TRANSPORT NEW TECH

La révolution numérique dans le transport maritime

26èmes Rencontres du Risk Management | AMRAE 2018

Les intervenants

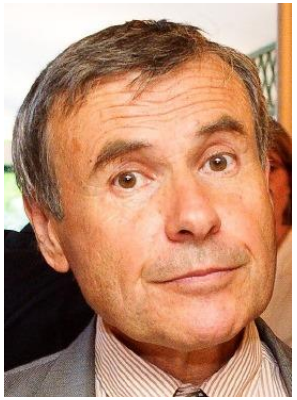
1. Frédéric Moncany de Saint-Aignan
2. Julien Raynaut
3. Pascal Matthey
4. Guy-Louis Fages

Capitaine Frédéric Moncany de Saint-Aignan, Président du Cluster Maritime Français

Julien Raynaut, Directeur Juridique, Bureau Veritas Marine & Offshore

Pascal Matthey, Head Global Marine Risk Engineering, XL CATLIN

Guy-Louis Fages, Responsable Risques et Assurances Trading, Transports, Gaz et Energies Nouvelles, TOTAL

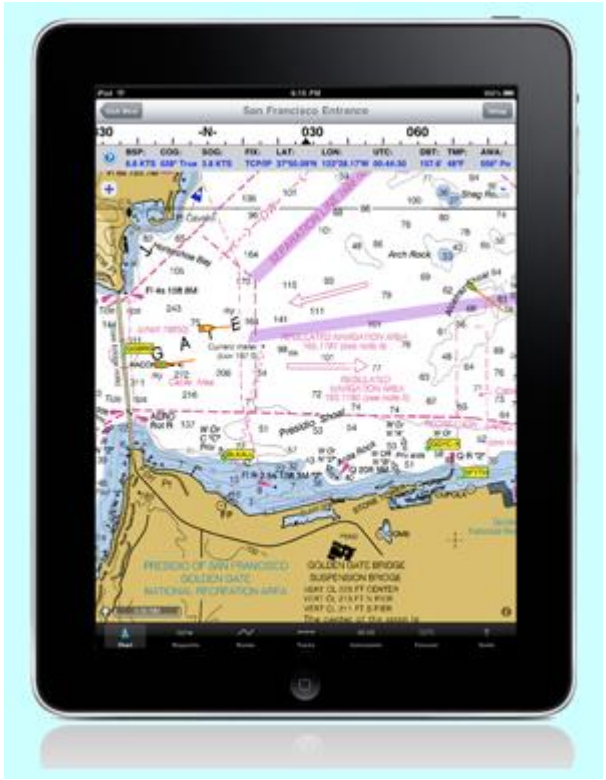


Sommaire

1. Digitalisation
2. Drones Maritimes et Navires Autonomes
3. Cyber-sécurité

1.Digitalisation

1.La digitalisation
Mouvement de dématérialisation avancée
considérations générales

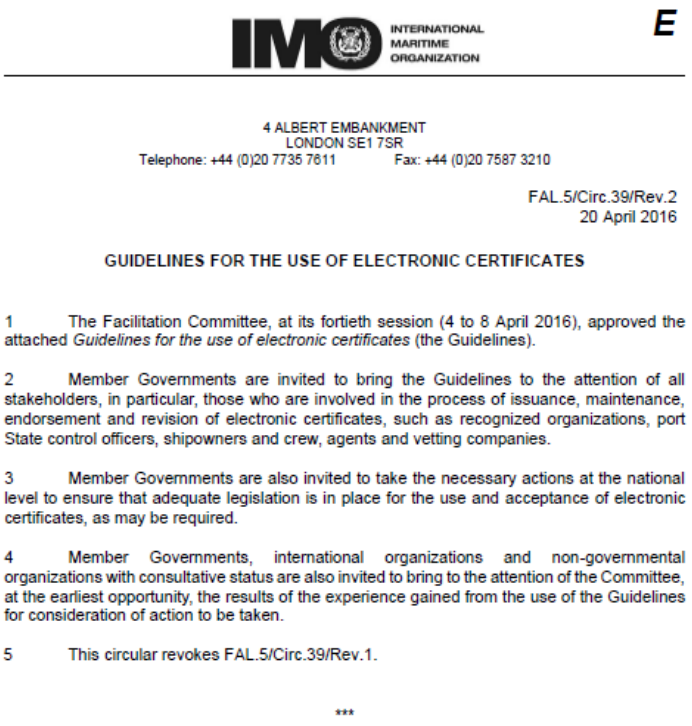


1. La digitalisation
Mouvement de dématérialisation avancée

Le transport maritime et les ports ont toujours évolué puisque les progrès techniques et technologiques sont inhérents à toutes les activités humaines. La modernisation navale semblait néanmoins ralentie à la fin du XX^{e} siècle, avant que plusieurs éléments fassent évoluer les choses. La digitalisation modifie comme ailleurs bien des choses. Les obligations réglementaires, du respect de l'environnement et la hausse du prix des carburants sont les éléments qui pèsent maintenant sur les acteurs et obligent à l'innovation. D'une autre manière, la recherche de la productivité et de la compétitivité dans un contexte de concurrence et de marché dégradé oblige à l'innovation. Dans ce contexte, l'apport de la digitalisation se traduit depuis deux décennies par des changements sur les navires comme dans les ports, modifiant autant le management des outils, le travail des hommes, les processus logistiques et la commercialisation.

