Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTRY OF ENVIRONMENT, ENERGY AND THE SEA

« CYBER SECURITY »

REINFORCING THE PROTECTION OF INDUSTRIAL SYSTEMS ON A SHIP

JANUARY 2017 EDITION

Directorate-General for Infrastructure, Transport and the sea

Maritime Affairs Directorate

Table of contents

PREFACE ... 1

A- RISK ASSESSMENT ... 4

A1- Vulnerabilities of the ship ... 4

A2- Risks ... 5

B- ENFORCING PROTECTION OF ICS ... 6

B1- Level 1 : Global security strategie ... 6

B2- Level 2 : Passive monitoring system ... 7

B3- niveau 3 : Hardening configuration of industrialof control system chain ... 7

C- CONTROL OF INTERNET OF THINGS CONNECTED TO ICS ... 8

D- CONCLUSION ... 9

E- APPENDIX N°1 - Definitions ... 10

E- APPENDIX N°2 - Risks matrix ... 11

E- APPENDIX N°3 - Convergence IT / OT to hardenig ICS ... 12

E- APPENDIX N°4 - Tell me more ... 13

SENSITIZATION ON THE SECURITY OF INDUSTRIAL SYSTEMS

For an industrial installation, insurance companies no longer hesitate to classify the risk "cyber" first and this well before the risk of terrorism and natural disasters. This new approach comes on the one hand from the awareness of the threat through attacks in the destructive format of STUXNET / HAVEX / DRAGONFLY ... and on the other hand from an industrial system which has been open to subcontractors and to the Internet Of Things (IOT).

In addition, it is necessary to differentiate the computer dedicated to an industrial system (Operationnel Technologie) and the so-called conventional Information Technologie like office computer (IT). The cyber security solutions of classical information have been designed to address privacy issues as a priority and to block all suspicious activities. These intrusive solutions do not fully guarantee the safety of an industrial installation. Thus, these solutions can generate too many errors of judgment of a detection program (false positive) which leads to a shutdown of the industrial system.

The digitization of the ship is now a reality. Ship no longer benefits from an "air gap" level of computer security consisting of physically isolating her from any computer network. The ship therefore integrates naturally into the web. The vessel consists of a set of industrial systems operated by automata controlling the ship's driving, energy and commercial operations.

In this context, the aim of this guide is to make maritime companies aware of the risks specific to the industrial Internet on board the vessel in order to adapt risk-based rules of use.

A- RISK ASSESSMENT

Today, Industrial Control systems (ICS) use frequently information technology. ICS have not been designed to cope with the cyber threats they introduce on board of the ship. Therefore aboard the ship, programmable logic controllers (PLCs) are ubiquitous and manage steering and cargo operations.

A1- VULNERABILITIES OF THE SHIP

Critical industrial systems on board of the vessel may be classified as follows:

- propulsion system (main engine, power, driving),
- safety management system (fire, waterway),
- cargo management (safety system in charge of cargo transfer, stability management),

The vulnerability of an industrial system is no longer to be demonstrated. APTs (Advanced Persistent Threat) like STUXNET illustrated their skill in sabotage. The vulnerabilities of a system can relate to seven domains (Extract from investigation Maritime Affairs Directorate of september 2016 : http://www.developpement-durable.gouv.fr.vpn.e2.rie.gouv.fr/Surete-des-navires.html) :

(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.

A2- RISKS

The cyber risk for the ship is twofold:

- The deterioration of the company's image may lead to a loss of competitiveness of the company,
- The sabotage of the ship by a dormant system or operated on demand which can lead to the loss of the ship, the loss of the crew or damage to the environment.

With reference to the surveys carried out by the Maritime Affairs Directorate and to the audit of a vessel carried out by the French Network and Security Agency (ANSSI / Agence nationale de la sécurité des systèmes d'information), the risk assessment applied to shipboard industrial systems can be materialized as follows (Extract from appendix n°2) :

Operation	Risk	Potential Impact	Risk assessment	Mitigation of the risk	Risk assessment after mitigation
Management of critical industrial system on ship	**(1) Offensive Economic Intelligence Act**	A breach of the company ‘s image	**Medium**	Global security strategy	**Low**
	(2) Spying	Loss for competitiveness of the company	**Medium**	Global security strategy	**Low**
	(3) Sabotage	▪ Loss of the ship, ▪ Loss of crew, ▪ Damage to the environment.	**High**	Global security strategy and management of internet of things (IOT)	**Medium**
				Global security strategy and management of internet of things (IOT) + passive monitoring	**Low**
				Global security strategy and management of internet of things (IOT) + passive monitoring + Hardening configuration of industrial supervision chain systems	**Very low**

B- ENFORCING PROTECTION OF ICS

There is no ideal or "one-size-fits-all" solution. When assessing cybersecurity on board the ship, three levels of protection can be integrated into an industrial plant protection management system set up by a shipping company.

