à 27 Mhz	3000 km de jour Monde de nuit	En BLU ou en ASN
Radiobalise RLS	406 Mhz et 121,5 Mhz	3000 km de jour Monde de nuit	Émet le MSSI et la position GPS À partir de 2020, des radiobalises équipées du *Return Link Service* de Galileo seront commercialisées. Ce service permettra à l'utilisateur de la radiobalise d'être informé (via une LED de la réception de son signal de détresse
INMARSAT	Communication via un réseau de satellites	Mondiale par Zones	Fleet 77 sera fermé le 1er décembre 2020
NAVTEX	Onde Radioélectrique 518 khz	Moyenne portée	
SART	Transpondeur RADAR (9,2 – 9,5 Ghz)	Dépend de la hauteur du radar	Veille 96h Émission 8 h

AIS	Ondes VHF	30 à 50 Nq	Système d'identification et de positionnement sommaire
LRIT	Communications satellites	mondiale	Système d'identification longue distance Au moins 4 positionnements pas jour, depuis 2006
VTS	Ondes VHF	30 à 50 Nq	Système de positionnement pour améliorer la sécurité et l'efficacité de la navigation

4. Perspectives d'avenir

4.1. Les Formations – le savoir faire

CERTIFICATS D'OPERATEUR SMDSM - LONG RANGE CERTIFICATE - LRC –

Depuis 1999, la réglementation STCW impose les certificats d'opérateur SMDSM suivants :
Pour les navires de commerce

- Certificat restreint d'opérateur (CRO) type « (SRC) Short Range Certificate » (en anglais ROC, Restricted Operator's Certificate) : valide pour tous les navires exploités dans la zone A1 ;
- Certificat spécial d'opérateur (CSO) type « (LRC) Long Range Certificate » : valide pour les navires français navigant dans toutes les zones; pour les navires de charge de jauge brute inférieure à 300 UMS ; les navires de pêche neufs de longueur inférieure à 24 mètres et les navires de pêche existants de longueur inférieure à 45 mètres ;
- Certificat général d'opérateur (CGO) type (LRC) « Long Range Certificate » (en anglais GOC, General Operator's Certificate) : pour tous les navires et dans toutes les zones.
- Certificat restreint de radiotéléphoniste maritime (SRC) Short Range Certificate pour les navires naviguant dans les eaux internationales ou étrangères 7.

Dans les eaux territoriales françaises, l'utilisation des talkie-walkie VHF de moins de 6W est autorisée sans certificat de radiotéléphoniste .
Depuis 1999, plusieurs pays (Grande-Bretagne, Italie, Duché de Luxembourg, Suisse) ont créé le « (LRC) Long Range Certificate de Yacht » valide pour les navires plaisance navigant dans toutes les zones.

Il est a prévoir que les formations prévues au STCW vont évoluer pour s'adapter aux nouveaux réseaux et en particulier au réseaux intégrés qui relèvent plus du bon emploi des nouveaux systèmes d'information (informatique) que des communication radioélectriques traditionnelles.

4.2. Évolutions portées par l'OMI, l'IUT et l'Europe

Du point de vue opérationnel, les navires sont de plus en plus souvent gérés au moyen d'une assistance à terre. Les données correspondant aux critères essentiels, tels que l'état de la cargaison, les performances du moteur et la consommation de carburant sont régulièrement transmises du navire à la terre, tandis que l'utilisation du large bande sur les navires situés à proximité des côtes se généralise pour transmettre les documents à fournir à l'entrée et à la sortie des ports. A l'heure actuelle, quelque 12 000 navires utilisent des microstations (VSAT) pour les communications large bande. Ce service n'est assuré qu'à une distance minimale à partir des côtes de 125 km pour la bande 14–14,5 GHz et de 300 km pour la bande 5925–6425 MHz.

Tout cela s'inscrit dans un contexte de hausse continue de la demande de spectre de la part de presque tous les secteurs des radiocommunications. La marine marchande, par l'intermédiaire de l'OMI, a particulièrement intérêt à ce que la CMR-15 maintienne l'attribution actuelle du spectre aux services maritimes existants.

Depuis la création de cette organisation en 1959, l'OMI et ses Etats Membres, en étroite coopération avec l'UIT et d'autres organisations internationales comme, en particulier, l'Organisation météorologique mondiale (OMM), l'Organisation hydrographique internationale (OHI), l'Organisation internationale de télécommunications mobiles par satellite (ITSO) et les partenaires COSPAS-SARSAT, se sont efforcés d'améliorer les radiocommunications de détresse et de sécurité en mer, celles relatives à la sécurité et d'autres radiocommunications maritimes.

Les transports maritimes sont sans doute la plus internationale de toutes les grandes industries du monde – et l'une de celles qui présente les risques les plus élevés en cas de fortune de mer. Il a toujours été admis que le meilleur moyen de renforcer la sécurité en mer était d'élaborer une réglementation internationale respectée par toutes les nations maritimes.