1. La digitalisation
Mouvement de dématérialisation avancée
aspects juridiques

1. La dématérialisation en question : réalité du transport maritime
2. Les avancées générées par la dématérialisation
3. Les certificats électroniques



IMO INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

FAL.5/Circ.39/Rev.2
20 April 2016

GUIDELINES FOR THE USE OF ELECTRONIC CERTIFICATES

1 The Facilitation Committee, at its fortieth session (4 to 8 April 2016), approved the attached *Guidelines for the use of electronic certificates* (the Guidelines).

2 Member Governments are invited to bring the Guidelines to the attention of all stakeholders, in particular, those who are involved in the process of issuance, maintenance, endorsement and revision of electronic certificates, such as recognized organizations, port State control officers, shipowners and crew, agents and vetting companies.

3 Member Governments are also invited to take the necessary actions at the national level to ensure that adequate legislation is in place for the use and acceptance of electronic certificates, as may be required.

4 Member Governments, international organizations and non-governmental organizations with consultative status are also invited to bring to the attention of the Committee, at the earliest opportunity, the results of the experience gained from the use of the Guidelines for consideration of action to be taken.

5 This circular revokes FAL.5/Circ.39/Rev.1.

***

1. La digitalisation
Mouvement de dématérialisation avancée
E-Certificate

Electronic certificates by Bureau Veritas Marine & Offshore

Bureau Veritas Marine & Offshore (BV) is issuing e-certificates in conformity with IMO guideline FAL.5/Circ.39/Rev2.

Electronic certificates are issued in lieu of paper certificates following agreement with both the Flag Administration and the ship manager. Once issued, BV e-certificates are:

- sent by email to the recipients agreed with the ship manager
- uploaded to the Veristar Info website and the My Veristar mobile application

This document provides a simple guide to how BV e-certificates can be identified and verified.

BV e-certificates are electronically signed using the latest security technology. The electronic signature is applied by CERT Europe, a third party with expertise in this domain.

The electronic signature may be displayed in different ways depending on the PDF reader used to open the certificate. Below is an illustration of the electronic signature using Adobe reader:

The chosen solution for electronic signature guarantees that:

- The electronic signature applied to the certificates is permanent and can be recognized and verified over time.
- The electronic signature can be verified by the PDF reader even when there is no internet connection as it is contained in the document itself
- BV e-certificates are not signed manually. They contain an electronic stamp, a QR code and a web URL for certificate validity verification *(refer to "How to verify BV e-certificates")*

This document is electronically signed and does not require a manual signature as defined in IMO guideline FAL.5-Circ.39.

Click here for the verification website

BUREAU VERITAS
MARINE & OFFSHORE

surveyor name

By Order of the Secretary

1. La digitalisation
Mouvement de dématérialisation avancée
E-Certificate

How to verifiy BV e-certificates

1

Verify an e-certificate using the verification link in the pdf

Verification of BV e-certificates is simple:
click on the link provided in the PDF. The result will be shown immediately on the verification website.

This document is electronically signed and does not require a manual signature as defined in IMO guideline FAL.5-Circ.39.
Click here for the verification website

2

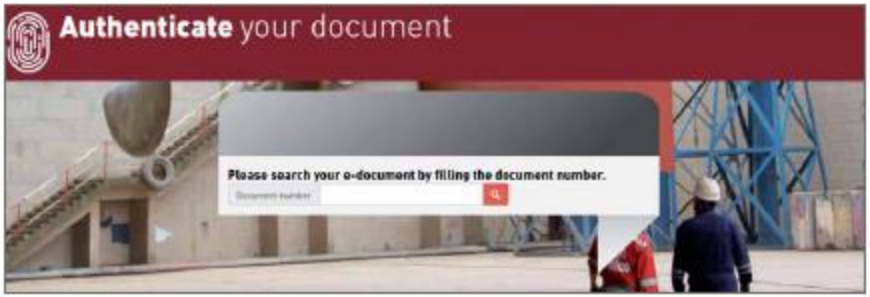
Verify an e-certificate by scanning the QR code

When the e-certificate is printed, it can be verified by scanning the QR code on the document using a QR code reader (available in app stores).

