CYBERSECURITY

Menaces et méthodologie

Système d’Information et automatisme dans le domaine maritime et portuaire

V. SERUCH
5 April, 2018

INDUSTRIAL CONTROL SYSTEMS (ICS) & MARITIME

Industry specifics

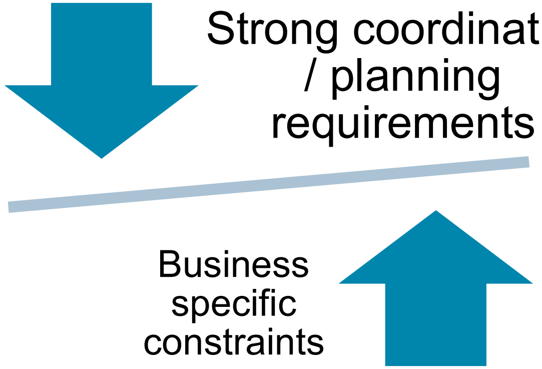
ICSs are typically mission-critical applications with a high-availability requirement.

Maritime additional requirements:

- Always-on environnement
- Strong scheduling / operational constraints.
- environmental constraints.

To move further on :

- More automation – tendency to unmanned ships.
  - No accommodation and related cost.
  - Less power
  - More cargo



Strong coordination / planning requirements

Business specific constraints

PORT INFRASTRUCTURE

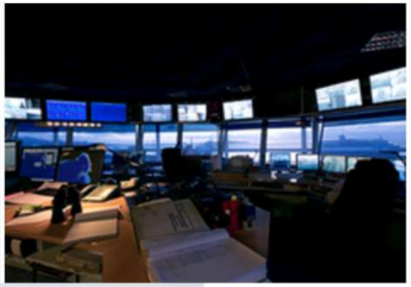
Terminal Operations & Management

Automated Gates

Physical Security

Crane Monitoring and Control

Wireless Devices & Tracking



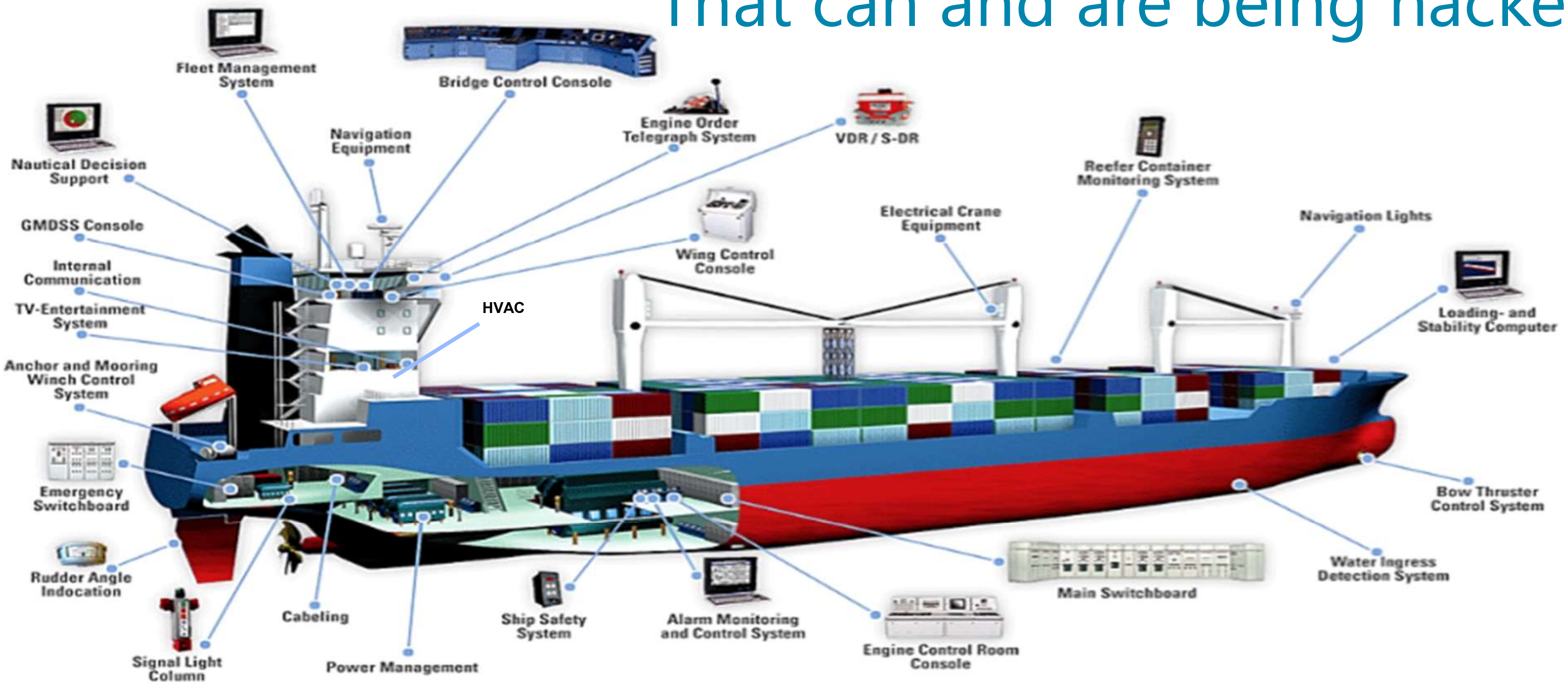
VTS Systems

CYBERSECURITY

MARITIME CYBER ALLIANCE
SUPPORTED BY AIRBUS

SHIP SYSTEMS

That can and are being hacked


Fleet Management System
Bridge Control Console
Navigation Equipment
