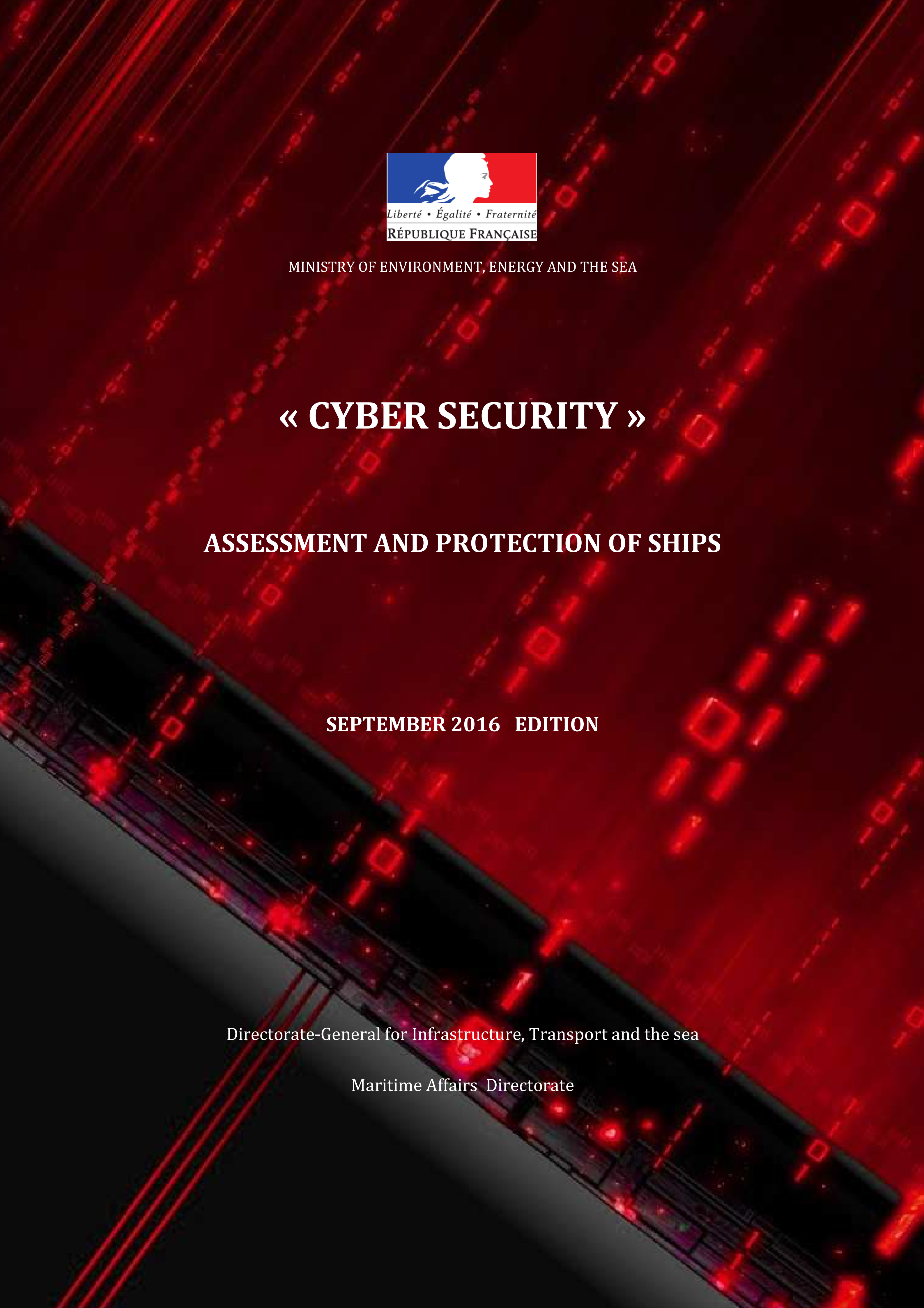


Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTRY OF ENVIRONMENT, ENERGY AND THE SEA

« CYBER SECURITY »

ASSESSMENT AND PROTECTION OF SHIPS

SEPTEMBER 2016 EDITION

Directorate-General for Infrastructure, Transport and the sea

Maritime Affairs Directorate

Table of contents

STUXNET, SHAMOON STUXNET, SHAMOON, DUQU, DRAGONFLY (HAVEX), GAUSS, FLAME, SANDWORM, IRONGATE… this “Prévert-style inventory” resembles an arsenal of cyber weapons that gives the officials in charge of the industrial control systems security (ICS) the chills. Now well know and discovered in 2010, the first cyber weapon, STUXNET has partially destroyed the Iranian nuclear programme. Thereafter, the derivatives of this new technological weapon have worked to destroy 30 000 computers of the oil company SAUDI ARAMCO. This digital arsenal chase has raised awareness of the reality of the threats of cyber sabotage, cyber terrorism and cyber espionage.

Henceforth, we can reasonably ask the question of the digital vulnerability of ships. Can the remote takeover of an oil tanker be feasible ? Fiction ? Reality ? Until now only terrestrial, maritime and port infrastructures seem concerned. In 2011, the port of Anvers detected an anomaly in its container management system. The investigation concluded to “cyber-concealing” of several containers from South America.

Ships are a means of transport amongst many other, long known as being apart from the web connections. However are they totally out of the “triangle of motivation” of the cyber threat : money theft, sensitive data theft, activism/terrorist acts ? The Maritime Affairs Directorate (DAM) wished, a year ago, to analyse the vulnerability of ships to the digital threat.

This document resulting from the exploitation of data collected during a survey carried out on board sixty eight ships, will not bring you the ultimate high technology tool against an act of cybercrime. Nevertheless, this survey indicates the guidelines to follow in order to set up a management of communications and information systems security on board ships.

Based on the good practices observed, these propositions will help to improve the security and safety management on board ships, in accordance with IMO directives and the recent circular MSC.1/Circ.1526 of 1 June 2016 – para1.1.8.

I invite you to take charge of these recommendations to preserve your ship and our environment against a digital malicious act.

Thierry COQUIL

Maritime Affairs Director

A- SHIPS IN CYBER SPACE

Early March 2016, the company VERIZON specialised in the conception, construction and analysis of networks provided in the 2016 report regarding 100 00 accidents, including the analysis of 2 260 compromised data in 82 countries. This report illustrates two interesting scenarios. One concerns the mysterious and unexplained manipulation of machines controlling the treatment process of a water station. The other describes a malicious act against a maritime company. The hackers got into a "web shell" in the company's network and established a precious merchandise list transported on board the ship. From this, all there was to do was to send a team on board the ships to collect the real merchandise. The criminal group committed several errors which enables the company VERIZON to identify the threat. The maritime company has since reinforced its security measures, including the execution of routine vulnerability analysis of its software to face future digital attacks. This last illustration demonstrates that the maritime world is no longer totally safe from malicious acts via its information system management. This threat will heighten with the generalisation of the setting up of beacons on high value containers (company Traxens).

It is therefore important to address this threat and to face it.

A1- DIGITALISATION OF THE MARITIME WORLD

Firstly, it seems necessary to recall the context of this type of transport. Sea trade is today essential and indispensable to our global economy. Every country is now interdependent of trades that are mainly carried out by sea. Almost 50 000 ships and one million seafarers participate in this worldwide trade. In this trading context, the digital field has constantly grown the last 25 years on board commercial vessels. The computing world is nowadays omnipresent on board. This technology regulates communications as well as the control and management of the ship's cargo.

This technological transformation of the commercial ship has deeply changed the way it is managed. Nowadays exchanges happen daily between the ship, the company, the port, the maritime agent… The ship no longer benefits from an "air gap" type digital security level, consisting in physically isolating it from all digital networks. The ship naturally connects to this planetary web of networks.