B1- LEVEL 1 : « GLOBAL SECURITY STRATEGY »

Goal : Provide a permanent framework for the security systems on vessel,

Fonctional requirement : This principle corresponds to two thirds of the measures to be put in place - by the top management of the company - to face a cyber threat. These management measures concern training, management of procedures through standards or tools adapted to a shipping company (Safety management system and ISPS code).

Industrial information systems must be integrated into the company's policies, like any other information system, from the outset of the project.

Rules of use : This global security of the industrial system of the ship must concern the use of rules of **basic security hygiene measures** adapted to the industrial system of the ship:

- **Physical access control to equipments :** protect access to the network, lock PLC cabinets, control access to the engin, cargo, bridge control room,
- **Network segregation :** establish a flow map. Separate networks by dedicated equipment or VLANs. Filtering flows by means using of firewalls, tracing rejected flows and analyzing them,
- **Account management (logical access) :** Define a management policy, do not leave the default accounts on devices, manage the passwords,
- **Configuration hardening :** install only the necessary software, do not leave development tools on production servers or operator work stations, deactivate remote configuration and programming modes on critical assets,
- **Management of event and alarm logs :** Activate traceability functions where devices and software permit this, centralize logs and generate alerts for abnormal events,
- **Backup & restor :** Define a backup policy allowing the reconstruction of an installation following a malicious act,
- **Mapping facilities :** Equipment, manufacturer, serial number, history,
- **Documentation :** Define a policy for managing documentation,
- **Malicious code detection :** Define a malicious code detection policy, Give priority to protecting hardware and applications in direct contact with the outside world and users,
- **Protection of PLCs**: Protect access to PLCs with a password, Deactivate remote configuration and / or programming modes when this functionality exists.

B2- LEVEL 2 : « PASSIVE MONITORING SYSTEM »

This step follows a risk analysis of industrial systems on board the vessel.

Goal : Scan the network for weak signals (Behavioral Detection). These measures will not prevent an incident but will make it possible to detect it and to limit its effects as far as possible. The sooner an incident is detected, the more measures can be put in place to reduce and contain the effects.

Fonctional requirement : To have on board the ship an operational capacity to prevent, detect and respond to a cyber attack which target the ship's industrial Internet.

Rules of use: This security corresponds to the following measures:

- **Monitoring censor :** Passive monitoring consists to positioning a censor on network.. This object monitors the inventory and the orders made on the industrial network. The system learns the mapping of the installation. A visual representation of the network is then defined according to the natural evolutions of the system. Knowledge of the network is achieved by a mathematical model (gauge) : the matrix compares to the outcome all that is out of the question of the conduct of the exploitation of the industrial system. The monitoring system can be integrated into a Security Operation Center (SOC). This principle uses the mode of action of the attacker who maps the attacked system.
- **Configuration management :** This measure consists of comparing the programs and configurations active in the devices (version N executed) with a backup version identified as the reference (version N saved). Before the commissioning of new versions, an analysis of the discrepancies between versions N and N-1 should take place.

B3- LEVEL 3 :« HARDENING CONFIGURATION OF INDUSTRIAL CONTROL SYSTEM CHAIN »

This step follows on from the risk analysis and applies to the vessel's sensitive system by **partition the network** essential to the vessel's operation.

Goal : Raising the level of difficulty of grasping the industrial system by an attacker,

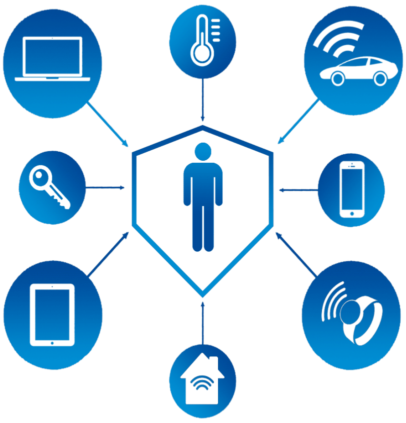
Fonctional requirement : In order to raise the level of protection of the on-board industrial system, equipment should be available to deal with malicious acts. The ideal system is to have a fully certified chain : from the supervision to the PLC through the switch, the firewall. This chain can be certified. It should be noted that the certification of the sensors / actuators appears difficult. Also they should be secured by physical protection. In addition to this certification, an active monitoring of the failures of the industrial system (patches) should be carried out. The robustness of this system is based on a certified chain and a Computer Emergency Response Team (CERT) watch.