Le Comité de la sécurité maritime de l'OMI est le principal organe technique de l'OMI traitant des questions relatives à la sécurité. Plusieurs Sous-comités de l'OMI le secondent dans ses travaux et en particulier le « sous-comité de la navigation, des communications et de la recherche et du sauvetage » (NCSR).

Le Groupe mixte OMI / UIT d'experts des questions de radiocommunication maritime a également été créé pour définir les futures exigences des radiocommunications maritimes, en tenant compte des besoins opérationnels définis par l'OMI et des besoins réglementaires définis par l'UIT.

Le Groupe se réunit, selon les besoins, entre les réunions du Sous-comité de la sécurité de la navigation, des communications et de la recherche et du sauvetage (NCSR). Le Groupe fait rapport au Sous-Comité NCSR et, le cas échéant, aux réunions des Commissions d'études et / ou Groupes de travail compétents de l'UIT-R. Le Groupe mène ses travaux sur la base d'un mandat approuvé par le sous-comité NCSR et approuvé par le comité de la sécurité maritime (MSC).

Le Sous-comité sur la sécurité de la navigation, des communications et de la recherche et du sauvetage (NCSR) entreprend actuellement un exercice de cadrage pour établir la nécessité d'un examen des éléments et des procédures du SMDSM.

Par ailleurs la règle 19 du Chapitre V de la Convention SOLAS indique que « tous les navires d'une jauge brute égale ou supérieure à 300 qui effectuent des voyages internationaux, les navires de charge d'une jauge brute égale ou supérieure à 500 qui n'effectuent pas de voyages internationaux et les navires à passagers, quelles que soient leurs dimensions, doivent être pourvus d'un système d'identification automatique ».
Seuls les navires entrant dans le champ de la disposition précitée ont ainsi une obligation internationale d'emport d'un matériel AIS opérationnel, de sa mise en fonctionnement et de son entretien. L'AIS est également utilisé en pêche pour laquelle il existe également des dispositions communautaires et nationales. En plaisance, l'AIS est employé par les participants de manifestations sportives.

Ainsi l'AIS tend à se généraliser, non pas sous l'influence d'une normativité internationale ou nationale opposable, mais du fait de l'intérêt sécuritaire qu'il représente.

4.3. Evolutions portées par le marché

Les rapports officiels indiquent que le marché mondial des VSAT maritimes (communications bidirectionnelles par satellite – type INLMARSAT) était évalué à 1,92 milliard de dollars en 2017 et devrait atteindre 5,19 milliards de dollars en 2025, avec un taux de croissance annuel de 13,3% de 2018 à 2025.
De plus en plus d'entreprises adoptent aujourd'hui l'IoT dans le but d'aider les applications et les flux de communication des équipages à fonctionner de manière transparente sur l'ensemble du réseau.
L'internet des objets (IoT) comprend une grande variété d'objets et d'appareils physiques, ainsi que de l'électronique, des logiciels, des capteurs et des connectivités réseaux permettant à ces appareils de collecter et de partager l'information. Tous ces appareils connectés et les données qu'ils génèrent ouvrent le champs des possibles pour les organisations, quelle que soit leur activité ou leur taille.

Voici quelques exemples de ce que l'IoT peut apporter dans le domaine maritime : améliorer la manutention du fret en utilisant la couverture satellite entre deux escales, réduire les coûts administratifs de la conformité réglementaire, réduire la consommation de carburant et accroître l'efficacité et la sécurité.

Une étude de 2018 indique que les armateurs prévoient de dépenser 2,5 millions de dollars pour des solutions basées sur l'IoT au cours des trois prochaines années et s'attendent, en moyenne, à réaliser des économies de 14% avec les IoT au cours des cinq prochaines années.