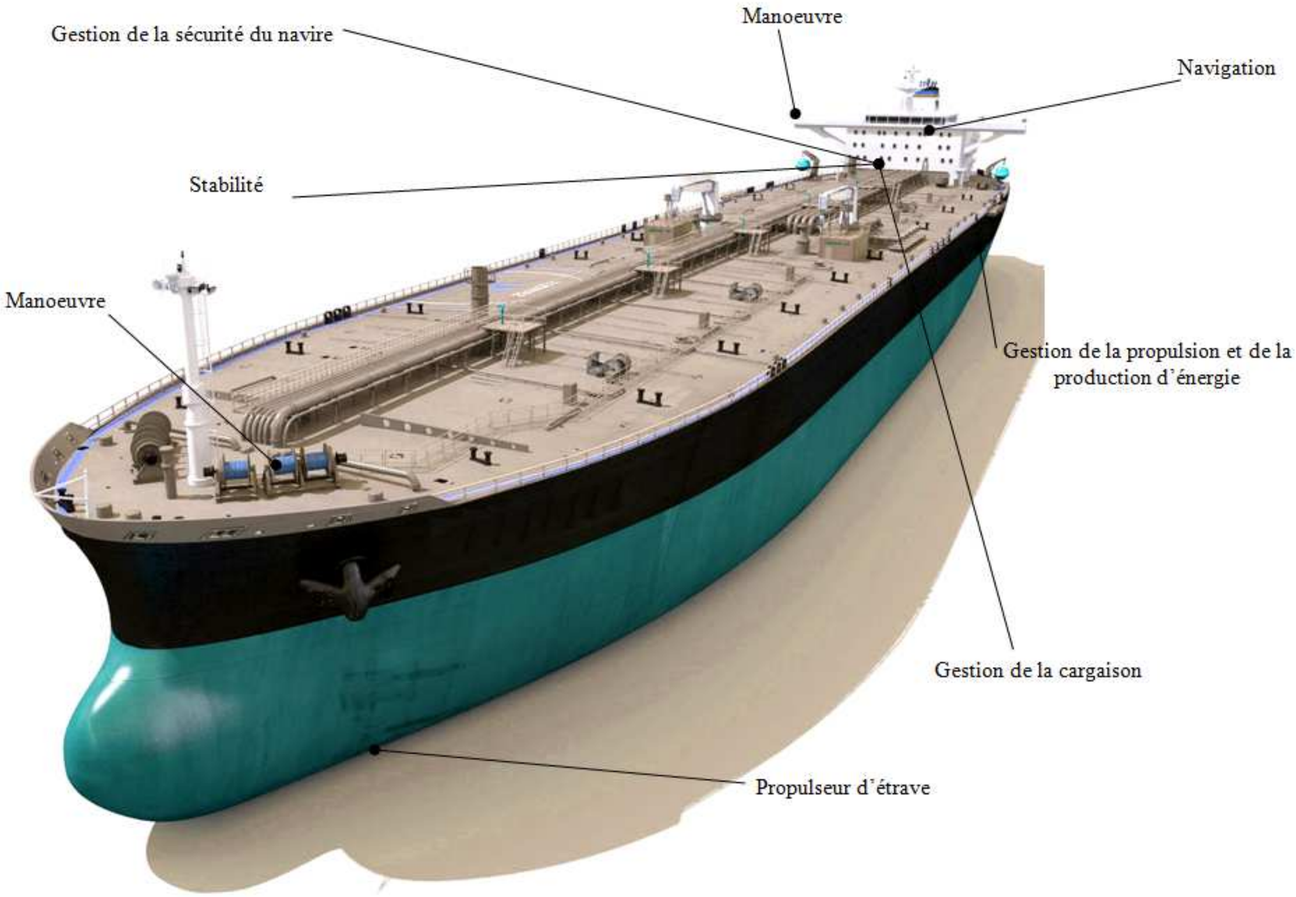
Our ship has now become a complex ensemble of industrial systems. The running of systems is unfortunately not exempt from digital faults. Onboard systems can therefore be the entry point for a malicious act. These simple observations demonstrate that the ship can be vulnerable to a malicious act that can impact on:

- **A breach of the company's image** (offensive intelligence act),
- **The ship's commercial cyber espionage** (10% of the world's attacks),
- **The ship's cyber sabotage**,
- **Cybercrime** (two third of attacks worldwide).

Even though malicious acts against a ship remain very limited today, it is still necessary to protect it. Protecting a ship means preserving the operational and organisational means of this type of transport. The final goals aim at ensuring that no malicious act can jeopardise the running and operation of the ship.

A2- SPECIFIC VULNERABILITIÉS OF SHIPS

The last 3 years, the global navigational satellite systems (GNSS), the Electronic charts display information system (ECDIS), the Voyage Data Recorder (VDR), have been analysed. They have uncovered several digital flaws needing correction. Several equipment seem particularly sensitive to a cyber-attack. The description of the vulnerability elements is mentioned in **appendix n° 1** of the document.


Gestion de la sécurité du navire
Manoeuvre
Navigation
Stabilité
Manoeuvre
Gestion de la propulsion et de la production d'énergie
Gestion de la cargaison
Propulseur d'étrave

B- SURVEY ON SHIP'S CYBER SECURITY

In order to put in place a risk-based security approach for ships' information systems (IT), it is important to be able to correctly identify the values and the goods to protect. This implies a rigorous approach according to the type of ship and its exploitation.

To this day, only the international code for the security of ships and the port installations (ISPS code) defines a recommendation relating to the digital processing management. This code states that the vulnerability of the digital system should be the subject of an assessment in the framework of the ship's security in order to arrange an adequate measure to a possible threat.

It is in this context that the Maritime Affairs Directorate has put in place an assessment process of the level of the ship's cyber security. The latter is determined through a survey carried out over the period of one year on board ships flying French flag and a extensive ship audit carried out by the French Network and Information Security Agency (ANSSI).

B1- NATURE OF THE SURVEY

The considering of the ship's vital sectors and basic security hygiene measures of the ship's information systems have led to the defining of 9 items (**Appendix n° 2**):

(1) Generalities on the management of the ship's Information System Security (ISS),
(2) Location of the IT/OT on board the ship,
(3) Protection of information sharing with the outside,
(4) Access management,
(5) Updates and renewal of software,
(6) Definitions of users,
(7) Regular data backups,
(8) ISS incidents,
(9) Control of ship's ISS activity.

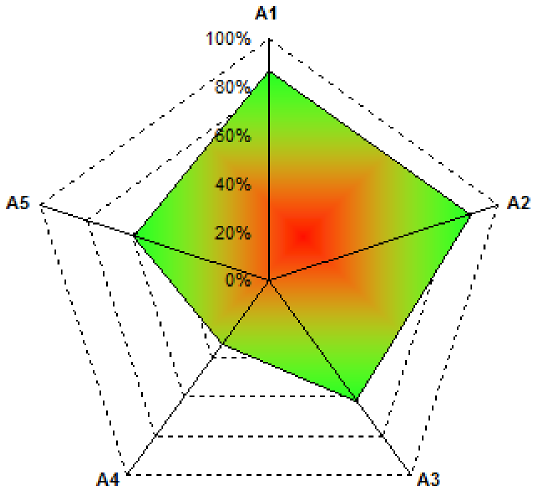
These nine items propose a group of 34 closed questions that allow a direct and simple response processing.

This survey was conducted on board 68 ships under French flag with a certification in terms of security. These ships represent 26 French companies.

B2- SURVEY ANALYSIS

Survey ‘s questions are referenced on appendix n°2.

GENERALITY ON MANAGEMENT OF THE SHIP’S ISS:



Extract from the analysis:

In general, this survey shows that French companies, on the one hand, rely on an internal service to manage the ship’s information system and on the other hand, have a company policy in terms of information system management. However, it is important to note that this policy is, in general, very incomplete with regards to the two following items:

- The person in charge on board the ship is only defined in 62% of cases (captain, chief engineer, electronic engineer, purser),
- The hardware and software list mapping of the ship is only classified in 59% of cases,

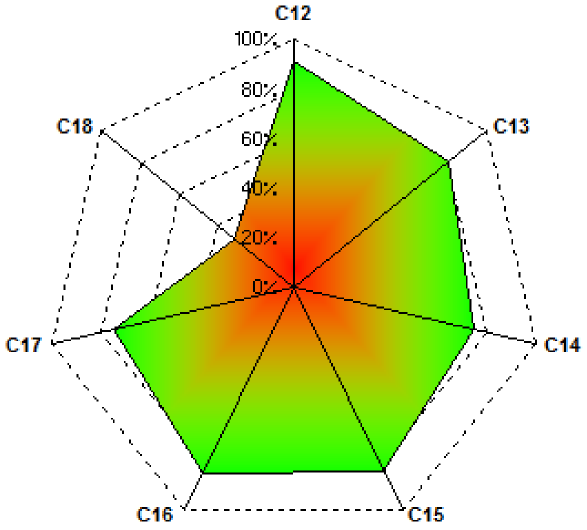
The sensitive item of this section shows that only 32% of surveyed ships were subjected to a ship’s information system risk assessment. The nature of this assessment was not subject to an analysis for the 20 ships that positively replied to this question.

Finally, in addition, it should be noted that around 79% of surveyed ships carry out a remote maintenance between ship and shore.

<u>LOCATION OF INFORMATION SYSTEMS ON BOARD SHIPS</u>:

Apart from a few exceptions, the whole information systems are located in the ship's restricted areas, as defined on the ship's security plan.

<u>PROTECTION OF INFORMATION SHARING WITH THE OUTSIDE</u>:



<u>Extract from the analysis:</u>

This section allows to distinguish 4 elements:

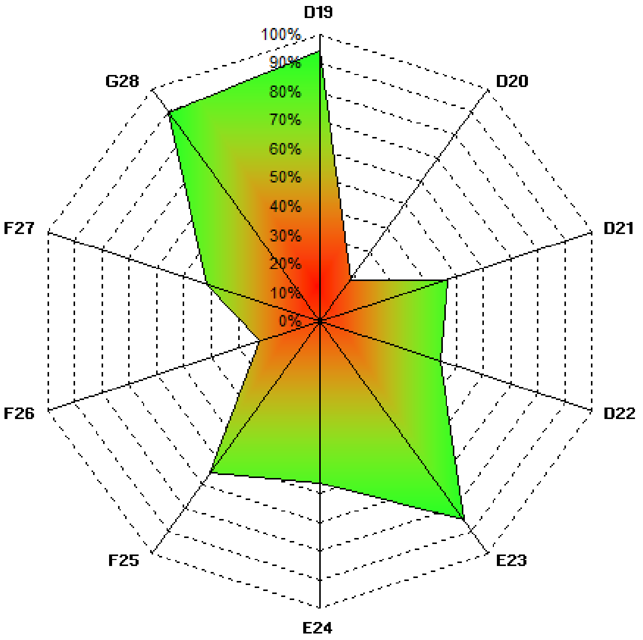
- The first shows that a third of the surveyed ships have an internet connection on critical information systems (networks linked to navigation, propulsion, the ship's energy management, cargo management). These vital systems have two third of the time a direct connection via a USB port (questions C10/C11 are not shown on the graph).