Rules of use :

- **Critical equipment :** have a certified industrial system chain for sensitive vessel handling equipment,
- **Monitoring of API updates :** ensuring active monitoring by the company,

C- CONTROL INTERNET OF THINGS (IOT) CONNECTED TO ICS

Over the past ten years, internet has gradually evolved into an extensive network, known as the Internet of Things, linking billions of human beings and tens of billions of objects.



IOT, thanks to the omnipresence of its connected sensors and systems, provides the control system with information to identify and solve problems.

These systems will allow the maritime companies to benefit from a better profitability of the ship. This increase in efficiency will thus reduce the operating and maintenance costs of the ship.

Next IOT integrations in the maritime world concerns the tracking of containers. In 2017, the French company TRAXENS will equip 200.000 EVP of a container monitoring device. This smart box will allow the tracking at sea, ashore of the container through communication tools connected to surrounds GSM and satellite network. The ship will be equipped with a central unit to relay informations delivered by this container's device.

However, to be fully effective, these objects must be secured in order to avoid any malicious acts such as remote control of these objects that take part in a network of zombie machines to disrupt a system (DDOS type attack) .

<u>Goal :</u> Secure IOT connected to the industrial system,

<u>Fonctional requirement :</u> Internet of things may be required to collect sensitive data from the industrial system. This data can be stored on a CLOUD. It is necessary to ensure the need for an IOT in the conduct of the ship's industrial systems. The evaluation of the cyber security of industrial systems must make it possible to rationalize this need for the ship.

<u>Rules of use</u>: This security consists in adopting the following rules:

- **Assess the need for an object connected to an industrial system on bord of ship :** This evaluation must necessarily take into account the security of the IOT especially if the archiving of the data is transmitted to a CLOUD.

- **Define a policy for the use of IOTs :** The high level of the company should validate this commitment. This policy should rule on disabling or using these tools to exchange data between networks, disabling USB ports on systems, restricting the functionality of the IOT. The more limited the attack surface, the more limited the range of action of the cybercriminel via the Internet of things.

D- CONCLUSION

In computing sector, there are no less than four clusters of activities that are synchronized around management information systems (IT), industrial and technological computing (OT), computer networks and telecommunications, multimedia computing. The ship is built around a component of industrial computing to which it is necessary to integrate a computing component of management.

The encounter of these two worlds, which had evolved so far in parallel, creates vulnerabilities that must be understood. This means that IT and OT strategies must be harmonized, common governance and process models must be installed, security and data must be managed centrally and resources must be re-skilled to understand and know about the requirements of both disciplines. Failure to take these flaws into account could have serious consequences for the ship and the company.

To deal with this threat, it is necessary to set up rules of use concerning a best management practices for industrial computing. These rules must adapt to the peculiarities of the industrial system, which requires the availability of systems. The establishment of these rules must be drawn up in consultation with the ship's engine department, which has knowledge of the conduct of all the on-board equipment: propulsion, energy, stability, ship cargo management and alarm system .

In addition, the company can supplement these good practices with specific measures on sensitive equipment of the ship. These measures follow a risk analysis and may take the form of passive surveillance systems, network segmentation and certification of an industrial chain.

Finally, it is now appropriate to identify by the company the rules for the use Internet Of Things which are required to collect and process system information. These objects can be the gateway of an attacker. The implementation of all these measures must be part of a global policy for securing the ship's information systems.

E- APPENDIX N°1 – DEFINITIONS

- **APT :** Advanced Persistant Threat like STUXNET malware,

- **ACTIVE SYSTEM :** Physical actions on input and output system,

- **CENSOR :** Digital sensor on a network that monitors vulnerabilities,

- **CERT :** Computer Emergency Response Team,

- **CLOUD :** the exploitation of computing or storage power of remote computing servers over a network,

- **DDOS :** Distributed Denial Of Service attack consisting in drowning in unnecessary information a service ("Mirai" type attack),

- **FIREWALL :** This system makes it possible to ensure the interconnection between an industrial network that is to be protected and another network,

- **ICS :** Industrial Control System, designates a set of human and material resources designed to control or operate technical installations (consisting of a set of sensors and actuators),

- **IOT :** internet of things,

- **IT :** Information Technologie,

- **OT :** Operationnel Technologie,

- **PASSIVE SYSTEM :** Device which analyzes the exchange of data without interfering with the system,

- **PATCHES :** application of corrections made to a system fault. In the industrial field, it is necessary to ensure that the patch is well adapted as it could call into question the proper functioning of the installation.