4.4. Tendances pour les communications maritimes à venir (SMDSM et eNAV)

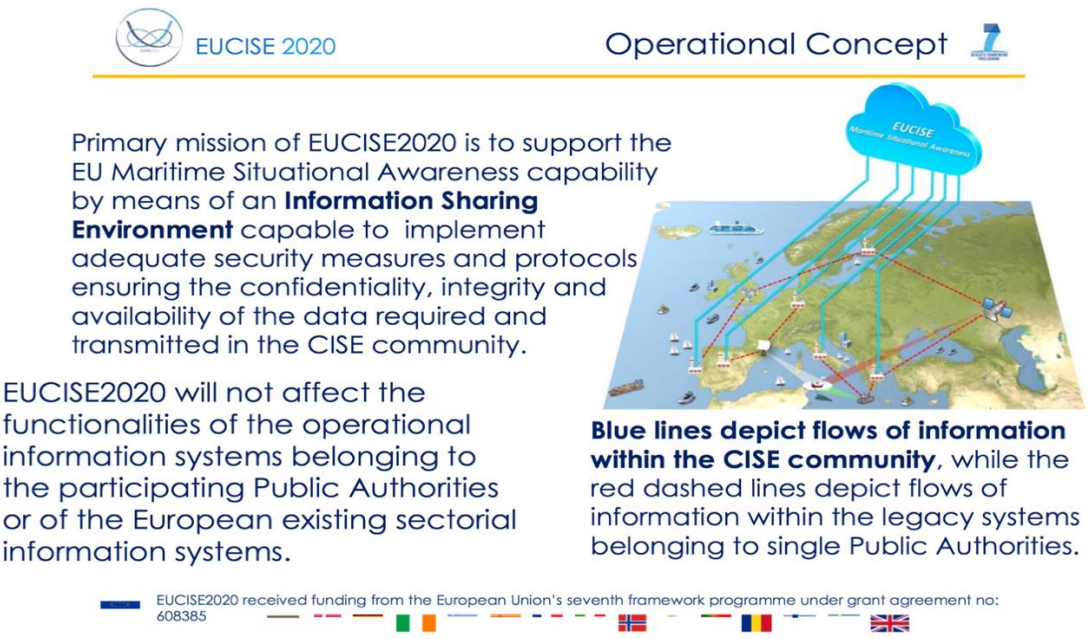
Les normes techniques de l'UIT et de l'OMI représentent l'état des technologies actuelles en matière de radiocommunications maritimes et de radionavigation et intègrent le SMDSM et l'e.Nav.

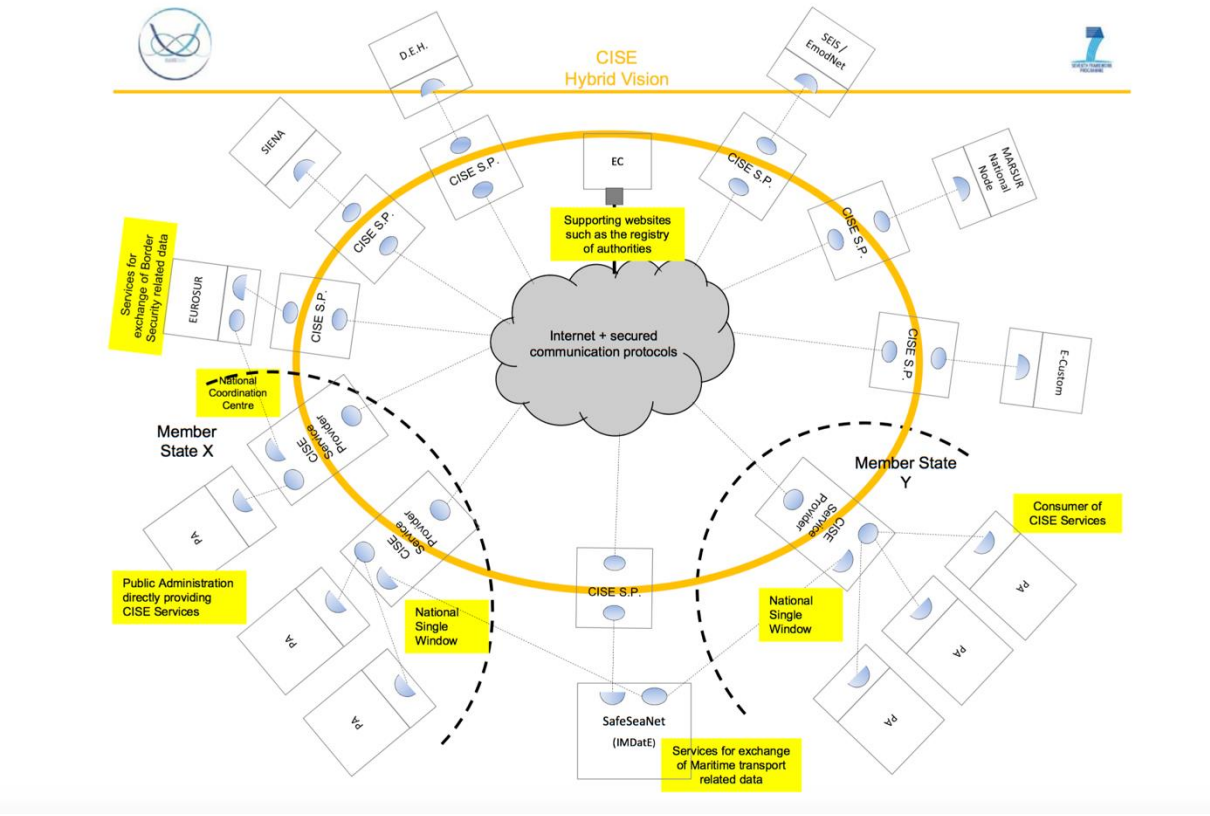
Les systèmes existants sont en cours d'amélioration et de nouvelles technologies continuent d'émerger, ces développements sont parallèles aux efforts visant à améliorer la sécurité en mer, à protéger l'environnement maritime et à déplacer efficacement les marchandises.

