
BUREAU VERITAS MARINE & OFFSHORE
SMARTSHIPS AND CIBERSECURITY
YOUR CLASSIFICATION PARTNER FOR TODAY AND TOMORROW
2024
BUREAU VERITAS
BUREAU VERITAS
1828

« Digitalizatión » in our lifes

This process offers new oportunities , but also new threats…..

CONTENT – SMART SHIPS

01

JF0

CONTEXT

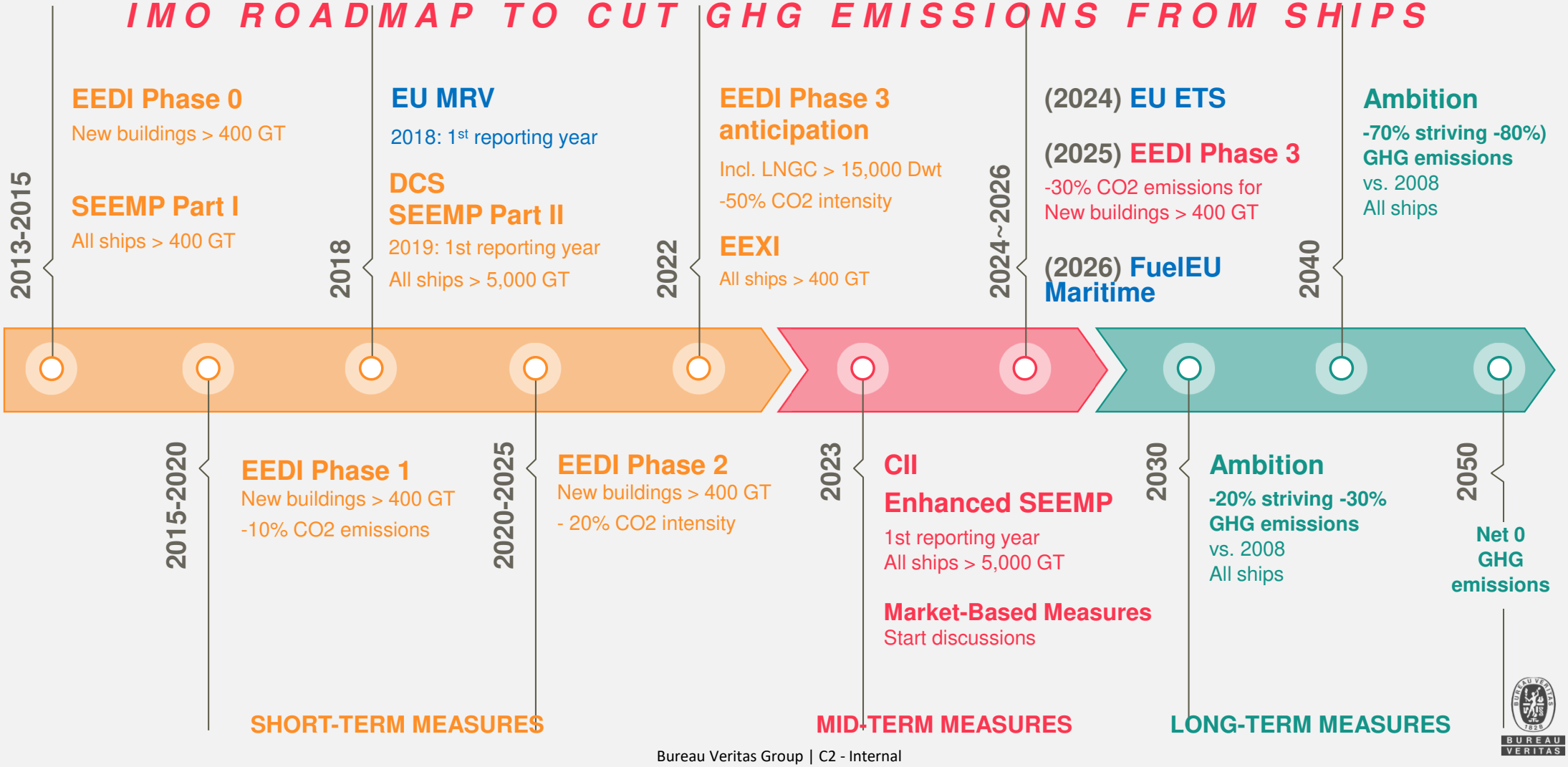
Diapositiva 4

JF0 This whole section reinforces the impression of slide 2

Jerome FLOURY; 2024-04-23T09:36:08.866

ENERGY TRANSITION

IMO ROADMAP TO CUT GHG EMISSIONS FROM SHIPS



ENERGY TRANSITION – WHAT OPTIONS?

