Unmanned shipping in Italy: a technical insight

Paolo Pagano

Head of «Technology Transfer» Research Sector
Director of CNIT Laboratory @ Port of Livorno

cnit consorzio nazionale interuniversitario per le telecomunicazioni

GECON 2026 (21st edition)
Pisa, Sep. 9th, 2026

Outline

- Foreword:
  - The CNIT research labs at the Port of Livorno
- Relevance for GECON communities
- Setting the scene (The Autonomous Ship)
  - the IMO regulatory framework
- MASS trials in Italy
  - Performance analysis
  - Cybersecurity requirements
- The Experience Building Phase
  - Cybersecurity through narrative
  - MASS & e-Navigation testing platform in Livorno
- Conclusions and Outlook

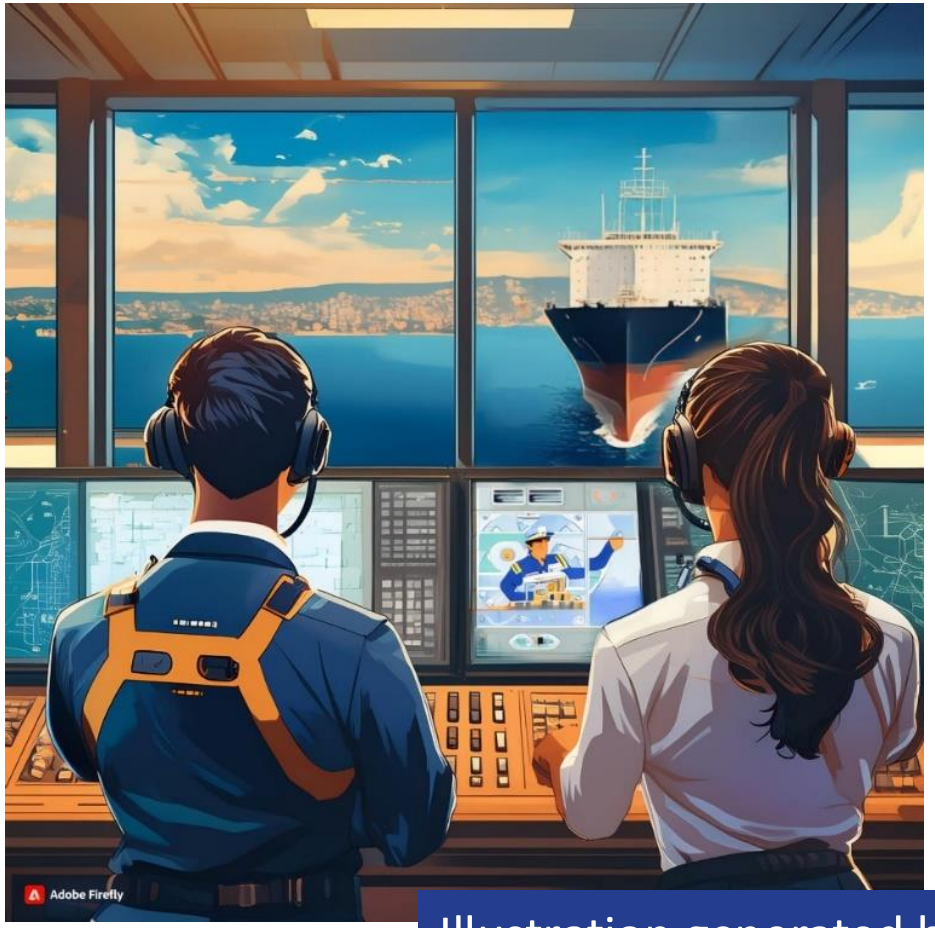
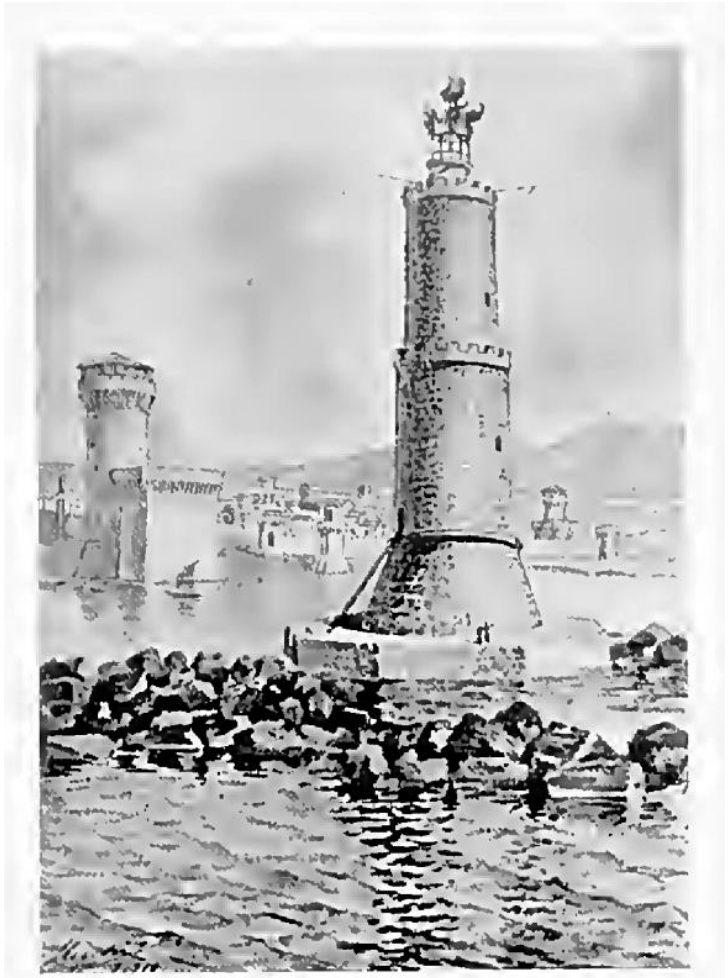


Illustration generated by AI



LIVORNO CON LE PRIME MURA PISANE E IL FANALE RIPRISTINATO. (DA ANTICA STAMPA).

Foreword

Port of Livorno

- Mid-size historical port:
  - industrial and institutional importance (Naval Academy);
  - passenger and freight hub (multipurpose), rail-road terminal, and car park;
  - core node of the TEN-T SCANMED corridor;
  - headquarters of the Maritime Directorate of Tuscany (ITCG) and the Northern Tyrrhenian Sea Port System Authority (AdSP);
  - research laboratory active for 13 years with structured collaborations with the ITCG and the AdSP.

Vulpes Veneta, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=93913824

Livorno: Port of the Future

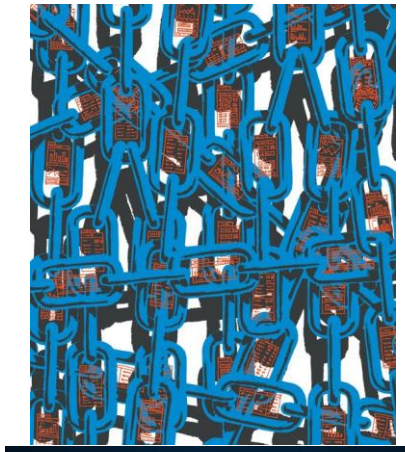
- An evocative venue: the «Glass Cube»
  - Original building by Arch. Carlo Reishammer (1840), destroyed in II WW (1943), Philological Restauration completed in 2015 (German Design Award 2018)
- CNIT Laboratory at the Port of Livorno:
  - Italian unique example of laboratory committed in the development of E2E ICT solutions at high TRL (> 6) tailored to Ports and Navigation
  - Pioneer of 5G in European ports according to Ericsson
- Founded in 2015:
  - Framework agreements w/ Livorno Port Authority (JLAB) and the Italian National Coast Guard;
  - Part of the National Laboratory of Photonic Networks and Technologies (PNT) in Pisa;
  - Part of CITEM – Livorno Center of Innovation and Technology for the Blue Economy.

GERMAN DESIGN AWARD

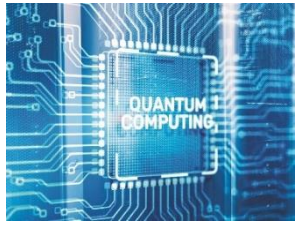
AdSP MTS

CAPITANERIE DI PORTO 1865 GUARDIA COSTIERA

Lab technical scope and profile



- ICT assets
  - T/NT nets, sensors, custody, cyber-security
- (Looking from the outside) at innovation trends
  - AI, Quantum, Automation, Green, UxV, etc.

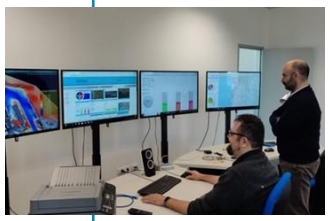


Experimental ICT infrastructure in Livorno

Cloud computing paradigm

Computational Resources

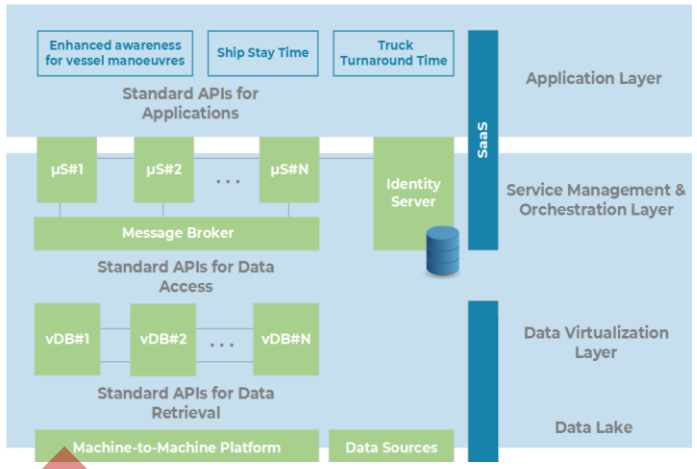
IaaS

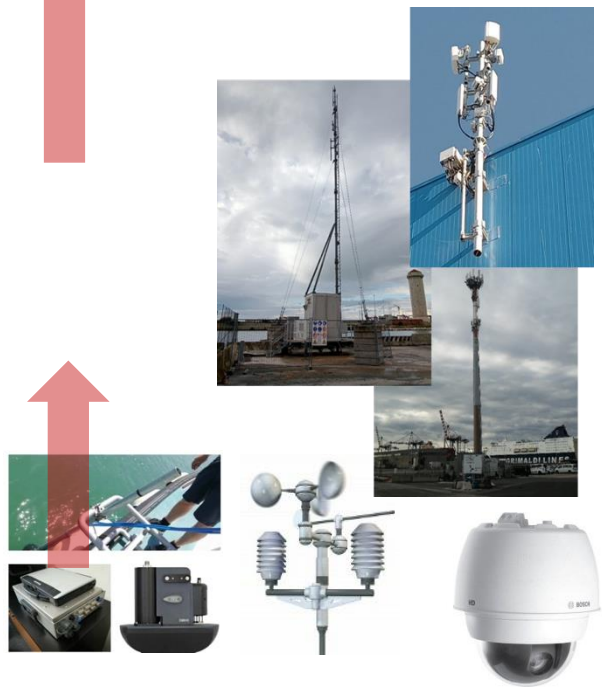


Connectivity Infrastructure

+ 3rd parties (AdSP, CGCP)

Devices & On-Field Equipment





SaaS

PaaS

INTERNET

VPN and firewall for external access (authentication based on RSA keys).