Ces nouveaux développements concernent (liste non exhaustive) :

- Les nouveaux systèmes satellitaires
- La transition vers les technologies numériques pour modernisation du SMDSM
- Les développements des NAVDAT, eNAV et VDES
- La surveillance des systèmes embarqués, par ex. Machine 2 Machine (M2M)
- Les technologies par satellite
- L'utilisation croissante des systèmes de téléphonie mobile dans les zones côtières
- L'expansion du rôle des systèmes pilotés par logiciel; besoin de mise à jour du logiciel
- L'intégration de systèmes, réseaux embarqués complexes
- Le développement de services de navigation électronique standardisés - émergence d'un nouveau modèle commercial axé sur les services
- L'augmentation massive de la connectivité des navires, et la demande de bande passante
- Les initiatives sur la cybersécurité dans tous ces domaines

Le programme Européen EUCISE qui a lancé ses travaux en 2020 travaille par exemple sur l'intégration et la fusion de données relatives à la sécurité de la navigation.





Exemple d'un « Cloud » maritime international

Les sujets en cours de traitement par l'OMI concernent les groupes de services numériques rassemblés sur une structure de données commune :

- VTS, MSI, service de pilotage, télémédecine, service de cartes marines • La structure commune de données maritimes (CMDS) sous-tend la navigation électronique
- Modèle de données hydrographiques universelles de l'OHI S-100 à utiliser comme CMDS
- S-124 (avertissements de navigation), S-129 (fond sous quille), etc.
- «Dispositif d'itinérance intelligent» : EfficienSea2 - Objectif: permettre un échange d'informations efficace, sécurisé et fiable
- VHF Data Exchange System (VDES)
    - Evolution de l'AIS - développé pour répondre aux demandes croissantes du système actuel
    - Destiné à atteindre sa pleine capacité opérationnelle d'ici 2021

- Systèmes de communications hybrides / cellulaires
    - connaissance de la situation 3G / HF dans l'Arctique; échange de données terre-navire indépendant des systèmes satcom embarqués (Fleetrange et KNL Networks)
    - Cellular SA pour une flotte de <100 km en Corée; réseau de communication sans fil haut débit pour les petits navires sans équipement de pointe (LTE-Maritime)
- AMRDS : Autonomous Maritime Radio Devices, sous contrôle réglementaire
    - stations mobiles émettant par radio, indépendamment des navires • Exemples: indicateurs de filets de pêche, balises temporaires sur glace, etc.

4.5. SYSTEMES A TERRE

En complément des systèmes embarqués, les systèmes à terre suivent une évolution comparable basée sur la technologie PNT :

- R-Mode - utilisant les signaux d'opportunité pour fournir une prestation « Positioning Navigation and Timing (PNT) » au nouveau système de Géolocalisation et Navigation par un Système de Satellites (GNSS) (voir : www.accseas.eu)
- eLoran - service PNT terrestre de forte puissance
- Positionnement absolu du radar - fixation de la position à l'aide du radar NT amélioré et des eRacons

Qu'est-ce que le PNT

Le positionnement est la détermination de la position géographique d'une personne, d'un navire ou d'un signal.