CAPEX driven

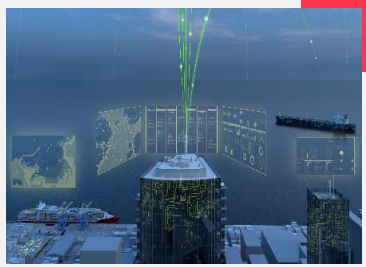
New / retrofitted hull design

New / retrofitted propulsion & power system

Alternative sources of energy

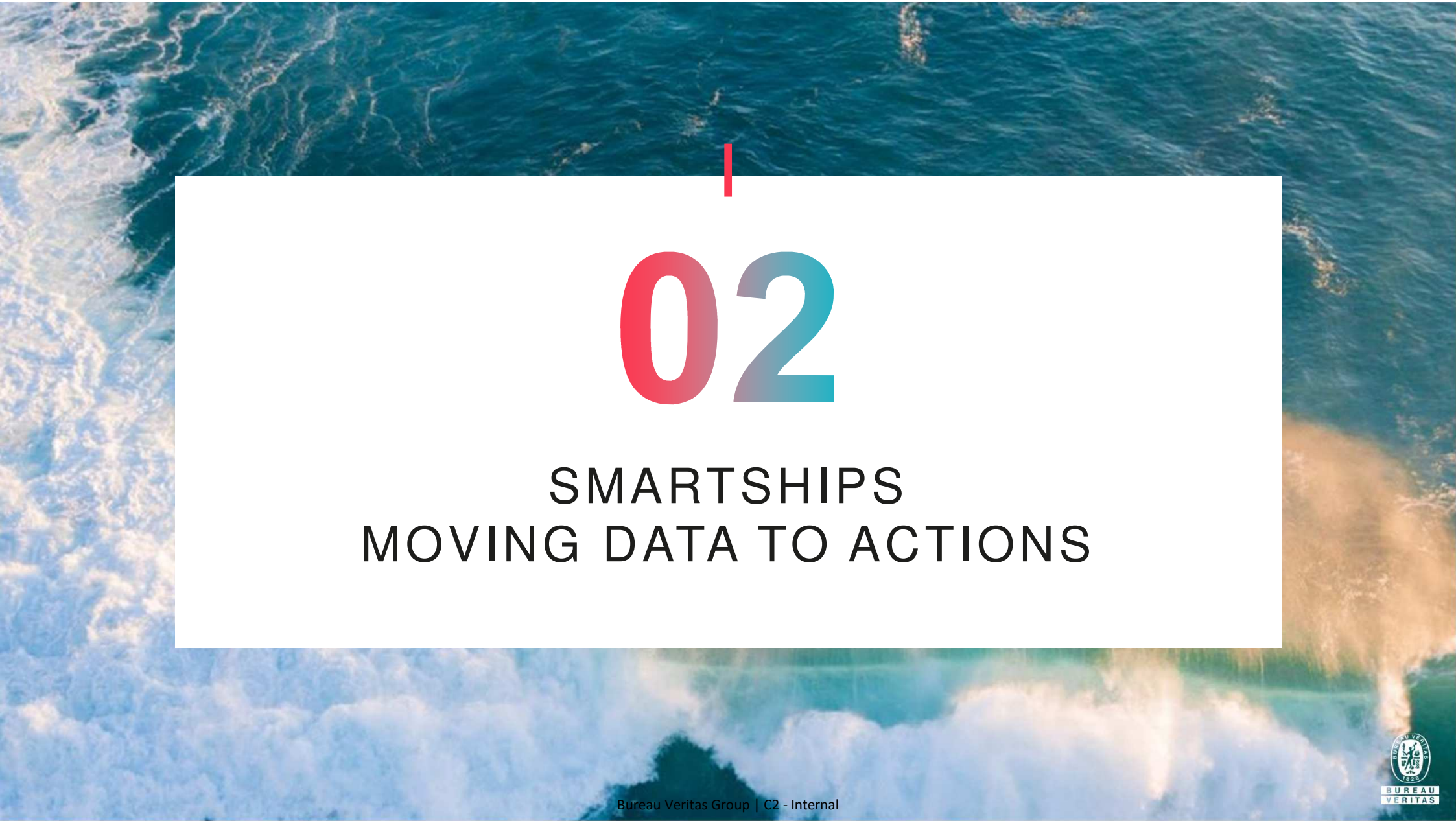
OPEX driven

Speed limitation



Operation optimization

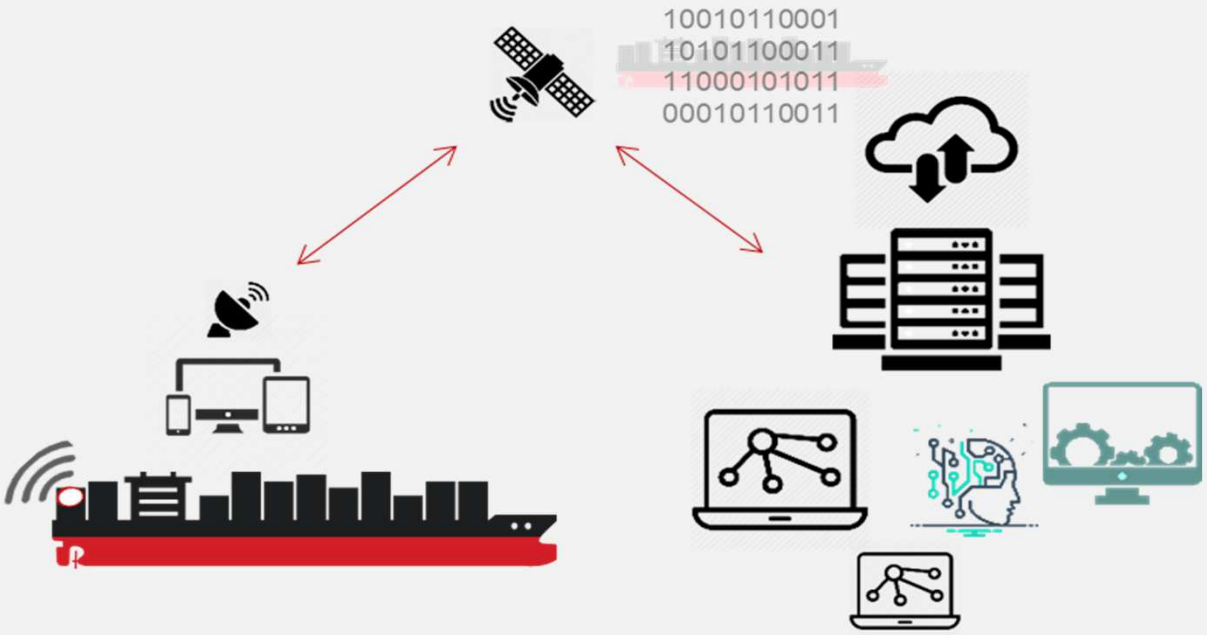
Enabled by digitalization



02

SMARTSHIPS
MOVING DATA TO ACTIONS

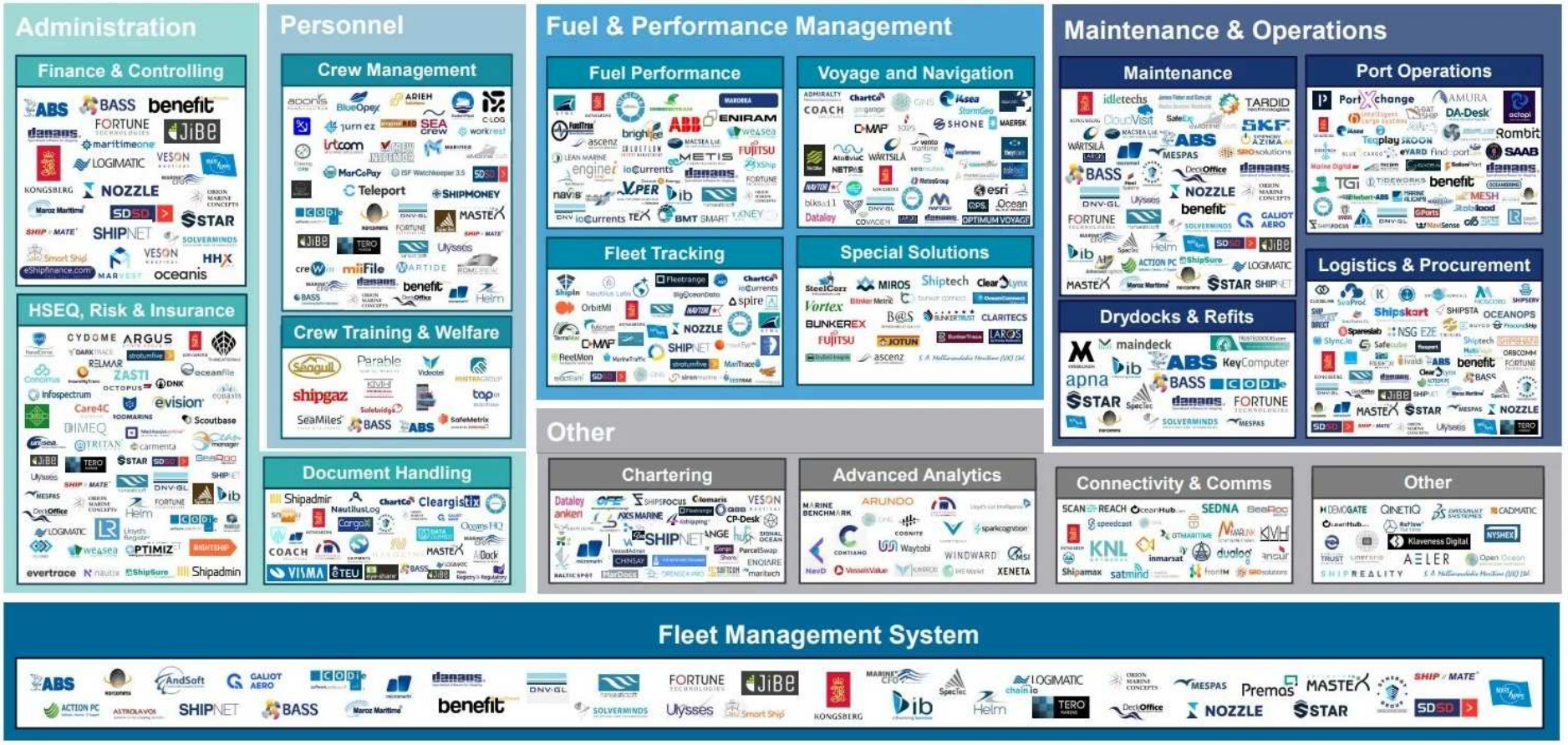
WHAT ARE WE TALKING ABOUT



SMARTSHIPS address the digitalization

- Ship's systems
- Ship's onboard processes and operations
- Ship's management and operations processes from shore

IN 2024, THE MARITIME SAAS MARKET IN 2024 REMAINS FRAGMENTED AND DYNAMIC BUT CONSOLIDATIONS ARE ACCELERATING



Source: Kongsberg

SMARTSHIP SOLUTIONS: TRANSFORMING DATA INTO ON-TIME ACTIONS

1 Data collection from multi sources

- **Ship data**
  - **OEM** Cloud (sensors)
  - **IoT supplier** Cloud (sensor)
  - **eReporting** (manual logs)
  - **Emails** (manual & replicated)
- **Company data** (ERP, VMS)
- **3rd party data platforms**

(AIS, weather, market intelligence, …)

2 Data integration

3 Data process

- Data analytics
- AI-ML models
- Scientific model

4 Data contextualization onshore

- ✓ Customized dashboards
- ✓ Notifications & alerts
- ✓ Periodical reports
- ✓ Simulations, predictions, optimizations
- ✓ **Valuable insights**

→ **Decision support**

5 Data actionable onboard

- ✓ Alerts / notification shared with shore
- ✓ **Recommendations**

→ **On-time actions**

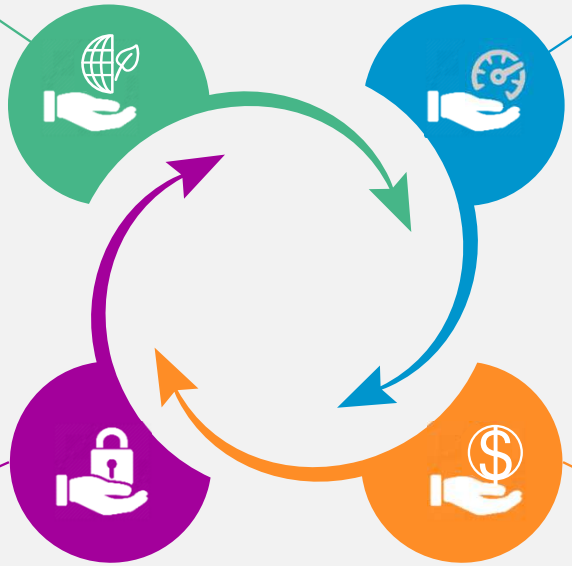
WHAT ARE THE EXPECTED BENEFITS?