- The second point concerns the management of data analysis. 91% of surveyed ships use an antivirus software allowing the network data analysis and external data analysis via a USB port> the downloaded data are not automatically executed in 84% of cases.

- The third point confirms the presence of a WIFI system on board ships (75% of surveyed ships). This system is unfortunately not always secure.

- Finally, the fourth element to remember in this section concerns the fact that **in 31% of cases, it is possible to link a personal device to the ship's networks.**

GOOD PRACTICES IN HANDLING INFORMATION (PASSWORDS, ACCESS, SOFTWARE, BACKUP):



Extract from the analysis:

Sections 4 to 7 of the survey illustrate the information systems management of the ship by the crew. The positive points of this section concern the use, almost systematic, of passwords to access a network, the regular updating of the ship's software and the data backup. This management is very largely supported by the company's IT department. However, in breaking this section more closely, the following sensitive points arise:

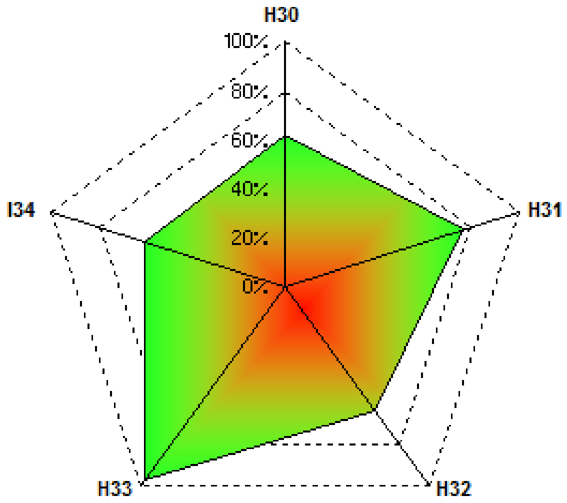
- Passwords management: **the frequency of their updating and their format are not suitable**. In only 18% of cases, the password is changed with a frequency varying from 6 months to 3 years. These passwords are not complex in 47% cases,

- The software used on board the surveyed ships are regularly updated. Updates on the official editor site are carried out in one in two cases,

- **Management of access rights on board the ship seems more concerning and poorly controlled**. In only 22% of cases, internet access or electronic mail viewing from an administrator account is impossible. Moreover, one in two ships have an anonymous account with access to the networks,

- Finally, data backups are carried out following a varying frequency in accordance with company practises: daily to monthly. It must be noted that using a backup platform like "cloud" is still very rare today: 10% of the surveyed ships indicated that they used this type of data backups for the ship.

INCIDENTS AND CONTROL OF THE SHIP'S SSI ACTIVITIES:



Extract from the analysis:

This last section illustrates the fact that very few ships declare having been the target of a malicious act. Only two ships declared having had to deal with a virus on the information network. Nevertheless, this information remains for information only as a ship could have been attacked without acknowledging it.

The principal lesson to learn from this section concerns the fact that French companies seem alerted to the management of a malicious act. Measures are obviously perfectible. Nevertheless, the idea of the recovery of the ship is taken into consideration. Therefore :

- 62% of the surveyed ships have a contingency plan in case of degradation of the ship's information system,
- In 76% of cases, it is necessary to look for the cause of the incident.

The axis for improvement are to be searched at the surveillance level of an abnormal activity of the information management system of the ship and the setting up of an activity auto control system for shipboard information systems. The survey shows that these controls are carried out in 60% of cases. The company's IT service is generally in charge of these controls or audits of the ship's information system.

C- SHIP'S PROTECTION TOOLS

The information system security (ISS) is based on 3 principles: confidentiality, integrity and availability. The last two points are key elements for the ship's management. Therefore, regardless of the deliberate malicious act, it is important to ensure the ship's continuous running : Ensure the continuous running by the defining shipboard critical networks. These networks correspond to the following definitions:

- Critical networks: networks linked to navigation, propulsion, the power management, cargo management, passenger's management and alarms management should be classified as "critical",

- Non-controlled networks: these networks are not subjected to a security surveillance from the ship or the company (Wi-Fi network of a passenger ship). It is nevertheless necessary to verify the partition of the different networks onboard the ship.

Tools to implement in the framework of information protection security on board the ship are threefold **: technological tools, management tools and training.**

C1-TECHNOLOGICAL TOOLS

The technological tools must answer to 4 requirements in terms of best practices :

- Manage the network's architecture,
- Manage the access authentication and authorisation,
- Manage the change and updating of the information systems security,
- Hardening configurations,

The data protection on board a merchant vessel does not require the same level approach as a warship. The strategy of an efficient cyber protection of a civilian ship can therefore use simple and cost effective means available on the market. The combination of technological tools to set up can be the following:

- **Antivirus**: this system does not correspond to an absolute protection. Nevertheless, this system is a pre-requisite that must be updated in order to dispose of the identified malware signature,

- **Firewall**: this tool enables to authorise only the legitimate flows to transit on the network. The first approach of a digital pirate will be to detect potential targets. If all doors are shut, the address will not be processed : the computer is therefore invisible to pirates,

- **VPN (Virtual Private Network)**: a VPN connexion is also called "tunnel". This system creates a protection envelop for all information transiting by its intermediary. As a complement, the VPN masks the connected computers' address and replaced them by those of the intermediary servers,

- **Anti-spyware**: some spyware are not considered as viruses. They cannot always be detected by an antivirus. It is therefore necessary to associate these 2 types of programmes to adequately protect the system. An antivirus generally contains an anti-spyware dispositive,

- **Messaging encryption software** : this affordable dispositive makes the message unreadable even if it is intercepted,

- **IDS (Intrusion Detection System)** : these tools enable to detect attacks/intrusions on the network on which it is used. It is a complementary tool to firewalls, faults scanner and anti-virus. An alarm alerts as soon as an activity linked to a suspicious conduct or signature is detected on the networks and the system,

- **NAS (Network Attached Storage)** : this system enables data back up and the storage on a centralised volume for clients of the network. The storage of data allows to consider the recovery of the system in case of a malicious act.

C2- MANAGEMENT TOOLS

Management tools to put in place should comply with international certification regulations. For a ship, these rules are the ISM (safety management) and ISPS (security management) Codes. Regarding ISM code, the safety management system includes references to information systems security on board the ship. However, these references are generally very basic. Regarding the security plan, it corresponds to a purely physical approach of information systems security on board. The ship's security plan and the safety management system are appropriate documents to include references to cyber security management:

- The company's cyber security policy,
- The management of incidents resulting from a malicious act : recovery of the ship,
- The auto-control or audit of the ship's information system,
- Data storage,
- Management of transactions between the operator and the Operationnel Technologie system, between interconnexions OT/IT systems and between the ship and external parties. The latter aspect is essential as an hacker will more easily rely on an external participant to bypass the measures in place by the company.

D- THE NEED TO ENHANCE THE PROTECTION LEVEL

Over the year, ships have become more and more dependent on their on-board computer system. Evidence collected during the survey have highlighted three areas of improvement:

- The first one concerns the need to “ring-fence” industrial systems on board the ship, to consider them as “sacred”.
- The second concerns the need to enhance the level of protection of the ship’s information system using systems tools adapted to the ship’s operation and a management system enabling it to face a cyber-attack.
- Finally, the third lesson concerns the need for seafarers more aware to this threat. They will therefore be able to better detect any system incoherence. This approach is now possible through a jointly drafted guideline by the ANSSI and the DAM (Guideline « Best practices for cybersecurity on board ships » - Edition october 2016). **The primary cause of attacks is linked to the attacker. It must however be noted that the human factor plays, most of the time, a key role in the success of an attack.**

D1- RINGS-FENCING THE SHIP’S INDUSTRIAL SYSYTEM

Previously working in closed architecture, supervisory control and data acquisition systems (SCADA) used on board ships are now potentially connected to internet. These industrial systems will remain, by definition, based on technologies that will no more evolve after construction. These systems are therefore vulnerable. **It is thus fundamental to fence these systems up and avoid interconnections with other ships’ management systems**. Interconnections are a source of vulnerabilities. In order to reduce the risk of a malicious act on the ship’s industrial system, it is necessary to integrate the following (Guideline « Industrial risks of ship » - Edition january 2017) :

- **Assess the risk**: this analysis is the starting point of any cyber security approach. Systems must be the subject of a methodical analysis. This assessment will have to be regularly reviewed,
- **Mapping out the ship’s installation**: this system illustration enables to, firstly quickly evaluate the impact of a malicious act and, secondly, to contribute to the resolution of incidents,
- **Control**: self-monitoring or internal audit enable to regularly verify the system, the actual level of the ship’s cyber security. This control must also determine stakeholder management,
- **Surveillance of the system**: this watch allows the prevention of threats. This operation must ensure the surveillance of an intrusion in the system,
- **Continuity plan**: the ship’s and the company’s emergency plans shall answer to all incident scenarios which may result in a failure or deterioration of a critical activity identified in the risks assessment,
- **Remote maintenance**: clear procedures and protective measures shall be implemented to regulate this type of operations. The company’s policy should define the limits of this remote maintenance.

