CHAIRE DE CYBERDÉFENSE DES SYSTÈMES NAVALS

NAVAL GROUP - THALES - IMT ATLANTIQUE - REGION BRETAGNE

ECOLE NAVALE

CHAIRE DE CYBERDEFENSE DES SYSTEMES NAVALS

A joint R&D initiative

For security in maritime systems

Team leads

- Dr David BROSSET
  - Associate Professor of Computer Science – Ecole Navale
  - Email: brosset@ecole-navale.fr
- Dr Caroline FONTAINE
  - Researcher at CNRS LabSTICC
  - Email: caroline.fontaine@imt-atlantique.fr
- Dr Patrick HEBRARD
  - *Cyber security team lead at Naval Group*
  - Email: patrick.hebrard@naval-group.com
- Prof Yvon KERMARREC
  - Professor of Computer Science - Ecole Navale and IMT
  - Email: yvon.kermarrec@imt-atlantique.fr
- Philippe LEROY
  - Cyber security team lead at Thales
  - Email: Philippe-rh.leroy@thalesgroup.com

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Creation of the chair : 2014

- **Chair of cyber-defense for naval Systems**
  - **2 missions : Research and Education**
  - **Strong technical orientation and focus with PhD students investigating**
  - **Sponsor**
    - General Officer for Cyber-defense (French MOD)
  - **Initial Partners**
    - Naval academy
    - DCNS (now Naval Group)
    - THALES
    - Institut Mines TELECOM / IMT Atlantique
  - **Cooperation**
    - Brittany region,
    - Pôle d'Excellence Cyber (PEC)
  - **Technical Partnership**
    - Naval headquarter (EMM/SIC), DGA, ANSSI
    - The other French MOD Cyber chairs
  - **An open environment for international cooperation**

CHAIRE DE CYBERDÉFENSE DES SYSTÈMES NAVALS

ECOLE NAVALE

DCNS THALES

ECOLE NAVALE

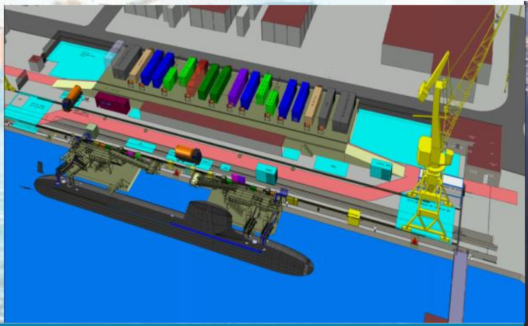
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

The context: naval system specificities

- **Ships at sea (civil, military)**
  - Partially isolated - Reduced crew
  - Technology and complexity
  - Lifetime more than 30 years
- **Harbor infrastructures**
  - Very sensitive
  - Contribute to world trade
  - High tech and IoT
- **Marine renewable energy**
- **Oil platform**
  - Environment impacts



ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Warship systems: a complex system

