MASS (Maritime Autonomous Surface Ships)

2nd ENISA Maritime Cybersecurity Conference

14 October 2022

Luca Gargano & Santiago Encabo
Senior Project Officers
Ship Safety & Security Unit

EMSA
European Maritime Safety Agency

MASS (Maritime Autonomous Surface Ships)

- Right name? - Autonomy vs Automation
- Natural evolution of technology

- But MASS brings something else – Technology exists BUT Operational Revolution – change of paradigm

MASS – Change of Paradigm

Regulatory

- Master of the ship
- Seafarers/qualifications
- Liability – 3,200 incidents EMCIP annually
- Safety standards
- Pilotage

Infrastructure

- Remote Control Stations
- Communications
- Ports
- Digital

MASS – Change of Paradigm

Operational

- Co-existence with conventional ships
- Obligation to render assistance
- Training
- Enforcement: Inspections/Surveys
- Pilotage
- Cybersecurity, e.g, routeing – positioning spoofing might have more critical consequences in MASS – collisions, etc.

Technology

- Software certification
- Standards/Protocols, including testing, e.g. communications protocols, connectivity, collision avoidance - COLREG
- Ports
- Communication costs?

Why autonomous or automated ships?

Aspirations of

- Improved safety – human factor
- Improved sustainability – alternative fuels, routeing
- Lack of seafarers
- New business models – new shipowners?
- Financial benefits - OPEX

What is going on? (non-exhaustive)

- **EU Projects – AUTOSHIP, AEGIS, MOSES, MASS 5G, MUNIN (2015)**
- **EMSA – RBAT and CMORCC**
- **JAPAN – DFFAS Project – Demonstration 790 km Feb/Mar 2022 Containership congested routes**
- **Finland – One Sea environment**
- **Realities:**
- Yara Birkeland & ASKO Autobarges - Norway
- Avikus (South Korea) – voyage of 10,000km without human intervention

Regulatory Side

IMO

Non-mandatory Code in 2025, and mandatory in 2028

Until that moment – Alternative Design

European Commission

EU Operational Guidelines on trials of MASS

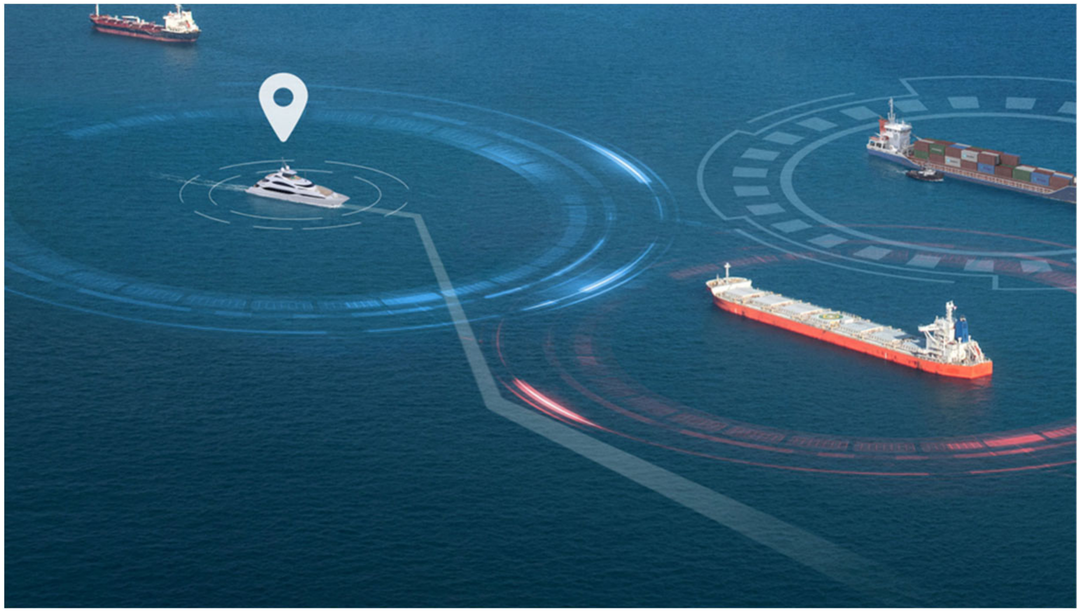
SAFEMASS study, Risk-based assessment tool (RBAT), seafarers

WORKSHOP 29 NOVEMBER

MASS needs to communicate

Operations:

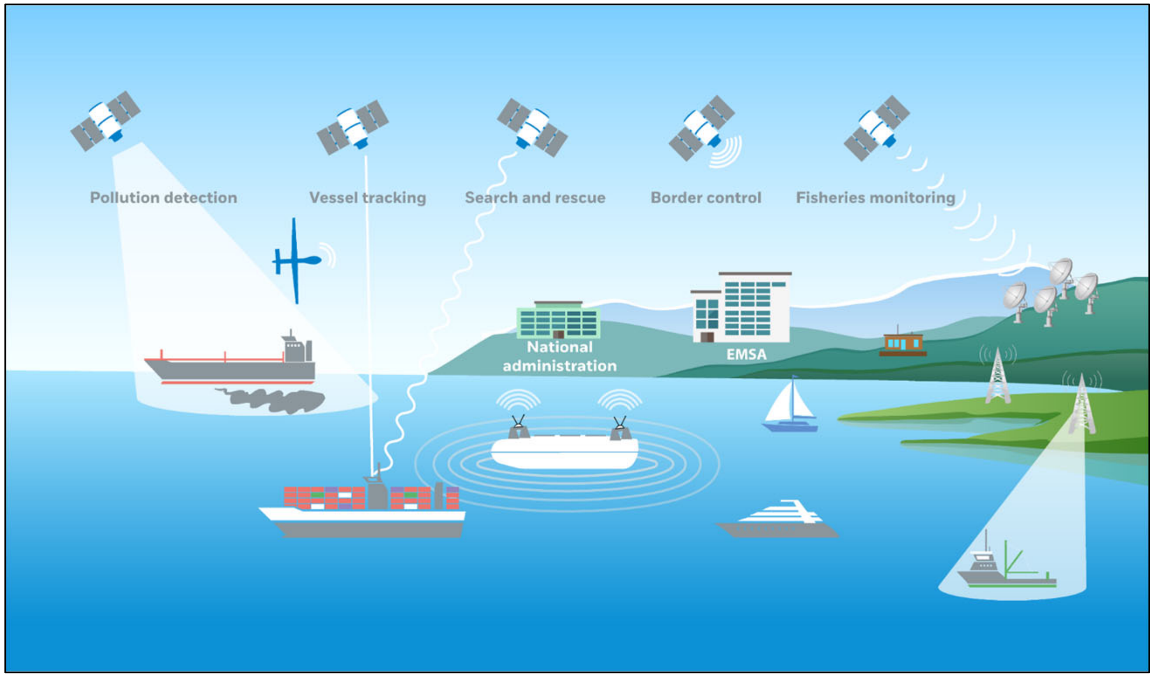
- Situational Awareness – video, sensors, voice, etc.
- Decision making
- Execution
- Mitigation measures, e.g., redundancy



MASS needs to communicate

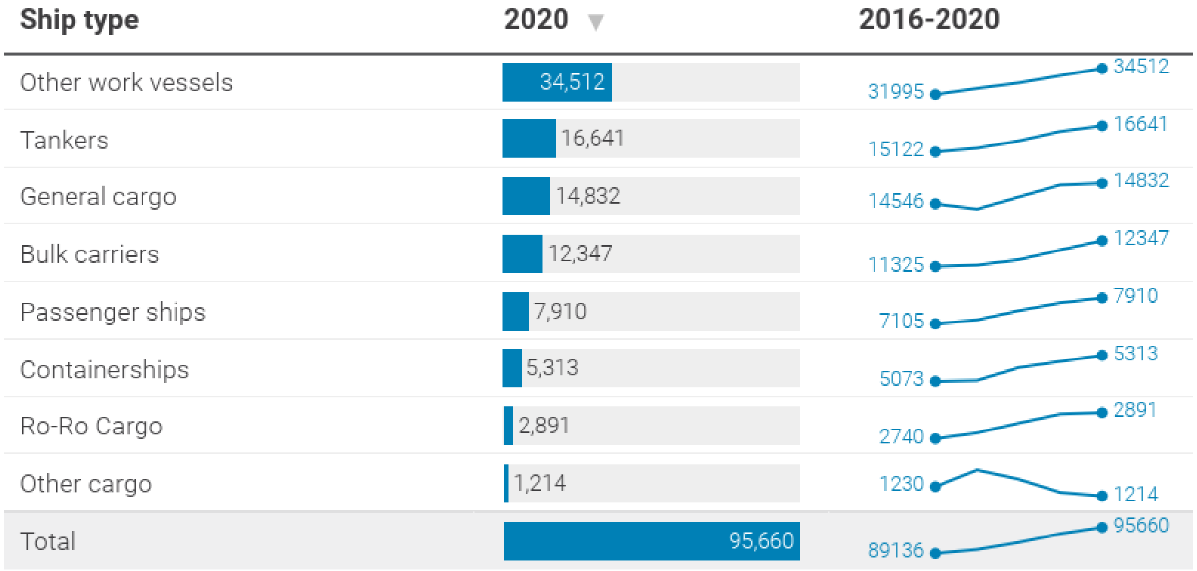
Third parties:

- Other conventional ships
- Remote control station
- Shipowner fleet management
- Government: Vessel traffic monitoring, SAR, naval ships, rules innocent passage, incidents, etc.
- Emergencies
- Obligation to render assistance
- Ports
- EU Single Window – mandatory ship reporting (e.g., HAZMAT)



Impact

- **Global fleet 95,000 ships approx.**
- **Annual growth 1.4%**
- **>500,000 port calls annually EU**
- **Adoption of MASS? soon to knov**
- **Needs:**
- Video signals transfer
- Voice
- Sensors digital data
- Positioning – routeing
- Cybersecurity
- Redundancy



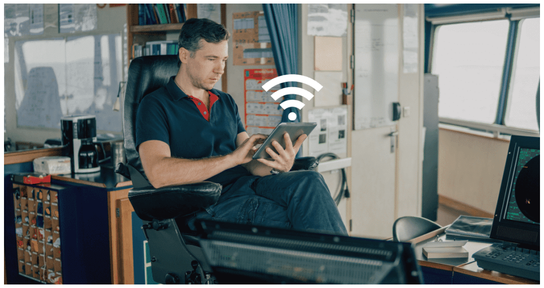
Ship type	2020 ▼	2016-2020
Other work vessels	34,512	31995 34512
Tankers	16,641	15122 16641
General cargo	14,832	14546 14832
Bulk carriers	12,347	11325 12347
Passenger ships	7,910	7105 7910
Containerships	5,313	5073 5313
Ro-Ro Cargo	2,891	2740 2891
Other cargo	1,214	1230 1214
Total	95,660	89136 95660

MASS – Cybersecurity aspects

Cybersecurity on a traditional ship

Elements to be assessed (some):

- Password management on board
- Access control system
- Usb stick policy
- Social engineering and phishing…
- …



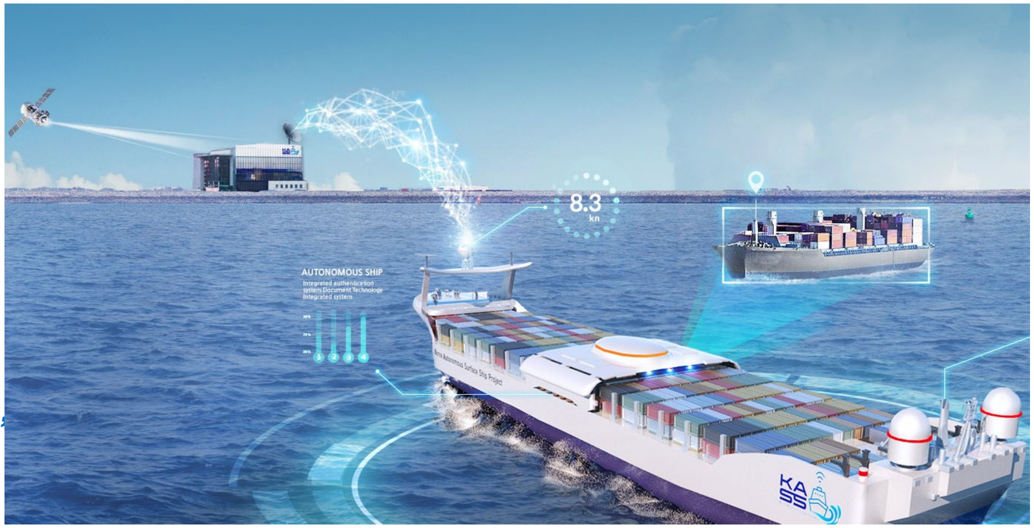
Cybersecurity on a MASS

Elements to be assessed:

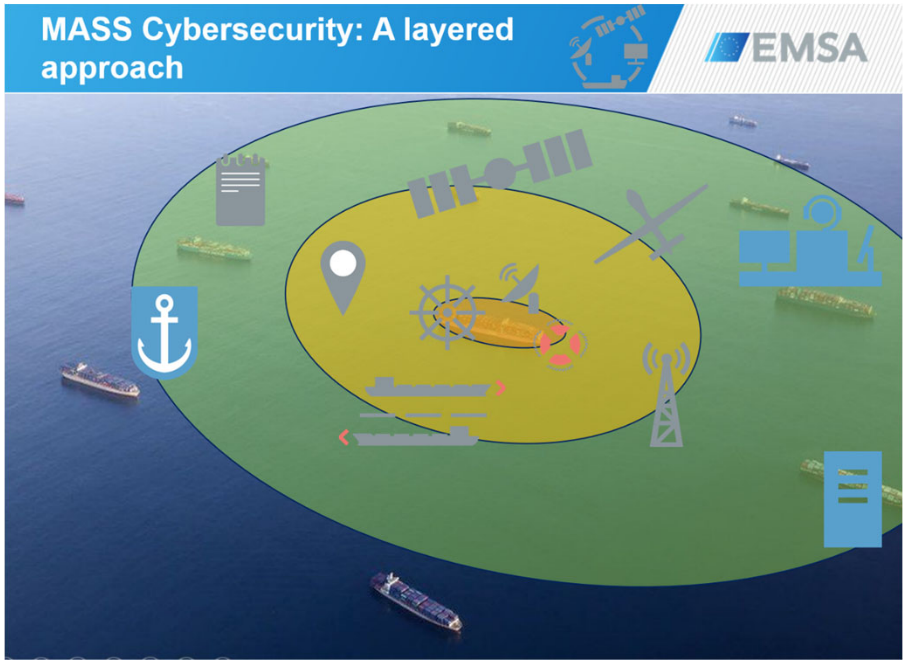
Change of focus

Networks

- Navigational networks *(Communication protocols IEC)*
- Automation and Safety *Networks (Sensors to control Operational Technologies)*
- Line-of-sight Networks *(VHF channels near the cost)*
- Ship to Shore Networks *(Satellite communications, Inmasart, Iridium etc.)*



MASS cybersecurity. Layered approach



MASS Cybersecurity: A layered approach

- **Core layer**
  (shipboard operations related)
- **Periphery layer**
  (exchange of data for safety & security reasons, primarily)
- **Edge layer**
  (communication with SCC for supporting operations)

Different layer → different impact

Potential countermeasures

Channel coding, channel hopping multiple-input mitigation measures etc.

Against → jamming attacks

Redundancy of sensor technologies, use of remote image sensors etc.

against → spoofing and man-in-the-middle attacks

Cryptography, segregation and segmentation of OT networks etc.

against → communications attacks

Strong passwords, disabling unused ports or services, updating of all components etc.

against → OT systems attacks

Third-party security certification, setting additional requirements for vendors etc

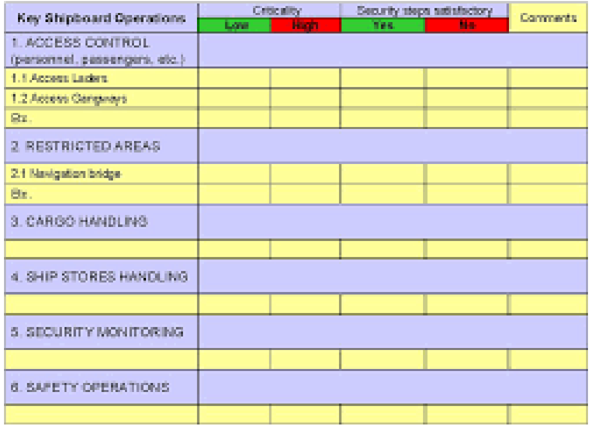
against → supply chain attacks

Where to address cybersecurity?

Ship Security Assessment

ISPS Code A8.4.2

- Identification of existing security measures, procedures and operations
- Identification and evaluation of key shipboard operations that is important to protect
- Identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures
- Identification of weaknesses, including human factor, in the infrastructure, policies and procedures



Key Shipboard Operations	Criticality		Security steps satisfactory		Comments
	Low	High	Yes	No	
1. ACCESS CONTROL (personnel, passengers, etc.)					
1.1 Access Laders					
1.2 Access Gangways					
Etc.					
2. RESTRICTED AREAS					
2.1 Navigation bridge					
Etc.					
3. CARGO HANDLING					
4. SHIP STORES HANDLING					
5. SECURITY MONITORING					
6. SAFETY OPERATIONS					

Cybersecurity on MASS – Final considerations

- More critical considering the heavy reliance on ICT for ship control
- The impact would be more disruptive
- The human factor is less relevant
- More structrural than operational, hence cybersecurity should be set from te ship design
- Still limited attention has been paid on the subject

emsa.europa.eu

twitter.com/emsa_lisbon

facebook.com/emsa.lisbon

EMSA

European Maritime Safety Agency