D2- RECOMMANDATIONS TO RAISE THE SHIP'S LEVEL OF CYBERSECURITY

In February 2016, the Maritime Affairs Directorate submitted a document to the International Maritime Organization (IMO) relating to cybersecurity elements applied on ships. This document allowed to actively participate in the works of the MSC96 committee. IMO circular MSC.1/Circ.1526 dated 1 June 2016 now mentions the need to rely on existing IMO codes to manage ships' cybersecurity. Raising the ship's cyber security level means applying a set of rules of use that will lead to integrating the ship's industrial systems management, technological tools management, seafarers training and relevant procedures into existing security and safety management systems. **The 7 following recommendations can serve as guidance for companies to raise this level of protection**.:

R1

Carry out an assessment of the ship's information systems security. This assessment can be based on BIMCO's guidelines on cyber security on board ships, standard ISO/IEC 27001 on information technologies, the NIST framework from the National Institute of Standards and Technology of the United States of America, standard NF EN 31010, the DNVGL-RP-0496 guide or others. This assessment should decide on at least :

- The ship's hardware and software mapping,
- The definition of the ship's sensitive sytems,
- Systems vulnerabilities management.

R2

Draft a ship's IT/OT (IS) company policy. This policy should at least define :

- The person in charge of ship's ISS,
- Access control, IS security measures (good practices),
- Records management monitoring, the « reinforced » control of remote maintenance and information sharing,
- The outline of a plan ensuring the ship's operational continuity,
- The preparedness to dangerous situations : crisis unit, use of a SOC (Security Operation Centre),
- Make a reference to paragraph 2.3 of IMO circular MSC.1/Circ.1526 dated 1 June 2016.

R 3

Apply good practice measures in terms of the ship's IS management. These measures shall include the management of:

- Access rights, privileges, data storage,
- Passwords, mailbox protection,
- Training and awareness campaign,
- The changing and updating of the ship's software programs.

R 4

Apply a control of ship's information systems sharing. It is necessary to develop a procedure defining the condition of access to the ship's sensitive equipment. This procedure defines:

- The access mode to these systems (USB, CD, PC…),
- Authorised members allowed to access these systems,
- Operations that need this access (maintenance, replacement, integration),
- The traceability of this access,
- Limitation of WIFI connections during the ship's sensitive operations (approach, management of sensitive operations defined at the level of the company's SSI policy,
- Prohibition of wireless equipment unless using an encryption system (keyboard, mouse, vulnerable systems by radio waves (Keysniffer),
- Prohibition of non-referenced computing tools and particularly those connected to the network (Shadows IT).

R 5

Set up a operation continuity plan following an incident. It is necessary to draft a procedure that should include the following items:

- Define the sensitive elements (results from the ship's ISS assessment),
- Available backup sytem when the system is out of order
- Description of backup mode and recovery mode,
- Isolatation of the faulty system.
- Periodicity for continuity plan exercises,
- Periodicity for restoration of stored data.

R 6

Monitor and manage the ship's IS incidents:

- Carry out an activity monitoring of the ship's IS,
- Ensure supervision,
- Analyse abnormal activities on the ship's management system.

R 7

Apply physical protection measures of the ship's information systems.

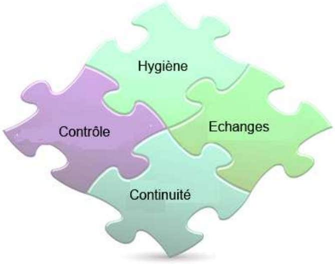
It is highly recommended to locate IS inside ship's restricted areas.

D3- IMPLEMENTING THE RECOMMANDATIONS

Critical points.

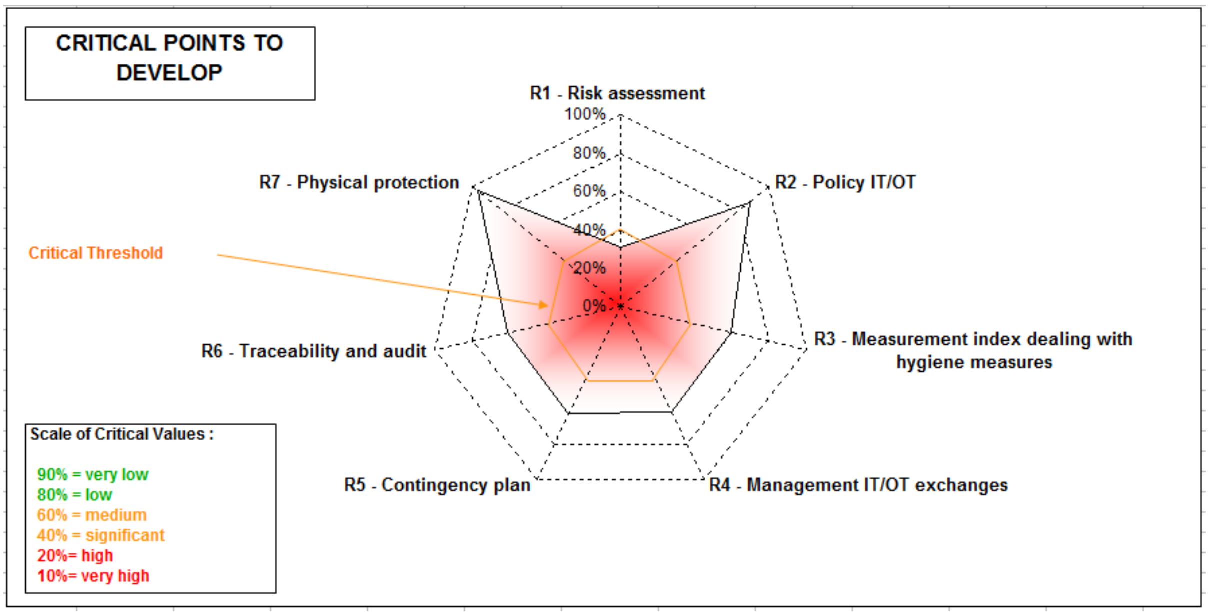
The survey data analysis demonstrates that French companies have taken into account the management of information systems security through a policy and a physical protection of these systems. However, it shows that the information systems risk assessment remains marginal. This assessment is nevertheless the foundation of any further step in the establishment of cyber security on board ships. This action allows to reduce the criticality relating to the management of the following four domains:

- **Good practices** for on board **computing activities**,
- **Information sharing** with external parties,
- Operational **continuity**,
- **Monitoring** of malicious activities towards the ship.



It is necessary to alert the companies on the need to carry out a risk assessment in order to reinforce the counter-measures to face a cyber malicious act. It must be noted that this assessment is made mandatory for French flag vessels in compliance with European regulation EC 725/2004 article 3.5. This article imposes the application of article B8.3 of ISPS code*: a Ship Security Assessment should address the following elements on board or within the ship: 1- physical security; .2 structural integrity; .3 personnel protection systems; .4 procedural policies; .5 radio and telecommunication systems, **_including computer systems and networks_**; .6 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.*

This assessment is approved by the flag state authority within the ship's security plan approval.

