Colombia mar 2019

VI CONGRESO INTERNACIONAL DE DISEÑO E INGENIERÍA NAVAL

COPINAVAL
CARTAGENA DE INDIAS - COLOMBIA

XXVI CONGRESO PANAMERICANO DE INGENIERÍA NAVAL, TRANSPORTE MARÍTIMO E INGENIERÍA PORTUARIA

Organizan:

COTECMAR

ESCUELA NAVAL ALMIRANTE PADILLA

ARMADA DE COLOMBIA

INSTITUTO PANAMERICANO DE INGENIERÍA NAVAL

BUQUES AUTÓNOMOS Y CIBERSEGURIDAD

Shipping 4.0
Moving to a digital age

→ Smart tech providing new opportunities

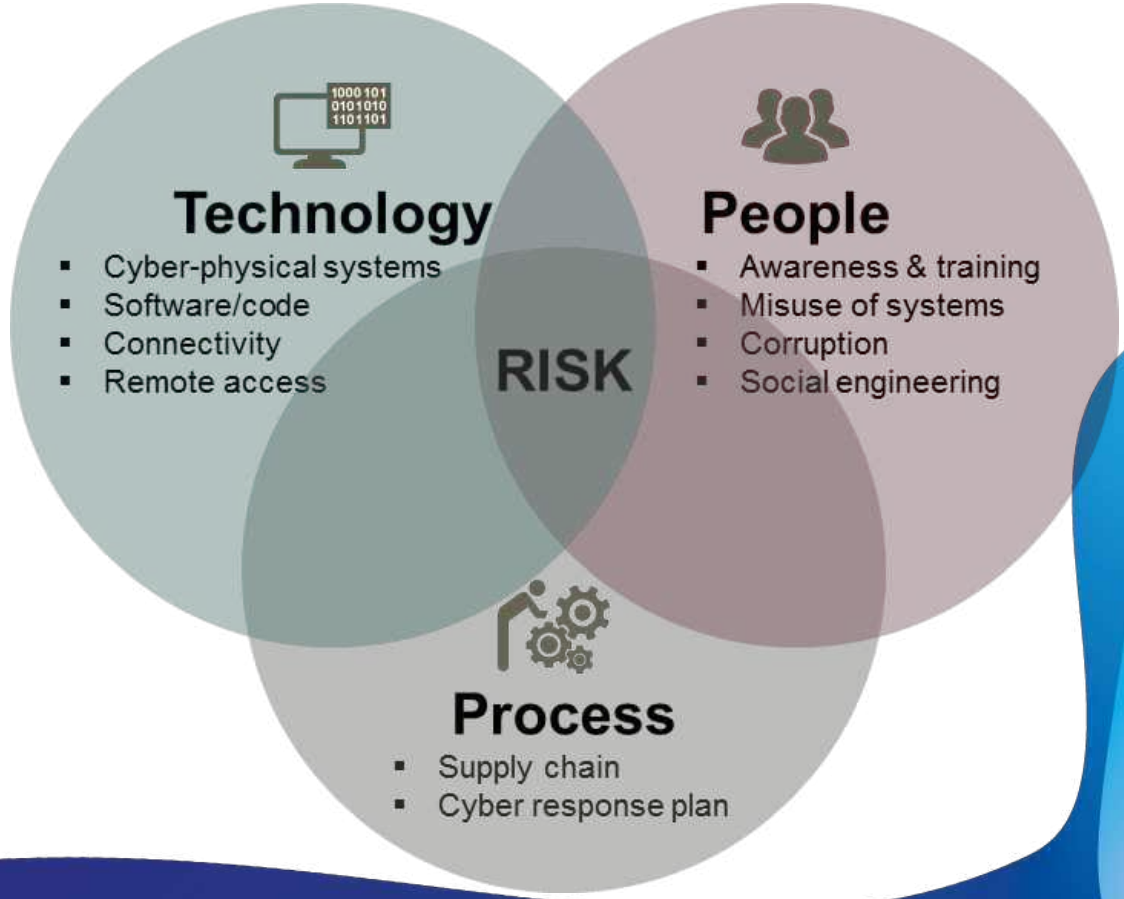
Improved safety
- Lower probability of human failure
- Reduced crew exposure to hazardous situations

Reduced environmental impact
- Emissions
- Lower probability of spills

Lower opex
- Reduced crew
- Improved fuel efficiency
- Reduced maintenance

Optimized fleet management
- Integrated logistics (cargo, spare parts)
- Digital asset integrity management (AIM)
- Monitoring, control & continuous verification

→ But also new threats and challenges



Cyber-enabled ships

More than just cyber security

What you need

Cyber security

Prevent intentional malicious actions (cyber attack)

Cyber safety

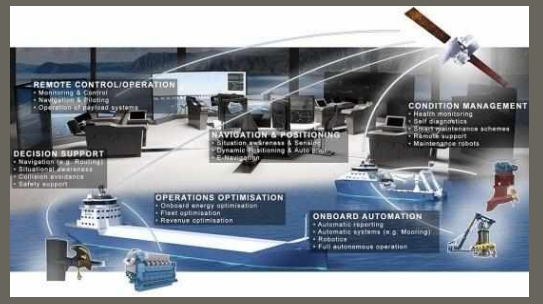
Prevent involuntary accidents and mistakes (system failure)

What you want

Cyber performance

Measure and improve health/performance of system/ship or operator

- Remote access and/or control
  - Condition monitoring & maintenance optimization (CBM, RCM, PdM)
  - Fuel consumption & emission control (MRV, IMO DCS)
  - Continuous verification (e.g. DP)
  - Fleet operations
- Autonomous systems/ships
- Digital twin-based asset management – VeriSTAR AIM^{3D}



Regulations: IMO, EU

a) EU = Two sources:

a.1) EU 2016/1148 (The Directive on security of network and information systems (NIS Directive). Includes ports but not ships
a.2) GDPR (=EU 2016/679). INCLUDES SHIPS. Already applicable (May 2018)
Creation of ENISA (EU Cybersecurity Agency). Much documentation on their website.

b) IMO:
MSC 428(98). Adopted 2017. Stands for "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS". In this MSC it is stated that Cyber risks must be properly addressed not later than first annual verification of the Document of Compliance from the Company after 1 January 2021. It is to be included in the ISM.

