Cyber Risk

A new challenge for Classification Societies

Pier Carazzai | 20 November 2017
Hong Kong

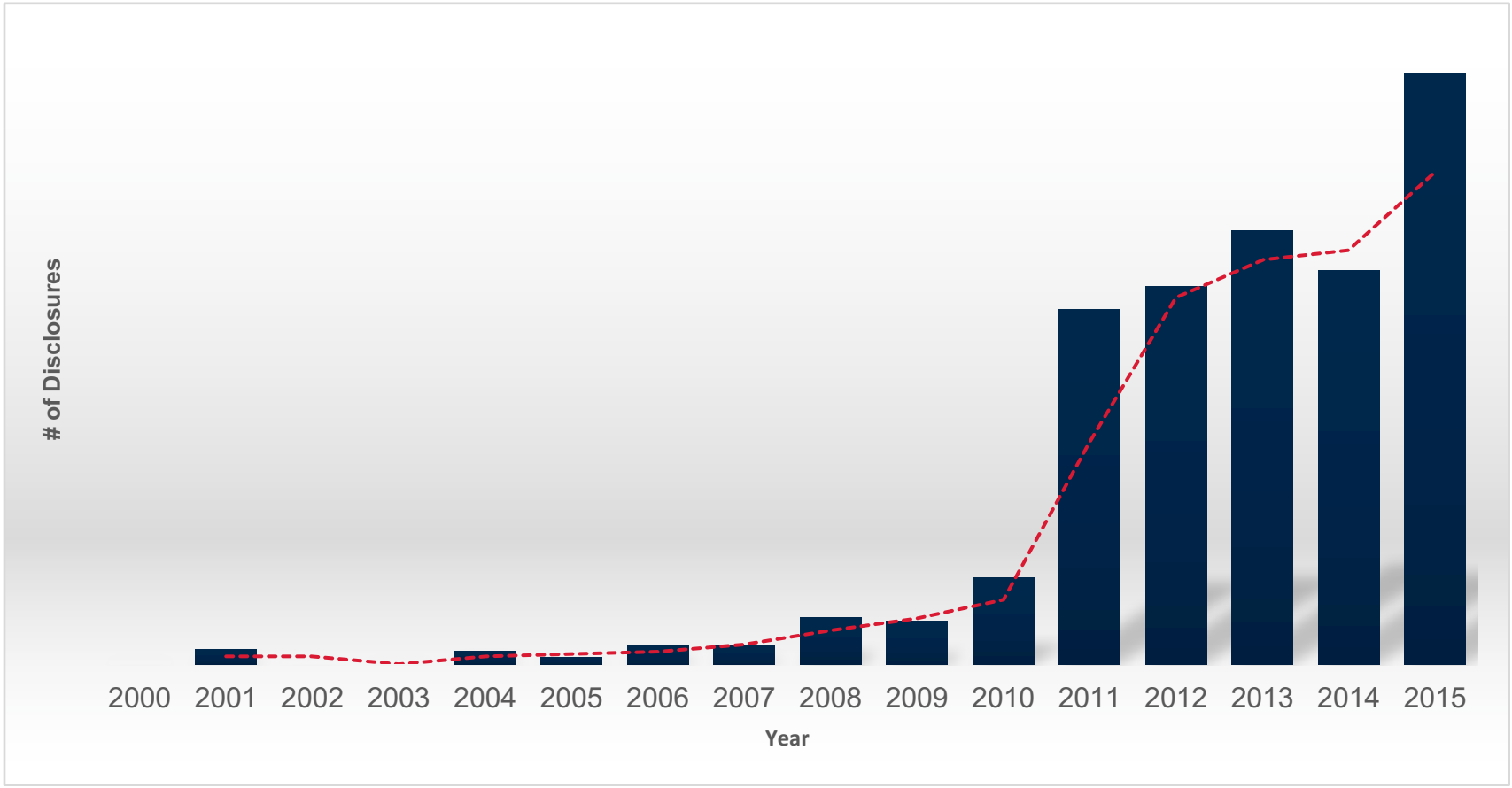
Safety Moment

Cyber Risks in the era of SMART vessels

Driving Factors

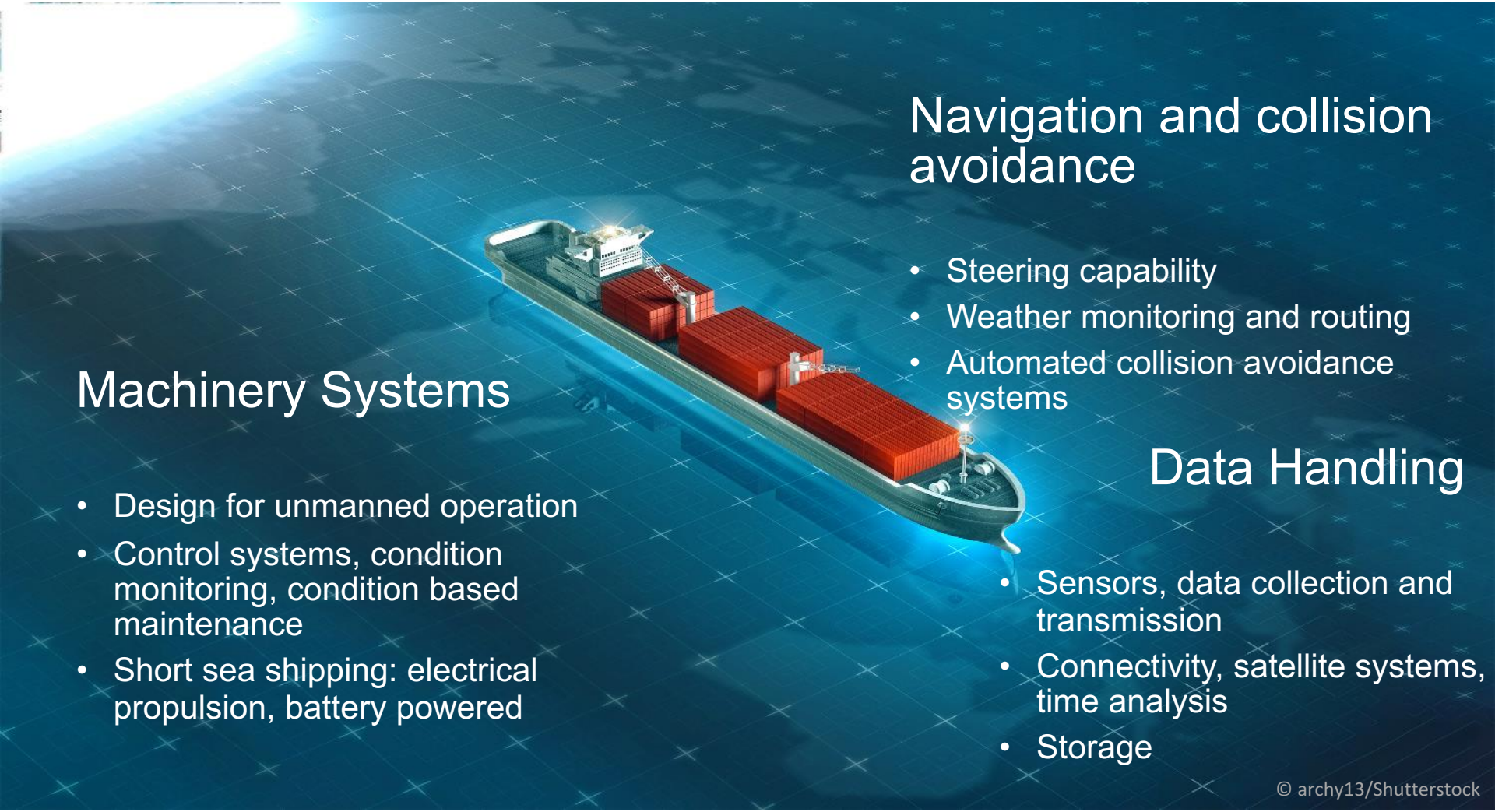
- USCG Policy Letter – 14 December 2016
- IMO MSC (98) – Specific Procedure ISM Code 2021
- TMSA 3 Compliance for Cybersecurity - 2018
- Oil Majors adding CyberSafety elements to vetting inspections
- BIMCO- Intercargo-Intertanko – June 2017
- Marine insurance Cyber exclusion clause
- *Increase in cyber-related maritime incidents*
- *SmartShip Technology*
- *Data-Centric Asset*

Control System-Specific Vulnerability Disclosure



- People are looking for OT vulnerabilities since Stuxnet attack on Iran (Siemens Step 7)
  - The statistic is sourced from the 2016 industrial control systems (ICS) vulnerability trend report, by Fireeye iSight Intelligence

Smarter ships….more automation….more connections …



Navigation and collision avoidance

- Steering capability
- Weather monitoring and routing
- Automated collision avoidance systems