Modern frigate, statistic

-2000 applications

-400 automatisms

-4 levels of confidentiality

-300 calculators

-350 Km of cable

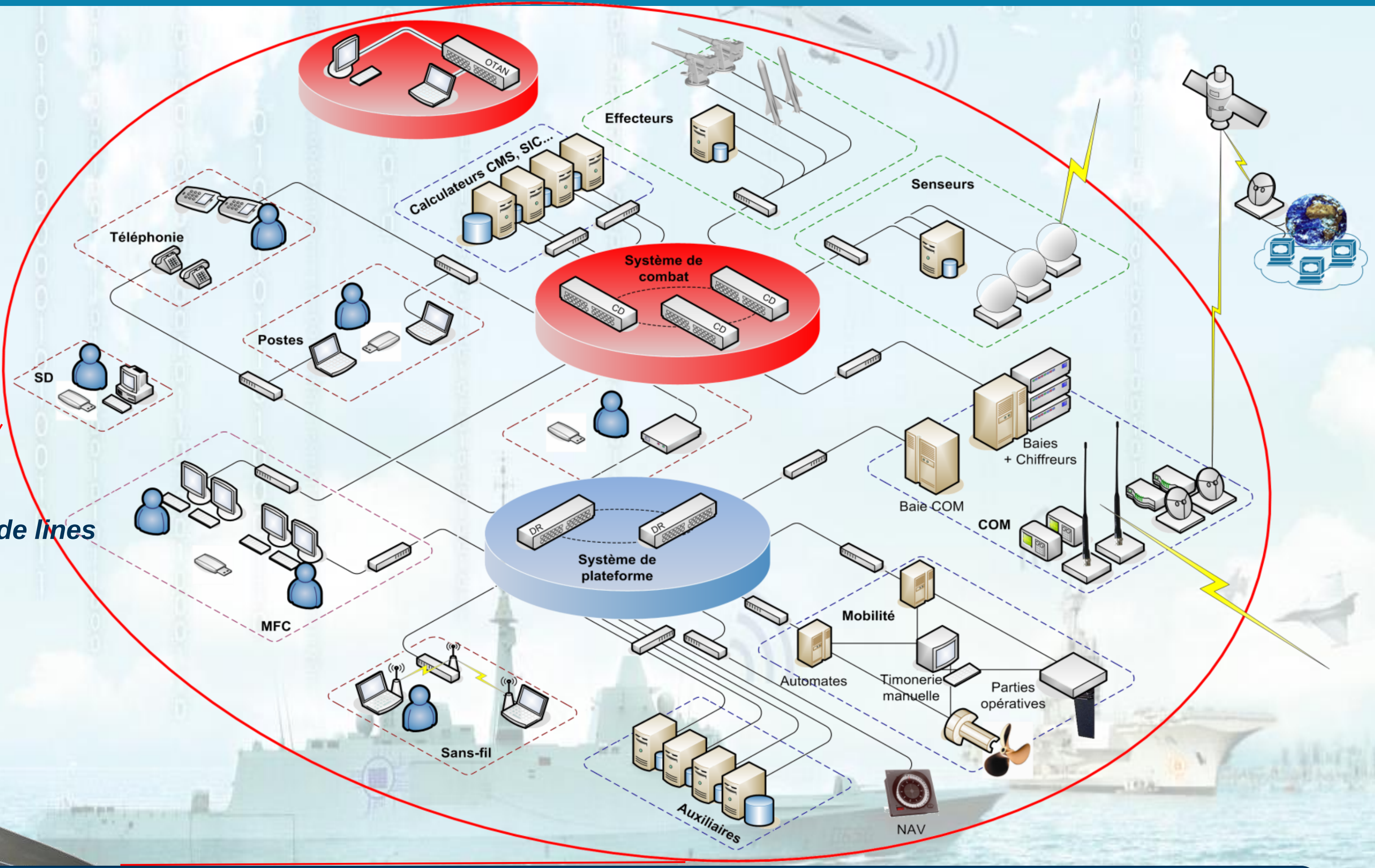
-150 network equipments

-30 real time calculators

-Software :