Nautical Decision Support
Engine Order Telegraph System
VDR / S-DR
Reefer Container Monitoring System
GMDSS Console
Internal Communication
Wing Control Console
Electrical Crane Equipment
Navigation Lights
TV-Entertainment System
HVAC
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Rudder Angle Indocation
Water Ingress Detection System
Main Switchboard
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

AIRBUS

Interaction entre le navire et son environnement?

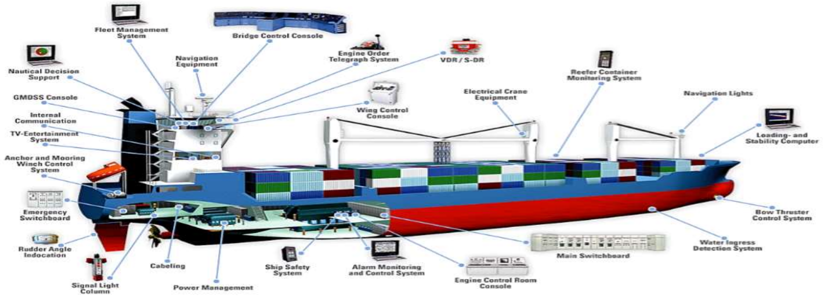
Navigation au large
ECDIS

Navigation côtière

Surveillance / maintenance systèmes

Localisation

Gestion équipage


Fleet Management System
Bridge Control Console
Nautical Decision Support
Navigation Equipment
Engine Order Telegraph System
VDR / S-DR
Reefer Container Monitoring System
GMDSS Console
Wing Control Console
Electrical Crane Equipment
Navigation Lights
Internal Communication
TV-Entertainment System
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Water Ingress Detection System
Rudder Angle Indocation
Main Switchboard
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