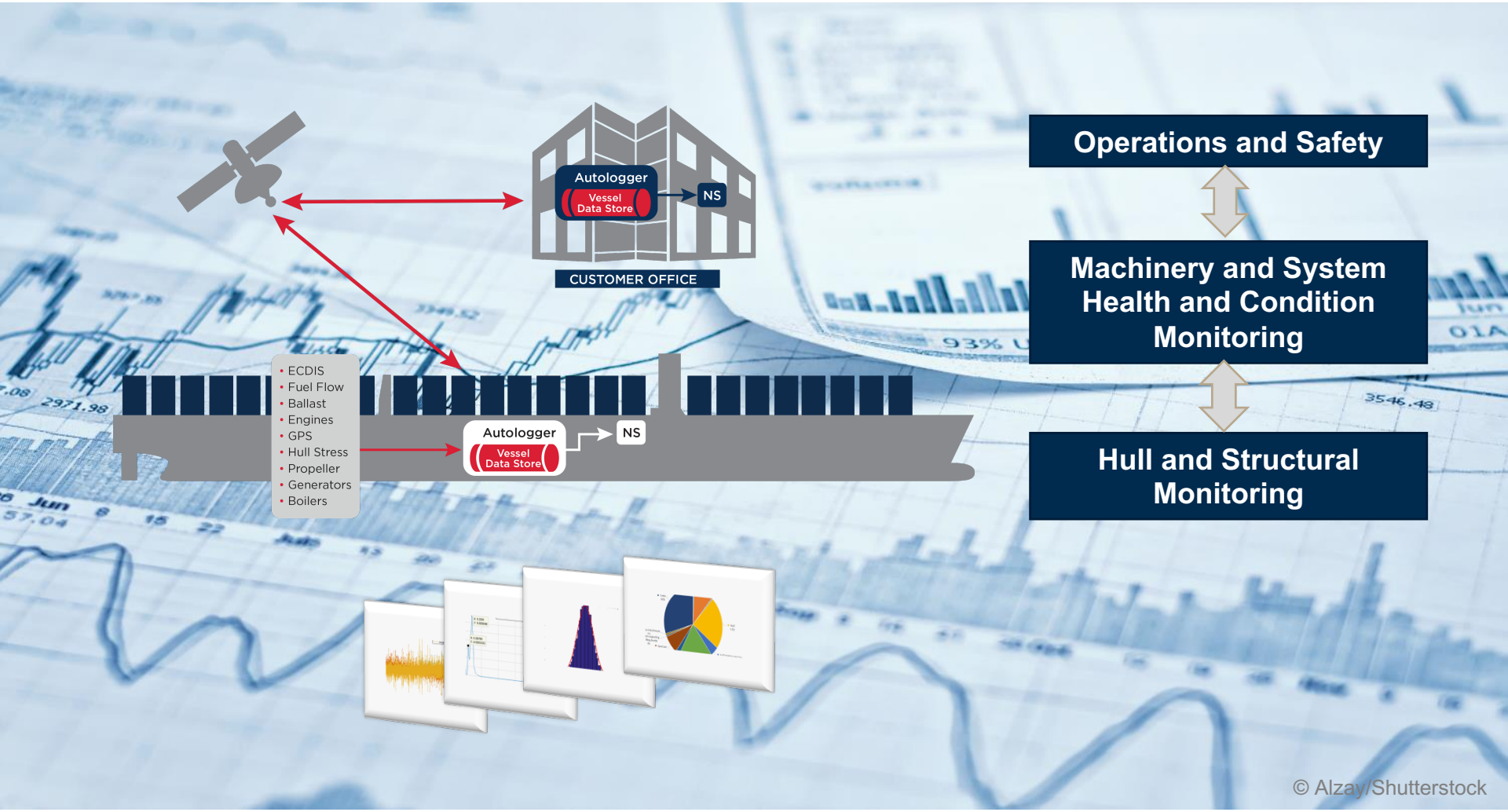
Machinery Systems

- Design for unmanned operation
- Control systems, condition monitoring, condition based maintenance
- Short sea shipping: electrical propulsion, battery powered