3

Verify an e-certificate using the certificate reference number

You can also check certificate validity by accessing the verification website from this URL https://ecertificates-marine.bureauveritas.com/. Once connected, enter the document reference.to verify validity.



1. La digitalisation
Mouvement de dématérialisation avancée
la vision de l'assurance

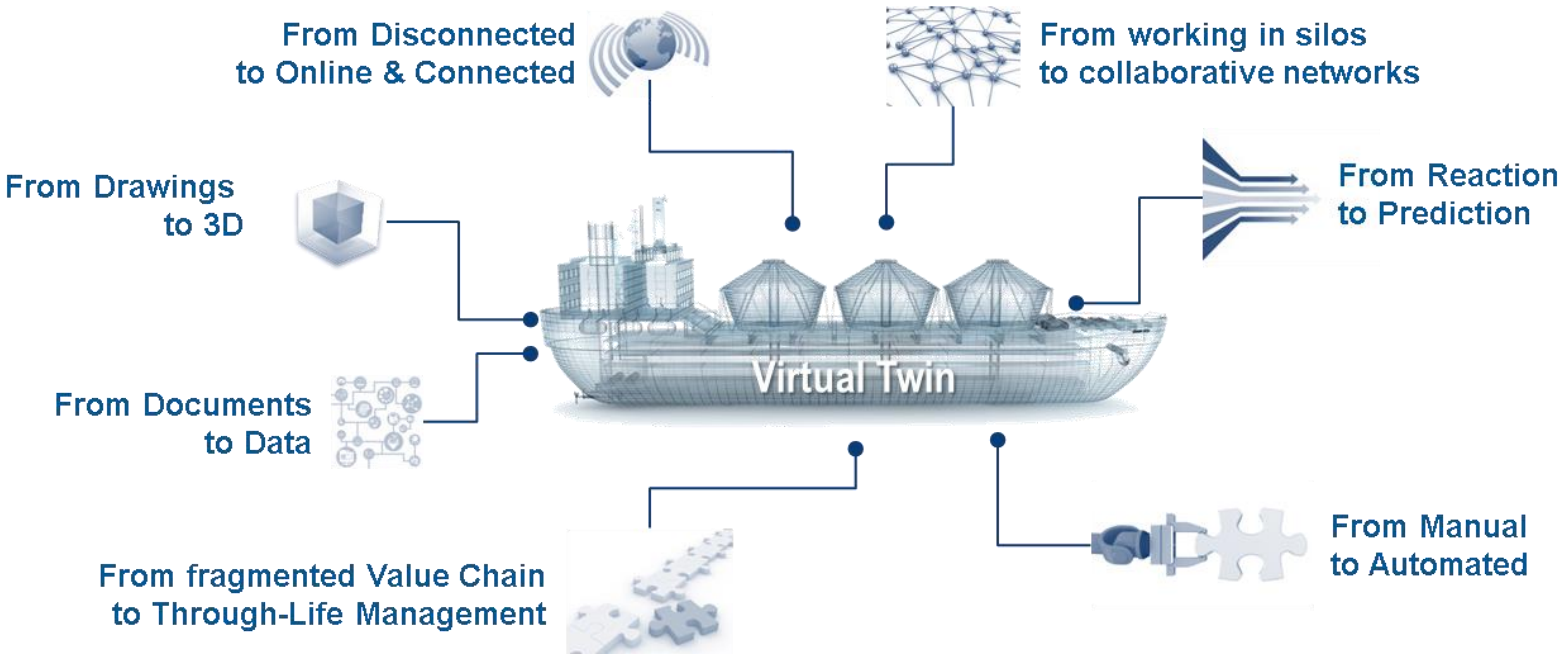
- Plateformes communes Assuré/Courtier/Assureur
- Certificats d'assurance
- Accréditifs bancaires
- Procédures douanières
- Gestion des sinistres
- Fraudes / Contrefaçons