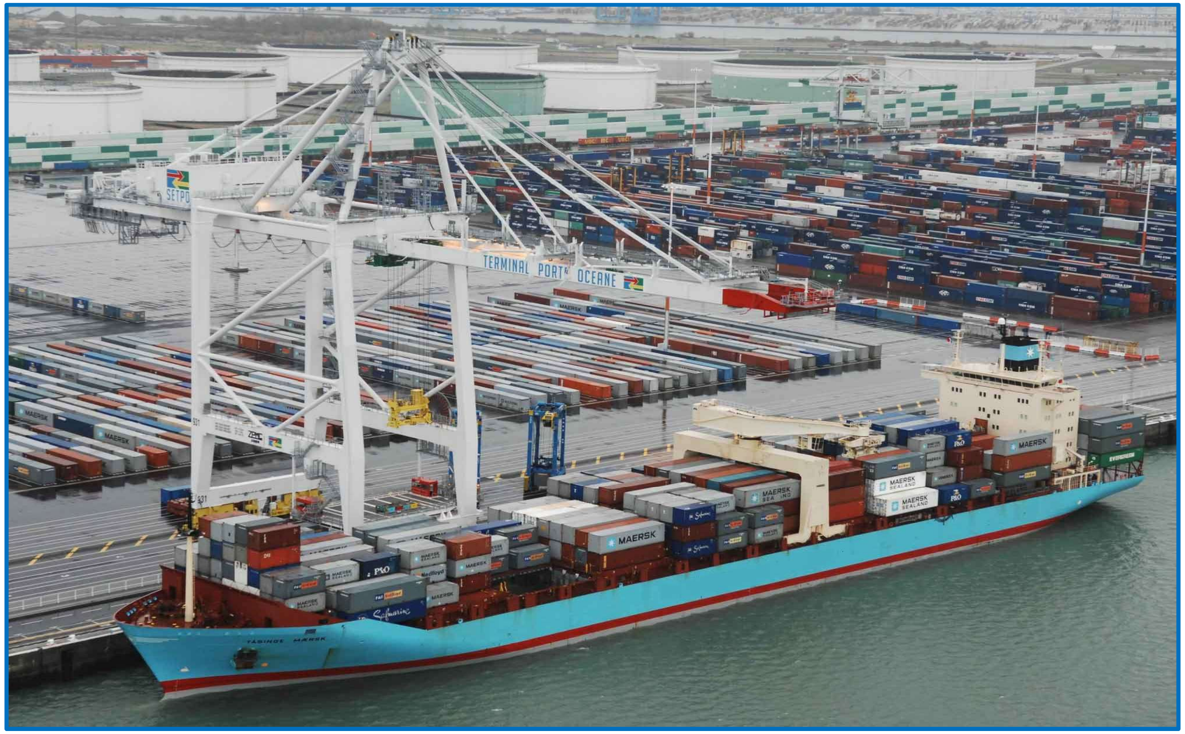
Gestion et chargement fret

Trajectoire /
Evitement collision

Détection flottabilité/voie d’eau

SHIPS AND PORT

ICS weaknesses



- Obsolete operating systems
- Old Industrial Processors with no protection
- Lack of cyber security awareness Training
- Lack of cyber security and safety policies
- Networks not segregated
- Lack of access-control to computers and networks
- Unpatched Legacy systems
- Lack of intrusion detection

MARITIME CYBER ATTACKS

Is reality

Demonstration made - it is possible to change a vessel's direction -> GPS spoofing.

A hacker caused a floating oil-rig located off the coast of Africa to tilt to one side, thus forcing it to temporarily.

Hackers accessed cyber systems in a port to locate specific containers loaded with illegal drugs and remove them from the port undetected.

Somali pirates employed hackers to access a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with

- valuable cargoes
- minimal on-board security.

MARITIME CYBER ATTACKS

Even not a target you can be a victim

In the Norwegian energy and oil and gas sector, more than 50 cyber security incidents were detected in 2015.

2017 : Ransomware Petya : cost the Maersk company as much as $300 million in lost revenue.

March 2018: Svitzer revealed in that it has also suffered a significant data breach. 50,000 emails containing private personnel information, auto-forwarded to accounts outside.

MARITIME CYBER ALLIANCE

More incidents on maritimecyberalliance.com

AIRBUS

Study 11 UK Ports: Do you intend to deploy any of the following digital solution areas?