BE MORE SUSTAINABLE

- Improve Energy Efficiency

BE MORE EFFICIENT

- More efficient collaborations
- Automate reporting from ships
- Increase ship's connectivity
- Improve monitoring
- Improve decision support



BE SAFE & SECURED

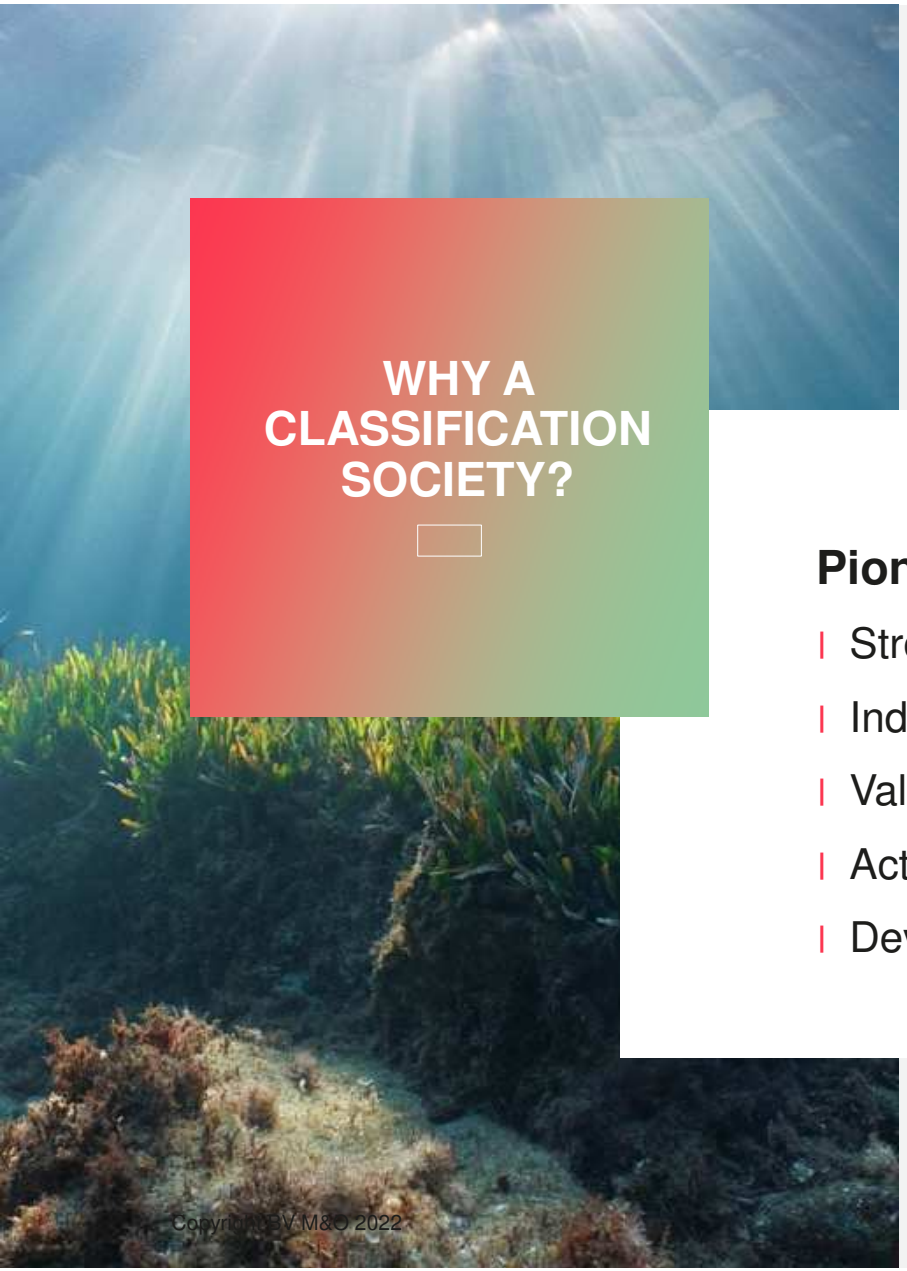
- Resilient software
- Robust data infrastructure
- Cybersecurity

SAVE OPERATIONAL COSTS

- Optimize ship's maintenance
- Optimize fleet's utilization

03

HOW BV CAN SUPPORT YOU?



WHY A CLASSIFICATION SOCIETY?

Pioneering innovation together with you

- Strong R&D
- Industry collaboration through JIP & JDP
- Validate innovative concepts through Approvals in Principle (AiP)
- Active in Regulatory and Standardization
- Develop BV Classification Rules and notations

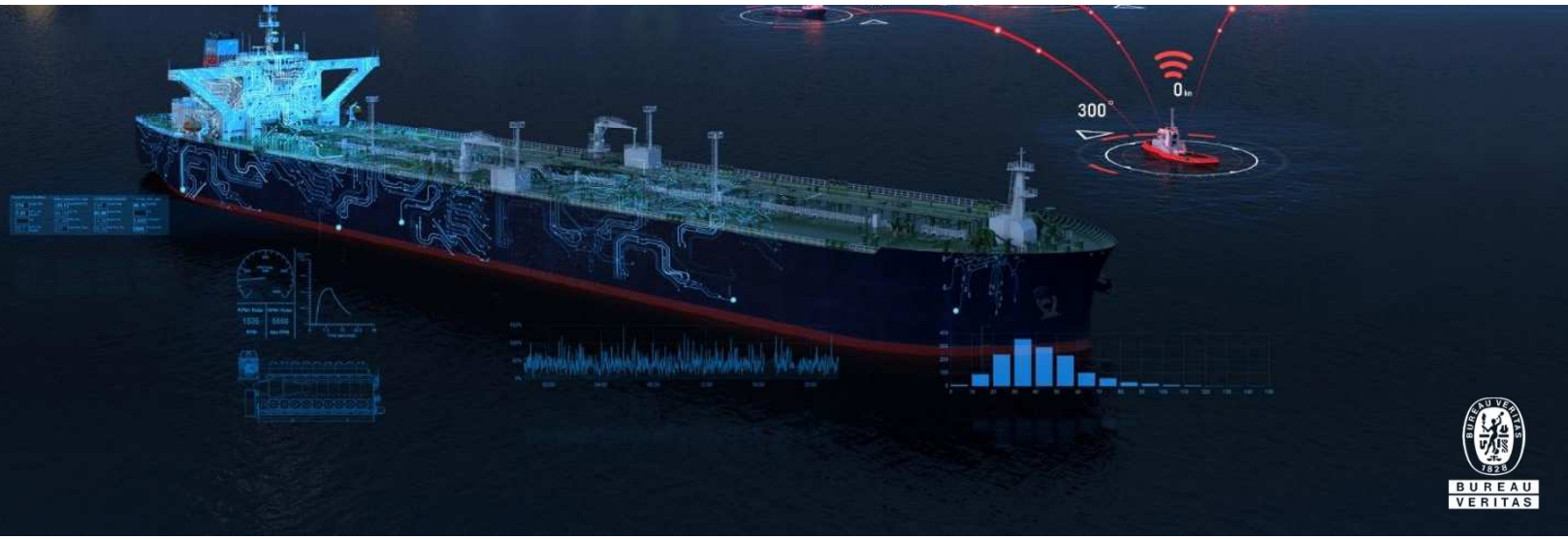
SMARTSHIPS

OUR VISION IS INSPIRED BY THE LIFECYCLE OF THE SHIP'S DATA

COMPUTER BASED SHIPS

AUGMENTED SHIPS

AUTONOMOUS SHIPS



BUREAU VERITAS

COMPOSITION OF THE CLASS MARK

Two-dimensional approach

SMART (_ _)

SCOPE

The scope of application of the smart function:

- **H** - Hull
- **M** - Machinery
- **N** - Navigation
- **MH** - Machinery Health Monitoring
- **EnE** - Energy Efficiency
- **X** - Special

DATA CYCLE

Smart group's number:

1 - Computer Based Ship
2 - Connected Ship
3 - Augmented Ship
4 - Remotely operated and Autonomous ship

BUREAU VERITAS

SUMMARY - CYBER RESILIENCE

01

From 2019 to 2024
Evolution in regulations

02

Ships in service

IMO Resolution

03

Future vessels

UR E26 Cyber Resilience for vessels

04

OEMs

UR E27 Cyber Resilience for equipment

Cyber security

Prevent intentional malicious actions (cyber attack)

Cyber safety

Prevent involuntary accidents and mistakes (system failure)

Now we have to define the problem……

"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!"

PIONEERING THE SAFETY AND PERFORMANCE OF CYBER SECURE SYSTEMS

Shaping a better maritime world.