Software Resources
- VMware/Proxmox hypervisors,
- Set of distributed VMs, organized in cloud tenants
- Docker Swarm, Kubernetes (Docker containers orchestration),
- Full virtualization of the data plane,
- Blockchains,

Wired Connectivity:
- Fiber Optics backbone (port, AdSP)
- TIM GBE (lab, CNIT)

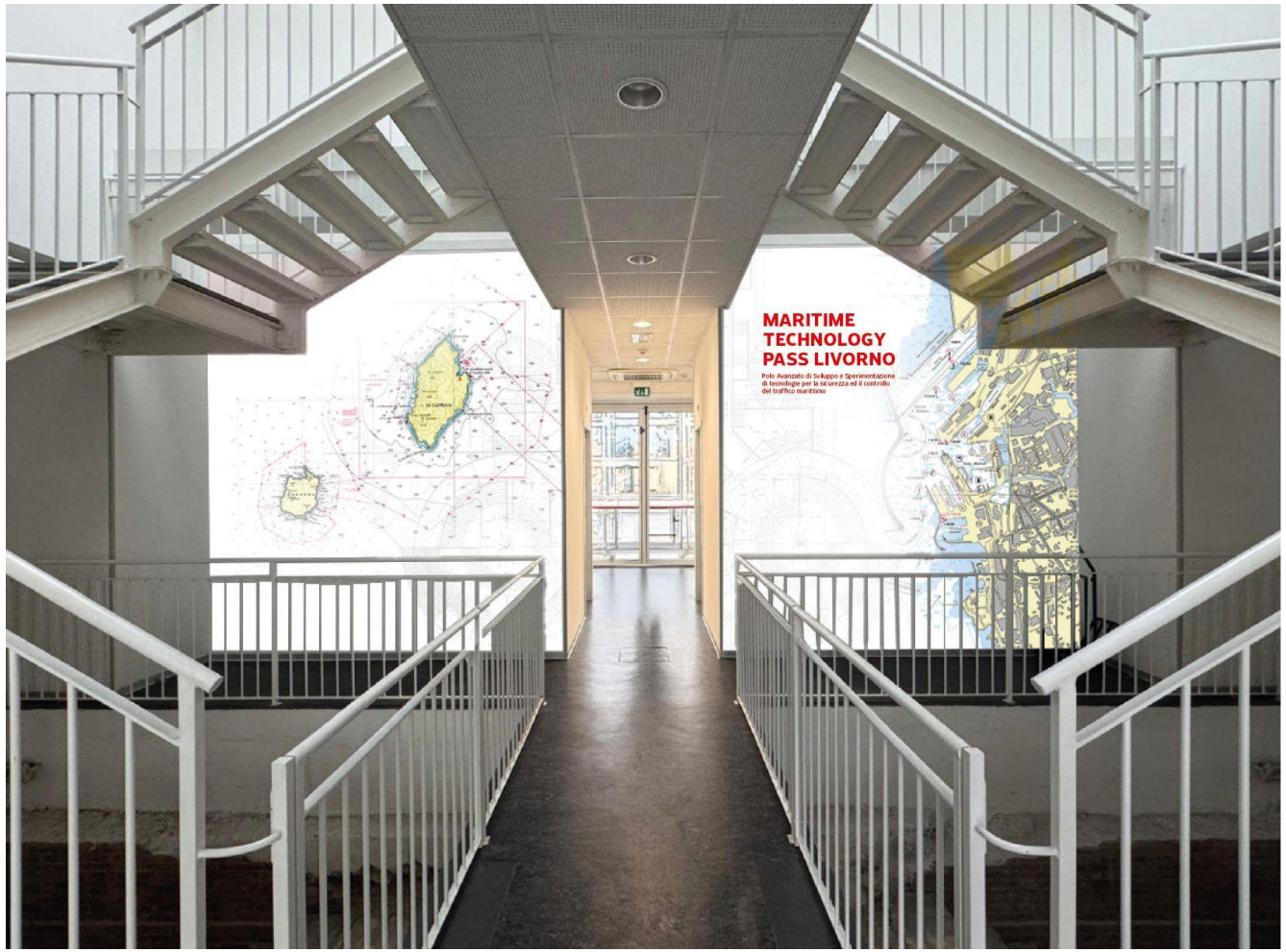
Wireless Connectivity:
- private 5G network (TIM/Ericsson),
- P2P 60 GHz, LoRA (indoor),

IoT Devices:
- Bathymetric probes,
- meteorological stations,
- meteo-marine stations,
- acoustic sensors,
- photonic/electronics radars,
- C-ITS equipment,
- HD cameras, Lidars
- Vessel ECDIS / AIS,
- GPS trackers.

Cybersecurity :
- Resilience and Business Continuity,
- Cyber-security processes (anomaly detction),
- SECOM framework

IoT Connectivity:
- WiFi, C-V2X, G5, 5G, 4G/NB-IoT (TIM commercial), SAT-Com .

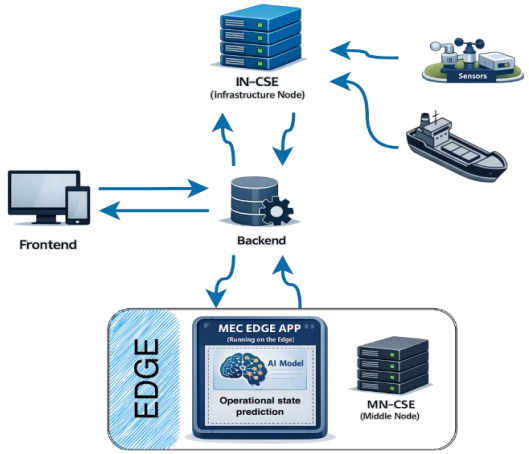
CNIT and Leonardo Electronics



- Leonardo Electronics Division (LED) and CNIT started in 2026 (see here):
  - Advanced Center for the Development and Experimentation of Maritime Technologies (Maritime Technology PASS);
  - to develop state-of-the-art technologies and systems for the Safety and Control of Maritime Traffic for the domestic and international markets.

MT-PASS
LIVORNO

Ongoing Development



MEC and OneM2M

Coastal Surveillance

Freight tracking and monitoring

AdSP MTS

PCS and logistics

Autonomous Vessel

Agenzia Spaziale Italiana

esa European Space Agency

Capitanerie di Porto 1865 Guardia Costiera

Setting the scene

How is GECON community engaged?

"As a global market for infrastructures, platforms, and software services emerge, the need to understand and deal with its implications and its interdisciplinary challenges is quickly growing. To address this, GECON encourages the submission of papers, which combine at least one economic/legal area and one technologic area."

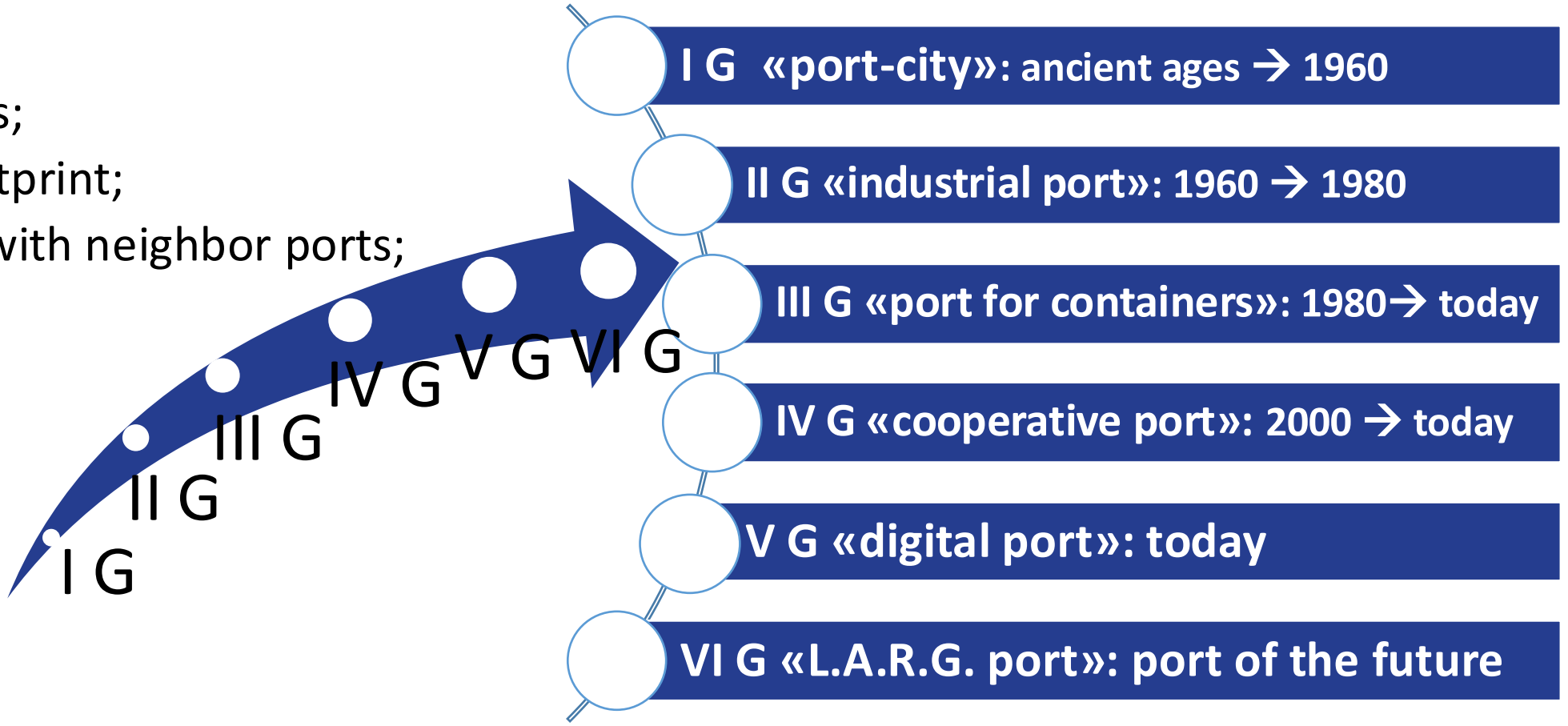
- GECON list of areas includes but is not limited to:
  - Economics
  - Applications and Technologies Transforming the Economy
  - Clouds, Grids, Systems and Services
  - Law and Legal aspects

The Maritime Global Market

- The global merchant fleet comprises approximately 112,500 vessels and more than 2.5 billion dwt of transport capacity, enabling over 80% of global merchandise trade by volume.
  - UNCTAD stats: https://unctadstat.unctad.org/insights/theme/108
- With fleet capacity expanding by around 85 million dwt annually and digital transformation becoming a strategic priority, maritime digital services have evolved into a market worth approximately $554 million. Growth is being driven by increasing demand for onboard IT management, cloud services, cybersecurity, operational analytics, and crew connectivity solutions.
  - UNCTAD stats: https://unctadstat.unctad.org/insights/theme/107
  - Valour Cosultancy: https://valourconsultancy.com/press-release-commercial-revenue-to-maritime-digitalisation-services-surpassed-over-530-million-in-2024/

Seaways nodes: generations of Ports

- Dimensions:
  - port purposes;
  - industrial footprint;
  - cooperation with neighbor ports;
  - digitalization.
- LARGe-ness:
  - Lean;
  - Agile;
  - Resilient;
  - Green.