Other regulations and standards

NIST Framework (NIST = National Institute of Standards and Technology). BIMCO Guidelines are based on that.
NOTE: Following slides from obtained from NIST presentation

TMSA3: Vettings/Charteres are including item 13 (Maritime Security) which was not existing on TMSA2 and also Cyber Sec is taken into account by "Change Management" (item7 of TMSA3) . So charterers are starting to ask for this…..

ISO 27001. Establish an Information Security Management system (ISMS). It is not mandatory. It explains how risks and controls have to be addressed. This can be certified.

NIST - Cybersecurity Framework Components

The Framework consists of 3 main components

Framework Core

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
	Supply Chain Risk Management	**ID.SC**
Protect	Identity Management & Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

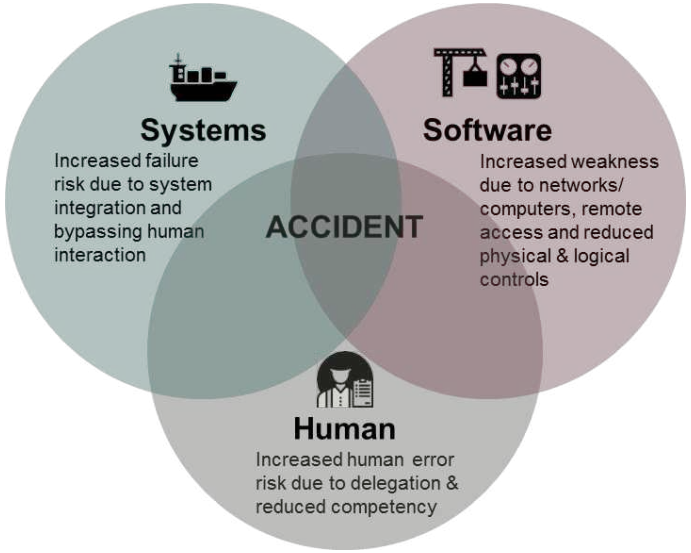
What techniques can restore capabilities?

Sabemos el marco regulatorio, pero hay que definir el problema……

"The boss is worried about information security, so he sends his messages one alphabet letter at a time in random sequence."

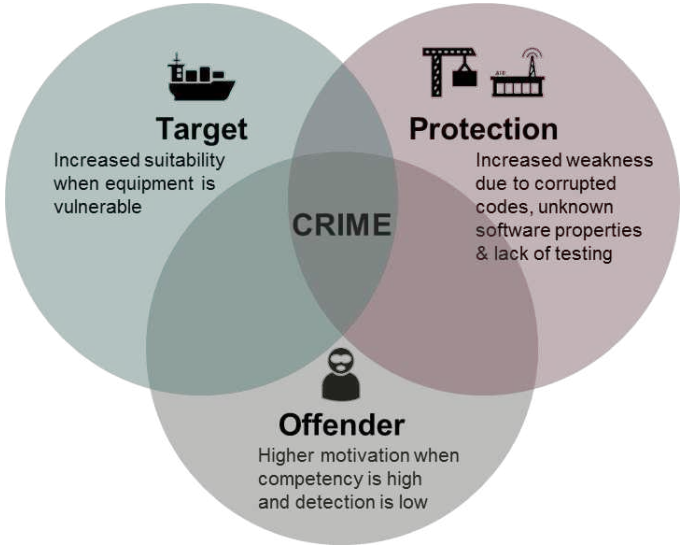
"I'm no expert, but I think it's some kind of cyber attack!"

Safety



- **SW-Registry** (NR 467, Jan 2018)
  - Based on IACS UR E22 (Jul 2017)
- **HWIL** (NR 467 & 632, Jan 2016)
  - Failure handling, safety risk based approach
- **Autonomous ships** (NI 641, Dec 2017)
  - Level of autonomy of on-board systems

Security



- **Cyber Managed** (NR 659)
  - For all vessels
- **Cyber Secure** (NR 659)
  - NC recommended
- **Supply chain certification** (NR 642, draft Dec 2017)
  - Products and Manufacturers

IT & OT

IT = Information Technologies.

Damage: Mainly financial and commercial (reputation)

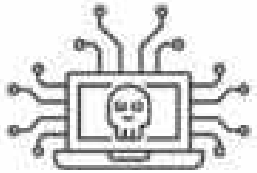
Examples: e-mails, e-Certificates, etc.

OT = Operation Technology

Damage: Not only money & commercial, but also life, asset and pollution of environment.

Examples: SCADA, Dynapos Systems, ECDIS, etc

easy target ?



Results of IHS survey (300 participants)

- **34% have faced a cyberattack in last 12 months**
- **Largest vulnerability is the people (47%)**, followed by 3rd party suppliers (19%), internal policies (13%) and eventually systems (6%)
- **51% have trained their staff on cybersecurity**, 72% set up dedicated policy but only 23% are certified (+9%) ongoing
- **50% have insurance** coverage and 70% have systems in place to report cybersecurity events

easy target ?

