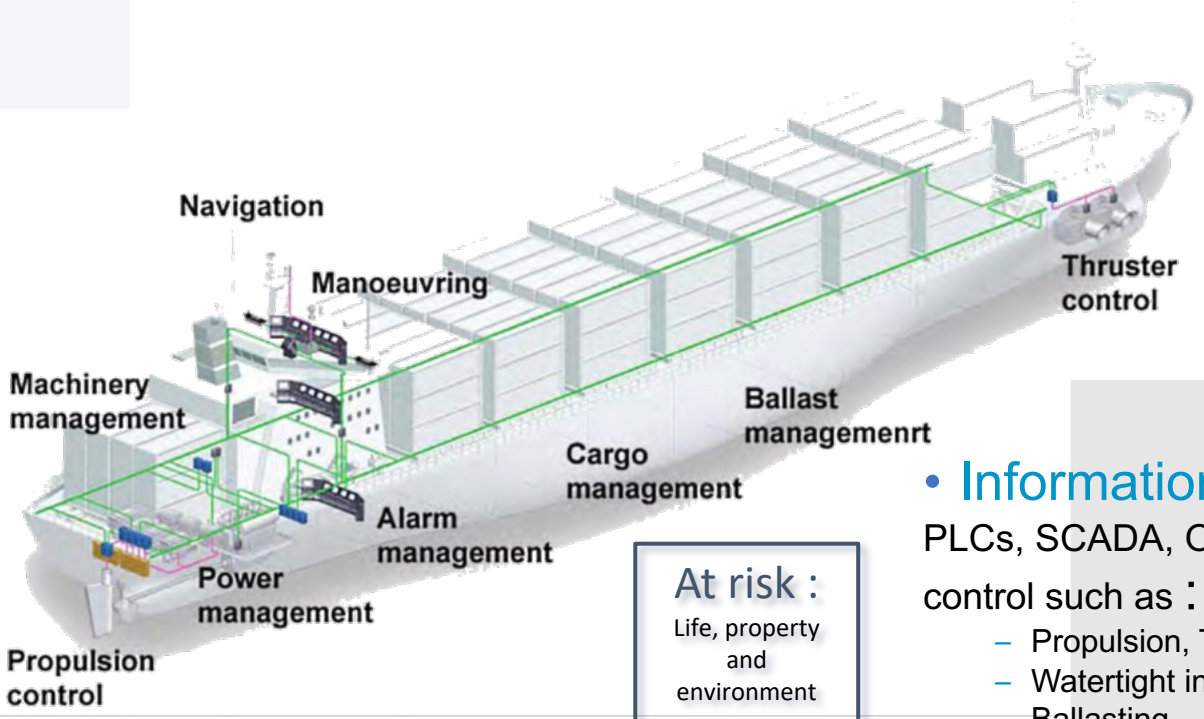
NOZOMI NETWORKS

Monitoring onboard networks

Who cares?

Systems involved on maritime sector



At risk :

Life, property and environment

+

All next

- **Information technology (OT)**

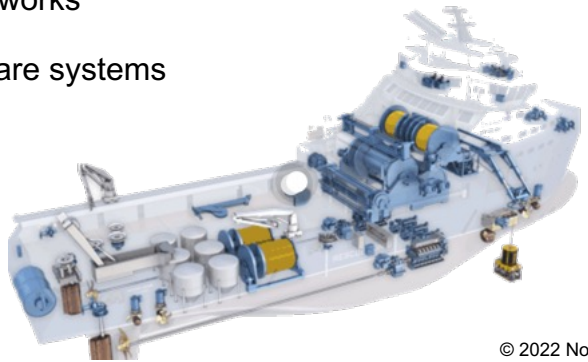
PLCs, SCADA, On-Board measurement and control such as :

- Propulsion, Thrusters and Steering
- Watertight integrity and Fire Detection
- Ballasting
- Power generation and Auxiliary systems
- Navigation and communication (ECDIS, etc.)
- Industrial systems (DP, Drilling, etc)

NOZOMI NETWORKS | Digital Ship

IMO (International Maritime Organization) Vulnerable systems could include, but are not limited to :

- Bridge Systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passengers facing public networks
- Administrative and crew welfare systems
- Communication systems



What can you expect?

Knowing what you have

- First step in every compliance requirement
- You will be surprised
- Create asset inventory
- Identify vulnerabilities, cyber risk
- Defining your normal
- Absolute necessity to segmentation
- Automate, automate, automate

Identify changes

- Unexpected changes in system and network
- ‘Let me fix that quickly’ – Risk behaviour
- Unexpected connectivity between networks
- Troubleshooting tool

Cyber threats

- (We need a skull!)
- Identify malware on the network
- See exploit of vulnerabilities
- New network actions
- Are you under attack? Don’t overreact!
- Incident Response
- Forensics tool

It’s now

- *January 1st 2021 is the date since which the MSC.428(98) resolution of the **International Maritime Organization** requires any flag ship or maritime company to integrate Cyber Security into onboard safety management systems.*

  For vessel owners, this means integrating Cyber Security risk into their SMS by developing and implementing onboard procedures and mitigation measures. First step required as stated by the IMO resolution is the inventory of at risk systems

The need is mostly driven by rules and regulations

- **ISM Code (International Safety Management)** : *Assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards*
- ***IMO*** *Resolution MSC.428 (98) on cyber risk management – from January 2021*
- **USA Cost Guards**
  To impose Cyber Security to vessel going to USA
- ***ENISA :*** *European Union Agency for Cybersecurity : Guideline for Navigating Cyber Risk – 17th December 2020*
- **National and regional Cyber security and Data Privacy laws and regulation**: *E.g US CG Cyber Security Profiles and CG-5P Policy Letter 08-16, EU GDPR, EU critical infrastructure – Directive(EU) 2016/1148, UK Code of Practice, etc …*
- **Cyber security exclusion clause in insurance**: (Clause 380) exclude coverage of cyber security incidents.
- ***OCIMF (Oil Companies International Marine Forum)*** *: Tanker Management and Self Assessment (TMSA) – As January 2018 / In Evaluation for dry-cargo ships*

Which can end with typical security incidents

Why Nozomi Networks

- Existing deployments on vessels and in harbors
- Designed to work off-line or over satellite com
- Centralized visibility of the entire fleet in the cloud
- Data analytics to help prioritize resources and budgets
- Alerts and incidents notification centrally in real time
- Specific maritime use cases
  - NMEA protocol support
  - Possibility to cover maritime specific situations with custom rules

NOZOMI NETWORKS | Digital Ship