- **PLC (Programmable Logic Controllers) :** An industrial programmable logic controller (PLC) is an equipment that makes it possible to carry out, continuously and without human intervention, the control of industrial processes machine or continuous process. Depending on its input data, received from the sensors, the automation of the sends orders to the outputs, the actuators.

- **SCADA :** Supervisory control software

- **SOC :** Security Operation Center,

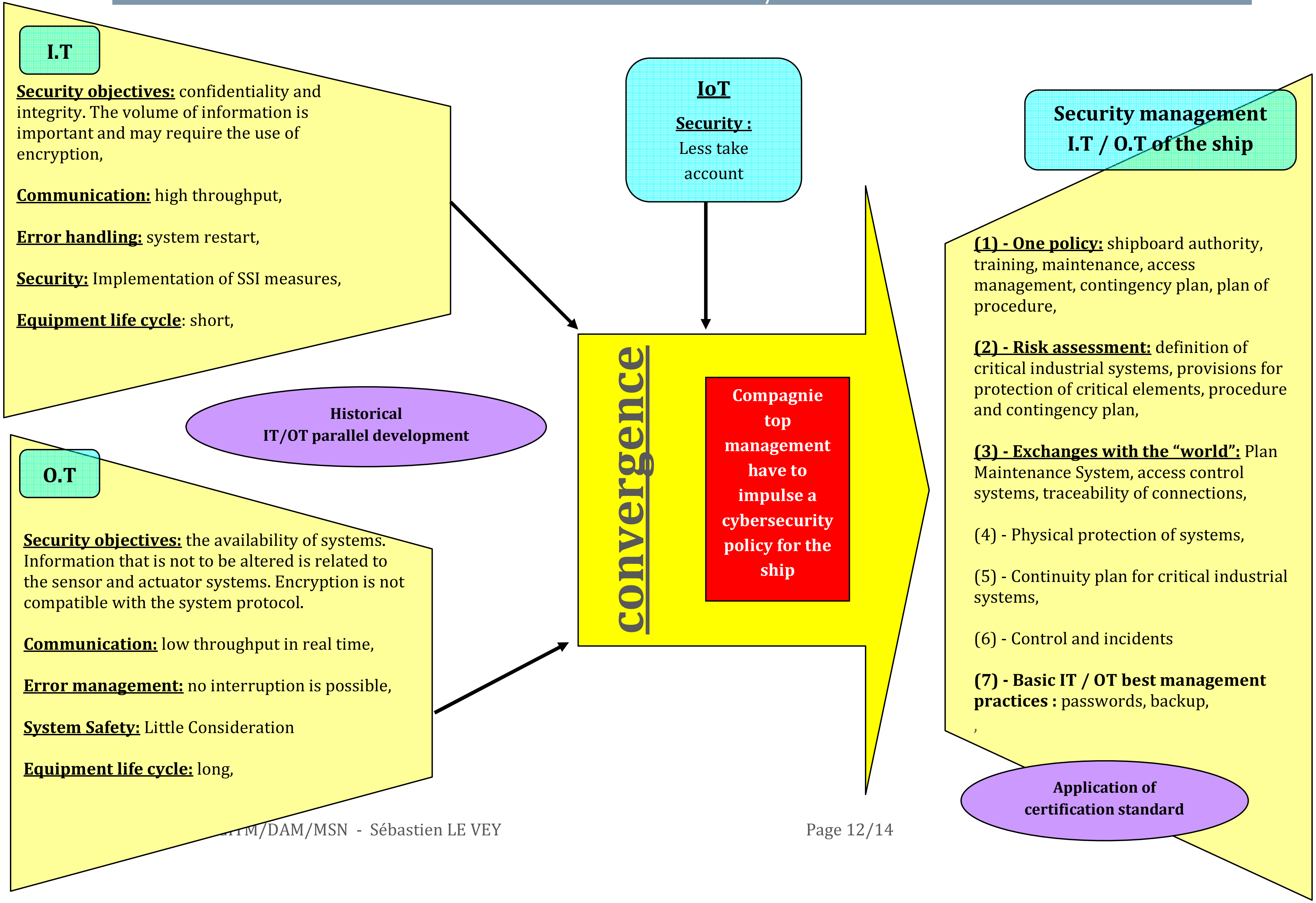
- **SWITCH :** The industrial switch makes it possible to interconnect different equipment or segments of networks communicating in Ethernet,