THE MAERSK CYBER ATTACK

In June 2017, Maersk was hit by the non-Petya malware as part of a national attack. The virus stopped the company's operations in Rotterdam, Los Angeles, Mumbai, Auckland, and many more ports around the world

Maersk reported a **$250-300 million** loss due to the disrupted business operations in July and August

MALWARE ON MOBILE OFFSHORE DRILLING UNIT

Offshore oil workers unintentionally uploaded malware (USB drives). **The malware disabled the signals to the dynamic positioning thrusters**, so the MODU drifted off of the well site. For safety reasons, the well was temporarily shut down.
It could have been a disaster for both the **workers and the environment !**

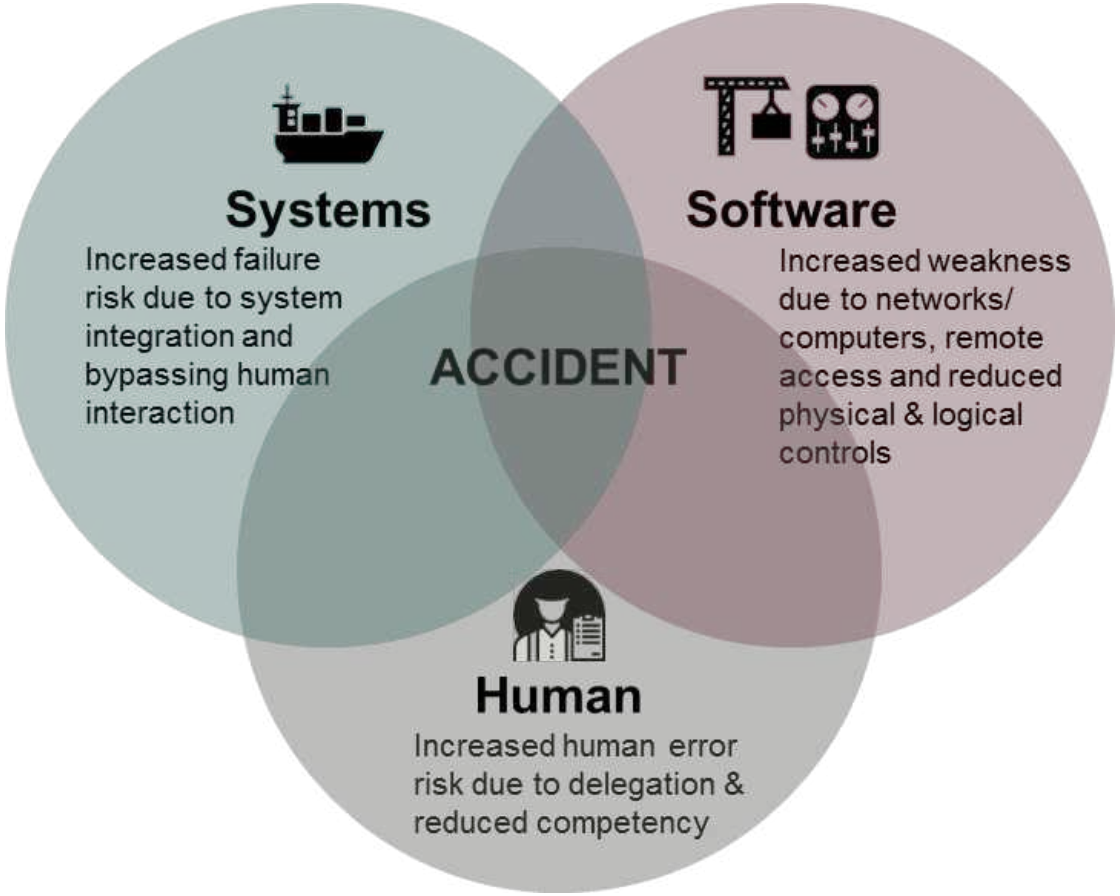
CLARKSONS

Perpetrators gained unauthorised access to computer systems, accessing confidential information and threatening to release information unless ransom payment is made.
Company share prices decreased by 2.71%

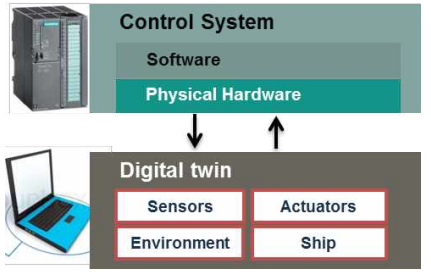
¿¿¿Cuál es la solución propuesta???

→ BV notations, rules & guidelines

→ Main dimensions of cyber safety



- **SW-Registry** (NR 467, Jan 2018)
  - On-board computer based systems
  - Based on IACS UR E22 (Jul 2017)
- **HWIL** (NR 467 & 632, Jan 2016)
  - Advanced HW-in-the-loop system testing
  - Complex/integrated on-board systems
  - Failure handling, safety risk based approach
- Autonomous ships (NI 641, Dec 2017)
  - Level of autonomy of on-board systems
  - Safety risk based approach



Two Class Notations

NIST

BIMCO

IACS

International Association of Classification Societies

CYBER MANAGED

✠ CYBER SECURE

CYBER MANAGED

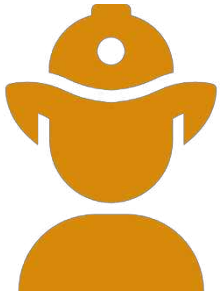
PROCEDURES

HUMAN

Roles are detailed and explained. Procedures are in place. Commander, CISO and crew are trained.

ORGANIZATION

Change Management Policy ensures security and safety during patch management and updates of IT and OT.



EMERGENCY RESPONSE

Incident Response (local and remote). Equipment vulnerabilities live status.