Data Handling

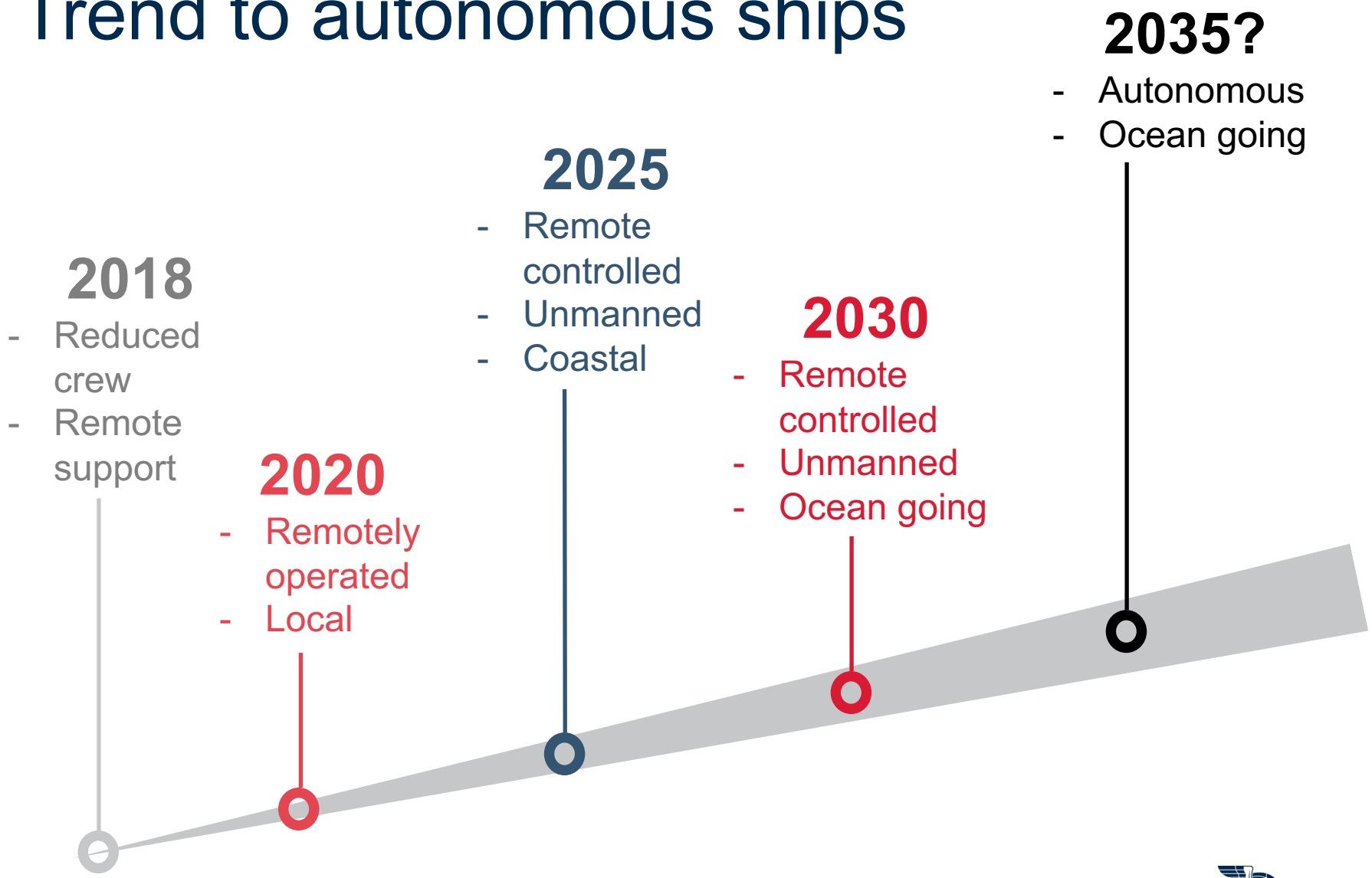
- Sensors, data collection and transmission
- Connectivity, satellite systems, time analysis
- Storage