Credits: prof. Francesco Russo – Easylog final event, May 27th, 2021

Vectors: Next-Generation Merchant Ships

- Next-generation merchant ships integrate advanced technologies and sustainable solutions to improve efficiency, safety and environmental performance.
  - Sustainable Fuels (LNG, methanol, ammonia, hydrogen) and Energy Efficiency
  - Digitalization & Smart Operations
  - Safety & Autonomy
  - Circular Design
  - Human-Centered On-Board env
  - Data-driven performance assessment

Illustration generated by AI

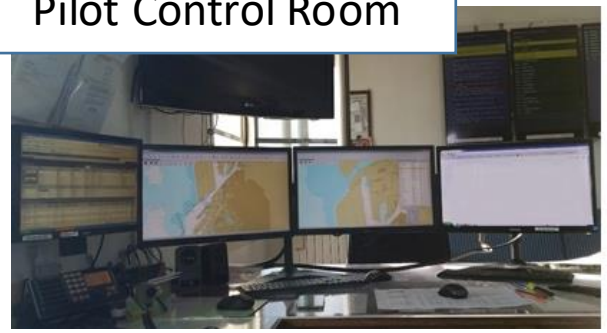
IHO IMO UNECE IALA

Essential elements

Vessel Bridge

Vessel Traffic Services (Coast Guard)

Pilot Control Room

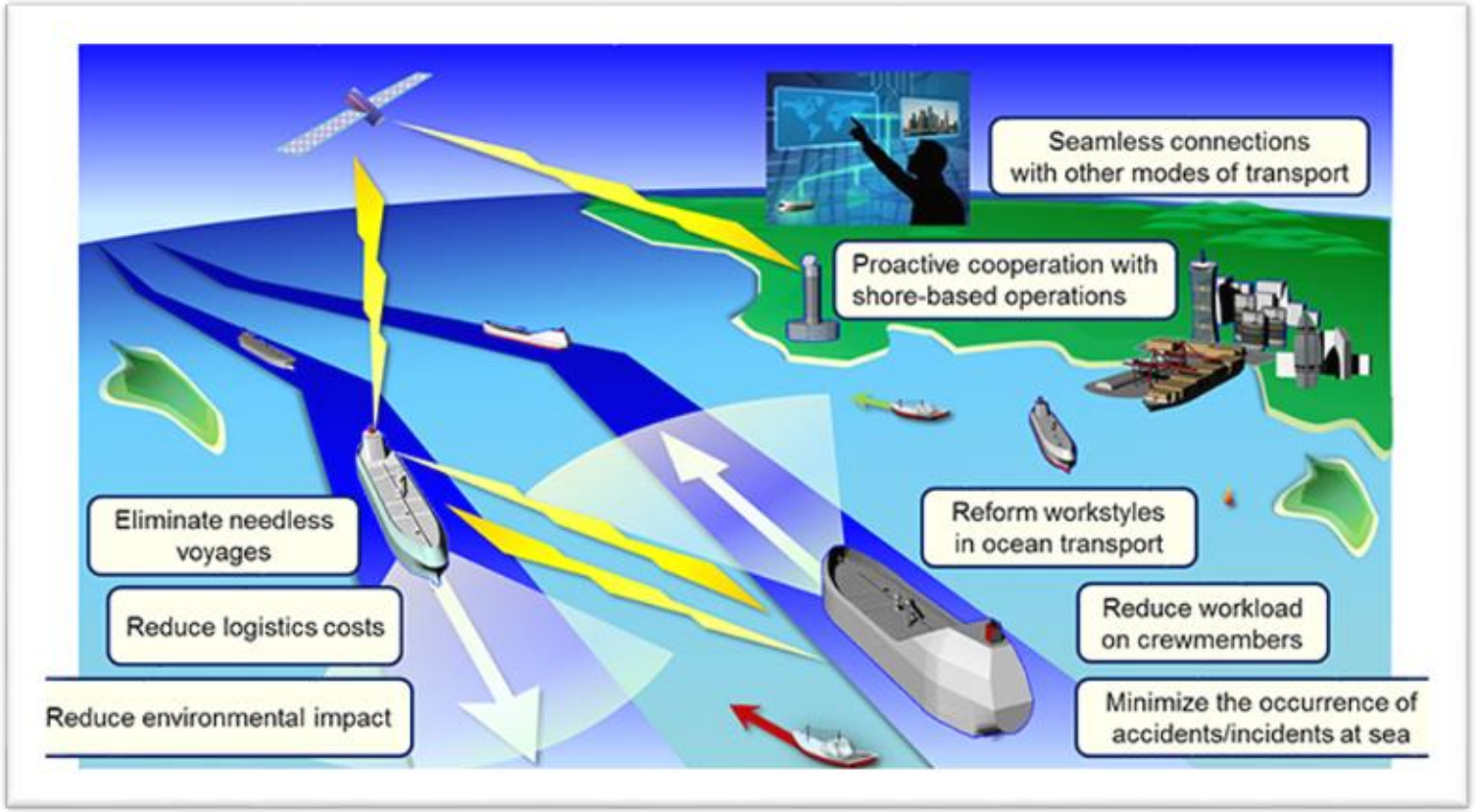


Remote Operations Center (Shipping Line)

- A Maritime Autonomous Surface Ship (MASS) is a vessel that uses automated or autonomous systems to navigate, operate, and perform missions with reduced or no onboard human intervention.
- A Vessel Traffic Service (VTS) is a marine traffic monitoring system established by maritime or port authorities, similar to air traffic control for aircraft to improve the safety and efficiency of vessel traffic and protect the environment.
- A port pilot guides ships safely through harbor approaches, channels, and berths, advising captains on local waters, traffic, tides, regulations, and maneuvering to ensure efficient, secure port operations and navigation.
- A Remote Operation Center for MASS monitors, supervises, and controls Maritime Autonomous Surface Ships from shore, managing navigation, safety, communications, mission execution, and emergency response while supporting autonomous decisions effectively.

In «medias res»

Autonomous ships in the world…Why?



Courtesy of Vice Admiral (ITCG) Luigi Giardino

Ship Automation Levels: industry and flags

- An autonomous ship should be able:
  - to monitor its own health and environment,
  - communicate obtained information, and
  - make decisions based on that without human supervision.
- The idea of autonomous ships has existed for decades and is becoming a reality:
  - IMO Maritime Safety Committee @ the 5th session (1964).
- Fully automatic dynamically positioned vessels:
  - common in the offshore industry in the 1970's;
  - use of on autonomous cargo ship demonstrated in Japan in the 1980's.
- Today:
  - fully autonomous Unmanned Surface Vessels (USV's) already opearional in coast guard and military applications;
  - MASS's are experimented by some flag states (e.g. Norway, Korea, Japan) and expected to turn operational soon.

INTER-GOVERNMENTAL MARITIME CONSULTATIVE ORGANIZATION

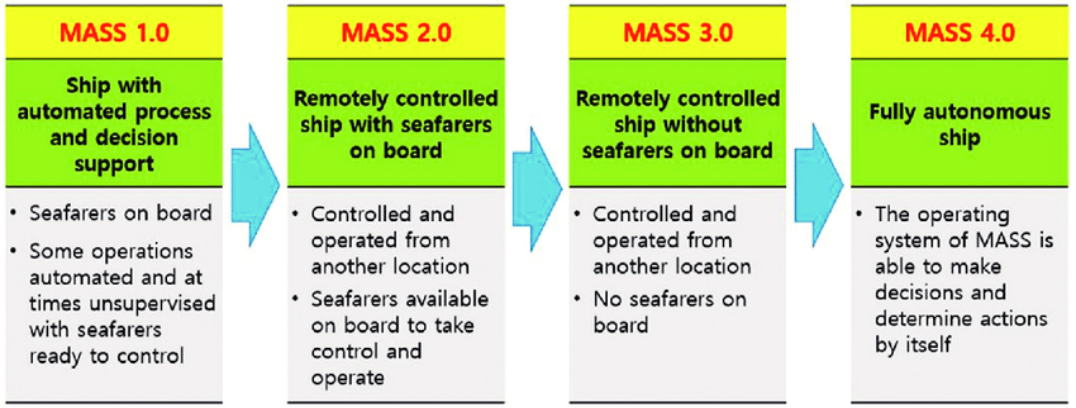
IMCO

MSC VIII/11
9 March 1964
Original: ENGLISH/FRENCH

MARITIME SAFETY COMMITTEE COMMITTEE - 8th session
Agenda item 11

AUTOMATION IN SHIPS

Note by the Secretariat



Towards unmanned shipping at the IMO

- Voluntary MASS code approved by IMO:
  - formal MSC.595(111) resolution
    - in force from July 1st, 2026
- Specifying high-level directives for:
  - ROC functionality
  - ship assets
  - port physical/digital infrastructure
  - ROC/MASS certification process
- Experience Building Phase
  - data collection and repositories to be agreed in Dec 2026 (MSC.112)
  - mandatory code development (2030-2032)
  - entry into force on Jan 1st, 2032

Illustration generated by AI

MASS shipping growth trajectory

- Total world fleet = 112,500 ships (*)
- MASS are limited in number (less than 1%):
  - receiving a boost from MASS code approval;
  - according to IALA, a gradual increase in autonomous vessels (no exponential adoption yet);
  - MASS will mostly be remotely operated (from a ROC)

Metric	Value
Regulatory phase	Transition → Conventional (2026–2032)
Expected CAGR	~7% – 10% (No official forecast, average of industrial analyses)
Growth drivers	Regulation (IMO MASS Code), safety, automation, crew shortage
Constraints	Certification, liability, safety validation, cybersecurity

- MASS shipping uptake will be incremental and co-exist with traditional one, impacting ports for the following:
  - Digitalization of operations
  - VTS / traffic management
  - New safety and regulatory procedures
  - Workforce shift toward shore-based roles
  - Efficiency and environmental gains

(*) UNCTAD (2025). Merchant fleet statistics and maritime transport data (https://unctadstat.unctad.org)

(**) IALA (2024). The Future of Maritime Autonomous Surface Ships (MASS) (https://www.iala.int)

Major Ports in Italy (*)

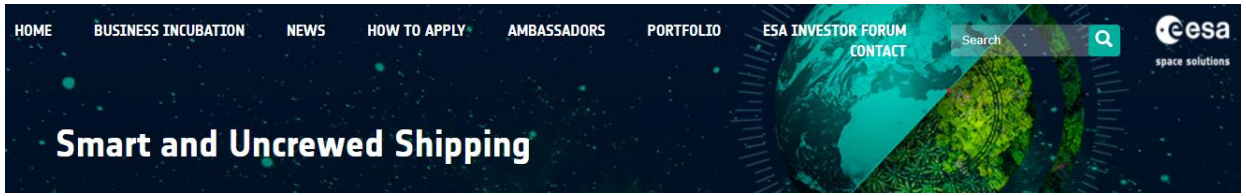
Exploiting MASS in Italian ports

The first trials of unmanned shipping in Italy

- Submitted to ESA Smart and Uncrewed Shipping Call for Proposals:
  - Supported by ASI;
  - led by TIM as prime contractor;
  - Framed into ESA/ITCG SMTF (see here the press release).
- Objectives:
  - integration of on-board, land-based and nomadic equipment with technological solutions already available from the ICT world;
  - standardization and replicability;
  - field trials and risk assessment;
  - end user requirements and valorization of skills already acquired.

co-funded by ASI in ESA Business Applications (BASS)
Grant n. 4000137214

Under the institutional supervision of the Italian Coast Guard



https://business.esa.int/projects/5g-mass

https://www.timenterprise.it/approfondimenti/porto-livorno-realta-contemporanea-tim-enterprise

Why a Ro-Ro case?

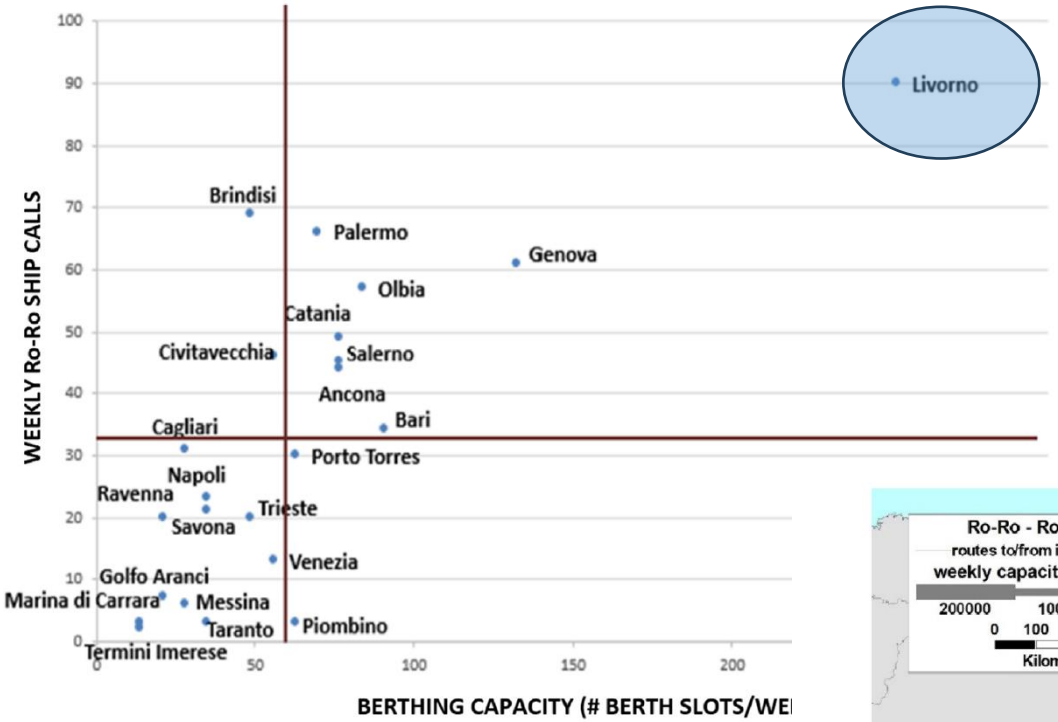


Fig. 6. Comparison between available berths and number of weekly calls per Italian po

- Vittorio Marzano et al, «Ro-Ro/Ro-Pax maritime transport in Italy: A policy-oriented market analysis», Case Studies on Transport Policy (2020), Elsevier - https://doi.org/10.1016/j.cstp.2020.08.001 .