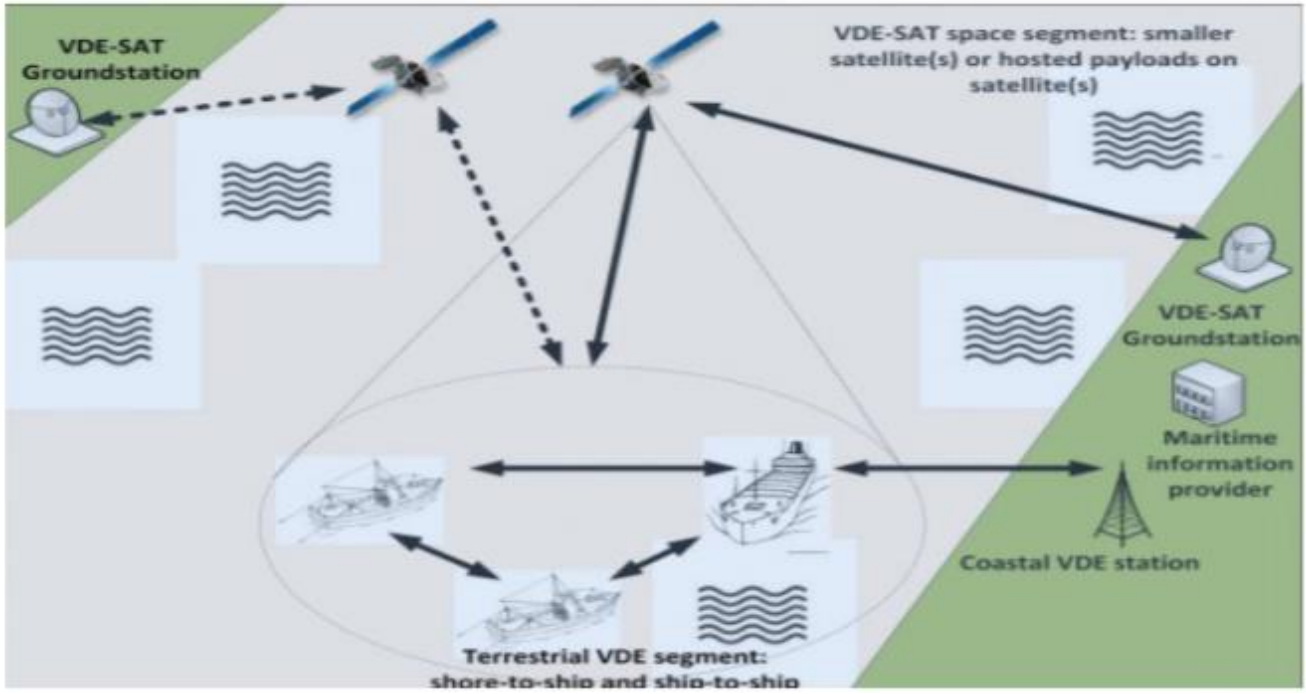
La navigation est un outil qui permet de calculer un itinéraire de la position A à la position B. Enfin, le timing relie les deux éléments ensemble, ce qui permet de déterminer la durée du voyage le long d'un itinéraire ainsi que l'heure locale exacte dans n'importe quel emplacements sur le globe. En utilisant des satellites pour soutenir ce trio d'outils d'information puissants, on a trouvé un moyen de visualiser une sorte de «grille» universelle sur la Terre, un peu comme la latitude et la longitude sur un globe terrestre. Cette grille permet des opérations complexes et des communications par satellite qui dépendent d'heures et d'emplacements précis pour un fonctionnement précis. Avec ces satellites servant de relais pour des informations précises, le PNT permet de modéliser la planète dans son ensemble d'un point de vue distinct.

4.6. La solution VDES - VHF Data Exchange System

Le système d'échange de données VHF (VDES) est un développement des communications radio à l'appui des concepts modernes de navigation électronique (eNAV).

C'est un système de communication à large bande potentiellement nouveau avec une capacité de transfert de données jusqu'à 300 kbps. Le système d'échange de données VHF (VDES), est basé sur le système d'identification automatique (AIS). Il a le potentiel de fournir aux navigateurs du monde entier un système de communication numérique efficace à faible coût.

Il permet ainsi de fournir de nombreuses données aux navires, telles que les informations de sécurité maritime (MSI), les données hydrographiques et environnementales, la protection contre le piratage, la mise à jour et la surveillance des systèmes embarqués (c'est-à-dire les systèmes de surveillance des moteurs et des cargaisons).

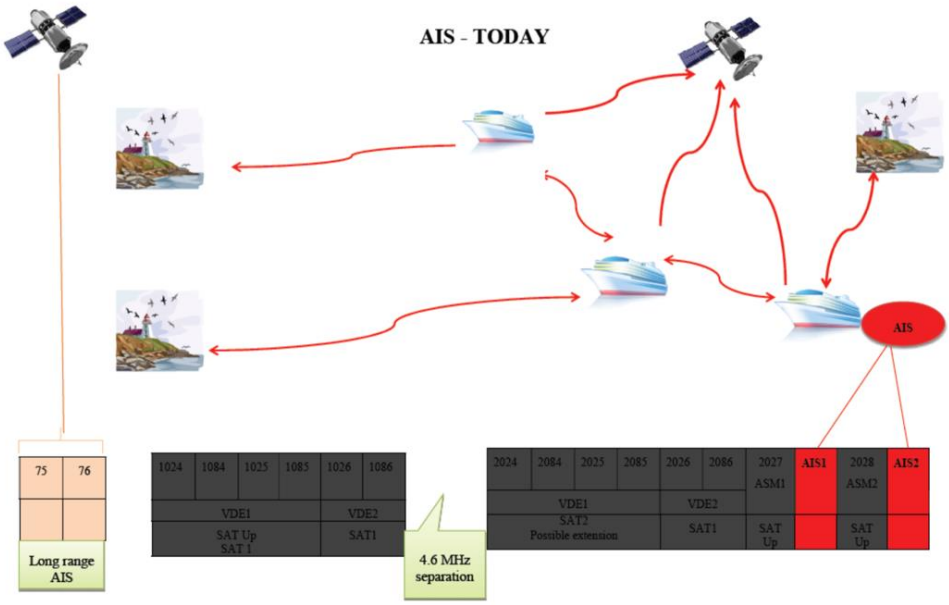


Il comporte de nouveaux canaux pour la messagerie spécifique à l'application (ASM) et de nouveaux canaux pour les données à haute vitesse (VDE)