BUREAU VERITAS

01

FROM 2019 TO 2024 EVOLUTION OF CYBERSECURITY REGULATIONS

EVOLUTION FROM 2019 TO 2024

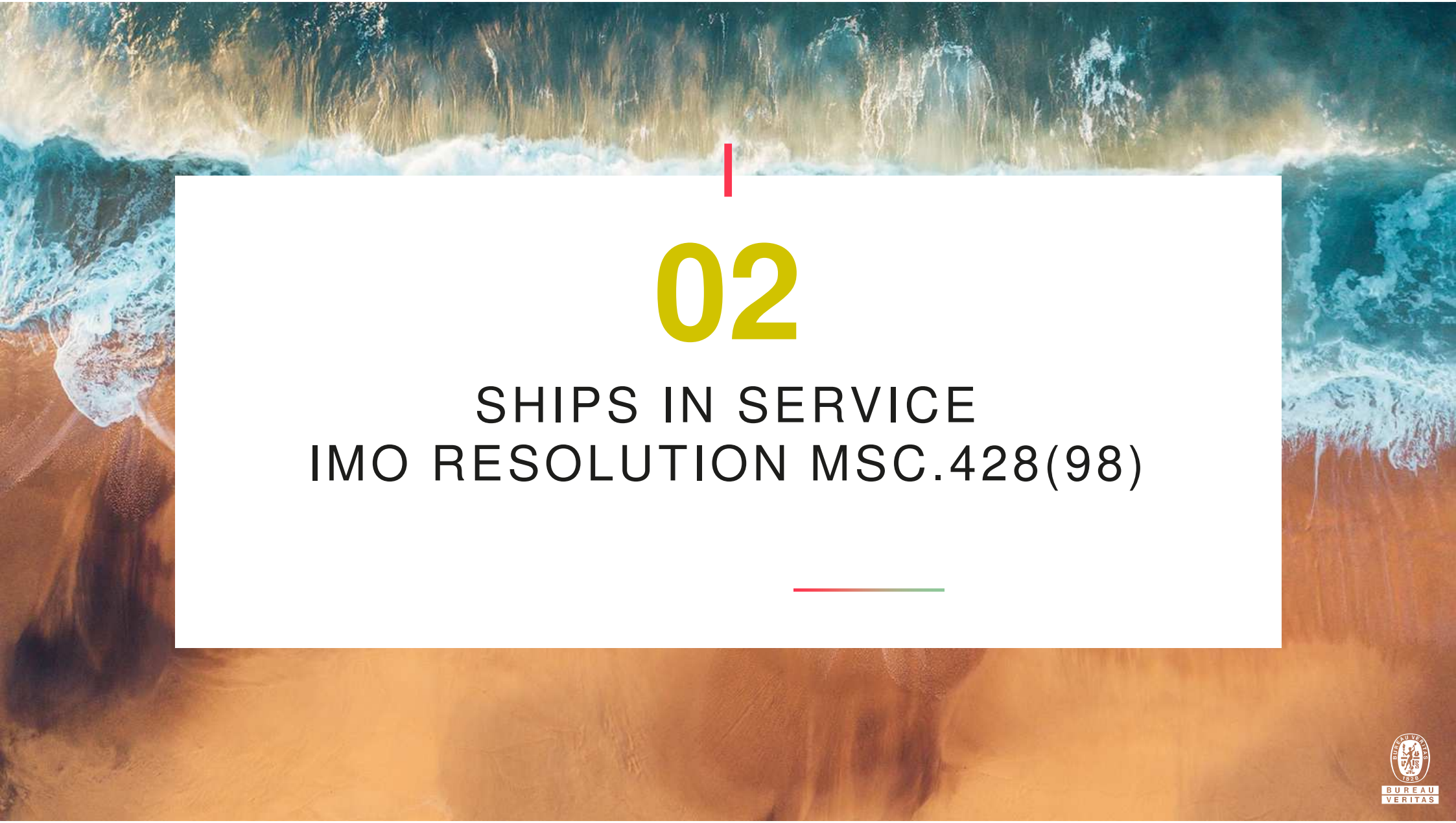
MANDATORY
CYBER SECURITY REQUIREMENTS
for a vessel to get Class from any Class Society

IMO Res. MSC.428(98)
Cyber Security for ships in service

AUDITED BY FLAGS + PORT STATE CONTROLS

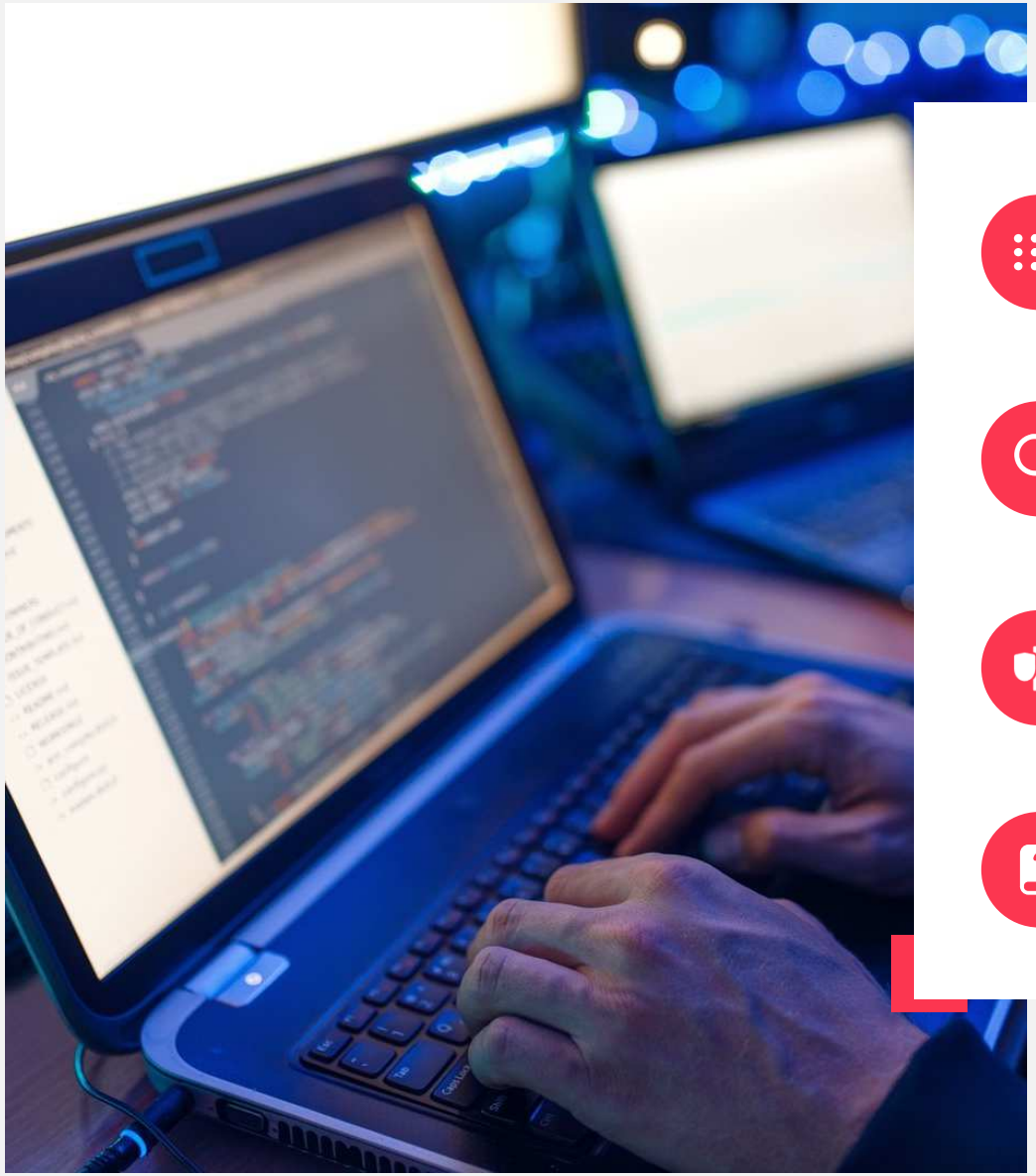
IACS UR E26
IACS UR E27
Requirements for vessels and equipment

Preparation phase



02

SHIPS IN SERVICE
IMO RESOLUTION MSC.428(98)



Cyber Inventory

Systems, equipment and network inventory (incl. remote access)
Yard information to be collected

Cyber Risk Analysis

Threats, effects, impacts, criticality, mitigation measures, residual risk
Methodology proposed in BV NR 659

Cyber Security Policy

Rules of Shipowner on Cyber Security for Fleet and on shore
Rules, roles, responsibilities
What is to be implemented

Cyber Handbook

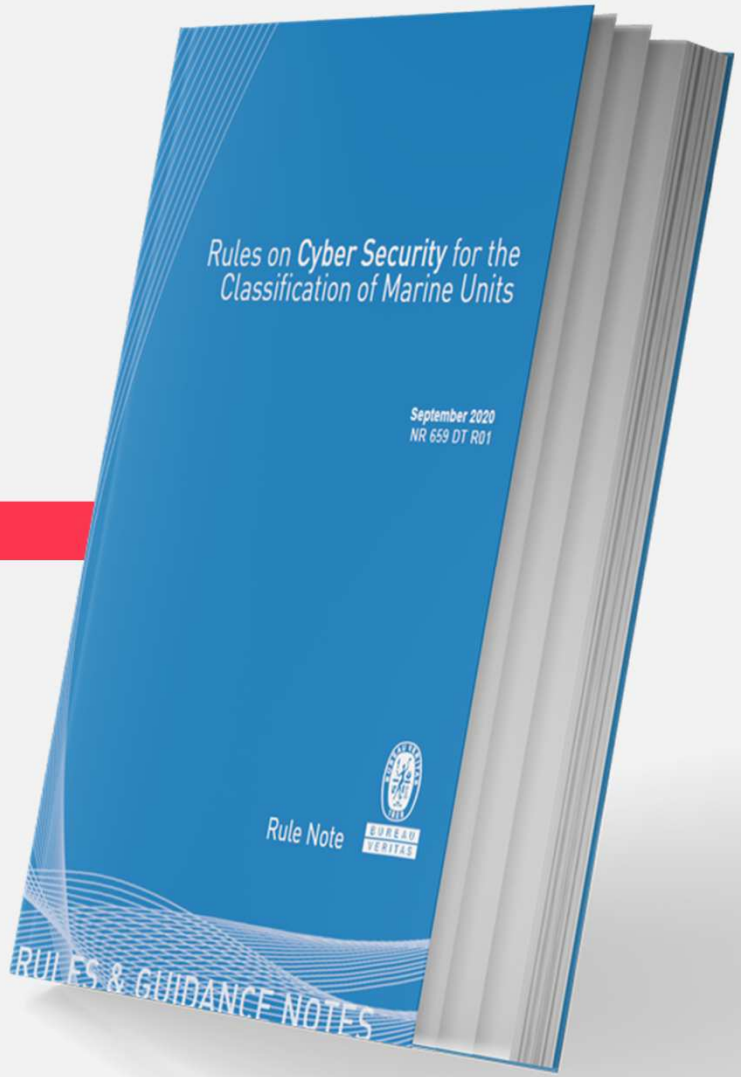
Onboard procedures on how to implement Policy
Monitoring, maintenance, incident response (from non-compliance to crisis management, back-up and recovery) procedures

HOW DOES BV M&O HELP SHIPOWNERS?