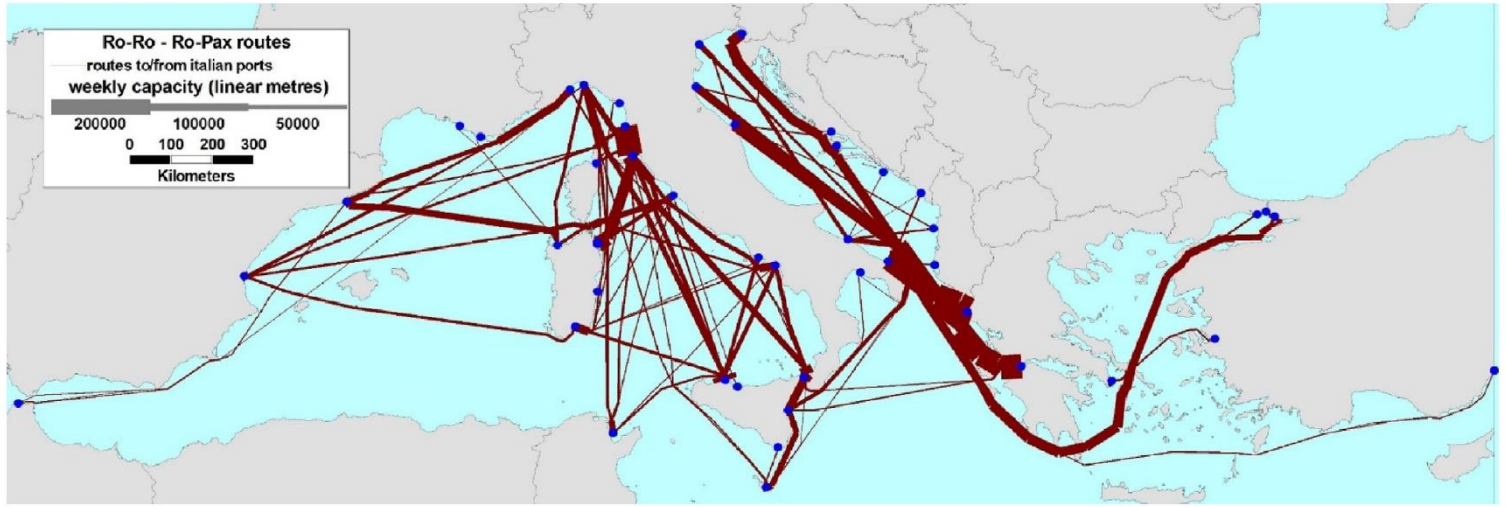
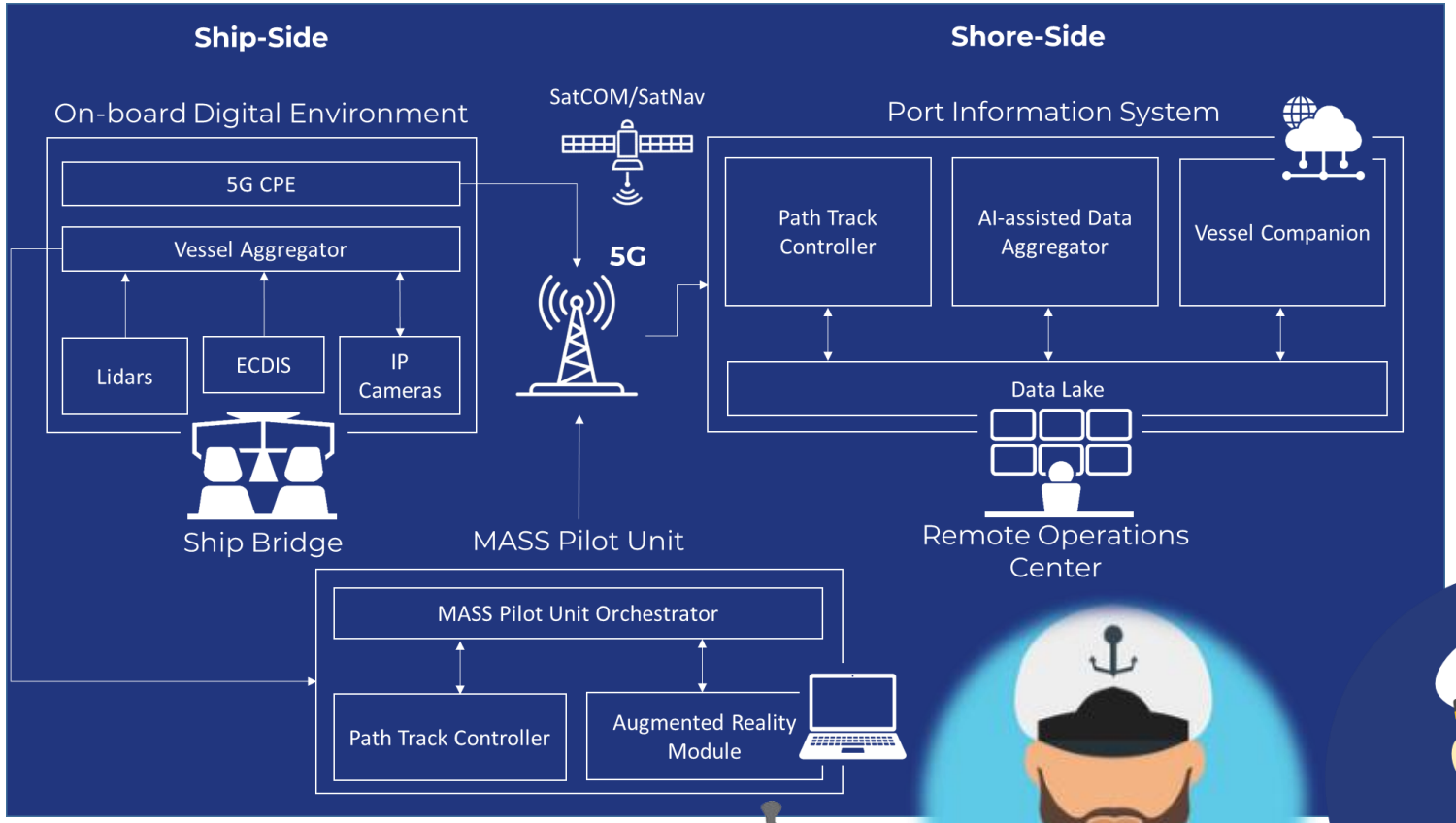
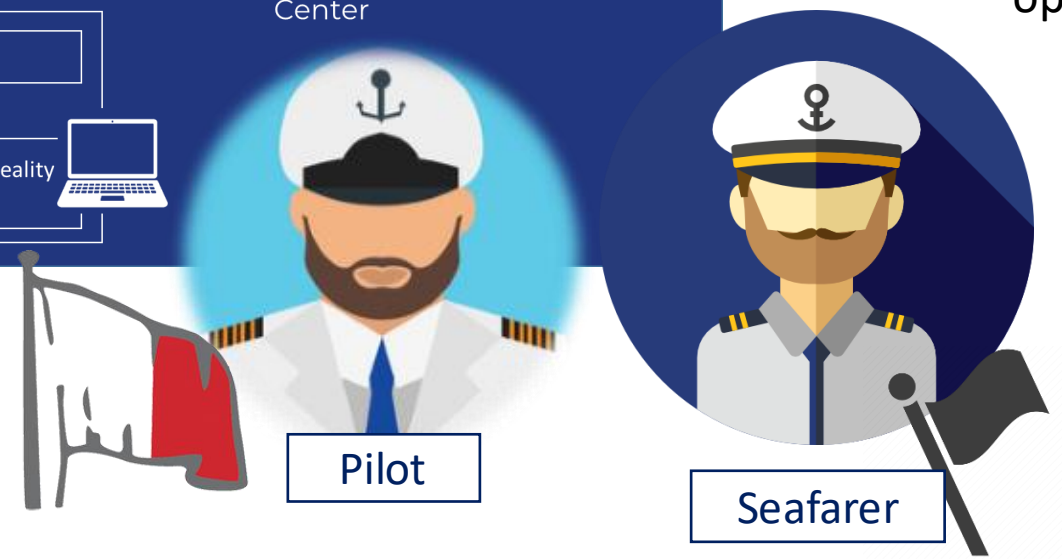


Fig. 2. Overall representation of weekly capacity [linear meters] of concerned Ro-Ro/Ro-Pax services in the study area (top) and focus on services calling at Italian ports (bottom).

credits: Daniela Tocchi, Università Federico II, Naples (I)

5G MASS architecture



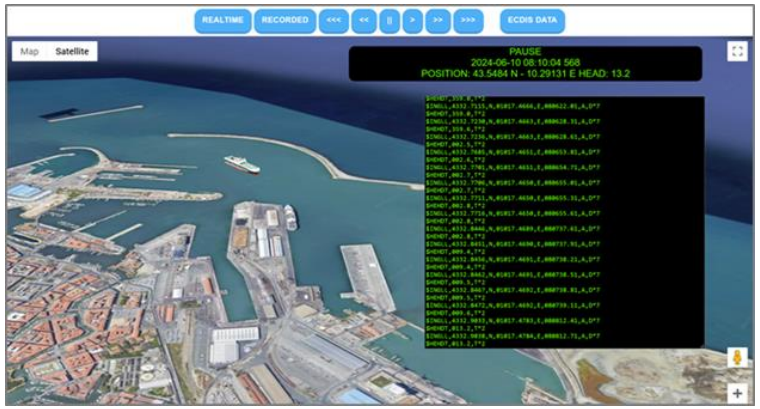


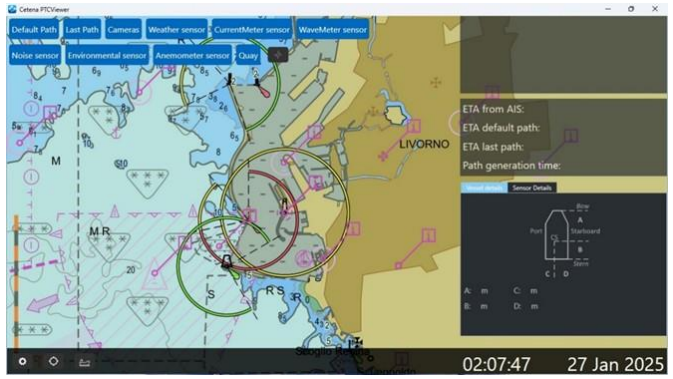
- 5G MASS system consists of:
  - a prototype ROC;
  - a retrofitted test vessel;
  - port physical/digital infrastructure.
- A new model of:
  - governing (digital) ship operations;
    - incrementally to higher automation degrees (MASS levels);
    - on the basis of the interaction between ship and port (maritime services).