-CMS : 35 millions of code lines

-SMS : 2 millions



Many technologies + public-military duality

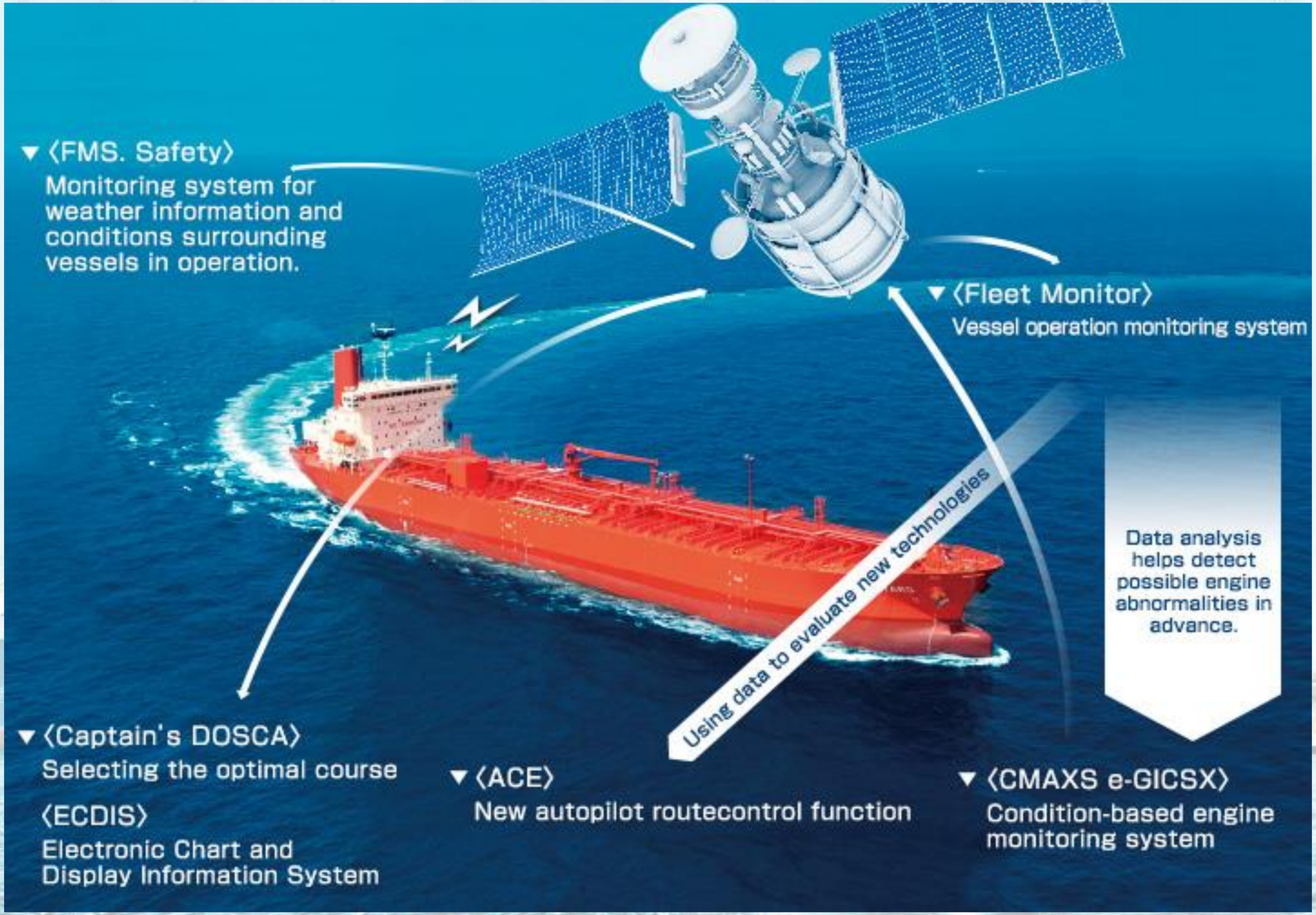
ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Context: Towards the connected ship



▼〈FMS. Safety〉
Monitoring system for weather information and conditions surrounding vessels in operation.

▼〈Fleet Monitor〉
Vessel operation monitoring system

Using data to evaluate new technologies

Data analysis helps detect possible engine abnormalities in advance.