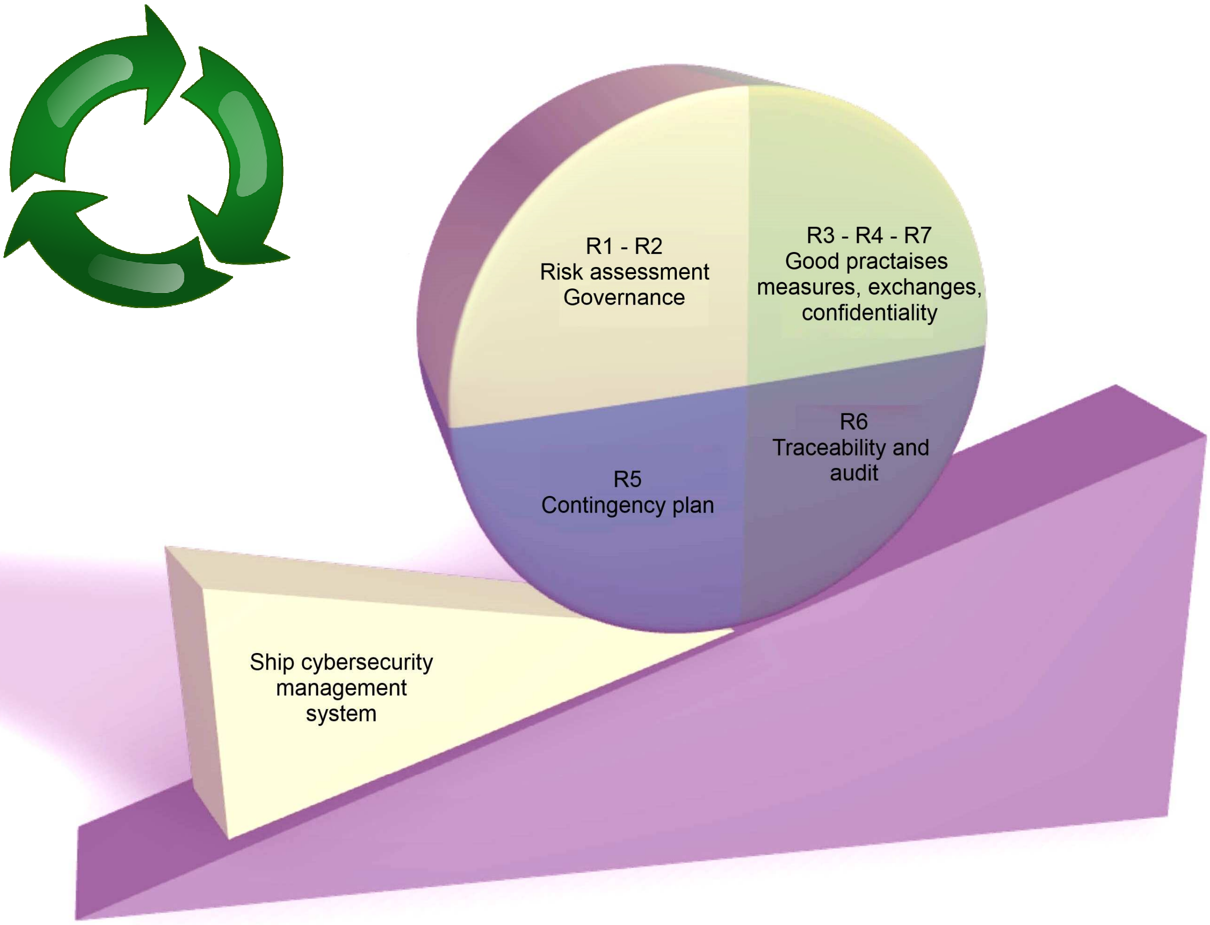


Implementation of cyber security on board ships.

The implementation of information systems security measures should rely on the DEMING wheel principle. The method is composed of four steps:

- Plan: prepare, anticipate
- Do: develop, achieve, put into place
- Check: monitor, verify
- Act: adjust, react

In application of this method and in reference to paragraph 2.5 of IMO circular MSC.1/Circ.1526 dated 1 June 2016, the seven recommendations allowing to reinforce the level of cyber security on ships can naturally be incorporated in the below wheel.



D4- WHAT FUTURE FOR SHIP CYBER SECURITY ?

The issue of cyber security on ships is raised.

The ship is linked to the web. Onboard systems can contain faults. The threat is relatively weak to this day. Technological and management systems tailored to the ship do exist. The shipping world has laid the first major milestone of guidelines. Everything is almost in place to protect the 50 000 ships. As we have seen, cyber attack against a ship remains marginal to this date. So why protect the ship ? The need to implement security measures does not improve the management of the ship operation but forces to invest in a field that is not profitable! The result of the equation looks simple, why bother investing in the ship's cyber security?

It is however important to keep in mind that not taking this threat into account on board ships could be catastrophic and cost a lot more money than an investment in this field. Imagine the consequences of a cyber-attack on a container ship of 19 000 TEU with a market value of up to 4 billion dollars !

Whatever the thinking, this type of threat is now inevitable for the maritime world : the more digitised the ships become, the more they are exposed to it. Consequently, it is essential to make ship-owners aware. It is also essential to support ship-owners in achieving the implementation of management tools, technological tools and the appropriate training. This survey illustrates the available means to face this risk which is not marginal at all.

Now how far should we go in supporting the French flag fleet?

This limit depends on the assessment of the threat. If the latter results in the management of viruses temporarily paralysing the ship's electronic mapping, the crew should be able to face this problem with appropriate procedures. If this threat resembles a sophisticated dormant cyber weapon using "ODay" type system vulnerabilities or an "air gap" type malware, it is obvious that the crew nor the company's IT support will be able to face it ! This type of weapon is nevertheless part of the arsenal of tools available to criminal groups, terrorist or state groups. In addition, let's not forget that the ship represents an excellent media outlet. In this context, we can reasonably question the need to have a "strategic cyber maritime fleet". At the image of our strategic supply that imposes a quota on ships, we can question the need for France to have a fleet of ships guaranteeing a level of requirement relating to cyber security through a labelling allowing to ensure our strategic supply.

France is not immune to a cyber-attack in retaliation to a choice made by our nation : **"People only accept change in necessity and see necessity only in crisis."** (Jean MONNET).

E- APPENDIX N°1 – THE SHIP'S SPECIFIC VULNERABILITIES

1- AIS (*AUTOMATIC IDENTIFICATION SYSTEM*)

The AIS is initially destined to help ship avoid collisions, to help port and maritime authorities to monitor the traffic and ensure a better control of the sea. The AIS receptors first appeared on bridges the last few years. AIS sends and receives GPS positions, speed, heading, type of ship, next port and estimated time of arrival, to and from surrounding ships. The AIS is a data sharing system between ships that was made mandatory by International Maritime Organization (IMO) in 2004. However, the AIS generalisation poses the problem of confidentiality linked to security: the selection of ships by pirates. The data transmitted through the AIS are available to all, including the scientific community. The AIS equipment includes:

- A VHF radio transponder,an automatic emission triggered in response to an interrogating received signal , fitted with 2 receiving channels and one for transmission;
- A control and display unit (Minimum Keyboard Display MKD) including the communication processor and the exit interfaces towards the other systems (ECDIS, ARPA).
- A GPS receiver giving the position of the ship and the UTC time necessary for the synchronisation of the AIS data transmissions;
- A DSC VHF receptor is sometimes integrated in the transponder and set on channel 70 for the sharing of text messages.

Based on automatic communications sharing by VHF radio between ships, and from ships to shore, it enables an identification in real time of emitting ships. **The system is potentially vulnerable**:

- **To interference,**
- **To false information**
- **To malwares** (the AIS is managed by mini computers)

Furthermore, the AIS system can also be used to issue false information that can be relatively easily "fabricated". The aim of these false messages (distress signal, false ship location…) is above all to attract attention and trap targeted ships. Thus, the AIS generates an alert in this case.

2- ECDIS (ELECTRONIC CHART DISPLAY INFORMATION SYSTEM)

An ECDIS is an “information and chart display visualisation system” that enables to show the position of the ship in real time on a map displayed on a screen.

The use of this system means there is no need for paper map anymore.

It provides the deck officer all information he may need to travel safely: instantaneous position of the ship (GPS), isobath and obstructions, nautical almanac (particularly for the sun and the moon), shore lights and beacons…It is also connected to Automatic Radar Plotting Aid (ARPA).

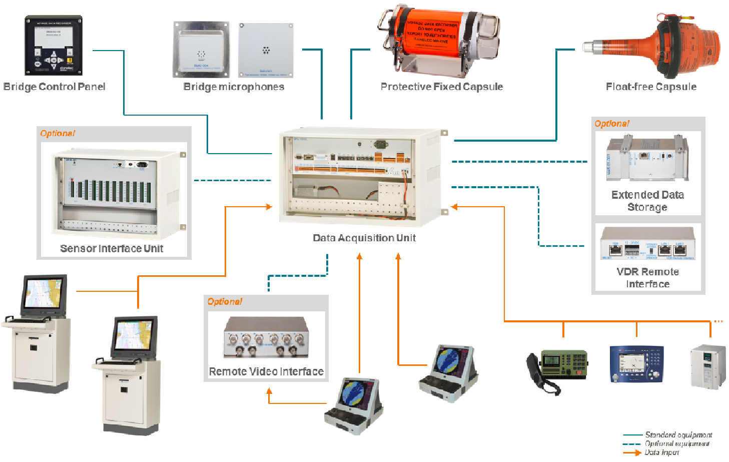
The system is compliant with IMO standards.

The ECDIS system presents a few underlying vulnerabilities in terms of software security that could lead to disastrous results for ships at sea. The ECDIS is based on a mapping system that uses an IT system to digitally display nautical charts and the exact location and tracking of its own ship.

The vulnerabilities of this system can include:

- **The system update medium**: CD/DVD, internet connection/Inmarsat or USB port,
- **The lack of update of the operating system that corresponds to a working station generally operating on a Windows type support that has not been updated.**
- This system is interconnected to the various ship’s sensors: radar, NAVTEX, automatic identification systems (AIS), speedometer, sounder, anemometer. These sensors are often connected to a local network on board ships (serial port/NMEA to LAN adaptators),

3- VDR / SVDR (VOYAGE DATA RECORDER)



The VDR system or SVDR is the ship's "aeronautical black box".