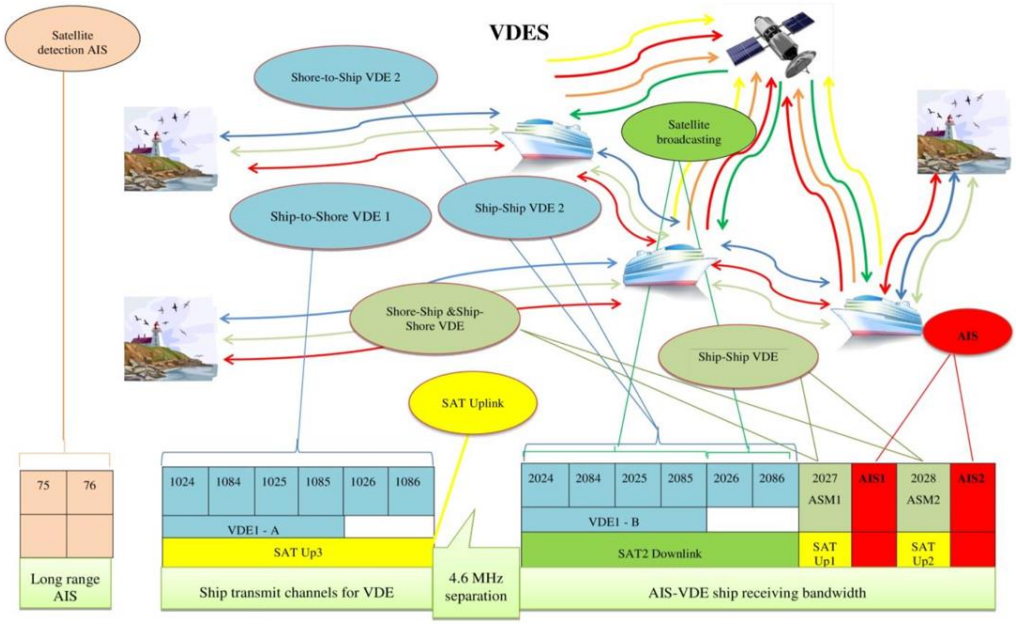
VDES répond au besoin de capacités nouvelles concernant l'échange de données numériques :

- Préserve la fonction d'origine de l'AIS pour l'identification, les rapports de position et le suivi, le soutien aux recherches et au sauvetage, etc.

- Fournit des capacités d'échange de données maritimes pour la sûreté, la sécurité, l'efficacité et la protection de l'environnement
- Fournir des données terrestres et satellitaires avec une interopérabilité et une disponibilité mondiales (y compris les régions polaires)
- Amélioration des débits de données et de la capacité
- Support pour eNav, communication de données maritimes



L'AIS actuellement en service, comparé au maillage du VDES



VDES and e-Navigation

La navigation électronique vise à améliorer la navigation de point à point et les services connexes pour la sûreté et la sécurité en mer et pour la protection du milieu marin.
A travers le VDES les solutions e-Nav prioritaires de l'OMI sont prises en charge:

- Reporting standardisé et automatique
- Utilisation de messages standardisés similaires
- Données statiques étendues : Communication améliorée des services VTS - Informations sur l'itinéraire, intentions de navigation
- Indication de cargaison dangereuse

Il offre fiabilité et résilience ainsi qu'une plus grande intégrité des informations de navigation :

- Données Meteo / Hydro, fenêtres de marée, avis de zone aux marins, données d'accostage, temps de dédouanement pour l'entrée / sortie du port

4.7. La problématique de la cyber-protection

" *It is only natural that the rise in digitalization will be accompanied by concerns of hostile attacks on the ship's systems. A technological breach can leave businesses exposed, risk operational downtime, and potential scrutiny by regulators over compliance policies* ".

Nabil Ben Soussia, Vice President – Maritime at IEC Telecom Group

Les technologies de l'information et de la communication sont l'une des clefs de l'efficience de la surveillance des espaces maritimes. Certaines technologies sont utilisées tant par les entités de contrôle que par les acteurs maritimes contrôlés. Placés à bord des navires, permettant leur localisation et l'émission de données, les dispositifs techniques permettent une communication à destination des navires environnant et des autorités de contrôle. Les systèmes de communication assurent ainsi une veille continue de la navigation, sans pour autant écarter la nécessité d'une veille humaine. Utilisés par les entités de contrôle et de surveillance, publiques et privées, les systèmes de surveillance exploitent les données issues des systèmes de communication. Ils les analysent et permettent une visualisation contextuelle, y compris de la survenance potentielle des menaces et des risques en mer.