▼〈Captain's DOSCA〉
Selecting the optimal course

〈ECDIS〉
Electronic Chart and Display Information System

▼〈ACE〉
New autopilot routecontrol function

▼〈CMAXS e-GICSX〉
Condition-based engine monitoring system

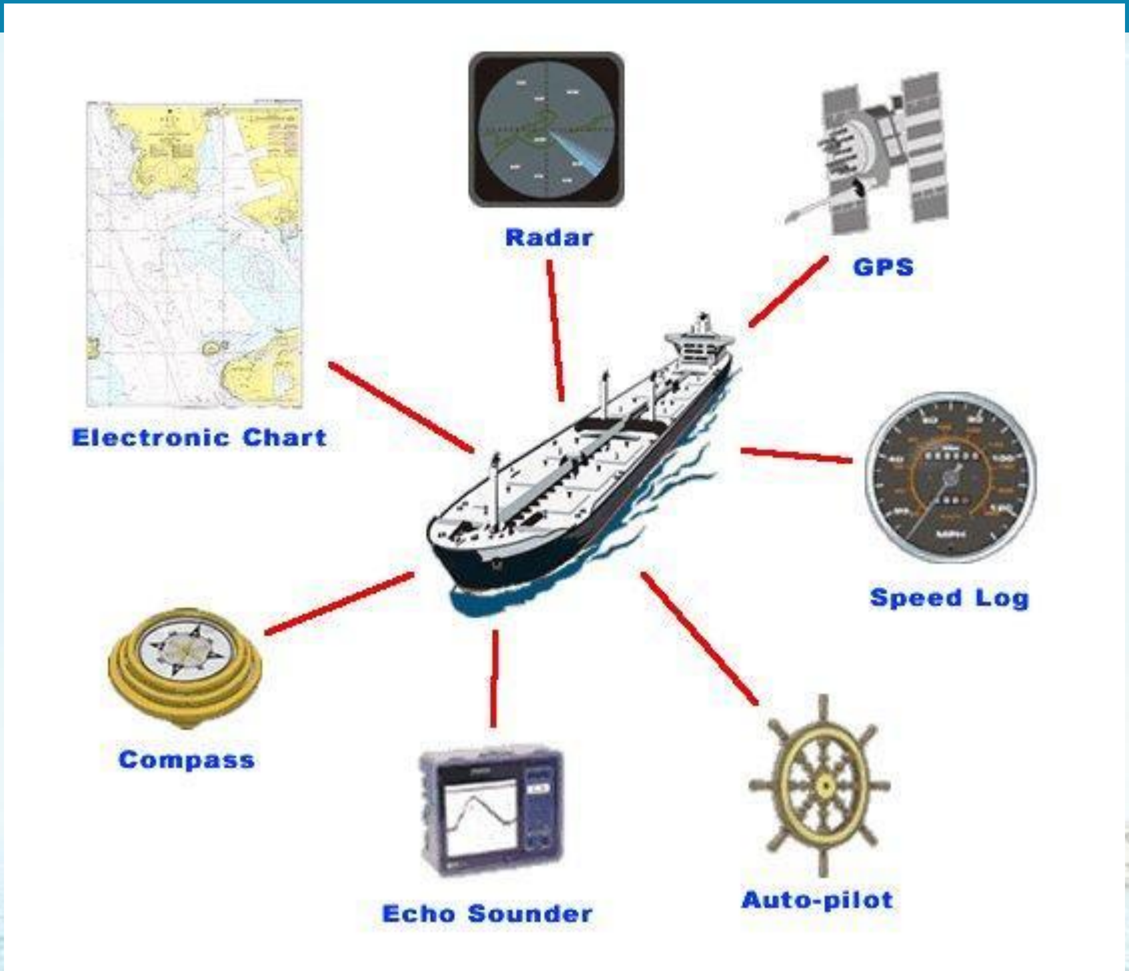
ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