Aller plus loin dans la révolution digitale - considérations générales

Aller plus loin dans la révolution digitale – focus sur l'AIMS 3D

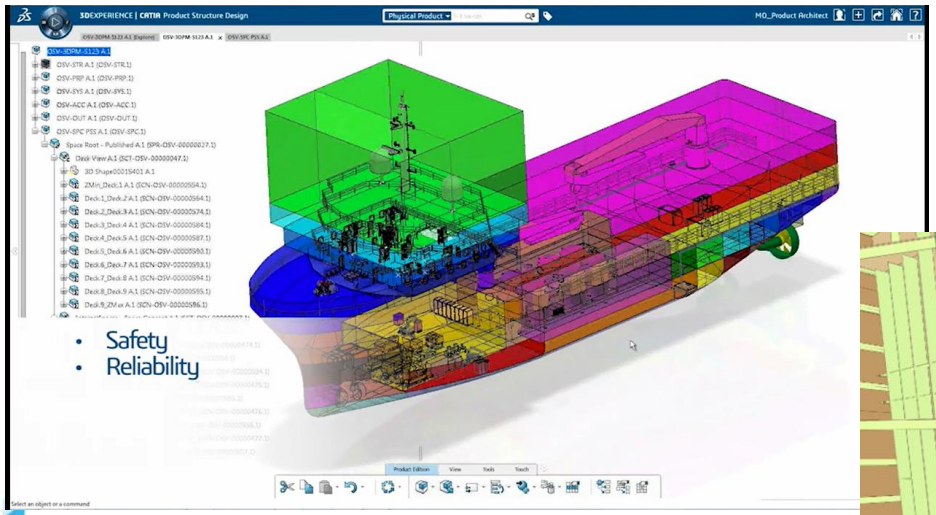
1. Technologie de digitalisation 3D : vers le jumeau numérique (Asset Integrity Management System)
2. La révolution digitale vers l'intelligence artificielle
3. Inspections ciblées / maintenance prédictive
4. Gestion modernisée de son infrastructure

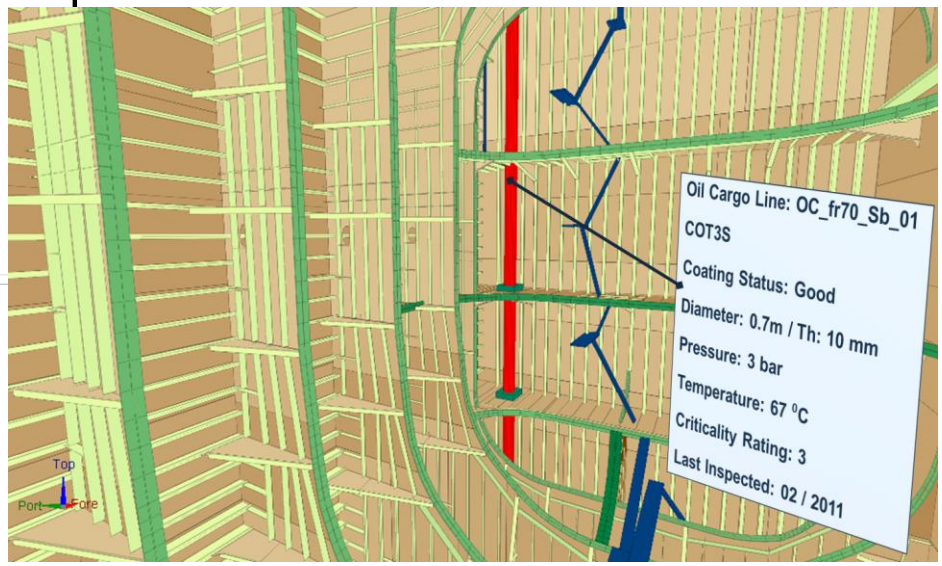
Aller plus loin dans la révolution digitale – focus sur l'AIMS 3D