1.Maintenance, monitoring, analytics, networks, remote management

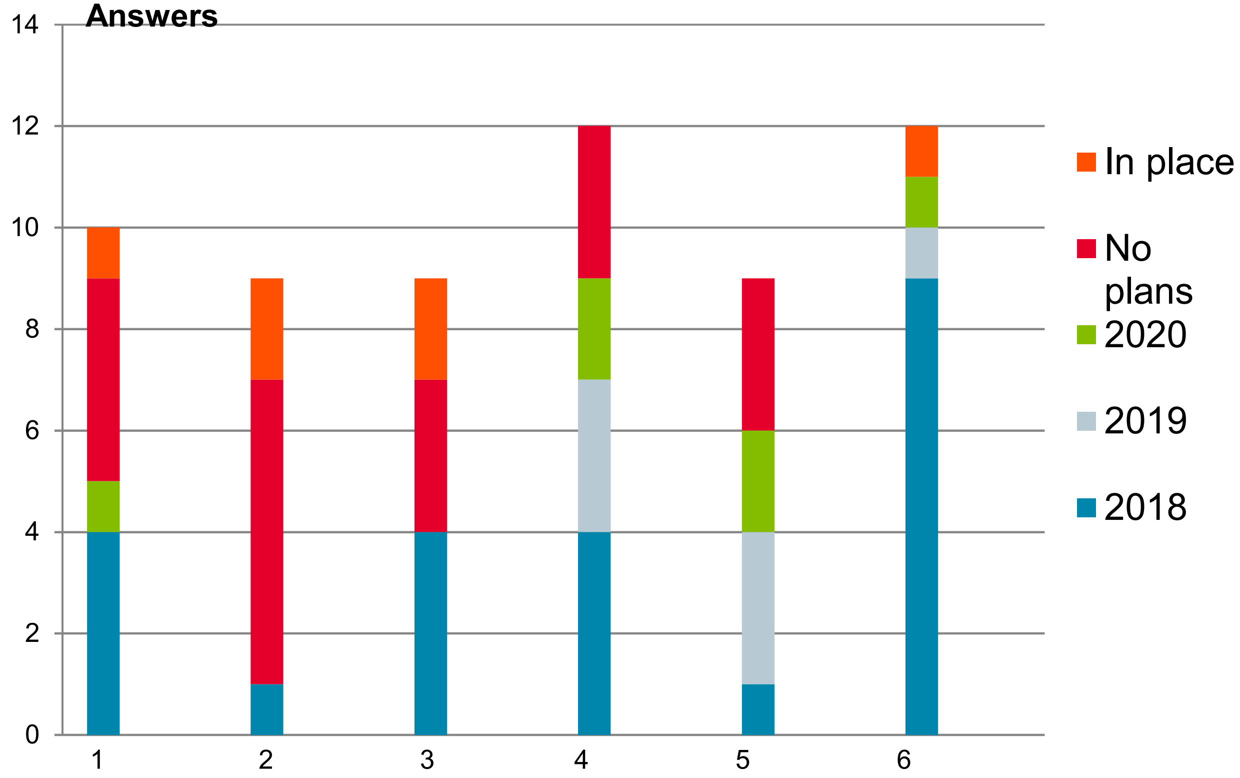
2. VTS/PMIS systems

3.Wireless networks

4.Standardized Port IT infrastructure and software

5.Machinery and automation integration, IoT

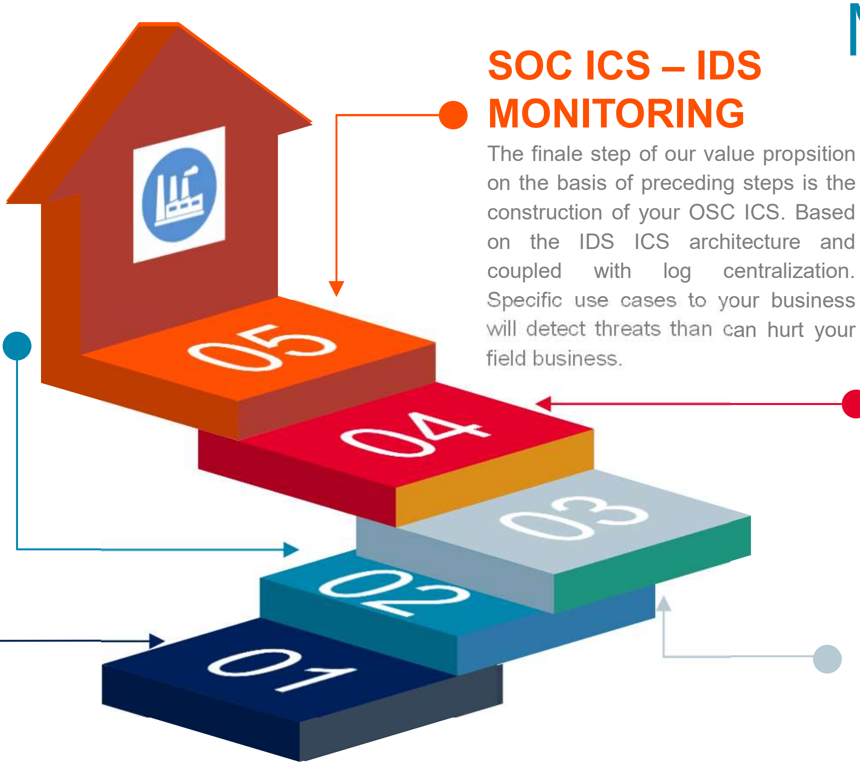
6.Safety and security, cybersecurity



The answers tend to say that UK ports are ready to invest in cybersecurity

METHODOLOGY

Methodology



MAPPING SOLUTIONS

Study phase : a comparative analysis based on the requirements criteria specific to your industrial environment. Providing a comparaison study with elligible solutions

ICS PROTECTION DESIGN

With the support of our ICS architects and our Cyber Range, a design of ICS architecture of your industrial environment will be created and made at the end of the design study. The Cyber Range makes it possible to validate the relevance and effectiveness of this architecture in the virtual environment and then move on to the implementation stage.

QUALIFICATION TESTS

In a virtualized industrial environment based on our Cyber Range, advanced performance tests of selected IDS ICS are performed to qualify the best IDS probe for your business. These tests are run on IDS ICS using the PCAP of your legitimate activity and incorporting malicious scenarios.

ICS CYBER PROTECTION

On the basis of the design study and the qualification tests, our architects implements the architecture IDS for ICS specific to your environment. These also provide the confirgruation of IDS to a central log collection to prefigure the next SIEM software that will be a central part of your ICS SOC.