Outre le besoin de protéger les réseaux de toute intrusion, la plupart des communications radio sont confidentielles. Toute personne qui capte de telles communications se doit de respecter le secret des échanges. Personne ne peut divulguer le contenu ou même l'existence de toute correspondance émise, reçue ou interceptée par la station sauf au destinataire du message.
Cette restriction ne s'applique pas aux messages de détresse, d'urgence ou de sécurité, ni aux messages destinés à toutes stations ni aux bulletins publics d'avertissement.

Par ailleurs, la généralisation de la télémaintenance n'est pas sans poser de problématique de cyber protection.
La maintenance à distance est de plus en plus utilisée pour éviter des arrêts coûteux du système, qui peuvent sérieusement affecter les opérations. Elle permet une lecture régulière des données qui peuvent ensuite être retransmises au siège social pour analyse et analyse. De plus, nous verrons l'essor de la réalité augmentée (AR), qui permettra aux experts de dépanner à distance.

Par exemple, l'Union européenne (UE) a déjà financé un projet de 6,5 millions d'euros pour des systèmes de ponts AR destinés à améliorer la sécurité et l'efficacité de la navigation à bord des navires.

Il est donc naturel que les systèmes du futur, prévoient d'embarquer également leurs propres système de protection.
Si ces cyber-menaces inquiètent c'est parce qu'aujourd'hui dans un bateau, presque tout est informatisé. Tout est connecté à Internet entre la terre et la mer.
Aujourd'hui il est possible pour un hacker (voire un État) de détourner des informations, de prendre le contrôle d'un navire, de sa cargaison (et cela a déjà été fait par les cartels de la drogue) ou même de son système d'armement.
Les spécialistes en cyber-défense ont identifié deux menaces principales, comme l'espionnage et le sabotage. Un "espion" peut par exemple "voler les données techniques" pour connaître avec précisions le trajet emprunté par un bateau et sa cargaison.
L'angoisse des experts en cyber-défense c'est aussi l'attaque des géants des mers, ces porte-containers géants qui débarquent dans les ports européens. Le plus gros au monde doit transporter 20 000 containers pour une valeur de deux à quatre milliards de dollars. On y trouve tout un tas de systèmes de cartographie, d'informations. Tous ces systèmes-là sont

potentiellement attaquables. "La passerelle peut ne plus avoir la maitrise de sa propulsion et de sa gouverne". "Un hacker pourrait complètement bloquer la barre d'un bateau."

En 2011, l'Agence européenne de cyber-sécurité (ENISA) a publié un premier rapport européen sur la cyber-sécurité maritime. Elle évoquait déjà les menaces qui s'amplifiaient. Elles mettaient en garde sur les conséquences désastreuses de ces cyber-attaques.
La même année, le port d'Anvers (dans lequel des milliers de containers sont débarqués chaque semaine sur les quais) avait été piraté par un cartel de la drogue. Ils avaient réussi à récupérer la marchandise avant que les douanes n'inspectent les containers.

En 2013, un groupe d'étudiants en école d'ingénieurs a fait une expérience en pleine mer : ils ont piraté un yacht de luxe pour le détourner de son trajet initial, en utilisant le système GPS.. C'était en fait un test organisé avec l'accord des propriétaires du bateau. Naviguant de Monaco à l'île de Rhodes, le yacht a été piraté en pleine mer Ionienne. Grâce à un faux boîtier simulateur GPS, ils ont envoyé des signaux de localisation avec de fausses données, des signaux plus forts que ceux transmis par les satellites. Les "faux signaux" se sont donc substitués aux vrais, en les brouillant. Le yacht a alors viré de bord, en modifiant le pilote automatique. "Les armateurs prennent de plus en plus en compte ces menaces", explique Eric Banel, secrétaire général d'Armateurs de France. Les politiques d'entreprises contiennent quasiment toutes un chapitre sur la cyber-criminalité. Quant aux constructeurs navals, comme DCNS qui construisent des bateaux pour la Marine nationale notamment, ils développent des moyens pour faire face à cette cyber-criminalité maritime, avec aussi des experts présents à terre pour surveiller les flux qui transitent entre la terre et le bateau.
L'école navale, Telecom Bretagne, DCNS et Thales se sont associés pour créer, avec le soutien de la région Bretagne, une chaire de cyber-défense des systèmes navals. Le but est de mettre en œuvre toutes les techniques pour lutter contre les menaces du cyberespace. Cette chaire universitaire mais aussi industrielle ambitionne de stimuler la cyber-innovation. Des

chercheurs qui devront trouver des parades à la vulnérabilité des navires en mer, du porte-container au méthanier en passant par les navires de guerre.