Aller plus loin dans la révolution digitale – focus sur l'AIMS 3D

3D MODEL & SMART DATA





Aller plus loin dans la révolution digitale – focus sur l'AIMS 3D

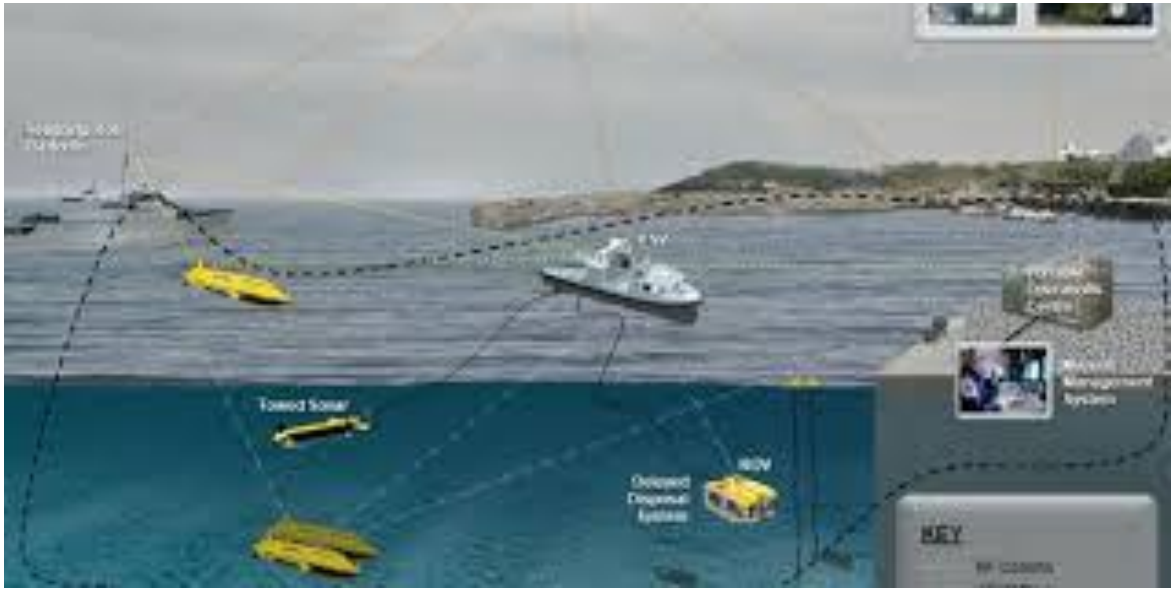
Key benefits

Aller plus loin dans la révolution digitale – vision de l'assurance

- **Logistique 4.0**
  - Interconnexion des objets
  - Flux dématérialisés
  - Terminaux autonomes
  - Traçage intelligent
- **La fin des INCOTERMS ?**
- **Redessiner la cartographie des risques**

2. Drones maritimes et Navires Autonomes

Drones Maritimes - considérations générales



Drones Maritimes - considérations juridiques

1. Définitions : le drone marin ou maritime (« **Unmanned Maritime Vessel** »)
2. Ancêtre du drone : le ROV – Remote Operated Vehicule (offshore)
3. **Classification** des drones maritimes
4. **Règlementation inadaptée** : question de l'applicabilité des conventions internationales (COLREG, SOLAS, Code ISM, STCW, LLMC etc)
5. **Responsabilités et Risques**

Drones Maritimes - vision de l'assurance

- **Outils de travail**
  - Assurances techniques
  - Couverture de l'objet
  - Prévention d'autres risques

- **Moyen de transport**
  - Risque émergent
  - Couverture de l'objet, des responsabilités et des cyber-risques
  - Limites de responsabilité

Navires Autonomes- considérations générales

1. Le Navire Autonome : une automatisation ancienne
2. Que sont les Navires Autonomes?
3. Le point de vue des Armateurs sur le Navire Autonome

Navires Autonomes- considérations juridiques

1. Définition du navire autonome (« Autonomous Surface Vessel »)
2. Absence de cadre réglementaire identique aux UMS
3. Aboutissement de la révolution digitale : parallèle avec les « driverless cars »
4. Impératifs de sécurité maritime « **BV Guidelines for Aunotomous Shipping** » Dec 2017

Navires Autonomes- considérations juridiques

Table 1 : Ship categories and level of autonomy

Ship category	Level of autonomy		Manned	Method of control	Authority to make decisions	Actions initiated by
Conventional	0	Human operated	Yes	Automated or manual operations are under human control	Human	Human
Smart	1	Human directed	Yes/No	Decision support Human makes decisions and actions	Human	Human
Autonomous	2	Human delegated	Yes/No	Human must confirm decisions	Human	System
	3	Human supervised	Yes/No	System is not expecting confirmation Human is always informed of the decisions and actions	Software	System
	4	Fully autonomous	No	System is not expecting confirmation Human is informed only in case of emergency	Software	System
Note 1: Definitions of the level of autonomy are given in Sec 2, Tab 16						

Navires Autonomes- BV Guidelines

Guidelines for Autonomous Shipping

December 2017

Guidance Note
NI 641 DT R00 E

Marine & Offshore
92937 Paris la Défense Cedex – France
Tel: + 33 (0)1 55 24 70 00
Website: http://www.veristar.com
Email: veristarinfo@bureauveritas.com

1.2 Scope of the guidelines

1.2.1 This Guidance Note sets out the main recommendations for the design or the operation of systems which may be used to enhance the autonomy in the shipping.

1.2.2 This Guidance Note is mainly focused on surface units which may be considered as a ship by the authorities (e.g. Maritime Autonomous Surface Ships of 500 GT or more). This excludes small ships (typically length less than 20 m) and unmanned underwater vehicles.

2.1.2 The threats for autonomous ships are very similar to those for conventional ships, but in addition new threats may arise from the reduction or absence of crew aboard. They are mainly coming from the environment, other ships in its vicinity and operations of the considered ship.

Compared to conventional ships, the management of the risks is transfered from the crew aboard to the sensors and the software and ultimately to the supervisors onshore.

2.1.3 It is required that autonomous or remotely controlled ships should be at least as safe as a conventional ship having the same purpose or design (e.g. carrying cargo or passengers).

For safe operations, autonomous ships should not be a source of danger to themself, to the other ships around, to the maritime infrastructures and to the marine environment.

Navires Autonomes- BV Guidelines

2 Safety and security conditions

2.1 General

2.1.1 To achieve an acceptable level of safety and security the general principles behind the recommendations contained in this Guidance Note are given in [2.2] to [2.7].