CYBER MANAGED

1) It will be applicable as for **new construction** as **for in-service** Vessel.
2) CYBER MANAGED is a way to control security with **manual procedures**.
3) A S**ecurity Risk Analysis** methodology is proposed with a standard template. This template and methodology may be used by the Shipowner to perform the security risk analysis by himself **OR** use a 3rd party contributor.
4) Minimum technical requirements for remote access management are **network connections** are detailed.
5) Roles are detailed and explained. Procedures are in place. Crew is trained.
6) Access to onboard equipment is regulated by organizational measures and strong antivirus cleaning processes
7) Change Management Policy ensures security and safety during patch management and updates of IT and OT.

SECURITY SOLUTIONS

CYBER SECURE

COMPLIANCE & SOFTWARE REGISTRY

Compliance of critical systems is managed and automatically ensured by installation of an IT solution on board or remote.

DATA INSPECTION

Access to onboard equipment is regulated by organizational measures and strong antivirus cleaning processes.

EVENTS & LOGS RECORDER

Traceability of events is ensured. Legal proof is generated with forensics capability.

RULES FOR DESIGN

✠ CYBER SECURE

EQUIPMENT SECURED BY DESIGN

Equipment have hardened systems and are secured by design.

VESSEL SECURED BY DESIGN

Physical accesses are managed from design. Network cables and Wi-Fi areas are secured. Design of systems and equipment is done with at least privilege policy.

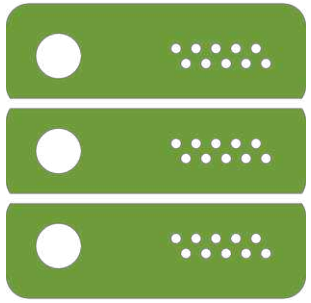
REMOTE ACCESS SECURED BY DESIGN

Network is mastered and secured as onboard than ashore. Remote access is taken into account during design phase.