SOC ICS – IDS MONITORING

The finale step of our value propsition on the basis of preceding steps is the construction of your OSC ICS. Based on the IDS ICS architecture and coupled with log centralization. Specific use cases to your business will detect threats than can hurt your field business.

CORRELATE IT & ICS, THE NEXT STEP !

Monitor your ICS

LPM
SIIV
IGI901
OIV
IGI1300
PROJET DE LOI DE
PROGRAMMATION
MILITAIRE
2014 / 2019
Data Breach
Cyber Attack
HACKING DETECTED

Services

- Evaluation of cybersecurity maturity
- Cybersecurity training
- Awareness

Detection & Investigation

- Anomaly detection
- Data lost prevention
- Investigative tool
- Industrial Threat Intel

Control & Defence

- Integrity control
- Host Hardening
- Protection against malicious programs
- Firewall & intrusion detection
- Application control

Context

- ❑ 2017 cyber criminals caused major service disruptions around the world.
  - Shadow Brokers (Stolen Data – NSA)
  - WannaCry (May 12th)
  - Petya/NotPetya/Nyetya/Goldeneye
    - Pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosnof.
    - Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank,

And also : **Bad Rabbit,** Wikileaks CIA Vault 7, Cloudbleed (leak of sensitive data), USA voters (198 Million Voter Records Exposed), Macron Campaign Hack

- ❑ 2018, we can anticipate the trend to become more pronounced
  - ▪ Attackers will use machine learning and AI.
  - ▪ Supply Chain Attacks to Become Mainstream – service disruption (e.g. Maersk in 2017)
  - ▪ File-less and File-light Malware (fewer IoC – harder to track)