5G MASS showcase

https://www.youtube.com/watch?v=xkd94o6aR18

- Offline analysis (Feb 2024 – Nov 2024):
  - 111 runs in/out of the port (usual schedule: 6 touches / month)
  - false alarms rate, detection accuracy and efficiency
- Real-time analysis (Nov 2024 – Dec 2024):
  - alert generation time, route recalculation time, safe fallback

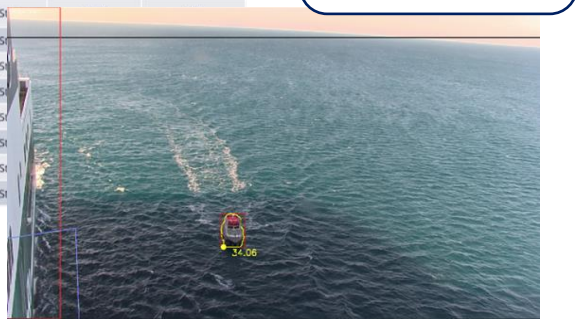




5G MASS results

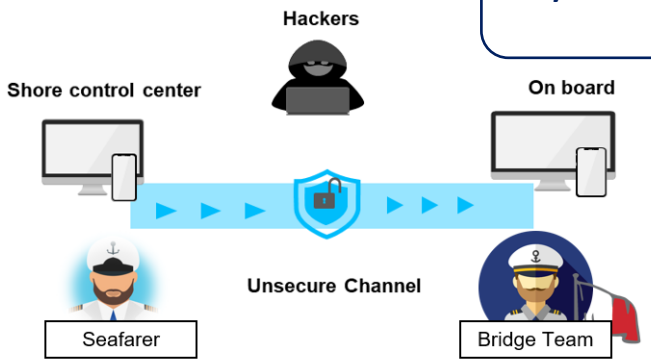
Network Assessment

Description	Device	Delta	Ship to obstacle distance
Tugboat (docked)	PTZ_C_Port	n.a.	253
"Punta vegliaia" (breakwater edge)	PTZ_C_Port	69.1	470
Edge A of the quay	PTZ_C_Port	19.46	232
Edge B of the quay	PTZ_C_Port	30	472
Corner of the quay	PTZ_C_Port	12.6	371
Pole on the quay	PTZ_C_Port	4.7	187
Corner of the quay / bollard	PTZ_C_Port	6.5	147
"Punta vegliaia" (breakwater edge)	PTZ_C_St		
buoy	PTZ_C_St		
lighthouse	PTZ_C_St		
Virgin Mary statue	PTZ_C_St		
Edge A of the pilots quay	PTZ_C_St		
Edge B of the pilots quay	PTZ_C_St		
Corner of the pilots quay	PTZ_C_St		
Quay I	PTZ_C_St		



Detection Accuracy

Operational Envelope



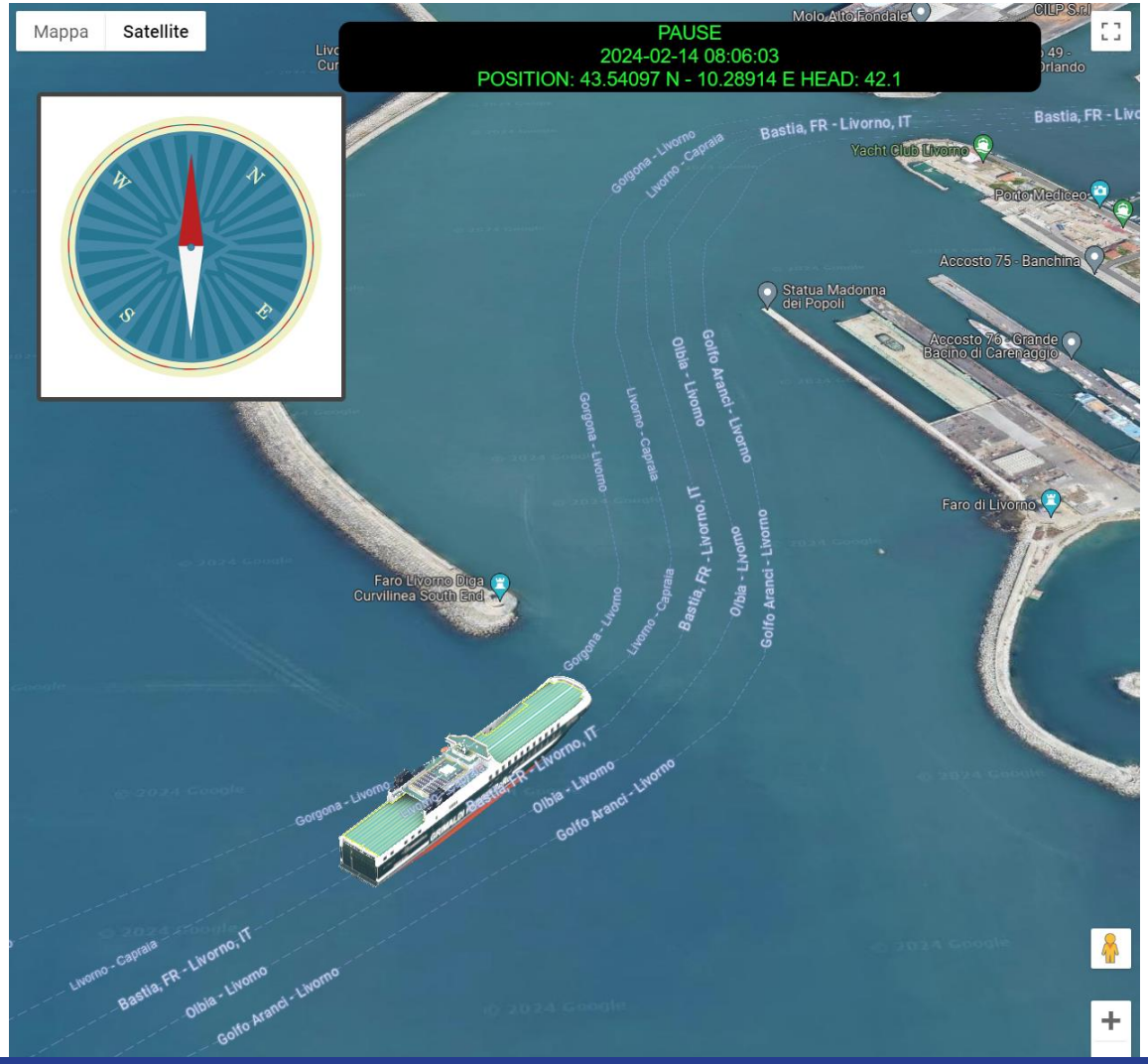
Cybersecurity

A. Tardo @ 78th National Assembly of Fedepiloti, April 8th, 2025, Rome (full recording in Italian)

MSC110/INF.5 Contributed by ITCG

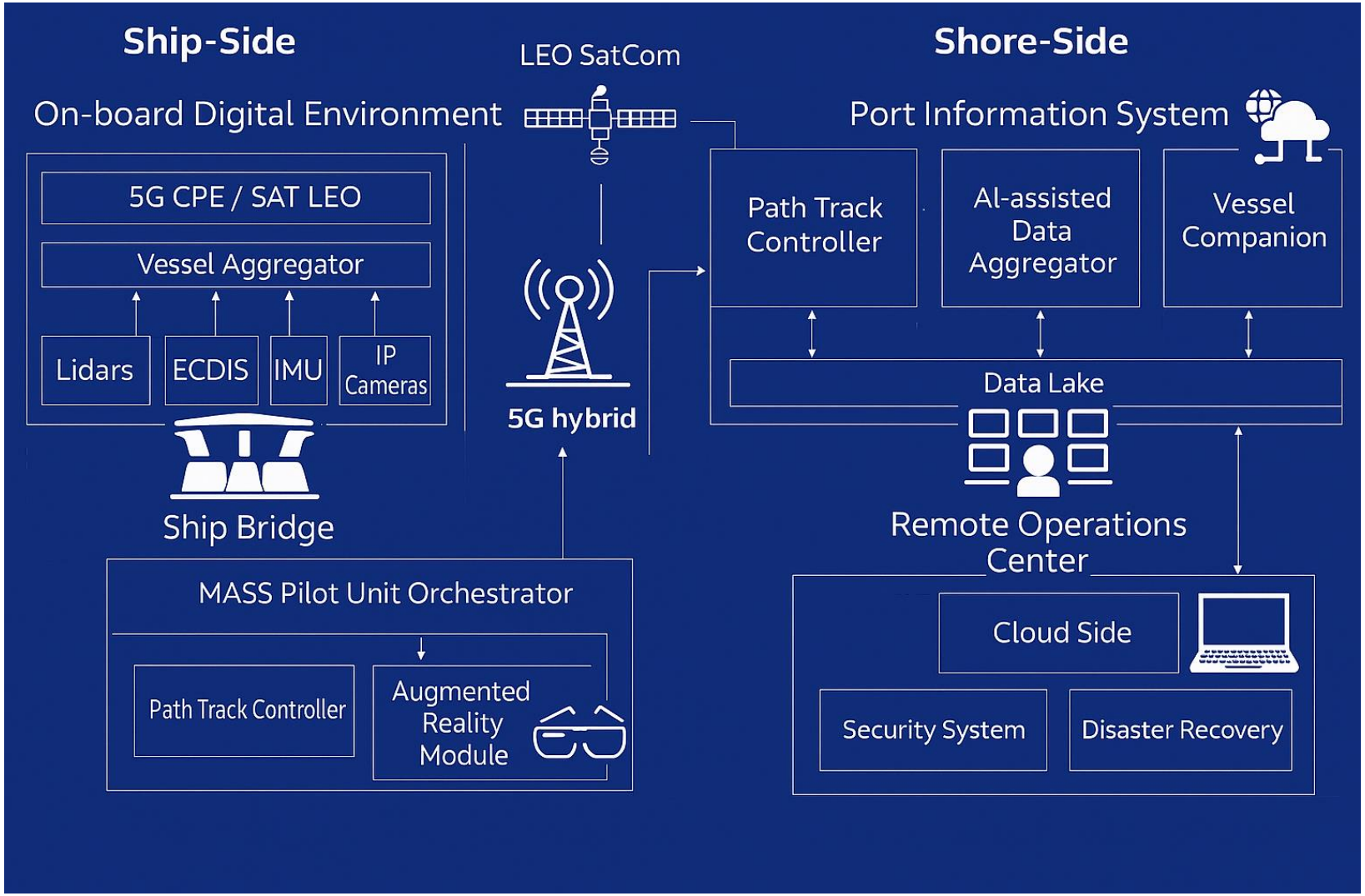
Cybersecurity in 5G MASS

- Cybersecurity elements of 5G MASS (out of scope in the funded project) but...
- Perimeter security:
  - infrastructure secured by design as framed in a 5G Private Network;
- Authorization management:
  - ROC services secured as implementing an Identity Provider and an Access/Authorization manager conforming to Open ID Connect (OIDC), based on IETF RFC 6749 and 6750;
- Secure data in transit:
  - E2E security of the shared information (IEC 63173-2 – SECOM) (*);
- Secure data at rest:
  - Data Stored in a dedicated tenant at the port (experimental) private cloud.



(*) Not relying on Maritime Connectivity Platform (MCP)

5G MASS extension (2026/27)



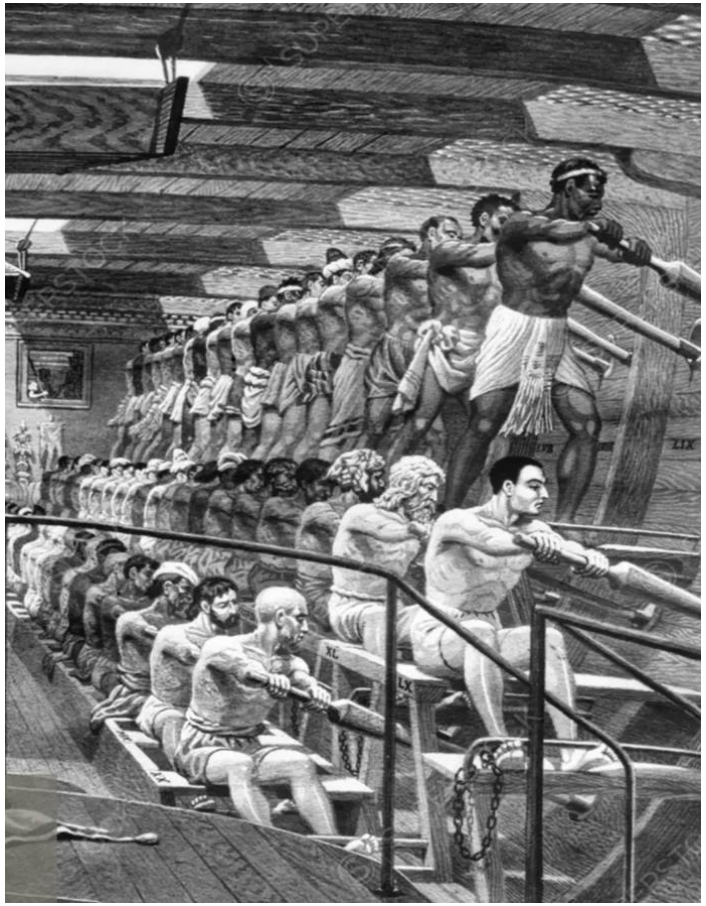
- Telecommunications
  - integration Private and Public Networks
  - integration with NTN (LEO constellations)
- Cybersecurity
  - critical infrastructure, service continuity (IEC62443)
  - secure ship-to-shore communication protocols (IEC 63173-2)
- Vessel retrofit (still MASS-1)
  - local computing farm
- ROC capabilities
  - ICT stack upgrade, more than one port
  - interoperability with VTS (feasibility study)