The context: critical information from various sources



30 different navigation equipements on board new ships

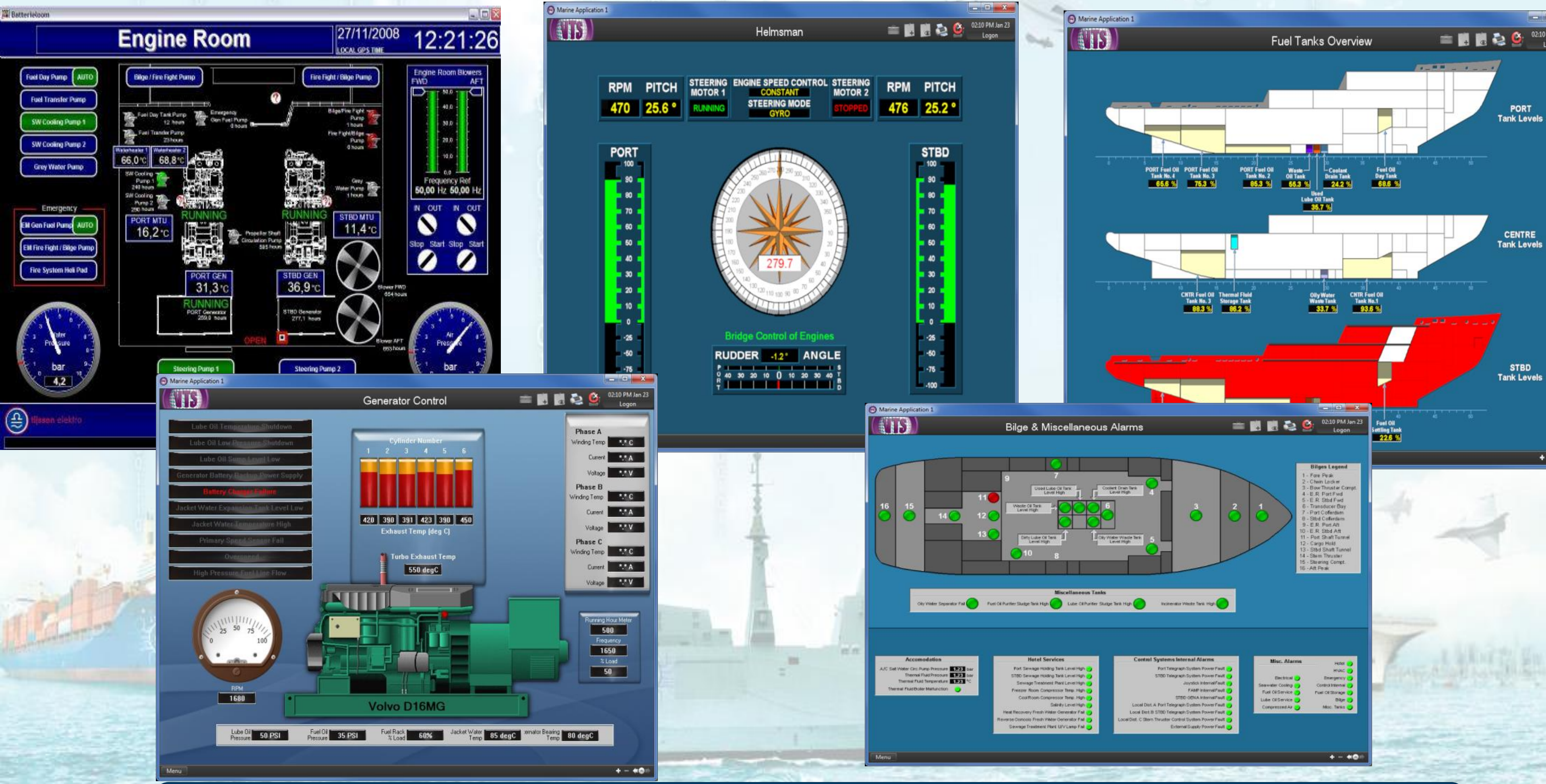
ECOLE NAVALE
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom
NAVAL GROUP
THALES

Technologies inside a ship

- **Public / Military duality**
  - Hardware : PC equipments, industrial systems (SCADA)
  - Operating systems : Linux, Windows
  - Applications: Internet technology (WEB, …), Java
  - Network : TCP/IP, Ethernet, WIFI
  - Network equipments : switches, routers, etc.
  - Communicating devices: GPS, sensors,…

- **Advantages :**
  - Costs reduction
  - Maturity
  - Performances
- **Issues :**
  - global consistency
  - Well known vulnerabilities
  - Weaknesses due to embedded components

A focus on SCADA inside a ship



Critical systems are monitored and controled and hundreds of SCADA systems operate

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Attacks are very common in the cyber space

… and also in the maritime context

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Nature of threats and attacks

Organizations and companies are more and more the target of

- **Generic attacks**
  - **Millions of new malwares are identified every year**
  - **Ships, harbors, oil platforms…. are also concerned as they include PCs and other devices**
- **Specific attacks**
  - **With a specific and identified target**
  - **A well thought and designed approach to reach its goals**
    - A spleeping agent
    - A silent agent which erases its traces and presence
    - An activation in synch with numerous infected targets on a specific triggering event to maximise its effects and dirsrupt

A few threats and attacks in a marine context

NAV sensor alteration

(e.g.; AIS, GPS)

Capture of communications

(no more confientiality)

Remote control of the engine and propulsion

Flooding of the communication networks

Corruption of the acquired situation

Corruption of the data coming from sensors

Unexpected m issile launching

Black out

« energy»