E- APPENDIX N°2 – RISKS MATRIX

Operations	Risks	Critical		Risk assessment before preventive measures	Preventive measures	Risk assessment after preventive measures	Rules of use	Tools
		Impacts on	Menace probabilité					
A - Management of critical industrial system on ship ▪ Propulsion ▪ Energy ▪ Cargo ▪ Stability ▪ Alarms	Offensive Economic Intelligence Act	A breach of the company 's image	**unlikely**	**Medium**	Global security strategy and management	**Low**	**OT best practice :** - IOT assessment, - Policy, - mapping, - acces control, - record, - restoring system	**A-certification standard** -ISM code, -ISPS code, -IEC 61162-460 -ISO CEI 27001, **B- Traning** - Sensitization, - Training of officer **C-Technological tools** - survey censor, - Standardisation PLC, - firewall, - VPN, - NAS
	Spying	Loss of competitiveness for the company						
	Sabotage	- Loss of the ship, - Loss of crew, - Damage to the environment.		**High**	Global security strategy and management of internet of things (IOT)	**Medium**		
					Global security strategy and management of internet of things (IOT)+ passive monitoring	**Low**	**Passive monitoring**	
					Global security strategy and management of internet of things (IOT)+ passive monitoring + Hardening configuration of industrial supervision chain systems	**Very low**	**Partition critical networks**	
B - Management of non critical industrial system on ship	Sabotage	Loss of competitiveness for the company		**Medium**	Global security strategy and management	**Low**	**OT best practice**	
C- Steering of the ship ▪ ECDIS, DP, ▪ AIS, GPS, ▪ Radar, VDR	Signal usurpation	A breach of the company 's image Loss of the ship, Loss of crew, Damage to the environment.		**Significant**	The navigation process must take account the possibility of a malicious act on the navigation tools.	**Medium**	Compare navigation environment system	
	Voluntary signal interference			**Significant**	The navigation process must take account a backup system	**Medium**	Contingency plan and weak monitoring signal	
D- administrative management of the vessel	Sabotage	Loss of competitiveness for the company		**Medium**	Global security strategy and management	**Very low**	**IT best practice** - Assessement, - policy, - control access ...	

Note: Risk = Vulnerability x (Impact x Threat);
Operational vulnerabilities are the result of the Maritime Affairs Directorate study of September 2016 "Reinforcing the level of protection of ships ".

E- APPENDIX N°3 – CONVERGENCE IT / OT TO HARDENING ICS



I.T

Security objectives: confidentiality and integrity. The volume of information is important and may require the use of encryption,

Communication: high throughput,

Error handling: system restart,

Security: Implementation of SSI measures,

Equipment life cycle: short,

Historical
IT/OT parallel development

O.T

Security objectives: the availability of systems. Information that is not to be altered is related to the sensor and actuator systems. Encryption is not compatible with the system protocol.

Communication: low throughput in real time,

Error management: no interruption is possible,

System Safety: Little Consideration

Equipment life cycle: long,

IoT

Security :
Less take account

convergence

Compagnie top management have to impulse a cybersecurity policy for the ship

Security management I.T / O.T of the ship

(1) - One policy: shipboard authority, training, maintenance, access management, contingency plan, plan of procedure,

(2) - Risk assessment: definition of critical industrial systems, provisions for protection of critical elements, procedure and contingency plan,

(3) - Exchanges with the "world": Plan Maintenance System, access control systems, traceability of connections,

(4) - Physical protection of systems,

(5) - Continuity plan for critical industrial systems,

(6) - Control and incidents

(7) - Basic IT / OT best management practices : passwords, backup,

,

Application of certification standard

E- APPENDIX N°4 – TELL ME MORE

ANSSI (French Network and Security Agency) :

ICS are today highly computerized and interconnected with IT systems or the Internet. As such, they are exposed to the same threats , with potentially more serious consequences.

Faced with these potential risks, ANSSI publishes guides about Cybersecurity for ICS. These guides are pragmatic to help all the the stakeholder of the industry to take into account the cybersecurity related issues. They offer a simple and appropriated methodology, illustrated by real situations.
For further question (website of French Network and Security Agency) : www.ssi.gouv.fr

ANSSI GUIDELINE :

regarding cybersecurity for Industrial Control Systems Managing Cybersecurity for ICS :

- Managing Cybersecurity for ICS - june 2012
- Use Case – june 2012
- Classification Method and Key Measures – janvier 2014
- Detailed Measures – janvier 2014

Watch system :

- French CERTA website : http://www.certa.ssi.gouv.fr/
- US-CERT website : https://www.us-cert.gov/

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTRY OF ENVIRONMENT, ENERGY AND THE SEA