It is mandatory since 1 July 2002 on all passenger vessels and all cargo ships of 3,000 gross tonnage and upwards.

The aim of this device is to help analyse the circumstances that resulted in an accident, by examining the recorded data.

The standard settings of a VDR are the following:

- The Data Acquisition Unit (DAU) is the heart of the marine equipment: VHF input, radar input, hard drive or removable flash disk, emergency autonomous battery, microphones, high resistance data recording capsule, Bridge Alarm Unit (BAU), sensor Interface Unit (SIU) that collects all other data, codifies them and send them to the Data Acquisition Unit (DAU),

- Data recording: date and time, the ship's position, surface speed (log), gyrocompass, magnetic compass, radar image, bridge conversations, radio communications (emission/reception), water depth (sonar unit), principal alarms (fire, engine room, etc.), status of watertight doors and hatches (opened or closed), status of fire doors (opened or closed), rudder angle, orders and responses with the machinery space, thrusters, true or relative wind speed.

Just like the ECDIS system, this system's vulnerabilities can include:

- **The system update medium**: CD/DVD, by internet connection/Inmarsat or USB port,
- **The lack of update of the operating system that corresponds to a working station generally operating on a Windows type support that has not been updated.**
- **This system is interconnected to the ship's sensors.**

4- GNSS (GLOBAL NAVIGATION SATELLITE SYSTEM)

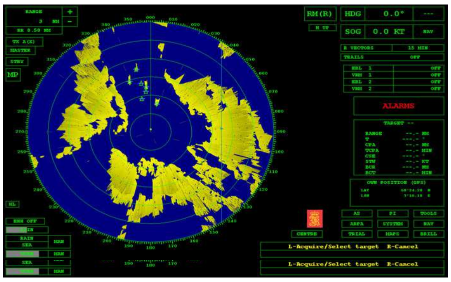
The GNSS ,through a set of satellites and a receiver, displays the position (2D and 3D), the speed, the route and time (UTC),.Therefore it enables to orientate and navigate at sea, on land or in the air. Several GNSS exist in the world today. The system offers a worldwide coverage and the one that is most used by the general public is the GPS that set up of 24 satellites situated at an altitude of 20 000km shifting in 6 quasi circular orbital planes inclined at 55° on the equator. The positioning principle is based on calculation algorithms of the distance between the GPS receiver and several satellites. The precision of the GPS can reach 10 meters. This precision can be impaired by atmospheric turbulence.

The satellite signals are not protected by encryption. It is therefore possible to intercept and duplicate them.

The system's vulnerabilities can include:

- **A weak signal strength – inherent weakness,**
- **The possibility of involuntary interference,**
- **The possibility of intentional jamming,**
- **Technical deficiency in the satellites constellation.**

5- RADAR / ARPA



The radar (Radio Detection And Ranging) is a system using electromagnetic waves to detect the presence and determine the position and speed of an object or an obstacle. The waves sent by the transmitter are reflected by the target and the return signal (called radar echo) is received and analysed by the receiver. The Automatic Radar Plotting Aid (ARPA) is the equipment associated with the navigation radar that allows the tracking of echoes and calculates the closest point of approach to help the watch officer with anti-collision.

The system's vulnerabilities can include:

- **The possibility of involuntary interference,**
- **The possibility of intentional jamming,**
- **The possibility of identity theft by altering the return signal.**

6- DP (POSITIONNEMENT DYNAMIQUE) OF THE SHIP

The dynamic positioning system is a system controlled by a computer that enables a ship to maintain its position by using its own means of propulsion.

This system is made of three parts. The sensors collect the information, the computer carries out the calculations and acts as an interface for the operator, and the actuators execute and drive the propulsion units. It is an automated IT system.

The system vulnerabilities correspond to the sensors' security weakness such as the GPS and to the interface human/IS/machine that uses an operating system that needs to be updated.

7- SYSTEME DE CONTROLE INDUSTRIEL (ICS , SCADA)

Onboard ships, risks are on :

(1) All ICS (Industrial Control System) networks : sensor and actuator management,
(2) SCADA (Supervisory Control and Data Acquisition) : Global network, work stations and ICS software monitoring the industrial process.

Onboard ships, ICS are common. Those systems are controlling :

(1)- propulsion, power management, piping systems,…),

(2)- steering gear, auto-pilot,

(3)- safety systems and cargo operation.

In general, the two main issues regarding industrial system security management are :

- The lifetime difference between the SCADA system (short lifetime 3-5 years) and the industrial system (long lifetime 15-20 years : frozen systems, difficult to upgrade).

- The « programming culture » which is not accustomed to preventive security approach.

Industrial systems vulnerability is no longer to be demonstrated. APT (Advanced Persistant Threat) of STUXNET type have already shown their skills in sabotage**.**

System vulnerabilities include the following 7 points :

(1) **Lack of secure development :** internal developments, lack of security integration, unlocked session,

(2) **Low level of access protection :** very simple access control with user or password management too weak or nonexistent, no antivirus on workstations and servers, users with Administrator privileges,

(3) **The lack of partitioning between management information systems and unsecured industrial systems :** this principle makes it possible to introduce via the computer management system into the industrial network. This flaw is the target of many recent attacks. These bridges are used to retrieve information from production directly into the control systems. This method of access allows both the collection of information and sabotage,

(4) **Absence of abnormal supervision of the system**,

(5) **Non-up-to-date and weak management protocols** (FTP, Telnet, VNC, SNMP ...) used without encryption that open access to login / password recovery, illegitimate connections to servers,

(6) **Increasing use of uncured standard computer systems :** These shelf-based products enable cost-reduction and interoperability (TCP / IP protocol, Ethernet standard or Microsoft Windows or Linux operating systems: due to their simplicity and generalization, the cost of these technologies has made them unavoidable). These systems are therefore prey to malicious software,

(7) **Lack of stakeholder control over industrial systems :** monitoring of subcontractors is often insufficient. The consequences of this non-management can be the loss of data, the deterioration of equipment, the endangerment of the ship's crew and the environment.

For further more informations read the guideline « Industrial risks of ship » - Edition january 2017.

8- SYNTHESIS ON SHIPBOARD SYSTEMS VULNERABILITIES:

Vulnerabilities	Measures to implemented onboard ship	Company systems where measures take place
(1) Fake signal (ECDIS, GPS, RADAR, DP, AIS)	Crosschecking of navigational information in particular during coastal navigation.	**Ship Safety Management System (ISM) :** Brigde procedures shall take into account the risk of malicious act on navigation systems.
(2) No access control to operating system (ECDIS, DP, SCADA)	Monitoring of access to unlocked operating systems.	**Ship Safety Management System (ISM) : cards R2, R4** The Company policy shall include interrelation of internal and external parties accessing critical navigation systems. This interrelation should be formalized by agreement between parties (Company, crew, service provider). **Ship Security Management System (ISPS) : card R7** Control of access to the ship can cover access to critical IS.
(3) No segregation between input/output systems (DP, SCADA)	Ensuring means to lockdown failed systems and to switch to back-up mode.	**Ship Safety Management System (ISM) : card R5** The implementation of an operation continuity plan following an incident shall result in operating the ship in backup or downgraded mode: redundant stand-by systems or backup mode. **Ship Safety Management System (ISM) : card R6** Monitoring of unusual events shall ensure early detection and alert. This type of incident may indicate the preparation of a cyberattack.
(4) Signal jamming (ECDIS, GPS, RADAR, AIS)		
(5) Lack of system monitoring (VDR, ECDIS, DP, SCADA)		
(6) Operating System not updated (ECDIS, VDR, DP, SCADA)	Following manufacturers intructions and managing Operating Systems and software settings.	**Ship Safety Management System (ISM) : cards R2, R3** The monitoring the update of Operating Systems using « system patches » ensures an up-to-date system.

E- APPENDIX N°2 – SURVEY

Ministry of Ecology, Durable Development and Energy
DGITM / DAM / SM2 / Shipping security mission

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SURVEY: Cybersecurity onboard a ship flying the French flag

For execution: bureau of regulations and inspection of shipping safety and security; Shipping Security Center.

- **Summary:** This survey aims to review the level of security of the information systems present onboard the ship (vessel's cybersecurity). On completion, the information from this study will contribute to establishing a standard for the vessel's vulnerability. This information can be taken into account for the regulatory revision of Decree 2007-937 and Decree 84-810.

Keywords:

✓ Information system mapping: all information describing the information system, and notably including a list of hardware resources (models) and software resources (versions) used, with the architecture of the network on which nerve points are identified (sensitive servers, external connections).

✓ Restricted-Access Area: area identified in the vessel's security plan.

✓ Sensitive service: piloting of the ship, vessel maintenance, operations linked to the management of the vessel's cargo (stability, cargo transfer, dual-hull ventilation, emissions, etc.), vessel's electronic messaging system.

✓ Complex password: word composed of at least 8 characters of different types (uppercase, lowercase, digits, special characters).