2.1.2 The threats for autonomous ships are very similar to those for conventional ships, but in addition new threats may arise from the reduction or absence of crew aboard. They are mainly coming from the environment, other ships in its vicinity and operations of the considered ship.

Compared to conventional ships, the management of the risks is transfered from the crew aboard to the sensors and the software and ultimately to the supervisors onshore.

2.1.3 It is required that autonomous or remotely controlled ships should be at least as safe as a conventional ship having the same purpose or design (e.g. carrying cargo or passengers).

For safe operations, autonomous ships should not be a source of danger to themself, to the other ships around, to the maritime infrastructures and to the marine environment.

2.2 Main ship capabilities

2.2.1 The autonomous ships should be capable of:

- managing a pre-defined voyage plan and updating it in real-time if relevant
- navigating according to the predefined voyage plan and avoid collisions with obstacles coming from the traffic or unexpected objects
- keeping a sufficient level of manoeuvrability and stability in various sea states
- withstanding unauthorized physical or virtual trespassing.

2.2.2 The autonomous ships should be designed to authorize a human to come aboard for controlling the ship, for example when a critical situation arises (e.g. fire, flooding, loss of propulsion etc).

During the sea trials or for survey in service, the autonomous ships should be designed to accept the presence of a human aboard or in their vicinity.

Regardless of the possibility of a remote control, the autonomous ships should be designed to be controlled aboard by either a portable device (e.g. laptop) or by a built-in control system.

The possibility for a human to take the control aboard should be granted only to the authorized personnel, in particular when the autonomous ships carry passengers.

A passenger of autonomous ships should have the possibility to activate an emergency push button in case of critical situation (e.g. passenger overboard, obstacle during docking).

Navires Autonomes- vision de l'assurance

120 TEU
électrique

6400 TEU
diesel

- Ce navire qui n'en était pas un….
- Statut légal
- Innavigable = Inassurable !

Navires Autonomes - vision de l'assurance

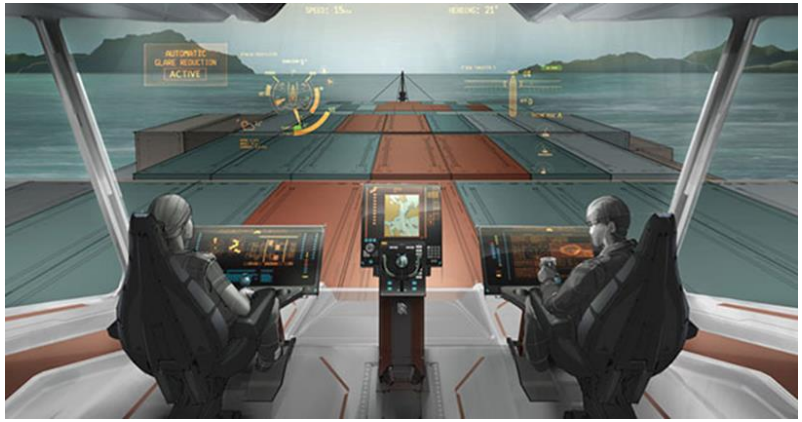
- Plus de 80% des accidents en mer ont une cause humaine
  - Fatigue
  - Mauvaise communication
  - Formation incomplète
  - Erreurs d'interprétation

- Les statistiques ne mentionnent pas les accidents évités par l'homme
  - Pannes techniques
  - Collisions
  - Incendie
  - Sauvetage en mer

3. Cyber - Sécurité

Cyber-Sécurité - considérations générales

1. Facteurs Humains
2. Security by Design
3. Comité France Maritime – Fédération autour de la Cyber-sécurité maritime



Cyber-Sécurité - considérations juridiques

1. Définitions du terme cyber-sécurité
2. Le cadre juridique et réglementaire existant
3. La cyber-conscience: vers une Certification Cyber des Navires ?
4. La cyber-navigabilité
5. Les cyber-responsabilités