ADDITIONAL CLASS NOTATION FOR VESSELS

CYBER MANAGED CLASS NOTATION

- Compliance with IMO Resolution MSC.428(98)
- Documentation proving implementation of robust cyber security risk management as required by ISM Code
- Covers OT and IT – Covers crew procedures and training
- 1 day survey on board by BV surveyor



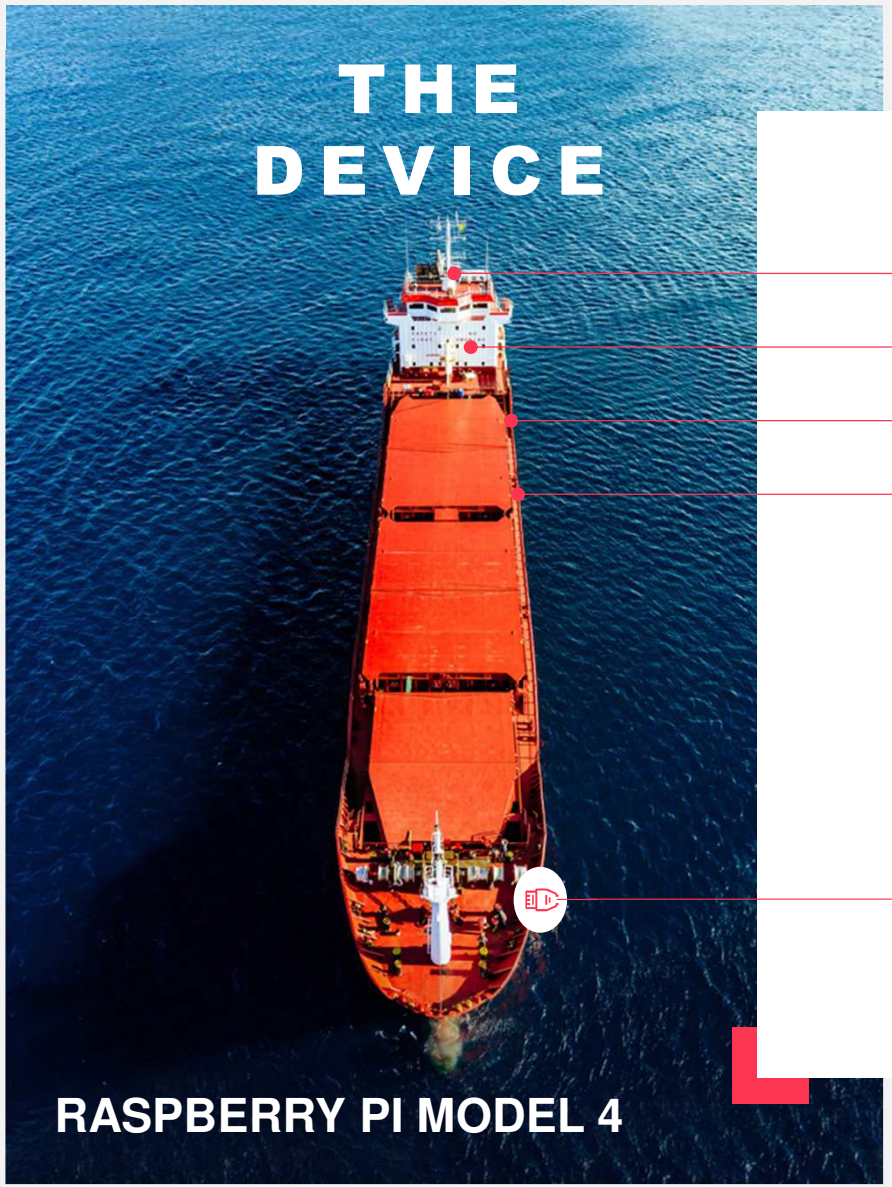
CYBER HEALTH ANALYSIS REPORT TOOL (CHART)

CYBER HEALTH CHECK

- Network **listening**
- Network **scanning**

DELIVERABLES

- **Network visualization** and traffic analysis
- **Gap analysis** with any standard
- **Wi-fi audit** is performed on the same occasion
- **Mitigation measures** suggestions
- **Penetration testing** can be requested by owner afterwards

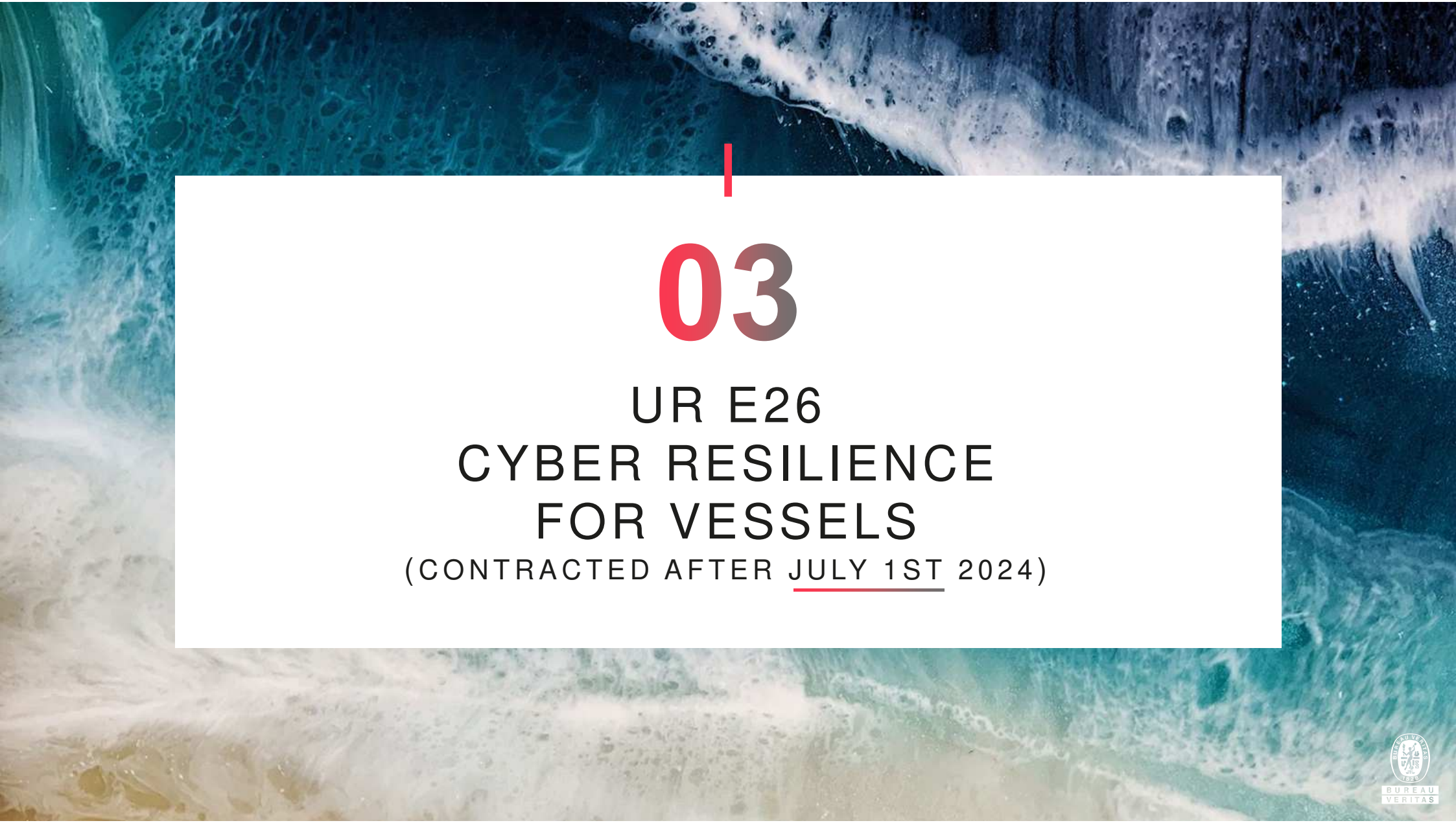


The device is plugged ON MULTIPLE LOCATIONS on board

- Communication
- Navigation
- Cargo
- Machinery

Both IT/OT sides

- **IT**
  - Application server
  - Core switch
- **OT**
  - Propulsion
  - Navigation network
  - IAS
  - …



03

UR E26
CYBER RESILIENCE FOR VESSELS

(CONTRACTED AFTER JULY 1ST 2024)

Entering into force on July 1st 2024

UR E26

CYBER RESILIENCE OF VESSELS

UR E26 aims to ensure the secure integration of both Operational Technology (**OT**) and Information Technology (**IT**) equipment into the vessel's network during the design, construction, commissioning, and operational life of the ship.