(unavailability)

Complete systems and their environment can be made unavailable

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

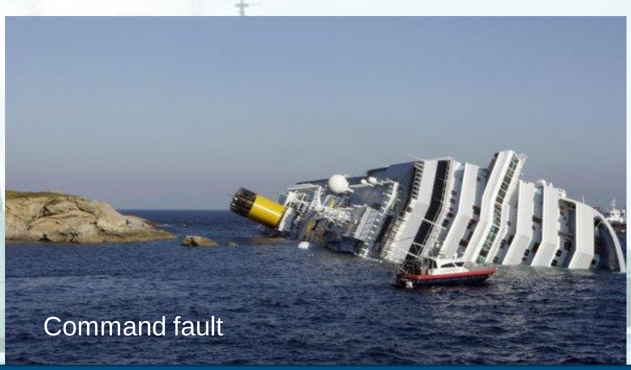
THALES

Cyber threats for naval systems

Uncontrolled shooting

Corrupted loading

Navigation error


Command fault

Cartography error

Consequences of cyber attacks on ships are very dangerous

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

New issues

- **To be taken into consideration :**
  - **Exponential development of threat**
    - ➔ Limitation of CYBER-PROTECTION solutions efficiency
    - ➔ Development of CYBER-RESILIENCE architecture
    - ➔ Development of CYBER-DEFENSE solutions
      - › Detect
      - › Alert
      - › React
    - ➔ Maintain in the time the level of cyber-security
  - **The warship context**
    - - Partially isolated
    - - Reduced crew
    - - Technology complexity
    - - No Cyber expert onboard
    - - Lifetime more than 30 years

Colander = Information System

CYBER SECURITY =
CYBER DEFENSE
+ CYBER PROTECTION
+ CYBER RESILIENCE

With OLS (Operation Level Support) for Security

These elements are the base for the research program of the chair

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Research Program

- Decision aiding system of cyber attacks
- Data and Information quality methods for detecting intrusion
- Naval systems software vulnerabilities and patch management
- Homomorphic encryption in naval environment
- SCADA architecture modeling with security concern
- *Real Time system cyber detection*
- Detection and Protection of SCADA systems
- Context aware system for cyber attacks detection
- *Naval system cyber attacks classification and modeling*
- Safe upgrade of software inside a boat
- Computer aided decision and cyber crisis

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Research program

- The PhD students are supervized by both experts from academy and industry
  - Strong connexion to the context and concerns for ships
- The French Navy provides an evaluation framework
  - When considered as mature, new approaches and solutions can be evaluated at sea
- Outcomes of the research program : to be integrated in operational programs of the French Navy

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

2nd mission of the chair : education

- **Raising awarness and motivate teams**
  - A platform with demonstrators to highlight how an attack can be triggered on a system
  - Demonstrate how to mitigate the weak points with new competences

- **Integrating security in the curriculum**
  - A new module for the Naval academy on cyber security issues
  - A new curriculum at IMT Atlantique on cyber security: with use cases from the naval context

- **Education through doctoral studies**
  - Naval officers to investigate new approaches for the ships of the French Navy

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Initial results : 3 years after the launching

- A coherent team of Phd students, postdocs, faculty members and industrials
- Synergies between the chair stakeholders
- A strong implication with the French Navy and French MOD: evaluation and test in real situations
- A platform to demonstrate initial results and raise awarness through ‘real world’ scenarios
- A new curriculum for the Naval academy and IMT Atlantique

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

NAVAL GROUP

THALES

Perspectives

- The chair has been extended of 3 years (up to 2020)
- A new research program to be approved by the partners that will investigate issues related to system modeling, cartography and threats impacts, computer aided decision in cyber crisis
- More connexions with the French Navy to implement and assess the R&D outcomes
- Develop cooperation with civilian ships and harbor infrastructures

NAVAL GROUP - THALES - IMT ATLANTIQUE - REGION BRETAGNE

ECOLE NAVALE

CHAIRE DE CYBERDEFENSE DES SYSTEMES NAVALS

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

THALES

NAVAL GROUP

Questions