Cyber-Sécurité – Guidelines BIMCO

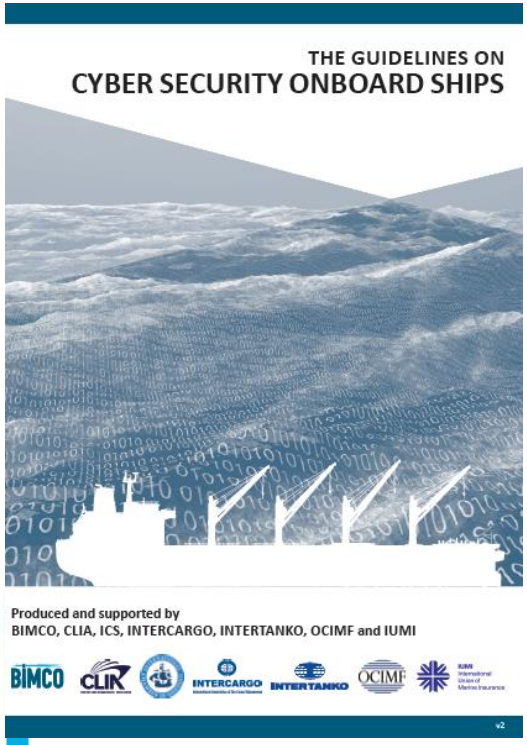
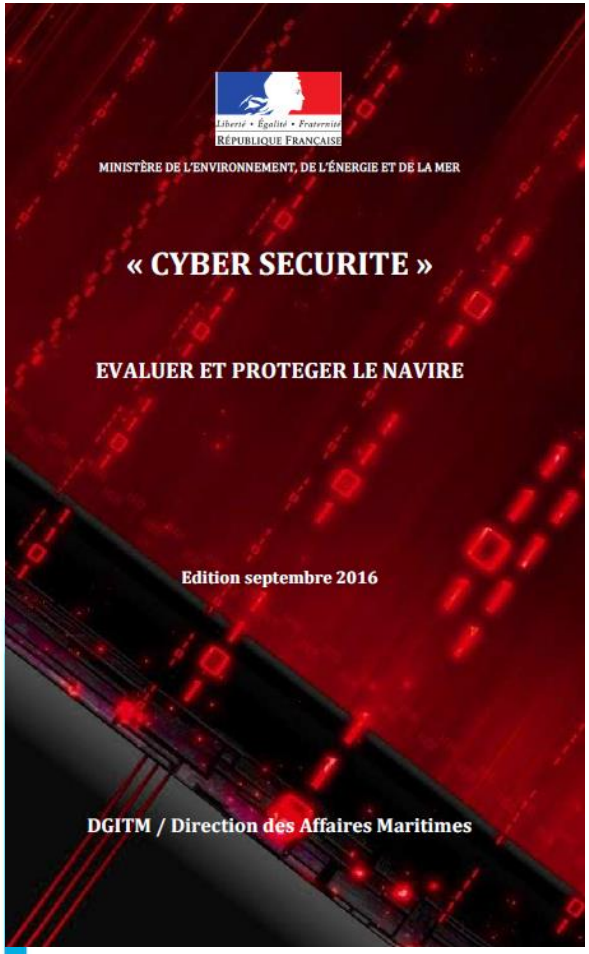
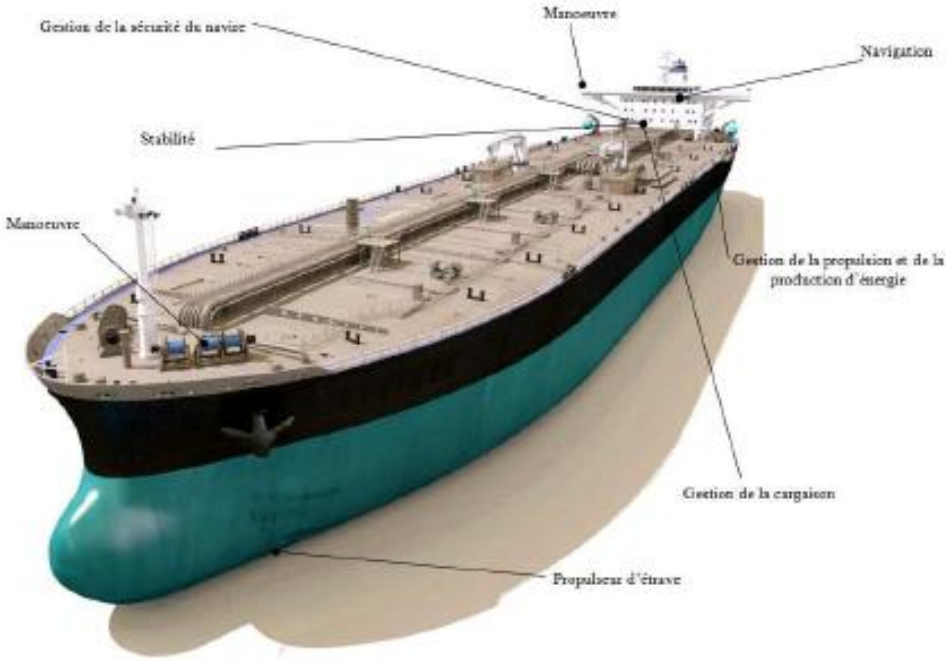


Figure 1. Cyber security approach as set out in the guidelines

Cyber-Sécurité – Affaires Maritimes



Ces 3 dernières années, les systèmes de positionnement automatique et par satellite, le système de cartographie ECDIS (Electronic Charts Display Information System), le système d'enregistrement des données (Voyage Data Recorder) ont fait l'objet d'analyses. Ces dernières ont révélé plusieurs failles numériques à corriger. Plusieurs équipements apparaissent ainsi sensibles à une cyber attaque. La description des éléments de la vulnérabilité du navire est reprise au niveau de l'**annexe N°1** du document.