This UR targets the ship as a collective entity for cyber resilience and covers 5 key aspects :

- Equipment identification
- Protection
- Attack detection
- Response
- Recovery

UR E26

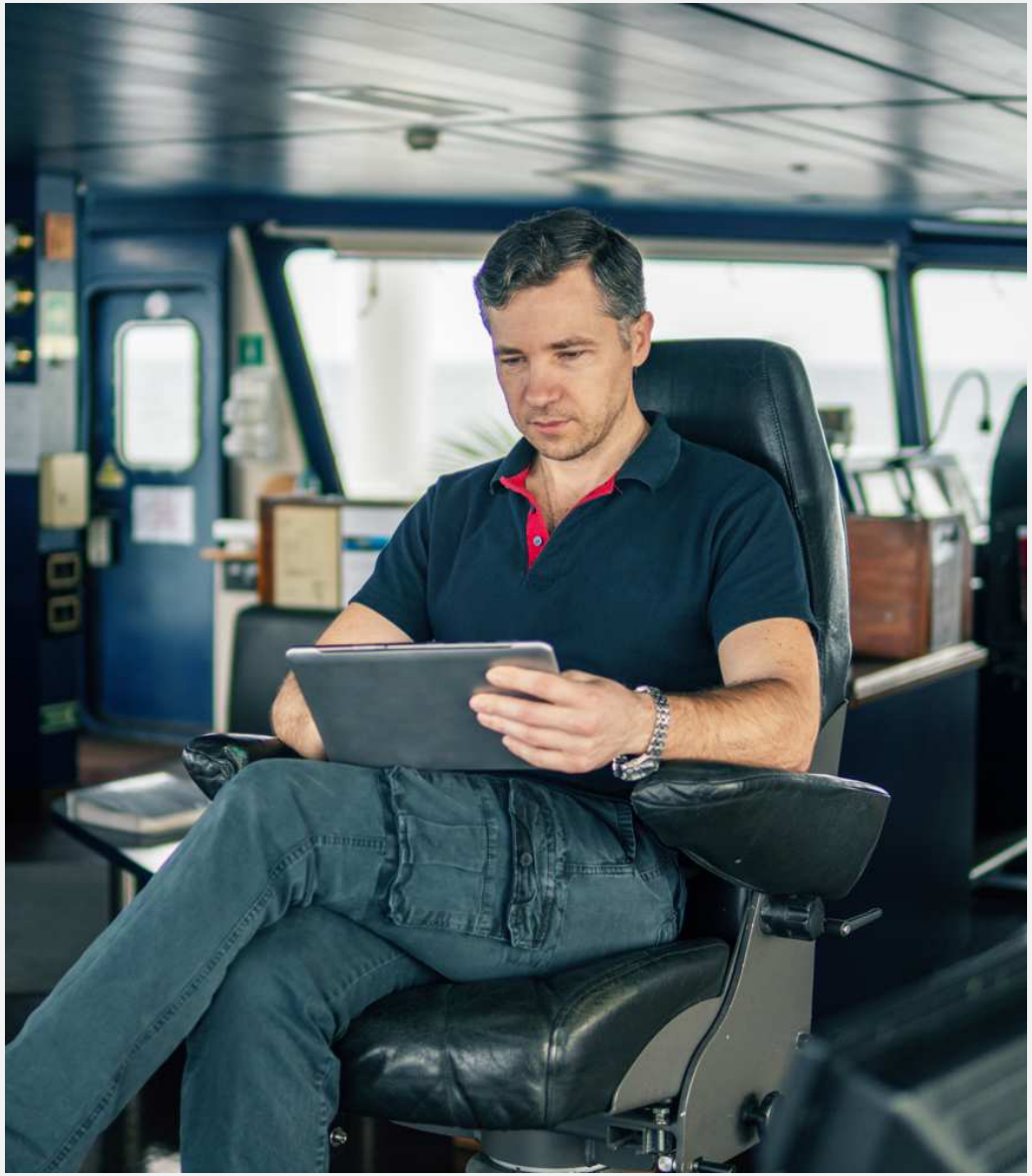
CYBER RESILIENCE OF VESSELS

Scope is

OT (Operational Technology – PLC, automation, navigational systems, machinery systems, cargo/ballast management systems,…)

+

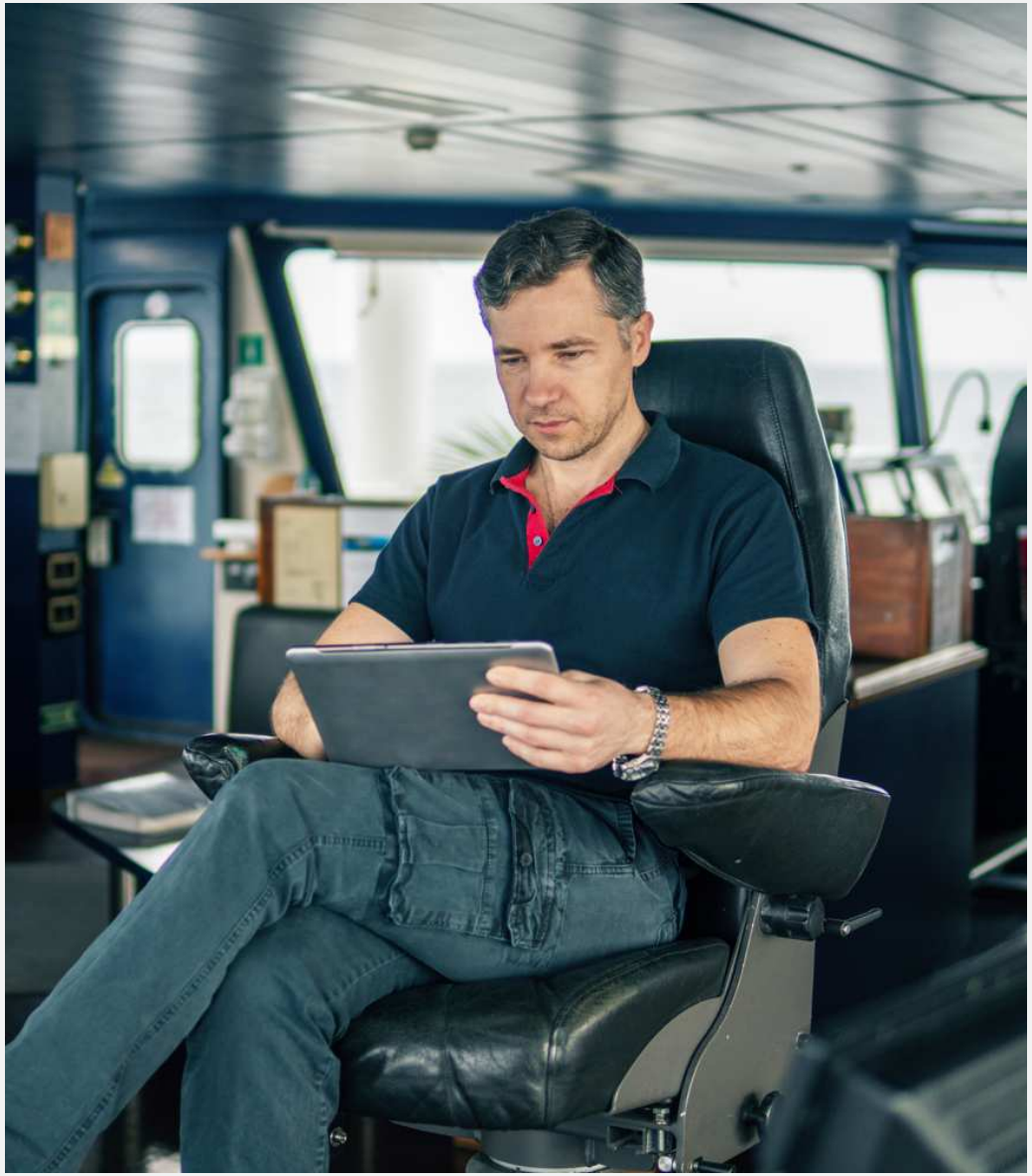
All IT (Information Technology – Computers, network security mechanisms) **connected to OT**