The PEACE project

- Appointed 2nd test vessel:
  - Oceanographic vessel
    - https://www.vesselfinder.com/it/vessels/details/7928677
  - Property of CNR, operated by Argo s.r.l., Italian flag

Consiglio Nazionale delle Ricerche

- The PEACE project (alignment w/ MASS-1)
  - Phase 1 (ongoing): GAIA Blu minimum retrofit to MASS-1 (5G MASS backgrond), self-funded
    - https://www.cnr.it/it/nota-stampa/n-14257/gaia-blu-strengthens-italy-s-role-in-autonomous-maritime-research-through-the-peace-project
  - Phase 2 (forthcoming): GAIA Blu minimum retrofit to MASS-2 operations as a new proposal
- New call for 2027/28 ship time:
  - new allocation requested for Phase 2

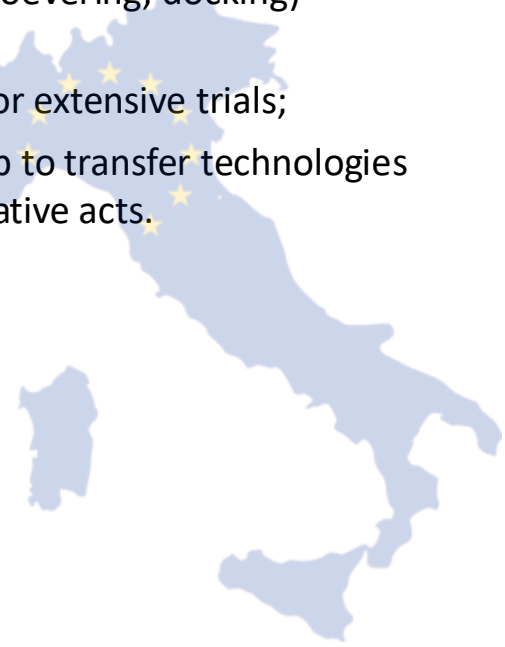


Is MASS reasonably safe?

Securing our Seaports

- Critical Maritime Infrastructures (CMI)
  - Directive EU 2022/2557
    - CMI: an asset, a facility, equipment , a network or a system or part of an asset, a facility, equipment , a network or a system which is necessary for the provision of an essential service.
    - essential service: a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety or the environment
- EU COM recommendations (EUMSS and Action Plan, Ocean Pact, EU action plan on cables, Action plan on drones and Counter drone Security)
  - a comprehensive, integrated, coordinated and targeted approach that brings together the civilian and military dimensions of the responsible actors involved, given that the security of the CMI may fall within more than one jurisdiction.

- Are the high-level directives for ashore facilities, vessels and communication capabilities in the MASS code securing our CMIs?
- Italy is actively seeking solutions:
  - to strengthen the digital capabilities (say detection, communication, physical and cybersecurity) of sea ports via dedicated R&D;
  - to secure processes (say manoevering, docking) enhancing assets (e.g. VTS);
  - to appoint natural testbeds for extensive trials;
  - to define a (reliable) roadmap to transfer technologies into best practices and normative acts.



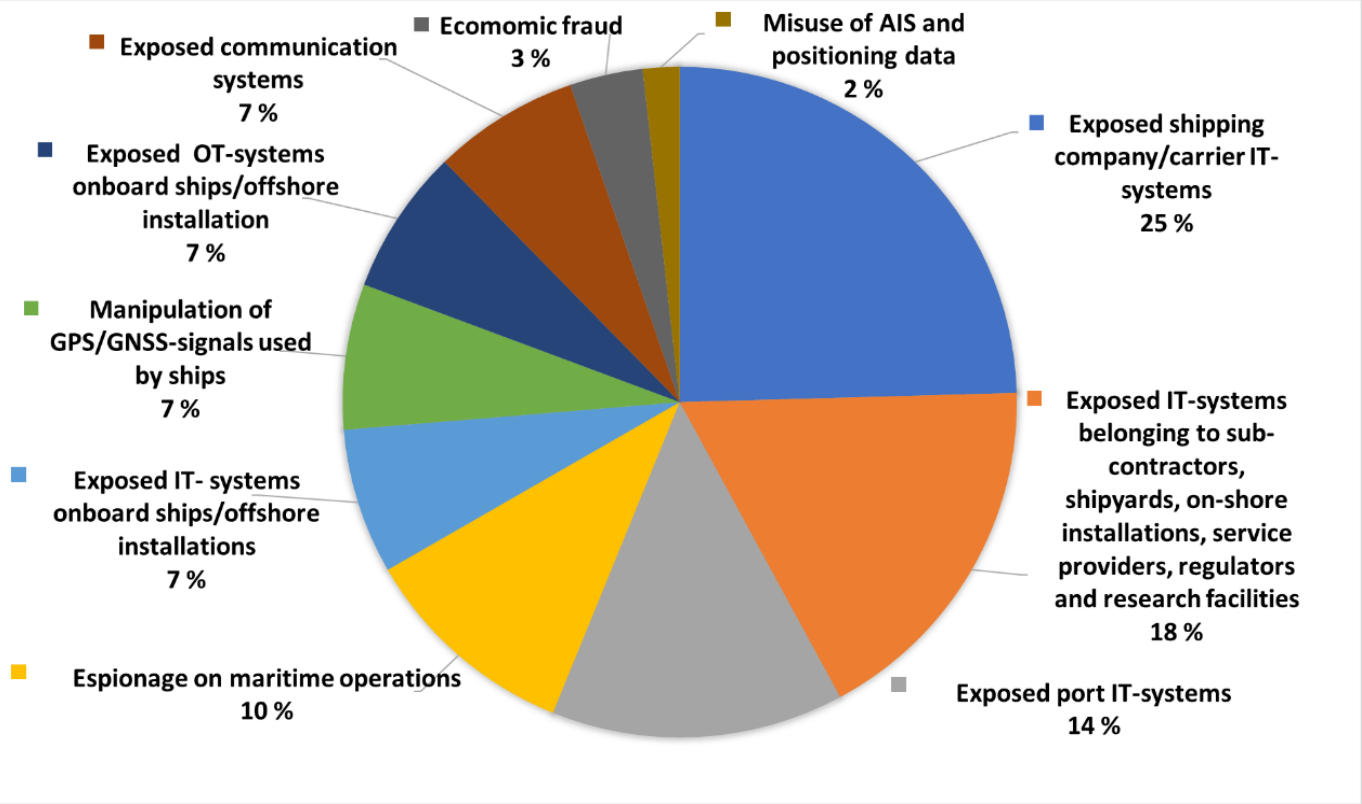
Exemplary Incident Report (2025)

- https://maritimecybersecurity.nl/incident/8dAmdxGmDM
  - Discovered by the French authorities at Port of Sète.
  - A Trojan deployed via Raspberry Pi devices with cellular modems installed on shipboard computer systems by a crew.
  - Under investigation by French counter-intelligence service (DGSI).
  - Ferry, operated by MSC subsidiary Grandi Navi Veloci and carrying 2,000+ passengers on France-North Africa routes, was temporarily detained.
  - This incident marks a significant escalation in maritime cyber threats from financially-motivated attacks to potential state-sponsored sabotage targeting navigation systems.

credits: NHL Stendel University of Applied Sciences - NL

An isolated event?

TransNav DOI: 10.12716/1001.15.03.04
referenced by: US DHS Report on "U.S. MARITIME TRADE AND PORT CYBERSECURITY, 2024"



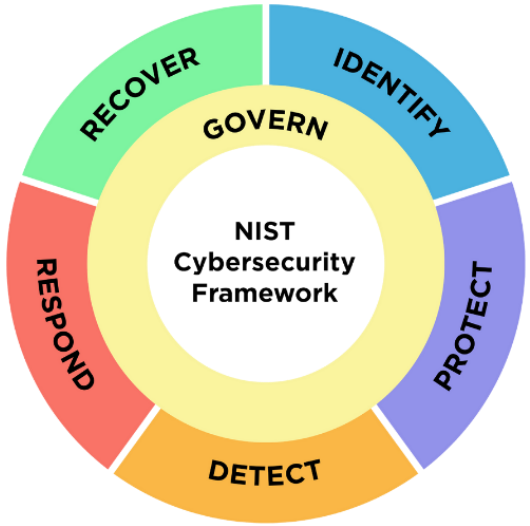
- In Italy (some examples):
  - Teenager Hacks Ship Routes in the Mediterranean – Ministry of Education (Jan 2025)
    - https://maritimecybersecurity.nl/incident/9BEmBGLzb7
    - https://www.bitdefender.com/en-au/blog/hotforsecurity/15-year-old-hacker-diverts-ships-in-mediterranean-sea-for-fun
  - ADSP Mar Tirreno Settentrionale Ransomware Attack (Mar 2024)
    - https://maritimecybersecurity.nl/incident/MyKmGkMmYW
    - https://www.halcyon.ai/attacks/medusa-attacks-adsp-mar-tirreno-settentrionale
  - DDoS Attack Against Marina Militare (NoName057(16) group, Feb 2024)
    - https://maritimecybersecurity.nl/incident/wW4mPV1oRI
    - https://thecyberexpress.com/cyberattack-on-italy-noname-targets-italy/
  - Vessels near Elba hit by AIS spoofing attack (Dec 2019)
    - https://maritimecybersecurity.nl/incident/9BEmBr5mb7
    - https://globalpolitics.in/view_cir_articles.php?url=NIAS%20Fortnightly%20on%20Science,%20Technology%20&%20International%20Relations&recordNo=786

credits: NHL Stendel University of Applied Sciences - NL

IMO MASS Provisions on Cybersecurity

- IMO MASS Code, represents one of the most significant expansions of the global cyber-attack surface in the history of critical infrastructures.
  - Word «Cyber/Cybersecurity» appears 10 times without further detailing specific provisions (e.g. on ROC/Vessel twinning)
- References:
  - Guidelines on cyber security onboard ships (MSC.1/Circ.1639)
  - Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1)

- External guidelines:
  - NIST CSF 2.0 framework relying on:
    - Identify, Protect, Detect, Respond, Recover, and Govern functions.
- IACS (for built-new ships):
  - UR E22/Rev.3 “Computer-based systems”
  - UR E26 “Cyber Resilience of Ships”
  - UR E27, “Cyber Resilience of On-Board Systems and Equipment”
- IAPH (see next)



https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx

«Understanding the 21st Century cyber threat landscape»

- Considering ports as critical infrastructures:
  - “Unique to port operations, for example, vessels represent potential conduits of cyber risk to the ports they visit, the companies managing them and the supply chain they support. Ships can be risky if their shipboard environments are lightly governed and have little to no oversight. When moored, a ship can potentially introduce cyber risks to a port facility through ship-shore connections.”

