Regulations, recommendations and status

**Regulations**

IMO Resolution MSC.428(98)

MSC-FAL.1/Circ.3

**Guidelines, recommendations and additional Class Notations**

Maritime industry guidelines

IACS UR E22

IACS Rec166

RINA Additional Class Notation on Cyber Resilience

**Received requests**

Gap-analysis vs. regulations and guidelines

onboard assets inventory

Training and awareness courses
## Recommendations and main gaps

### Main topics from recommendations and guidelines

- Risk assessment
- Definition of roles and responsibilities
- Asset identification and valuation
- Risk treatment
- Detection capabilities
- Response plans
- Recovery actions
- Continuous improvement

### Main gaps

- Too specific/non-inclusive risk assessment
- Roles and resp. are often not well defined
- Too little knowledge about onboard assets
- Not clear risk treatment
- Detection could be fine, response not always
- Poor or non-existent response plans
- Lack of awareness about recovery actions
- Untrained personnel
Provided activities & direct experiences

- Gap-analysis vs local regulations
- Gap-analysis vs guidelines (BIMCO/TMSA3/DCSA/…)
- Support to risk assessment
- IT/OT inventory
- Support to ISM manual integration
- Training and awareness campaigns
- Vulnerability assessment
- Penetration tests
Ships design and onboard systems

Over the years the Ship’s Design evolution increase the complexity of the onboard systems evolving from simple stand-alone Systems to Integrated Systems.

More and more the demand for ship to shore remote connectivity for maintenance, remote monitoring is increasing daily.
What we have onboard?

Last generation Ships has increased their functionality and performance of Primary and Secondary essential services by a strong dependence from:

- Electrical and Electronic Systems
- Software dependant Systems.

Essential systems and/or sub-systems based on:

- Microcontrollers
- Programmable devices including Software and Firmware
- Computer Based networks
- Smart Sensors

are weaknesses to be identified and highlighted in the process.
Where could be the problem?

**OT/IT Asset Inventory** is one tool adopted to identify and categorize the systems installed onboard - recalled by UR E22 – Rec 166

From new building ships to existing ships this is a solution to become confident of the type of the system present onboard during all the ship lifecycles.

- Inventory List of computer based systems
- Physical map of the computer based systems
- Physical Inventories including locations
- List of network communication devices and access
- Logical map of networks
- Software & Firmware Inventories
Training - Protection & Detection

Being aware of onboard processes and the importance or criticality of some elements/systems is the first step for proper management of cyber risks, starting with familiarization with the onboard systems, protection against unauthorized access, traceability of update/upgrade and detection of potential incidents.

Unfortunately, experience shows us that there is still a lot to do:

- Password in sight;
- USB ports of which - sometimes - the purpose is not clear;
- Logic cards with too easy physical access;
- Access keys to technical rooms / critical systems not properly managed;
- Poor awareness of abnormal behavior or containment and protection measures;
- Excessive trust in external maintainers;
- Lack of configuration management;
- Etc.
Any Questions
Thank You For ATTENDING