✠ CYBER SECURE

ROLES

Supplier



Rules for Equipment

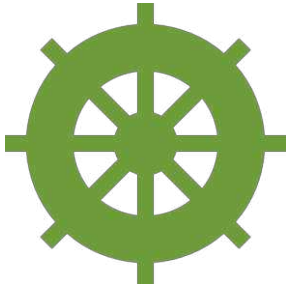
Shipyard

Rules for Design

Vessel Integrator

Rules for Security Solutions

Owner

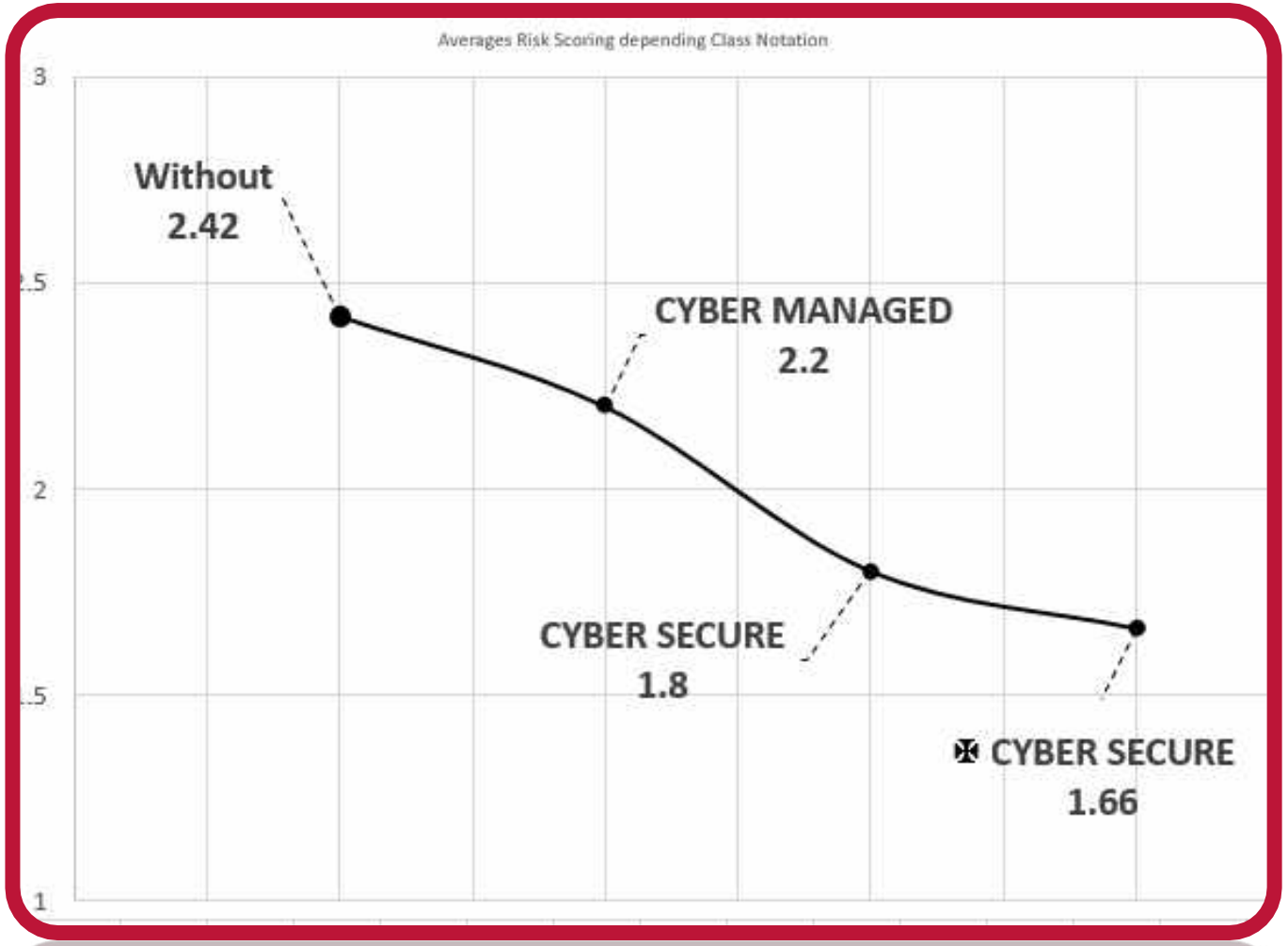


Rules for Vessel Management

✠ CYBER SECURE

1) This Class Notation **requires technical** equipment.
2) Because of **rules for design phase**, CYBER SECURE is mainly dedicated to **new construction (but also applicable to ships in service)**.
3) CYBER SECURE is a way to control security with **automatic software**.
4) Rules for vessel **cyber secure by design** are detailed. Design of systems and equipment is done with at least privilege policy. Physical accesses are managed from design. Network is mastered and secured.
5) Rules for **equipment cyber secure by design** are detailed. They will be assigned with construction mark (✠ or ✠ or •).

A scoring to take decisions and invest on the right need.

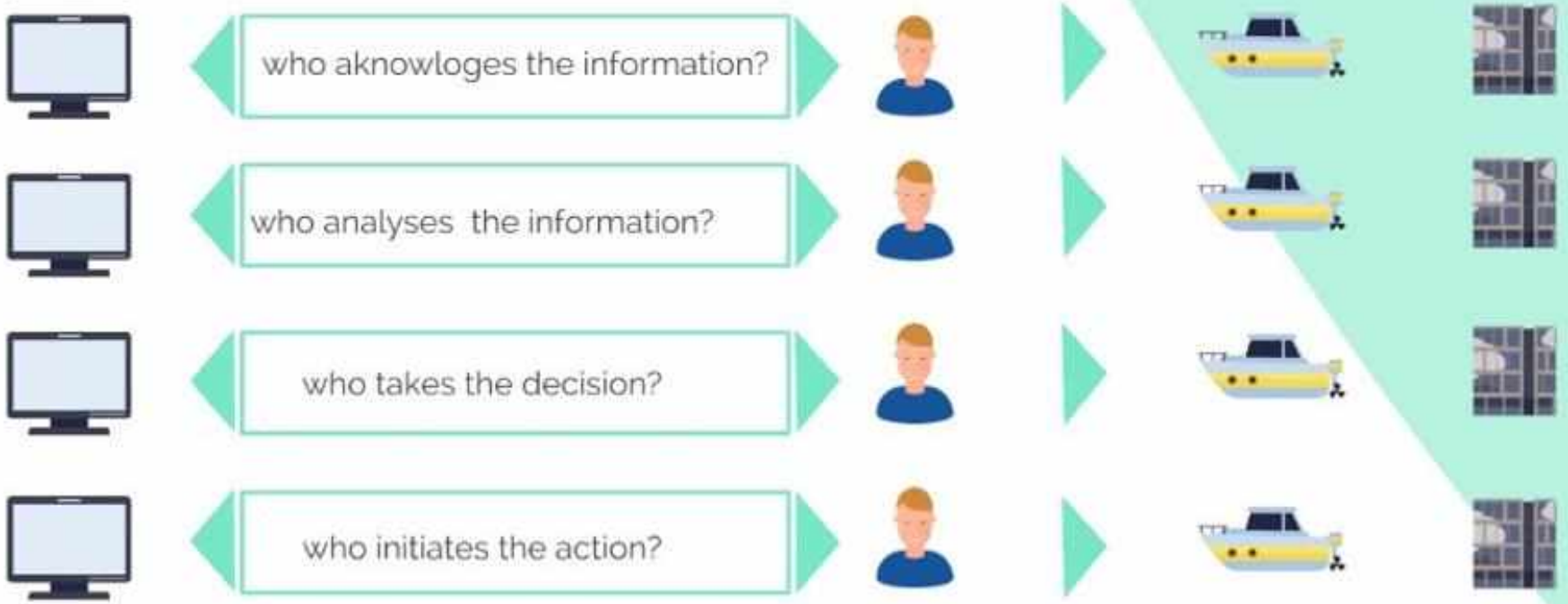


AUTONOMOUS SHIPPING

what does it actually means?

Autonomous ship	ships capable of **making decisions and performing actions** with or without human in the loop An autonomous ship **may be manned with a reduced crew or unmanned**
Unmanned ship	ship that does **not physically contain a human** and is capable of controlled movement. Unmanned ship **may be remotely controlled, supervised or fully autonomous.**

how "autonomous" a ship is?



There are **5 levels of autonomy** depending on the degree of decision making (authority) that is shifted from the human to the system.

Ship category	Level of autonomy		Manned	Method of control	Authority to make decisions	Actions initiated by
Conventional	0	Human operated	Yes	Automated or manual operations are under human control	Human	Human
Smart	1	Human directed	Yes/No	Decision support Human makes decisions and actions	Human	Human
Autonomous	2	Human delegated	Yes/No	Human must confirm decisions	Human	System
	3	Human supervised	Yes/No	System is not expecting confirmation Human is always informed of the decisions and actions	Software	System
	4	Fully autonomous	No	System is not expecting confirmation Human is informed only in case of emergency	Software	System

Partnerships @ work

BOURBON Smart Ship Program

→ Reliable operations, optimized cost

- Bureau Veritas has formed a strategic partnership with BOURBON to help **digitize** vessel operations. Smart Ship technologies enable owners to achieve better performance, reduce costs, and operate more sustainably.
- As well as providing classification notations and certification, Bureau Veritas is supporting BOURBON upstream to ensure risks are identified and mitigated. A pilot system of advanced automation of dynamic positioning (DP) has already been implemented on the Bourbon Explorer 508. Bureau Veritas provided risk analysis, design review, and onboard verification of the installation. It also assessed cybersecurity risks and certified that they have been managed as required by class.
- Bureau Veritas is now working on procedures that enable continuous verification and reduce the need for DP onboard operational and verification tasks.