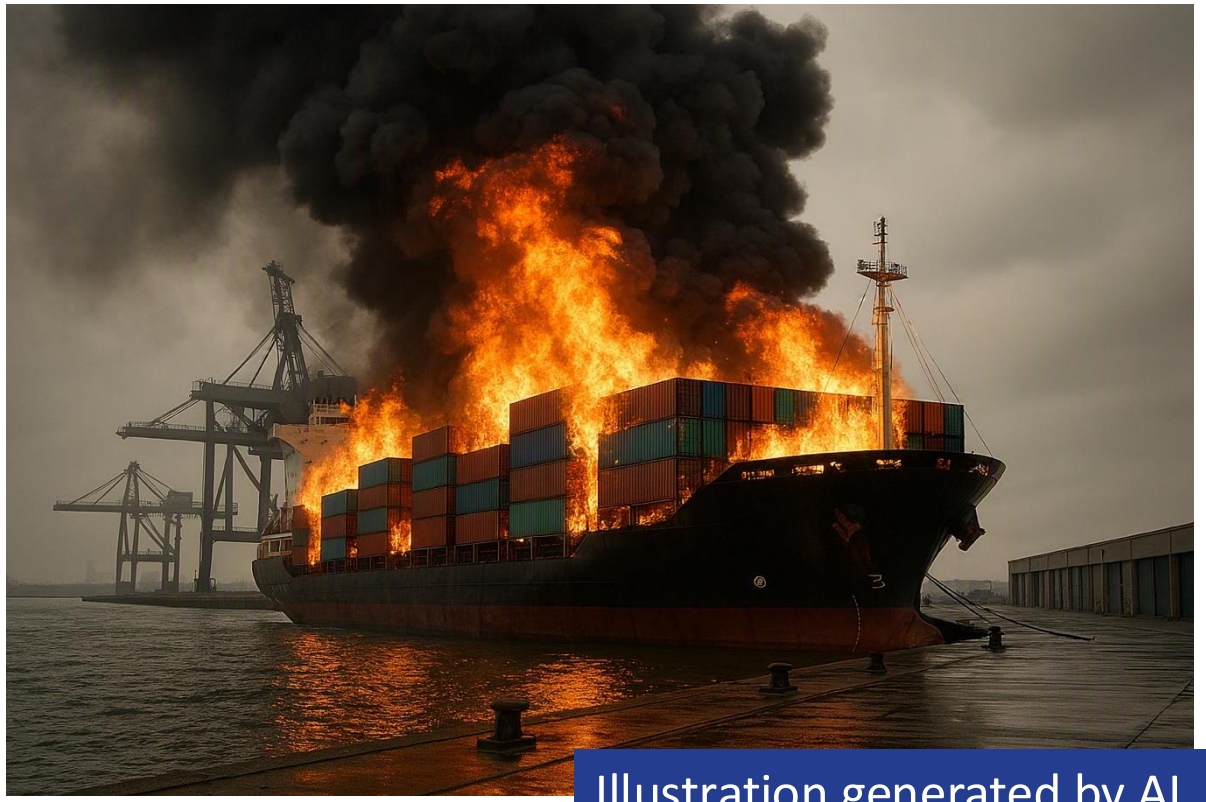


Illustration generated by AI

Quoting: IAPH Cybersecurity Guidelines for Ports and Port Facilities (Sec 4.)

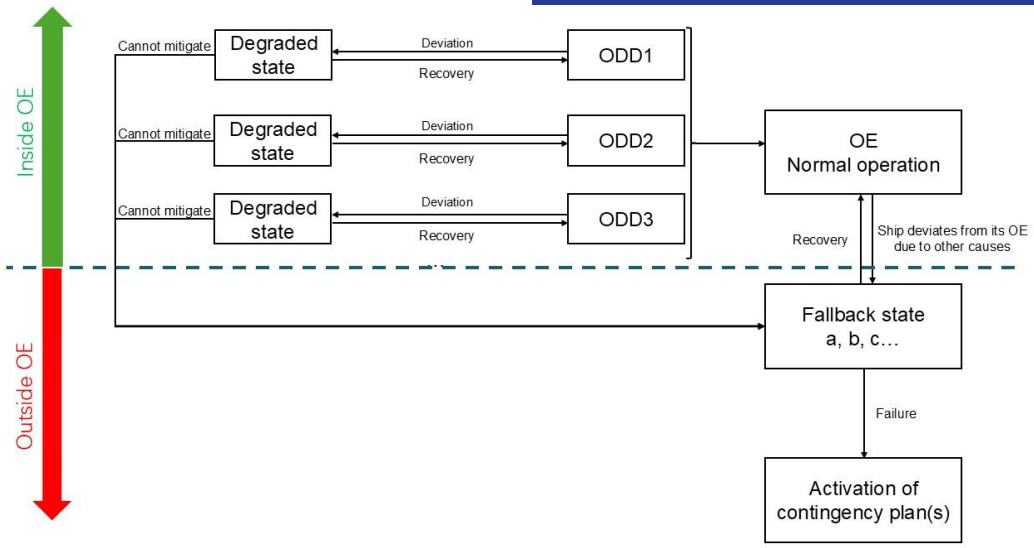
Cybersecurity in the IMO MASS Experience Building Phase through narrative

Credits to Mr Yves Van Seters
https://www.linkedin.com/pulse/ships-sail-themselves-already-hackers-dream-yves-van-seters-3lvkf/

«Securing the command link»

- MASS (< level 4) depends on a continuous data connection between the ship and its shore-based ROC:
  - that link carries commands, sensor data, and safety overrides to (e.g.) Autonomous Navigation Systems
- SECOM (IP) and VDES (non-IP) are standardized secure links getting rid of possible Man-in-the-Middle attack.
  - Private (T/NT) networks guarantee more control than public infrastructures. When possible, rely on them.
- How to guarantee Business Continuity in case of attack (Response Phase)?
  - A Trusted Autonomy must take care of transition to degraded and fall-back states and possible recovery when the system is under pressure.
  - IMO stresses on Human Oversight and Control (1st recall).

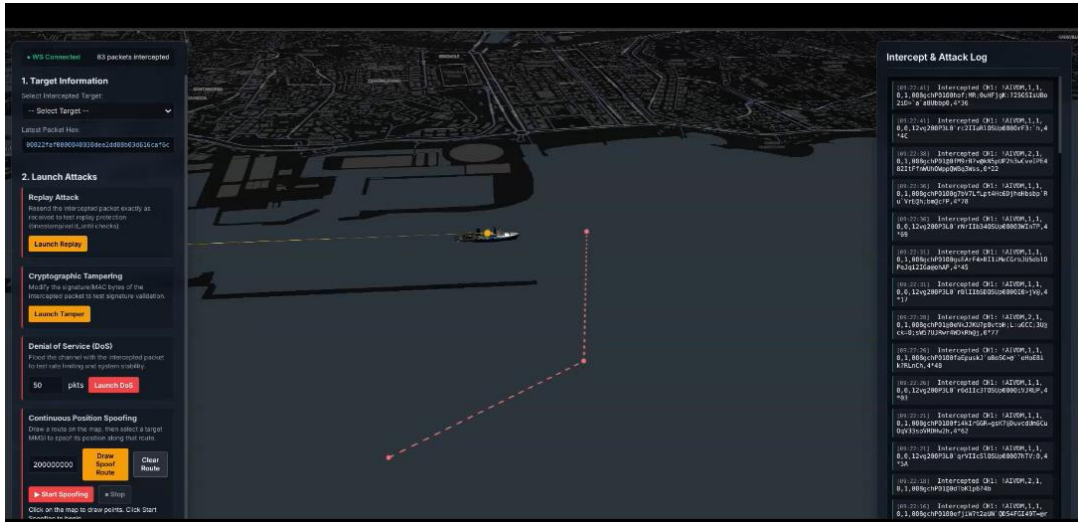
Illustration generated by AI



OE/ODD from the MASS code

«Lying to the Navigation System»

- Autonomous Navigation Systems (ANS) for MASS (< level 4) depend on sensor readings (e.g. GNSS, cameras, lidars, radars):
  - injecting false inputs into sensors, include malicious IoT sources in ports and vessels can lead to wrong decisions by the ANS.
- Filter out not authenticated sources (like AIS spoofing messages), limit the perimeter of Trusted entities as much as possible, what is unlikely to happen does generally represent a threat:
  - TESLA-VDES authentication protocol;
  - Certified sources (see MCP/MIR), hopefully not discovered through the Internet;
  - Recurring (ports and vessels) surveys to confirm conformance to standards;
  - IMO stresses on Human Oversight and Control (2nd recall).



«Poisoning the Machine's Mind»

- ANS for MASS (< level 4) will rely on AI;
- (LLM) Models can show hallucinations (i.e. AI-fabricated abnormalities or artifacts that appear visually realistic and highly plausible) and that's life!
  - what if these hallucinations come from hacks (e.g. LLM bias)?
- Some hints:
  - LLM Agent Failure Mode Analysis;
  - Adversarial Robustness Techniques;
  - Federated / Collaborative Learning;
  - IMO stresses on Human Oversight and Control (3rd recall).

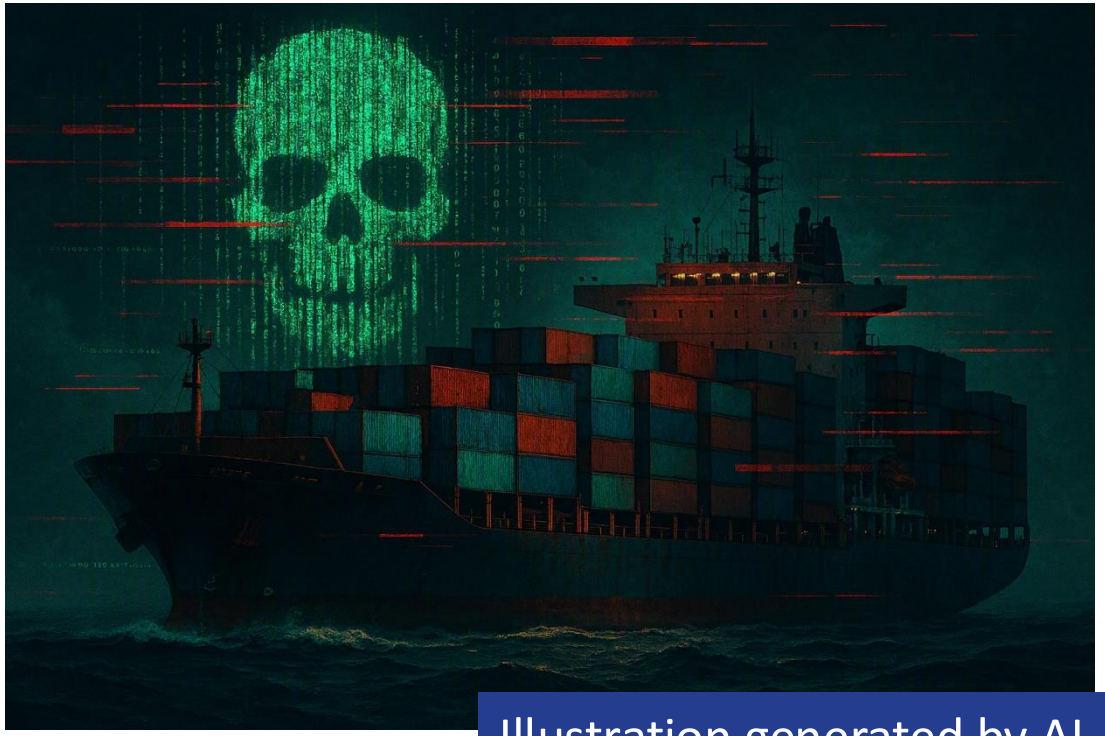
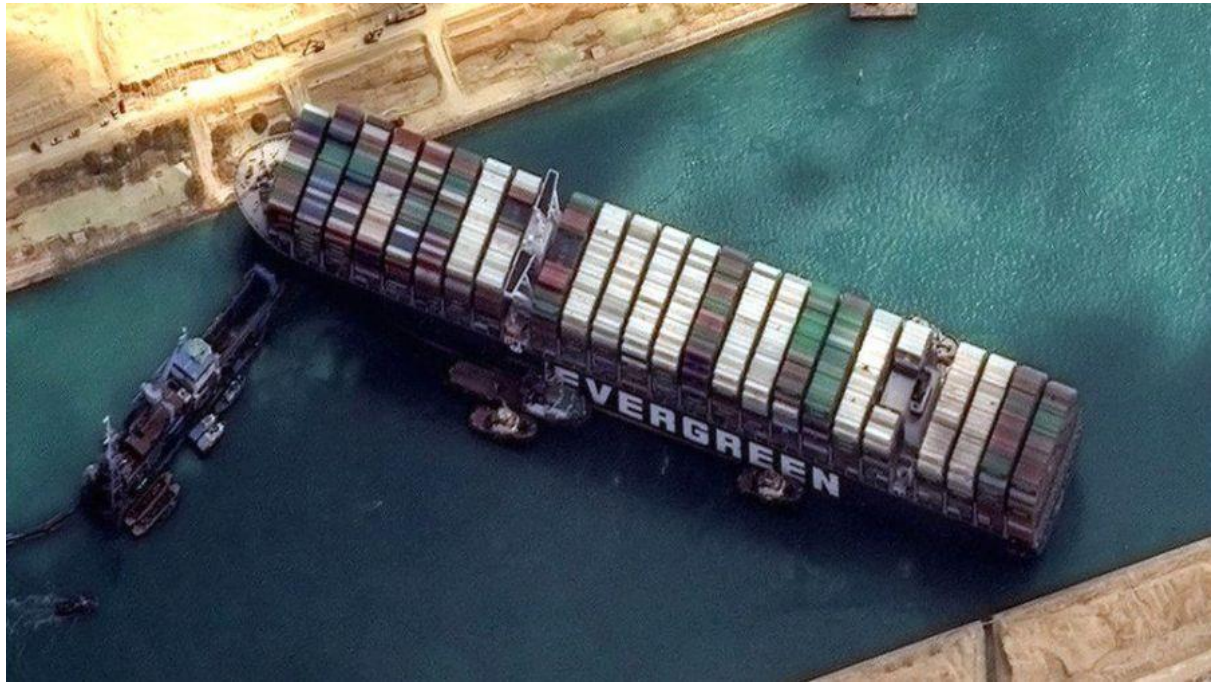


Illustration generated by AI

«Ransomware With Nowhere to Run»

- ANS for MASS (< level 4) will run third-party software;
  - “A ransomware attack that locks the steering gear of a vessel drifting in the Malacca Strait—with no crew available to engage a manual override—is not a data breach. It is a maritime crisis, and a multi-million-dollar ransom demand arrives alongside it.” (Mr. Yves Van Seters)
- Some hints:
  - Zero-Trust approach
  - NIST SP 800-160v1r1
    - Engineering Trustworthy Secure Systems
    - Simplicity and Minimization, Failure and Recovery, Trust and Composition, Monitoring and Accountability, Access Control and Mediation
  - IMO stresses on Human Oversight and Control (4th recall).