UR E26

MANDATORY REQUIREMENTS FOR

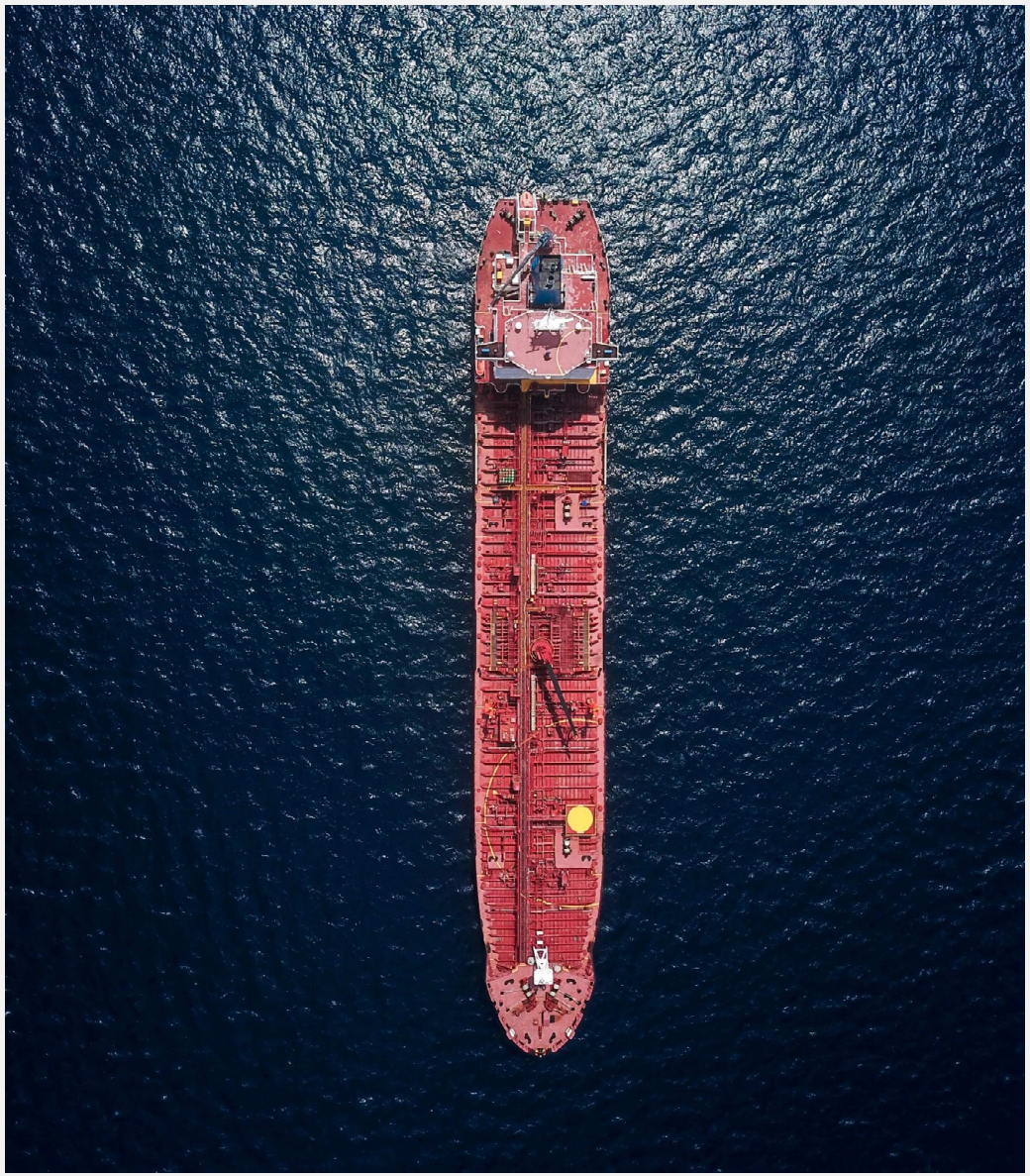
- ✓ Passenger ships (including passenger high-speed craft) engaged in international voyages
- ✓ Cargo ships of 500 GT and upwards engaged in international voyages
- ✓ High speed craft of 500 GT and upwards engaged in international voyage
- ✓ Mobile offshore drilling units of 500 GT and upwards
- ✓ Self-propelled mobile offshore units engaged in construction (ie wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, etc)



UR E26

NON-MANDATORY GUIDANCE TO:

- ✓ Ships of war and troopships
- ✓ Cargo ships less than 500 gross tonnage
- ✓ Vessels not propelled by mechanical means
- ✓ Wooden ships of primitive build
- ✓ Passenger yachts (passengers not more than 12).
- ✓ Pleasure yachts not engaged in trade
- ✓ Fishing vessels
- ✓ Site specific offshore installations (ie FPSOs, FSUs, etc)



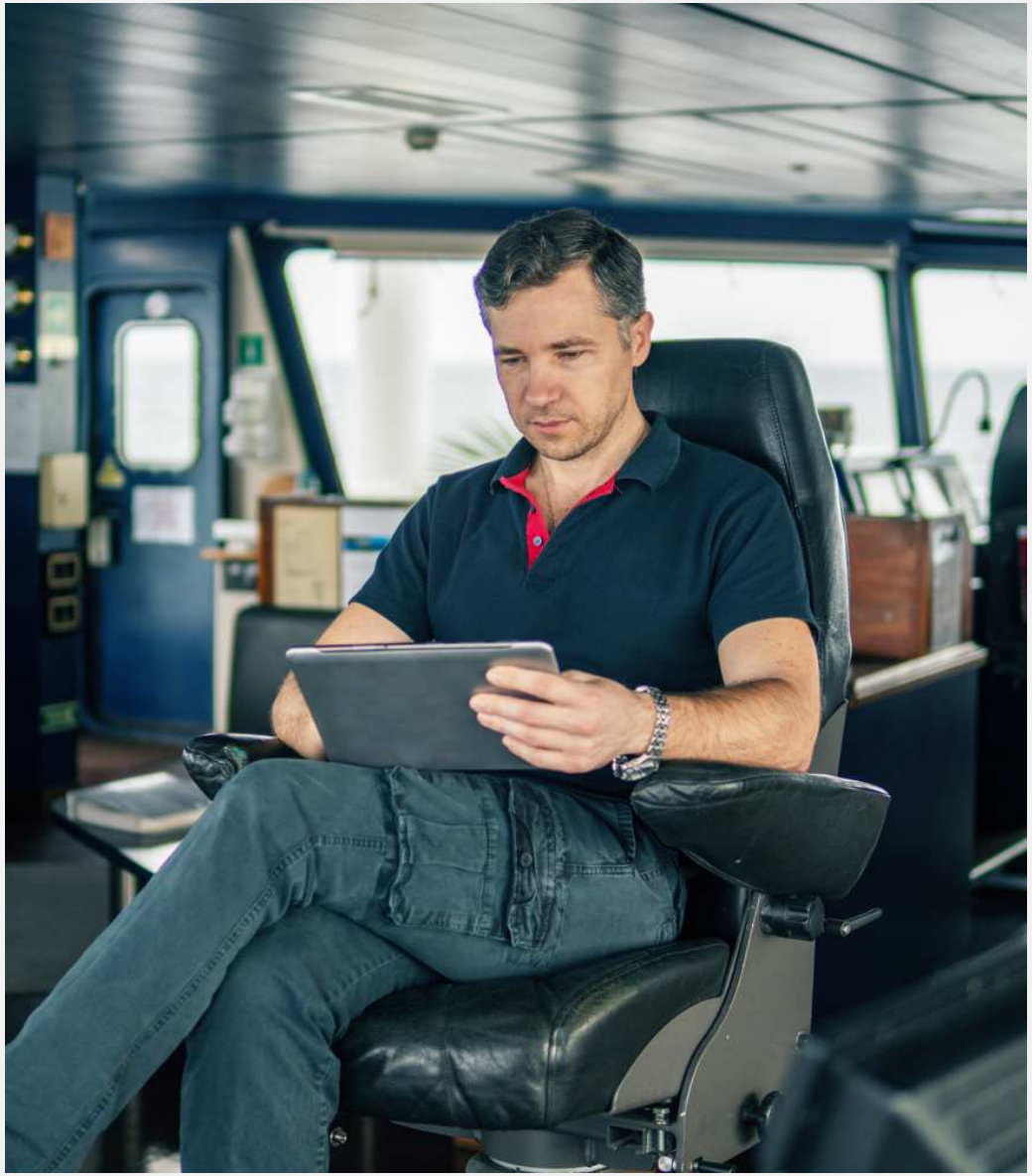
UR E26

NEW TECHNICAL REQUIREMENTS

UR E26 – REQUIREMENTS FOR VESSELS

New stringent requirements on:

- Network segmentation
- Network traffic protection and monitoring
- Logical and physical access management
- Remote access to onboard equipment
- Cyber incident detection ability
- Restoration & resilience



UR E26

WHAT WILL IT CHANGE?