BOURBON

BUREAU VERITAS

KONGSBERG

R&D @ work

EU H2020 project NOVIMAR

→ New waterborne transport concept: vessel platooning

- Definition:
- Vessel train consists of a manned lead vessel followed by a series of low-manned/unmanned digitally connected follower vessels

- Benefits:
- Concept will reduce operational costs and increase economies of scaledue to better usage of existing infrastructure
- Application:
- Inland navigation

- Duration:
- 2017 to 2021

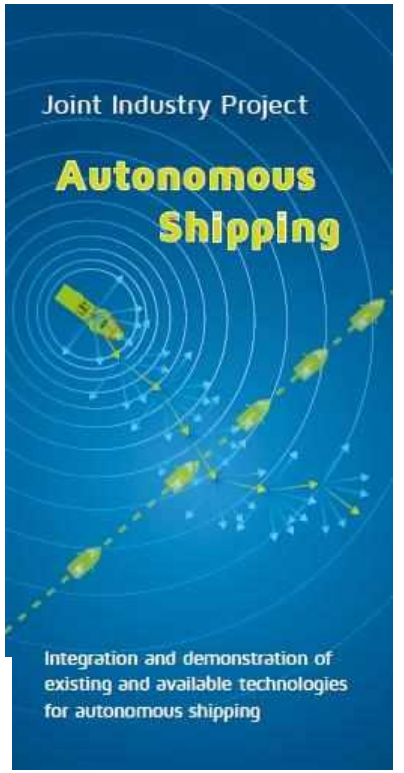
- Total cost:

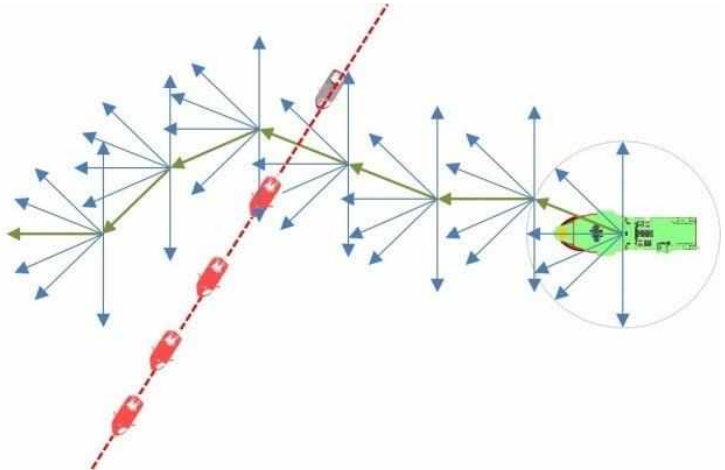
Find out more:
https://novimar.eu/concept/

R&D @ work

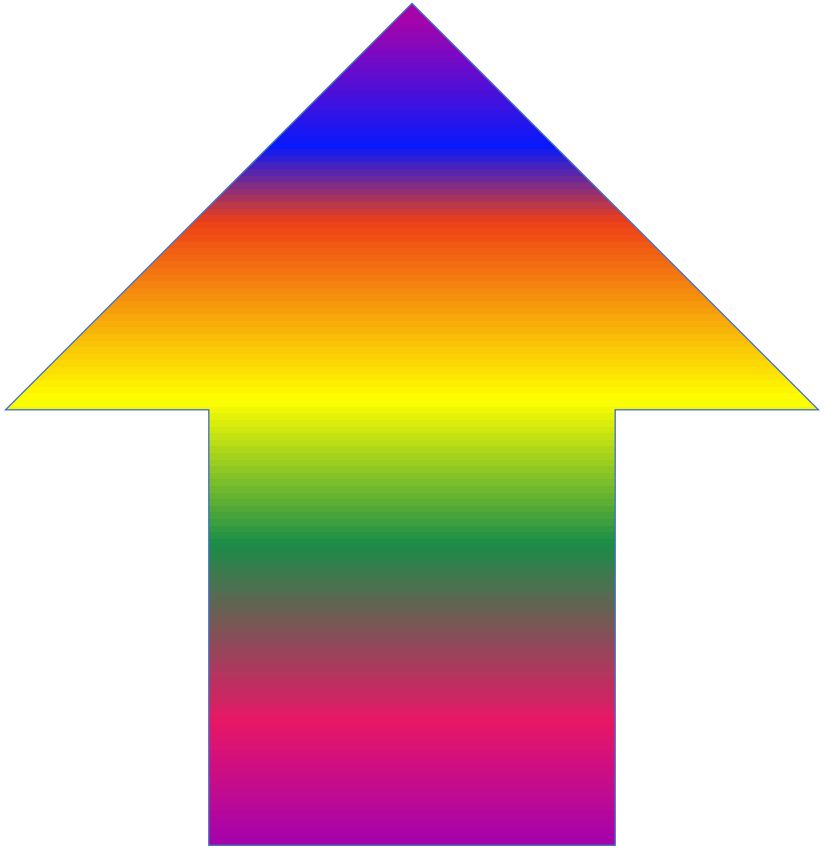
→ Dutch consortium pilots autonomous shipping

- The Dutch maritime cluster, Maritime by Holland, plans to stage a demonstration of its first autonomous vessel sometime between the end of 2018 and spring 2019.
- The vessel in question will not be new, but an existing offshore vessel, which will be provided by Dutch shipbuilder Damen Shipyards.
- The demonstration will be part of a wider-ranging, two-year programme being run by a 17-member consortium with a diverse membership: educational and research bodies, including MARIN, TNO and TU Delft; the Dutch infrastructure and defence ministries; classification society Bureau Veritas; Dutch sea pilots; companies, including SeaZip Offshore Services, DEKC Maritime and Fugro; as well as Damen Shipyards.