La prévention des incidents et attaques informatiques relève pourtant la plupart du temps de réflexes simples, qui concourent à une protection globale du navire. Le Guide des bonnes pratiques de sécurité informatique à bord des navires, dans sa version bilingue français-anglais, adapte aux spécificités du transport maritime le précédent Guide des bonnes pratiques de l'informatique (CPME – ANSSI, mars 2015).

Il est le fruit d'une coopération entre l'ANSSI et la Direction des affaires maritimes (ministère de l'Environnement, de l'Energie et de la Mer) et a bénéficié de la contribution d'une douzaine de compagnies maritimes françaises.

4.8. Les réflexes de base de la cyber-protection maritime

Les principaux conseils à retenir et à mettre en œuvre pour les membres de l'équipage :

- Bien choisir ses mots de passe Un mot de passe de qualité possède au moins 8 caractères de types différents, n'a pas de lien avec l'utilisateur et ne figure pas dans le dictionnaire. Définissez des mots de passe différents pour des systèmes ou des services sensibles distincts. N'enregistrez pas vos mots de passe dans un fichier ou dans un navigateur Internet, notamment en cas d'utilisation d'un équipement public ou partagé. Enfin, au-delà de l'utilisation d'un mot de passe fort, pensez toujours à verrouiller votre session, même lors d'une absence courte, afin d'empêcher tout accès non autorisé à votre poste.

- Utiliser sa messagerie avec vigilance Vérifiez l'identité de l'expéditeur. N'ouvrez pas de pièce jointe et ne cliquez pas sur un lien Internet provenant d'un expéditeur suspect ou inconnu.

- Séparer les usages personnels et professionnels Ne transférez pas vos messages électroniques professionnels vers une messagerie personnelle. N'utilisez pas de

moyens personnels de stockage (clé USB, disque dur externe, cloud…) pour enregistrer vos données professionnelles.

- Être prudent sur internet Réseaux sociaux, forums, formulaires, … : veillez à limiter la diffusion de vos informations personnelles via Internet. Avant un paiement en ligne, vérifiez l'authenticité et le niveau de sécurité du site Internet.

- Sauvegarder régulièrement ses données Anticipez une panne, une perte ou un vol, en sauvegardant régulièrement vos données, au moyen de supports externes dédiés, conservés en lieu sûr.

- Maîtrisez les logiciels installés sur vos équipements informatiques. N'installez que les logiciels dont vous avez réellement besoin, et toujours avec l'aval préalable d'un référent informatique. Ne téléchargez vos logiciels que depuis des sites fiables et effectuez régulièrement les mises à jour.

Les recommandations aux compagnies :

- La sensibilisation de tous les membres de l'équipage et, plus largement, des personnels de la compagnie, aux bonnes pratiques élémentaires de sécurité informatique, est fondamentale pour réduire efficacement les risques liés à de mauvaises pratiques.

- Pour veiller à la sécurité des données à bord, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires). Il sera ainsi possible d'en disposer suite à un dysfonctionnement du système d'exploitation, à une erreur de manipulation ou à une attaque informatique.

- Lorsque l'on accède à un système informatique, que ce soit un PC bureautique ou un système « métier », on bénéficie de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur » et les droits dits « d'administrateur ». Les différents comptes sur les systèmes de bord doivent être créés et gérés avec la plus grande attention.

- Dans chaque logiciel, application ou système d'exploitation, il existe des vulnérabilités potentielles. Une fois découvertes, celles-ci sont corrigées par les éditeurs, qui proposent alors aux utilisateurs des mises à jour de sécurité. Malheureusement, de nombreux utilisateurs ne procèdent pas à ces mises à jour et les attaquants peuvent alors exploiter ces vulnérabilités encore longtemps après leur découverte et leur correction.

- Si l'utilisation du Wi-Fi présente certains bénéfices, il ne faut pas oublier qu'un réseau Wi-Fi insuffisamment ou mal sécurisé peut permettre à des tiers d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes. En escale, la portée du Wi-Fi (une centaine de mètres) peut permettre des connexions non légitimes au réseau du navire depuis la terre.

- Dans un réseau « à plat », c'est-à-dire ne disposant pas d'équipement de filtrage, chaque équipement a la possibilité d'accéder à n'importe quel autre. Ainsi, la compromission d'un seul équipement pourra facilement s'étendre à l'ensemble du réseau. Il est en particulier essentiel de séparer le réseau bureautique connecté à Internet, par nature plus exposé aux attaques informatiques, des réseaux comportant les systèmes « métiers ». Les postes et les serveurs importants, les systèmes de navigation et de commande du navire, etc., doivent être isolés physiquement ou logiquement vis-à-vis les autres systèmes du navire.

= - = - =