CYBER REVOLUTION FOR MARITIME INDUSTRY IS ON ITS WAY

- **UR E26 cyber security requirements, optional until now, will have to be implemented in a mandatory way, as of 2024, for a vessel to be Classed by a Class Society.**
- **Documents produced by Yards** will accompany vessels during their whole life cycle, and will therefore have to be updated by Shipowners whenever necessary
- Dialogue is becoming necessary between Owner, Yard, selected manufacturers (UR E27 certified) and Class Society at the very early stage of design

HOW DOES BV M&O HELP SHIPYARDS

CYBER RESILIENT CLASS NOTATION

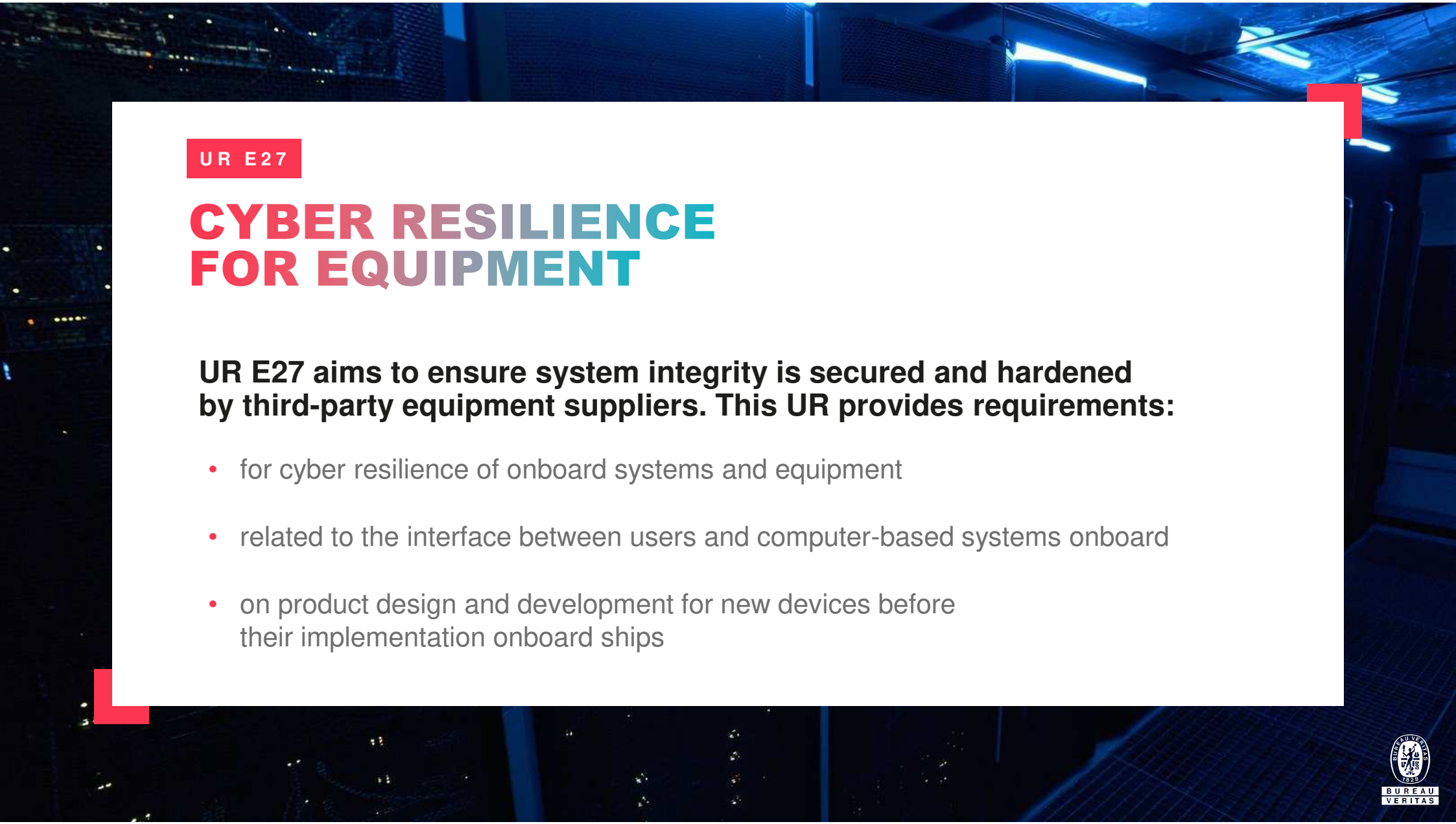
- ✓ Basic compliance with UR E26
- ✓ Cyber will be surveyed every year when ship is in service, along with other disciplines

CYBER SECURE CLASS NOTATION

- ✓ Compliance with UR E26, but complemented by more stringent requirements
- ✓ Recommended for:
  - Autonomous vessels
  - Military vessels
  - Demanding owners of highly connected vessels

04

UR E27 REV.1
CYBER RESILIENCE FOR EQUIPMENT



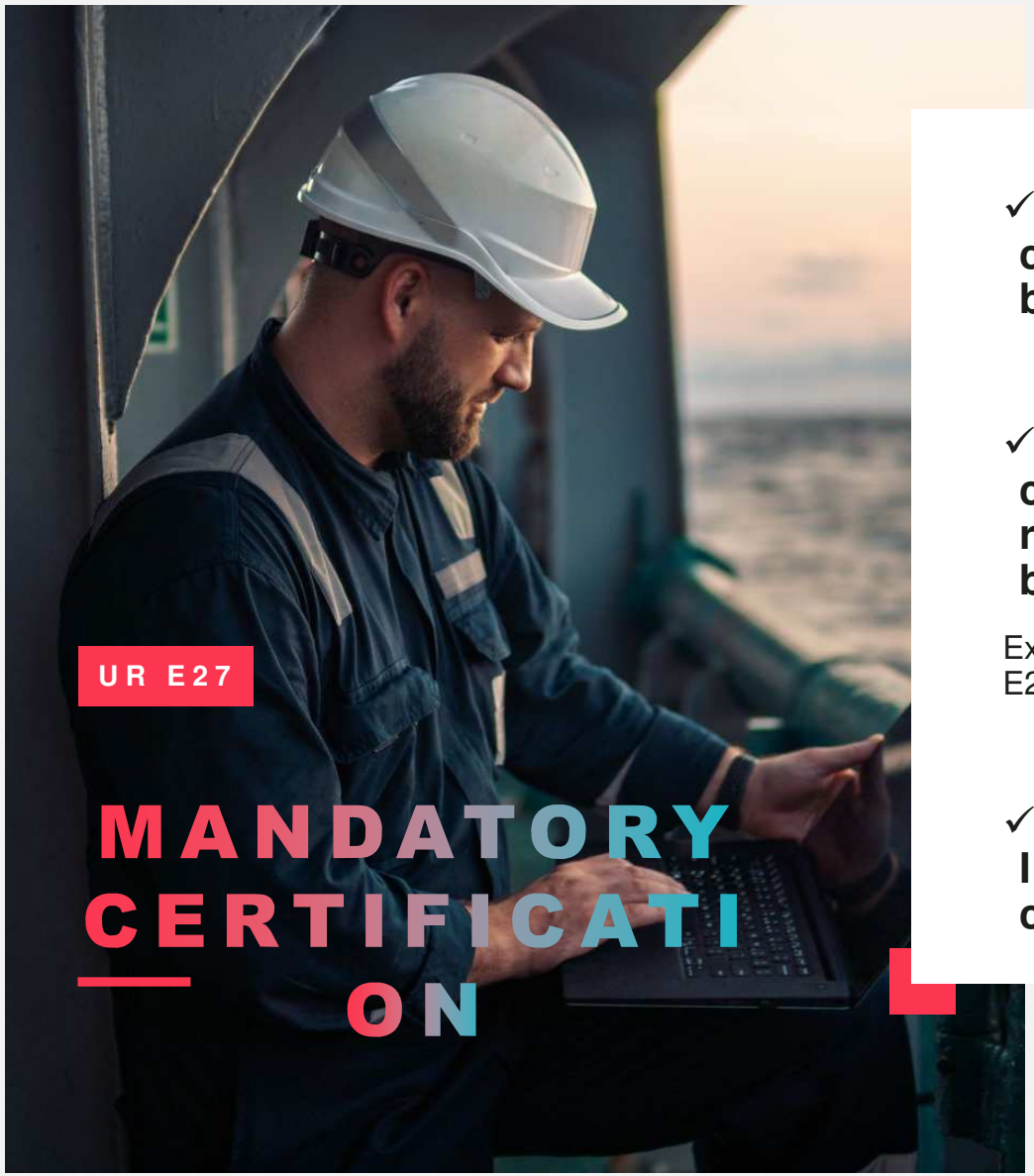
UR E27

CYBER RESILIENCE FOR EQUIPMENT

UR E27 aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements:

- for cyber resilience of onboard systems and equipment
- related to the interface between users and computer-based systems onboard
- on product design and development for new devices before their implementation onboard ships

BUREAU VERITAS



- ✓ **CBS system/equipment selected for UR E26 compliant vessels will have to be UR E27 certified by Class.**
- ✓ **Each Class Society will require her own UR E27 certification, as there is no UR E27 mutual recognition between Class Societies for the time being.**

Example : Equipment to go on a BV-Classed vessel will have to be UR E27 certified by BV.

- ✓ **UR E27 requirements being mainly derived from IEC 62443-3-3 requirements, it is easy to UR E27 certify an already IEC 62443-3-3 certified equipment.**


BUREAU VERITAS
1828
BUREAU
VERITAS
Shaping a world of trust