Cyber-Sécurité – Affaires Maritimes

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE
L'ENVIRONNEMENT, DE
L'ÉNERGIE ET DE LA MER

DGITM

Direction des Affaires Maritimes

- CYBER SECURITE -

renforcer le niveau de protection du navire

Pour aller plus loin :
www.ssi.gouv.fr

Objectif principal :

Sensibiliser les compagnies maritimes aux cybers menaces à bord du navire.

Des vulnérabilités …

- La vulnérabilité des systèmes embarqués et la dépendance du navire à ces systèmes,
- L'inter connectivité des systèmes d'information à bord du navire et vers l'extérieur,
- Le développement des moyens nomade,
- La non mise en œuvre de plan de sécurité de l'information et de plan de continuité d'activité à bord du navire,
- Le manque de formation de l'équipage pour évaluer un acte de malveillance.

… Des risques

- La dégradation de l'image de la compagnie pouvant aboutir à une perte de compétitivité de la compagnie,
- Le sabotage du navire par système dormant ou opéré sur demande pouvant aboutir à la perte du navire, la perte de l'équipage ou l'atteinte à l'environnement.

Cyber-Sécurité – vision de l'assurance

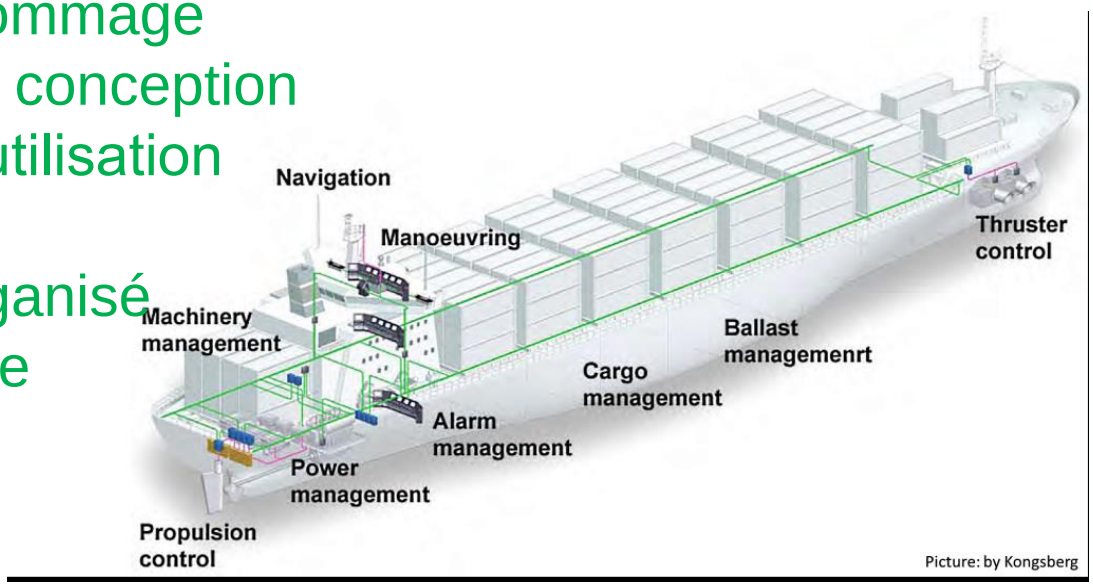
- Approche multi-branches
  - Energie
  - Corps
  - Facultés
  - Responsabilités
  - Informatique

- Assurances corps
  - Exclusion (CL380)

- Assurance facultés
  - Exclusions (CL380)
  - Exclusions (JSC2015/005)

Cyber-Sécurité – vision de l'assurance

- Origine du dommage
  - Erreur de conception
  - Erreur d'utilisation
  - Piratage
  - Crime organisé
  - Terrorisme



- Aujourd'hui
  - La plupart des dommages sont causés par des erreurs et omissions

- Demain
  - L'interconnection,un boulevard du crime ?

Cyber-Sécurité – vision de l'assurance

- Risque émergent
  - Analyse des causes
  - Etude des conséquences
  - Risque systémique
    - USD 400 mia/année

- Existence d'un marché ?

Cyber-Sécurité – vision de l'assurance

- ….utilisation d'un ordinateur, d'un virus ou d'un code malveillant….dans le but de causer un dommage.

- ….couverture (éventuellement) rétablie pour les vols commis à l'aide d'un système électronique utilisé dans ce dessein.
- terrorisme en général couvert pendant le transport

Conclusion