✓ Administrator network: privileged account for performing configuration and management operations on all or part of the information system: installation, configurations management, maintenance, IS upgrades, security supervision or management.

✓ Secure WiFi network: during the initial configuration, the login name and passwords have been changed; encryption protocol (WPA2 or WPA-AES).

✓ IS protection system: technical system installed to raise the degree of security of the information system. For example, it can involve solutions such as antivirus software (software designed to identify, neutralize and erase malware), data encryption systems (using a cryptographic process by which the comprehension of a document is impossible for anyone who does not have the encryption/decryption key, a firewall (software and/or hardware designed to protect the data of a network by filtering incoming traffic and checking outgoing traffic for compliance with predefined rules).

Reference documents:

✓ International Ship and Port facility Security code (ISPS) : B8.3.5 on evaluation of communications systems, including information technology systems and networks.

✓ Security instruction for shipping dated January 26, 2015 (client feedback process – DAM quality system).

✓ Technical memorandum on the security certification of shipping, dated February 25, 2015,

Date of application of the survey: August 1, 2015
Duration of the survey: one year

Survey report management:

copy n°1: Ship - document forwarded to the ship's captain.

copy n°2: Shipping Security Center manager – shipping security file.

copy n°3: Shipping security mission – shipping security file.

"SHIP CYBERSECURITY" SURVEY BASELINE

Vessel's identity:	
Vessel's IMO number:	
Location of the survey:	
Survey date:	
Survey team member(s):	
Survey conducted in the presence of:	

Information technology practices onboard the ship	**yes**	**no**	**Comment**
A- General aspects:			
A1: Does the company operating the ship have an information technology security policy?			
A2: Does the company operating the ship have an information technology department?			
A3: Is there an identified information system manager onboard the vessel?			
A4: Have the vessel's information systems undergone a risk analysis?			
A5: Does the vessel have a mapping of its information system?			
A6: Does the ship's information system undergo remote maintenance?			
B - Location of information technology networks:			
B7: Are the vessel's information technology systems for navigation management (piloting of the vessel, and communications systems) in a Restricted-Access Area?			
B8: Are the vessel's platform management information technology systems (propulsion, electrical power, maintenance, life onboard, training) in a Restricted-Access Area?			
B9: Are the ship's cargo management information technology systems (vessel stability management, cargo transfer, environmental protection) in a Restricted-Access Area?			
C. Protection of information interchanges with the outside world:			
C10: Are the networks employed for navigation, maintenance and propulsion of the vessel connected to the Internet?			
C11: Is it possible to connect to these networks via a USB port?			
C12: Does the vessel have IS protection systems?			
C13: Is data entered into the information system via USB ports subjected to analysis by an antivirus or similar system?			
C14: Does the vessel have a WiFi network?			
C15: If yes, is the WiFi network secured and, if so, by what algorithm?			
C16: Are files downloaded from the Internet or received by email opened or executed automatically?			
C17: Are files downloaded from the Internet or received by email always analysed by antivirus software?			
C18: Is the connection of personal devices to the vessel's information system physically possible? Is it authorized?			

Information technology practices onboard the ship	**yes**	**no**	**Comment**
D - Password management:			
D19: Is access to the vessel's sensitive services password-protected?			
D20: Is the frequency of password changes specified?			
D21: Are passwords complex?			
D22: Are passwords stored in an IT storage tool?			
E - Regular software updates:			
E23: Are the software products used by the vessel regularly updated?			
E24: Are updates downloaded from the software developers' official websites?			
F - Specification of IT user accounts:			
F25: Is there a centralized management system for user accounts and administrator accounts onboard the vessel?			
F26: Is access to Internet or consultation of electronic messages possible from an administrator account?			
F27: Are there anonymous or generic (trainee or contact) login accounts with access to the vessel's IT network?			
G- Regular backup of IT data:			
G28: Is there a specified frequency for IT data backups?			
G29: Are the vessel's data backed-up to a cloud Internet platform?			
H- Incident:			
H30: Is there a continuity plan for working in downgraded mode in the event of an incident?			
H31: Is there an obligation to identify the cause of an incident when one occurs?			
H32: Is there surveillance for "abnormal" events affecting the information system (massive data transfer, login attempt, etc.)?			
H33: Has the vessel already suffered the consequences of a cyberattack?			
I- Others:			
I34: Are there inspections or checks on the vessel's information systems security?			

✓

Complementary opinion of the survey team about the vulnerability of the vessel's information technology system:

Attachment(s):

E- APPENDIX N° 3 – GUIDANCE CARDS

The following cards include goals to achieve in order to mitigate risks related to cyber-threats.

Furthermore, these cards refer to some further guidance, standards or tools available that could be helpful for companies to reduce cyber-risks :

- Technological systems or software,
- Management regulations: ISM and ISPS codes
- French Network and Security Agency guidances : **http://www.ssi.gouv.fr/**

These **7** cards follow the recommendations from the French Maritime Directorate study and are also based on the IMO interim guidelines on maritime cyber-risk management (MSC.1/Circ.1526) for aspects regarding on-board practices.

- R1 / Assessment of the ship's information systems (**IS = IT + OT**) security,
- R2 / Ship's IS company policy,
- R3 / Good practice measures in terms of the ship's IS management,
- R4 / Control of ship's information systems access,
- R5 / operation continuity plan or contingency plan,
- R6/ Ship's information systems incident management,
- R7 / Physical protection measures of the ship's information systems.

R1- ASSESSMENT (digital reliability of the ship)

GOALS :

1. Determine the acceptable level of threat for the ship,
2. Define the scope of the assessment : Ship delivery after construction, flag change, IT maintenance management, dry-docking, external parties access to IT systems,…
3. Define criteria :

- Basic tools : mapping (private networks, uncontrolled networks), critical networks, equipment providers, nature of threats,
- Communication : satellite, TOIP, Wi-Fi, LAN,
- Propulsion/navigation : positioning systems (AIS, GNSS…), ECDIS, DP, Manoeuvring, GMDSS, Radar, VDR,
- Ship access control : CCTV, BNWAS, SSAS,
- Cargo control : CCR, stability, pumps…
- Passager management : control, private networks, Entertainment…
- Cross-cutting elements : router, switch, fire-wall, operating systems,

4. **Decide on ship's vulnerability :** output, incident probability threshold, key components, physical and computing access management, weaknesses, identification of risk areas by materialising the impact of a threat, continuous improvement, IT security technics and policies.

REFERENCE DOCUMENT: ISPS CODE

The IS security assessment is a sensitive document. It should be included in the ISPS ship security plan (ISPS code B 8.3.). Informations contained in the IS security assessment should be classified as « ship security confidential ».

MONITORING:

The monitoring of the assessment is done through the ship security plan approval by flag state administration in compliance with European Regulation CE 725/2004.

Cyber security assessment has to be updated in order to keep security measures proportionate to the level of threat. Security measures should not impair the ship's operational needs ake into account the operational needs. The key point remains the resilience of the system over time.

DOCUMENTARY OR TECHNICAL SUPPORT :

1. BIMCO guidelines on cybersecurity onboard ships.
2. Standard ISO/CEI 27001 on Information Technologies.
3. NIST from U.S. National Institute of Standards and Technology.
4. Standard NF EN 31010 (risk management, methods of risk assessment),
5. Classification Society Guidance : DNVGL – RP- 0496
6. Methods of work : EBIOS, MEHARI , OCTAVE …

PRINCIPLE :

Need for a global approach during the assessment so that protective measures cannot be bypassed.

R2- POLICY (Governance)

GOALS :

1. Endorsement from Company top management ,
2. Definition of ISS authority at company level and onboard ship,
3. ISS training policy,
4. Definitions of remote maintenance, access control, records management onboard ships,
5. Definition of ISS backup management onboard ships,
6. Engage in ISS risk assessment onboard ships,
7. Engage in mapping ships IS,
8. Enforce onboard IS good practice measures,

REFERENCE DOCUMENT: ISM CODE

The safety management system can include ISS company policy according to ISM Code chapter 2 « *SAFETY AND ENVIRONMENTAL PROTECTION POLICY*».

MONITORING:

The monitoring of the policy implementation is performed during internal and external audits.

DOCUMENTARY OR TECHNICAL SUPPORT :

1. ANSSI : Memento on ISS policy development (PSSI -version 03 March 2004),
2. ANSSI : Guidance on ISS policy development (Section 1 to 4) (Version 03 March 2004),
3. ANSSI : Development on ISS dashboard (Version 05 February 2004),

ISSP guidance aims to help ISS managers in developing an Information Systems Security Policy (ISSP) for their company. It includes 4 sections: (1) The introduction shows how to place the ISSP into the Company ISS standards and defines the basis of its legitimacy; (2) The methodology extensively presents how to develop an ISSP and includes guidance for defining security measures; (3) list of security principles ; (4) list of ISS reference documents (evaluation criteria, rules, standards, ethic codes, complementary notes …).