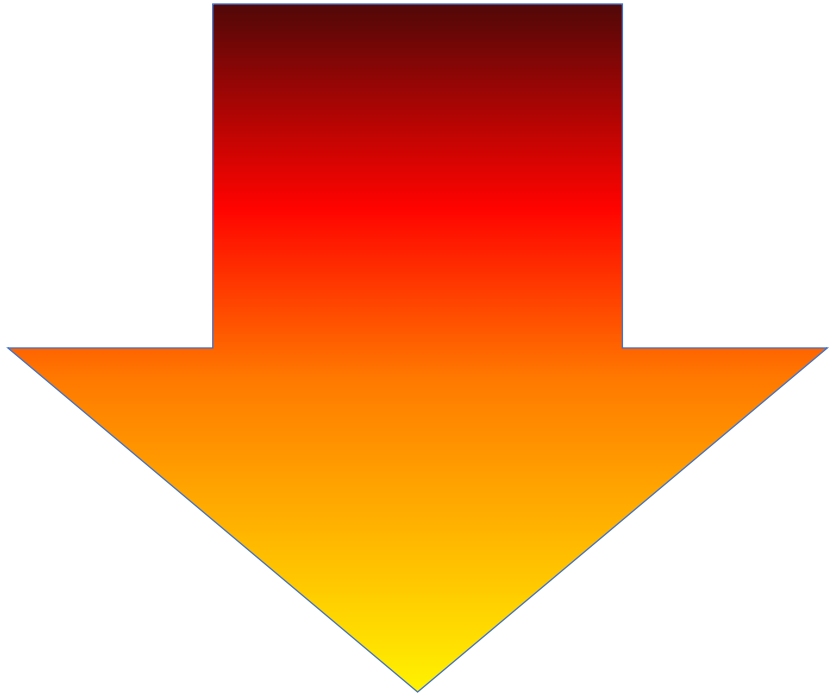


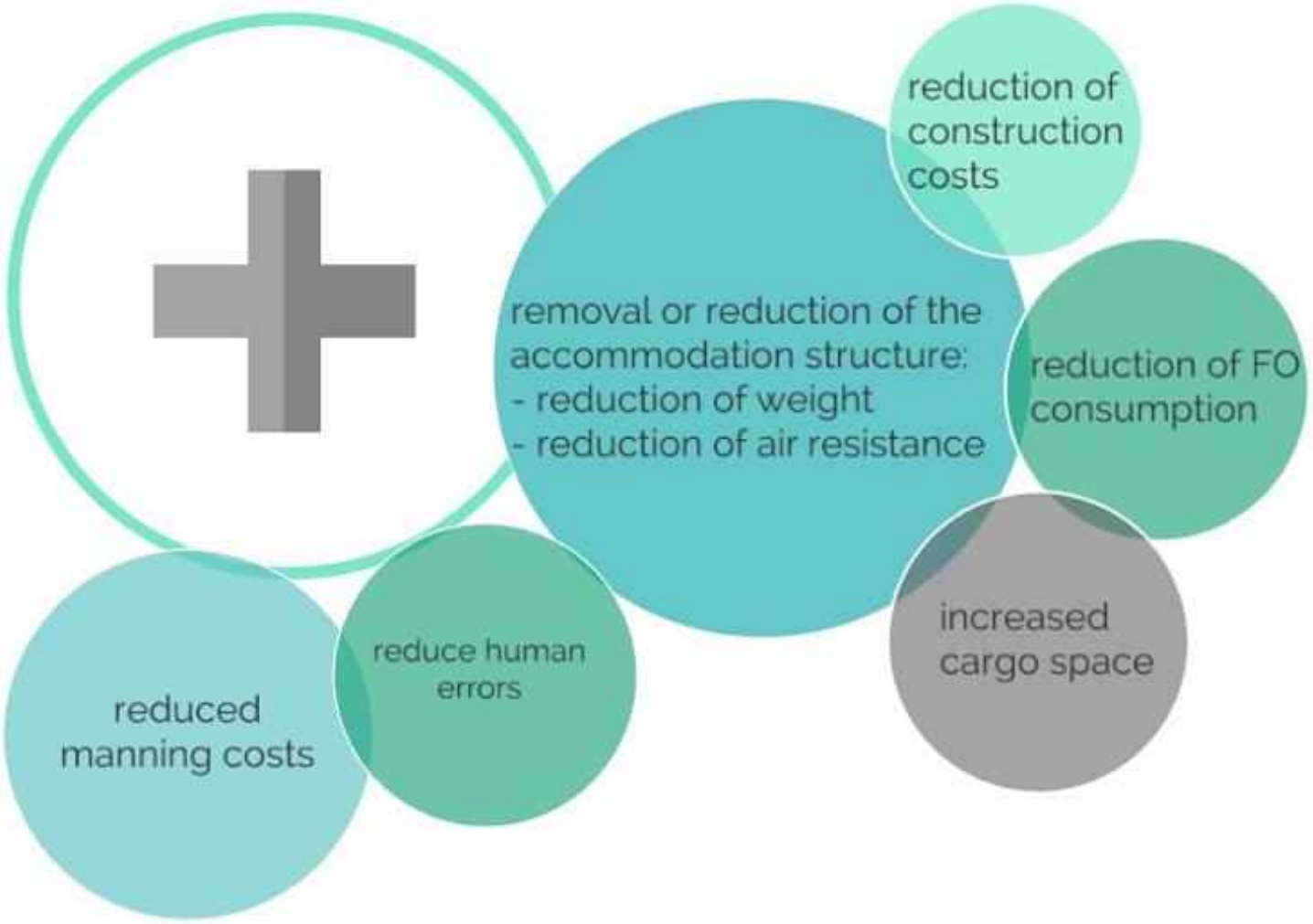


Find out more: https://maritimetechnology.nl/projecten/jip-autonomous-shipping/



Ups and downs



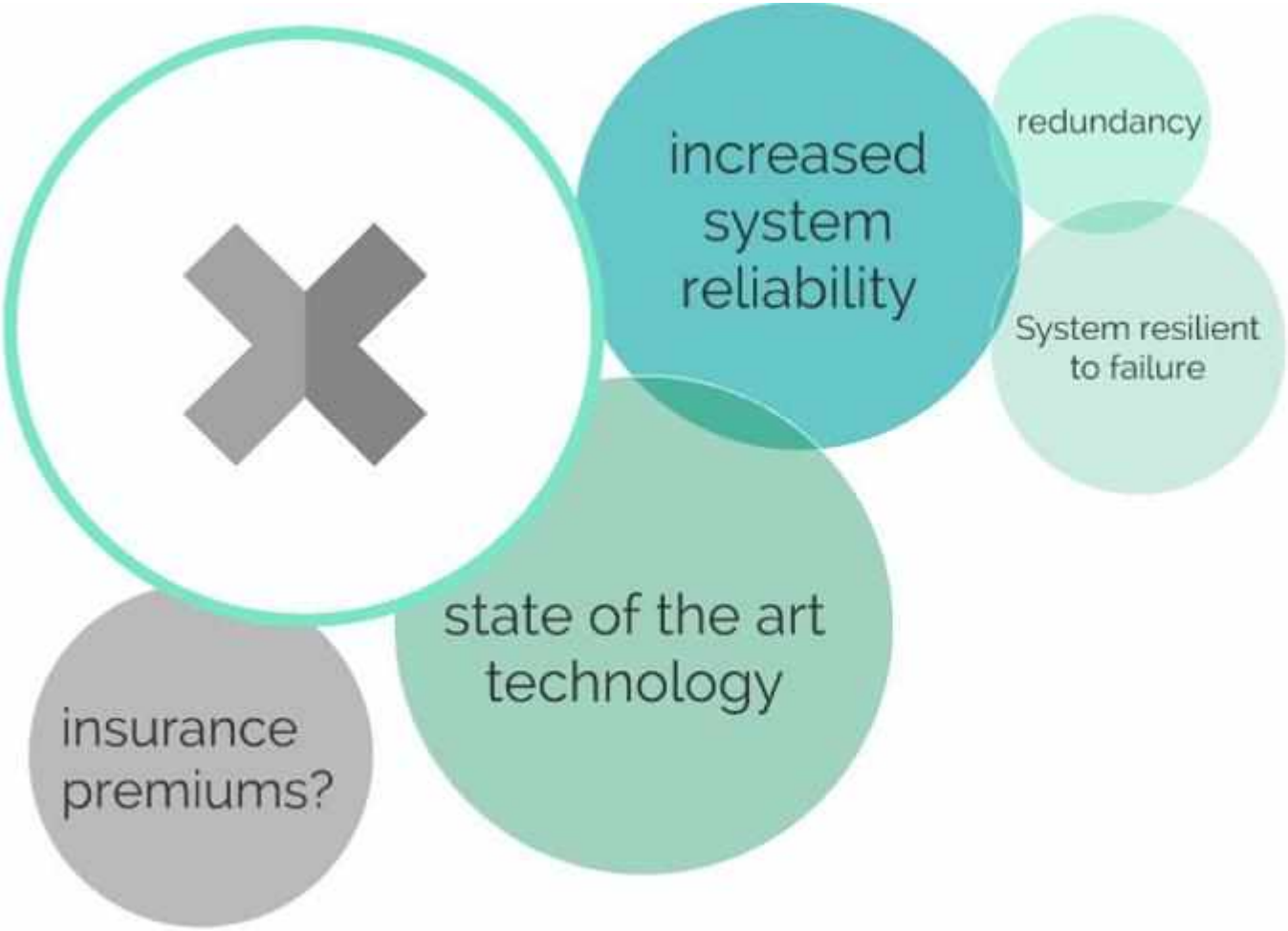


up to
5% reduction
construction costs

up to
6% reduction
FO consumption

manning cost
30%
OPEX

80% of
casualties are
caused by
human errors



Redundancy needs will increase the CAPEX by **10%**

(1)Article II (1)(b) HagueVisby Rules requires the carrier to 'properly man, equip and supply the ship' at the beginning of the voyage. Seaworthiness has the same meaning in both contracts for carriage of goods and insurance: Firemen's Fund Insurance Co v Western Australian Insurance Co Ltd and Atlantic Insurance Co Ltd (1927) 138 LT 108.

(2) To ensure the safe operation of each ship and to provide a link between the Company and those on board, every Company, as appropriate, should designate a person or persons ashore having direct access to the highest level of management.

(3) rule 5 places a positive duty on the vessel to maintain 'a proper lookout by sight and hearing as well as by all available means appropriate in the prevailing circumstances'

Colombia mar2019