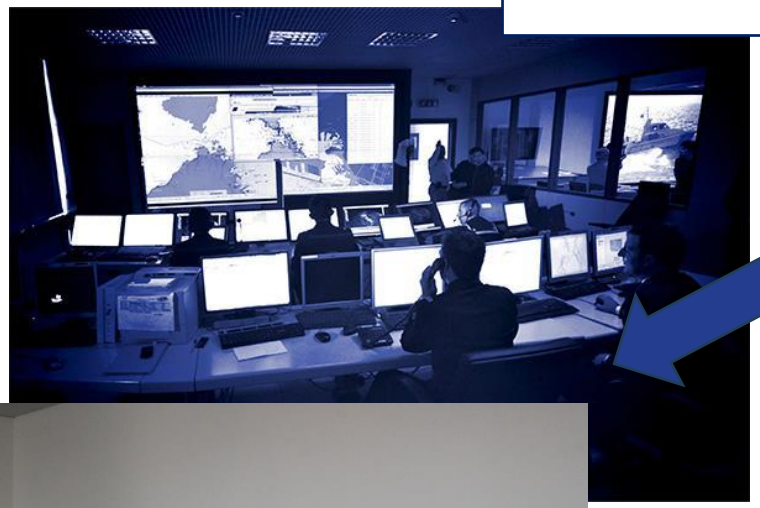
https://www.nytimes.com/2021/07/17/world/middleeast/suez-canal-stuck-ship-ever-given.html

Experience Building Phase in Italy starts from Livorno

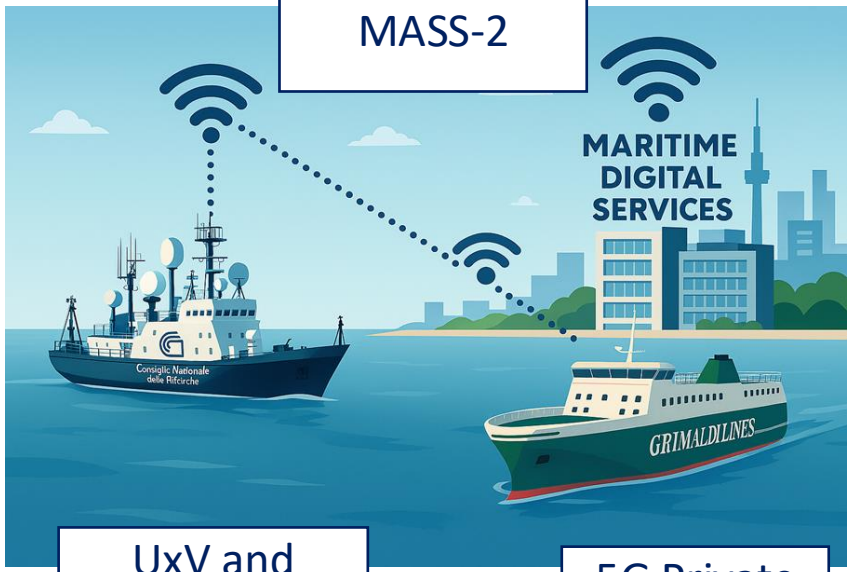
Italian MASS & e-Navigation testing platform (27/28)

enhanced radar system

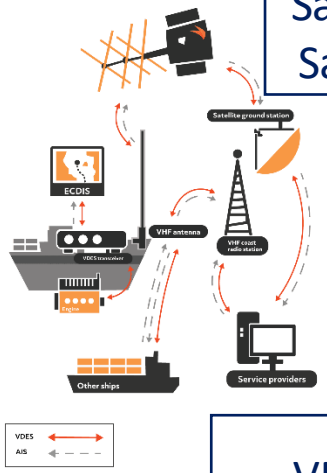
VTS



MASS-1 and MASS-2



SatCOM SatNAV

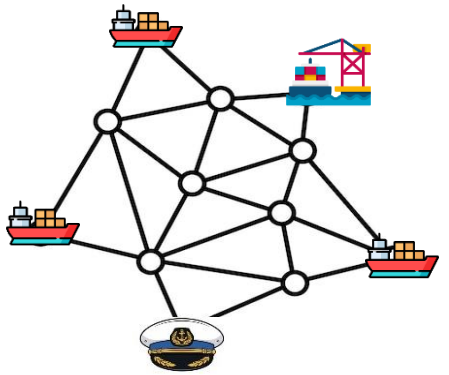


VDES

ROC

UxV and pilot/patrol boats

5G Private Network



Trust Model

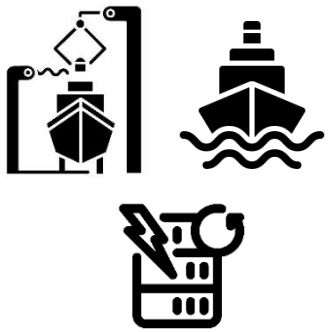
A possible roadmap

Retrofit,
New specs
(2026)

Trials
(2028)

New
Development
(2030)

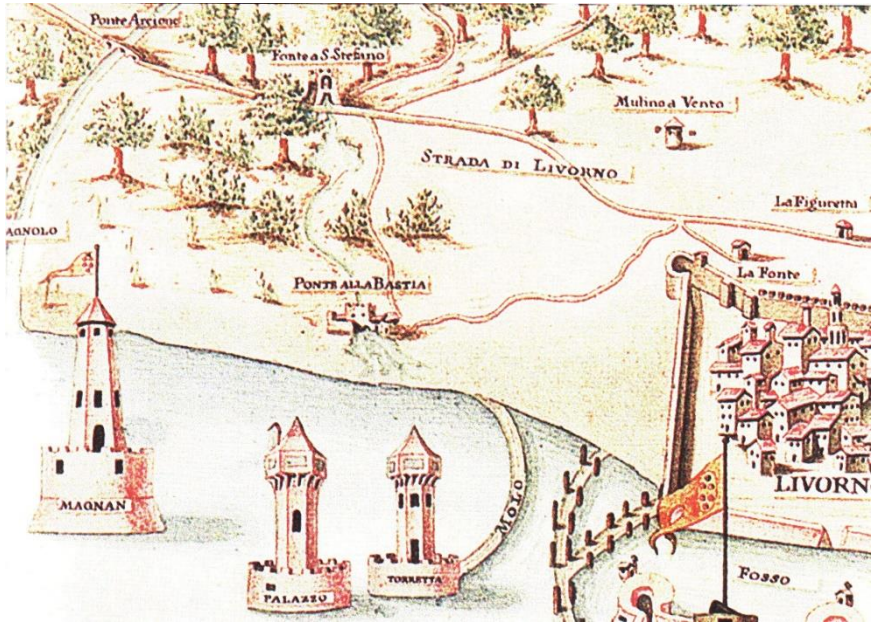
Mandatory
Code
(2032)



MASS-1,
MASS-2
service
deployment
(2027)

Cross-
fertilization,
Technology
Assessment
(2029)

FOT
(2031)

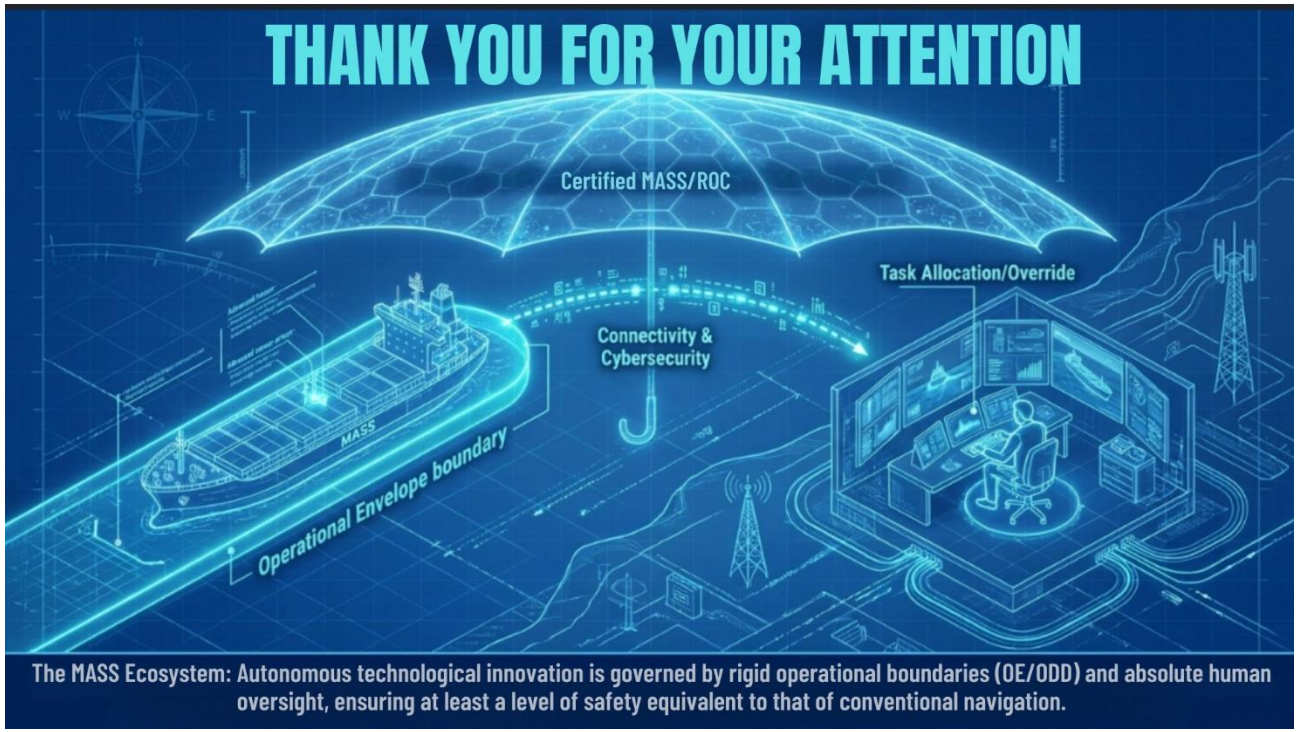


Takeaway message

https://business.esa.int/news/space-to-sea-solutions-event-to-be-held-naples-september

Thank you!

- CNIT Laboratory @ Port of Livorno:
  - has enabled a digital infrastructure capable of validating innovative services targeted to port communities;
  - has an unquestionable recognition in the international domain;
  - is involved in high-valued R&D for the security of Critical Maritime Infrastructures, and Autonomous Vessels;
  - is setting up a Testing Platform for validating digital and autonomous navigation in port infrastructures;
  - the activity requires a deep background in the scope of the GECON communities
    - collaboration and cross-fertilization is more than welcome.



https://jlab-ports.cnit.it