PRINCIPLES :

1. **The Security Policy must be apparent :** People should be aware of the Policy even if they don't have a detailed knowledge of the content..
2. The Company Policy must provide for a SOC (Security Operation Centre). This arrangement is used for detection, prevention, alert and decision-making in cyber incident response.
3. Cybersecurity will be ensured when standards and operational organisation are in place.

R3 – GOOD PRACTICE MEASURES
(Access and data exchange management)

GOALS :

1. Passwords :
- Definitions : structures, storage, changing periodicity,
- Protection of ship's sensitive systems,
2. Software : update management, update responsibility and authority, keeping an appropriate level of security,
3. Access to the ship's IS :
- Ship's IS accounts management at Company level,
- Ship's IS accounts management at ship level,
- Management of anonymous or generic accounts,
4. Data backup : ship's data recording periodicity, backup system, backup drive,
5. Define responsibilities and interrelations regarding ISS : ship's IS administrator, awareness,

REFERENCE DOCUMENT: ISM CODE

The ship safety management system can include ISS good practice measures according to ISM Code chapters 6 and 7:

1. ISM Code chapter 6 « *RESOURCES AND PERSONNEL* » : provisions regarding ISS training (awareness and management),
2. ISM Code chapter 7 *« DEVELOPMENT OF PLANS FOR SHIPBOARD OPERATIONS»* : develop procedures on ship's ISS management and good practices.

MONITORING :

Monitoring of good practices is performed during internal ISM audits,

DOCUMENTARY OR TECHNICAL SUPPORT :

1. ANSSI : Guidance on IS good practices (12 rules) : ISS seafarer awareness, (Version 1.1 March 2015),
2. ANSSI : Guidance on IS good practices : ISS Company awareness (Version 1.0 January 2013),
3. ANSSI : On-line tools :
- Password management : technical note 05 June 2012,
- Firewall management : technical note 30 March 2013,
- Encryption methods B1 and B2 21 February 2014,
- Computer work station strengthening : technical note 16 September 2015,
- Protection of VPN connection : 13 July 2015,
4. **Technical solutions :** NAS (network attached storage), firewall installation and setting, VPN technology, antispyware, « sandbox » technology, encrypted mailbox,

PRINCIPLE :

Principle of user's responsibility or user awareness level management, internal and external.

R4 – EXTERNAL ACCESS (Exchanges security)

GOALS :

1. WIFI network :
- WIFI data protection : networks partitioning, encryption systems,
- Reduce data transfer during sensitive ship operations (port manoeuvring, cargo operation, ...),
2. Networks connection : apply protection measures when connecting devices (USB, PC...)
3. Prohibit WIFI systems (radio vulnerability « keySniffer),
4. Avoid uncertified or unknown IT (Shadows IT) : access management,
5. Connections to ship's industrial systems :
- Management of connection ports,
- Connection traceability,
- Remote maintenance : port activation,

REFERENCE DOCUMENT: ISM CODE

The ship safety management system can include the management of exchanges with the outside world according to ISM Code chapter 7 *« DEVELOPMENT OF PLANS FOR SHIPBOARD OPERATIONS »* : develop a procedure regarding IS exchanges.

MONITORING :

The monitoring is performed during internal ISM audits (company and ship),

DOCUMENTARY OR TECHNICAL SUPPORT :

1. ANSSI : Guidelines on WIFI networks security : technical note 09 September 2013,
2. ANSSI : Guidelines on remote access security : technical note 07 September 2012
3. ANSSI : Cyber security for industrial systems : guidance January 2014,
4. **Technical solutions** : encrypted WIFI, networks segregation, basic mechanisms for authentication, deactivation of USB port, Business2Business management, Firewall for industrial system,
5. **Standard IEC 61162-460**
6. Install a separate printer for external parties (surveyor, PSCO,...)

PRINCIPLES :

1. **Autoprotection principle**, or « anything external is suspicious and should be treated as unsafe».
2. **Identification principle** : Limit and monitor external connexions, authentication of external accredited parties.
3. Particular attention must be paid to Wi-Fi systems and mobile devices.
4. Where remote maintenance is used, access monitoring and control must be reinforced. Contracts with service providers must include responsibility provisions.

R5- CONTIGENCY PLAN (operation continuity)

GOALS :

1. Develop and implement an operation continuity plan in case of cyber incident (downgraded ship's operation) :

- Confidential procedure : paper printed only,
- **Procedure for manual backup of sensitive elements,**
- Procedure regarding loss of communication,
- Procedure for the shutdown of infected system : seclude infected system to avoid malware spreading,
- Procedure for IT department emergency contact 24/24,
- Annual continuity exercise,
- Documentation update,
- Save a copy on external drive, reinstall the software, change passwords.

REFERENCE DOCUMENT: ISM CODE

The ship safety management system can include the management of ISS incident according to ISM Code chapters 8 and 9 :

1. ISM Code chapter 8 « *EMERGENCY PREPAREDNESS*» : include an operation continuity plan in case of cyber incident,
2. ISM Code chapter 9 « *REPORTS AND ANALYSIS OF NON-CONFORMITIES, ACCIDENTS AND HAZARDOUS OCCURRENCES*» : report et monitoring of ship's SSI situation.

MONITORING:

The monitoring is performed during internal ISM audit (company and ship),

DOCUMENTARY OR TECHNICAL SUPPORT :

1. **Documentary support** : Company and shipboard emergency plan ; Company emergency response management,
2. Guidance on SOC (Security Operation Centre),
3. Cyber incident management : standard ISO/IEC 27035,
4. Technical solution : data back-up in order to avoid « ransomwares » (card R3).

PRINCIPLE :

Lockdown principle or « always be able to lockdown an infected part». It is particularly useful in case of a virus or worm attack. Applying this principle can be compare to create a decontamination airlock. This airlock can be a sub-network where a less stringent security policy applies. Only few specific systems can be connected to the airlock (web server, mail antivirus) and it can be fitted with intrusion detection system…

R6 –INCIDENT MANAGEMENT (Traceability and audit)

GOALS :

1. Ensure proper implementation of ISS company policy,
2. The audit for compliance must be performed by qualified personnel,
3. The periodicity of internal audits must be formalized,
4. An audit report must be compiled for traceability,
5. Detection of ISS incident,
6. Report of ISS incident : records, traceability, collect of evidence,
7. Rectification of incident : identify root causes, action plan,
8. Experience feed-back : analysis, protection, system review, experience sharing.

REFERENCE DOCUMENT : ISM CODE

The ship safety management system can include provisions for IS internal audits according to ISM Code chapter 12 *« COMPANY VERIFICATION, REVIEW AND EVALUATION»* : The audit procedure should be adapted in order to collect additional elements regarding ISS management

MONITORING:

The monitoring is performed during ISM internal audits (company and ship),

DOCUMENTARY OR TECHNICAL SUPPORT :

1. Technical solution : port monitoring (network intrusion detection system (IDS)),
2. Technical solution : Appropriate setting of firewalls : it should screen unauthorized traffic, and report automatically every anomaly. Those systems should be regularly tested. Abnormal traffic must be scrutinized by a ship officer.
3. Documentary support : Guidance on SOC (Security Operation Centre),

PRINCIPLES :

1. **Regular checking of security measures implementation (better safe than sorry).** Initial and periodic verification of security measures is preventing from unintentional but actual deviation.
2. **Implementation of an in-depth defense, or « Mise en place d'une défense en profondeur, ou « several defensive barriers are better than one ».** Considering that, in complex systems, several defensive barriers are necessary, different protective measures should be used for various components, in particular functional measures.

R7- I.S. PHYSICAL PROTECTION (Confidentiality)

GOALS :

1. Consider navigational IS as Restricted Areas,
2. Consider propulsion and power management IS as Restricted Areas,
3. Consider cargo control and passengers control IS as Restricted Areas,

REFERENCE DOCUMENT : ISPS CODE

Access management is described in the ISPS Ship Security Plan according to ISPS Code A 9.2 and 9.2.4. Details of access control measures is confidential according to ISPS Code article A 9.8.1.

MONITORING:

The monitoring is performed through the ship security plan approval and during ISPS ship certification verifications,

DOCUMENTARY OR TECHNICAL SUPPORT :

1. **Ship Security Plan** : ISS description and localisation, ISS mapping,
2. Critical equipment redundancy (taken into account during the assessment),

PRINCIPLES :

1. **Physical security is the key component** of any protection system in order to ensure integrity, confidentiality and availability of information. Protection against unauthorized access is the first protection against damage or destruction.
2. Physical protection consist in using barriers, alarms, locks and other physical means to control physical access to IT spaces, computers or equipments. These measures are necessary to protect computers, devices and data from spying, thief, intentional or accidental destruction.
3. **Need for a dynamic risk management.** In a fast and continuously evolving world, especially in IT and communication domains, risk management must be dynamic and continuously updated. For any entity, it is necessary to be permanently informed regarding potential threats and published vulnerabilities and to develop plans accordingly: reaction for operation continuity to be applied in case of an attack or an incident. Beyond these plans, emergency response external support can be used, able to identify the attack, assess the damage and take containment and response measures.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTRY OF ENVIRONMENT, ENERGY AND THE SEA