Data-Centric Asset

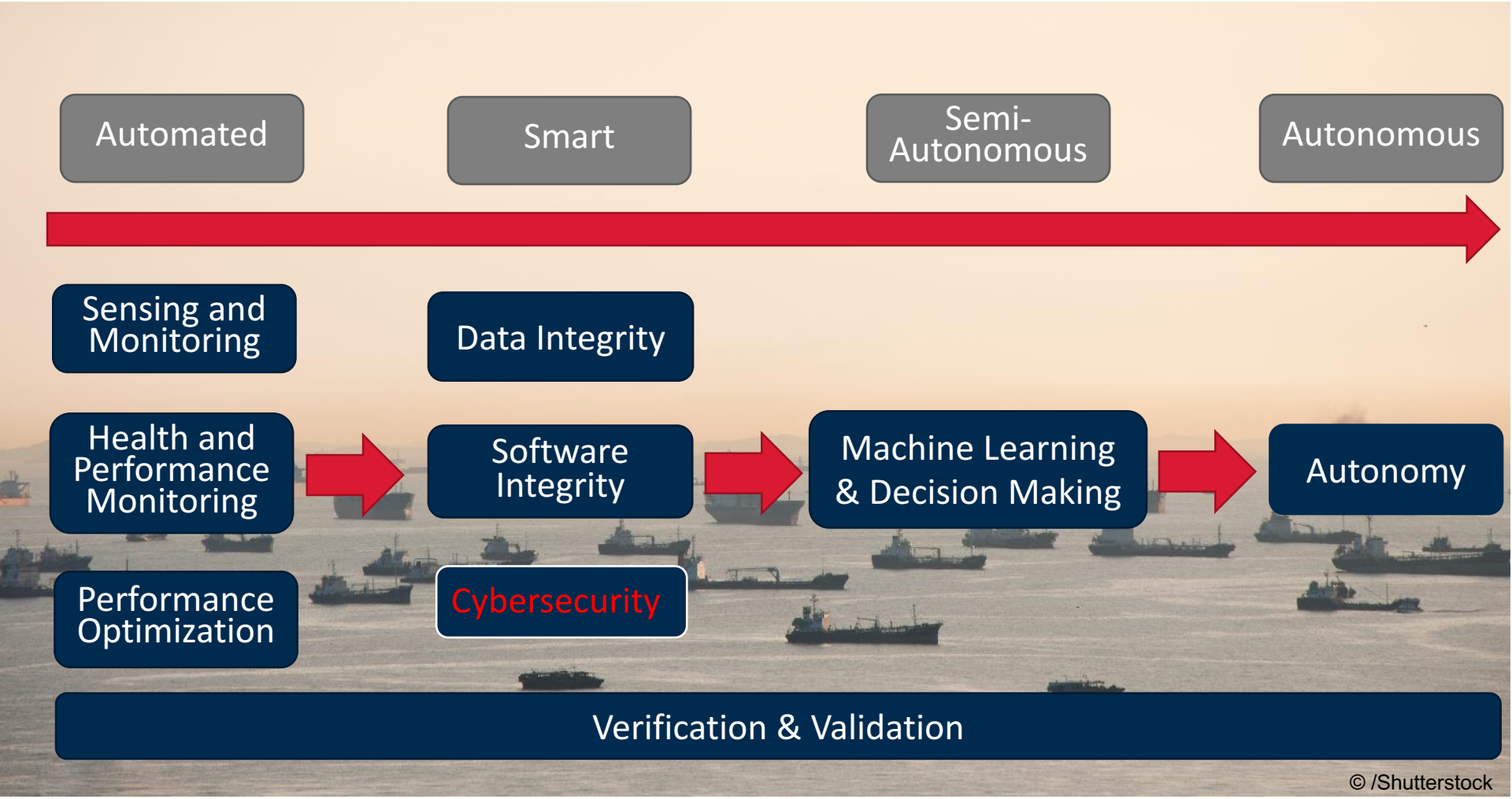


© Alzay/Shutterstock

Trend to autonomous ships



Long journey from Smart to Autonomous…Cyber Protection is needed from now on……



© /Shutterstock

Basic Questions to start with

- Who manages your OT systems and software upgrades?
- Do you have basic policies in place to upgrade systems?
- Are you formally tracking software version control?
- Is Cyber part of your safety culture onboard the vessels?
- Do you have examples of failed software upgrades?

……..better to perform an assessment ……

Value Proposition

The ABS CyberSafety® program identifies risks and increases awareness of and protection from cyber threats to:

- Enhance safety
- Minimize productivity loss
- Limit operational impact

- Only 38% of global organizations claim they are prepared to handle a sophisticated cyberattack
- Industrial Control System (ICS) specific vulnerability disclosures will increase over the next years at a 5% rate
- Distinct risks in the marine environment have serious consequences
- Most cyber-related threats are preventable with the right risk-based approach and systems in place

ABS Experience

ABS awarded research contract by the Maritime Security Center (MSC) to lead industry partnership to determine direction of cybersecurity in maritime industry

> "This research project will support the missions of the DHS Center of Excellence and the U.S. Coast Guard to address these concerns and vulnerabilities and will identify policies and risk management strategies to bolster the cybersecurity posture of the MTS enterprise."

– Dr. Hady Salloum
Director of MSC

MAJOR INDUSTRY RECOGNIZED CERTIFICATIONS:

PE (CONTROL SYSTEMS), CISSP, GICSP, CISA, CCNA, CCNP, SOFTWARE QUALITY CONTROL, PMP, ICS-CERT

200+ YEARS OF CUMULATIVE CYBER EXPERIENCE IN MARINE APPLICATION

CYBERSECURITY ASSESSMENT OF

30+ MARINE/OFFSHORE ASSET TYPES

FOR VARIOUS OWNERS

- NAVIGATION
- CONTROL SYSTEMS
- SURVEILLANCE SYSTEMS

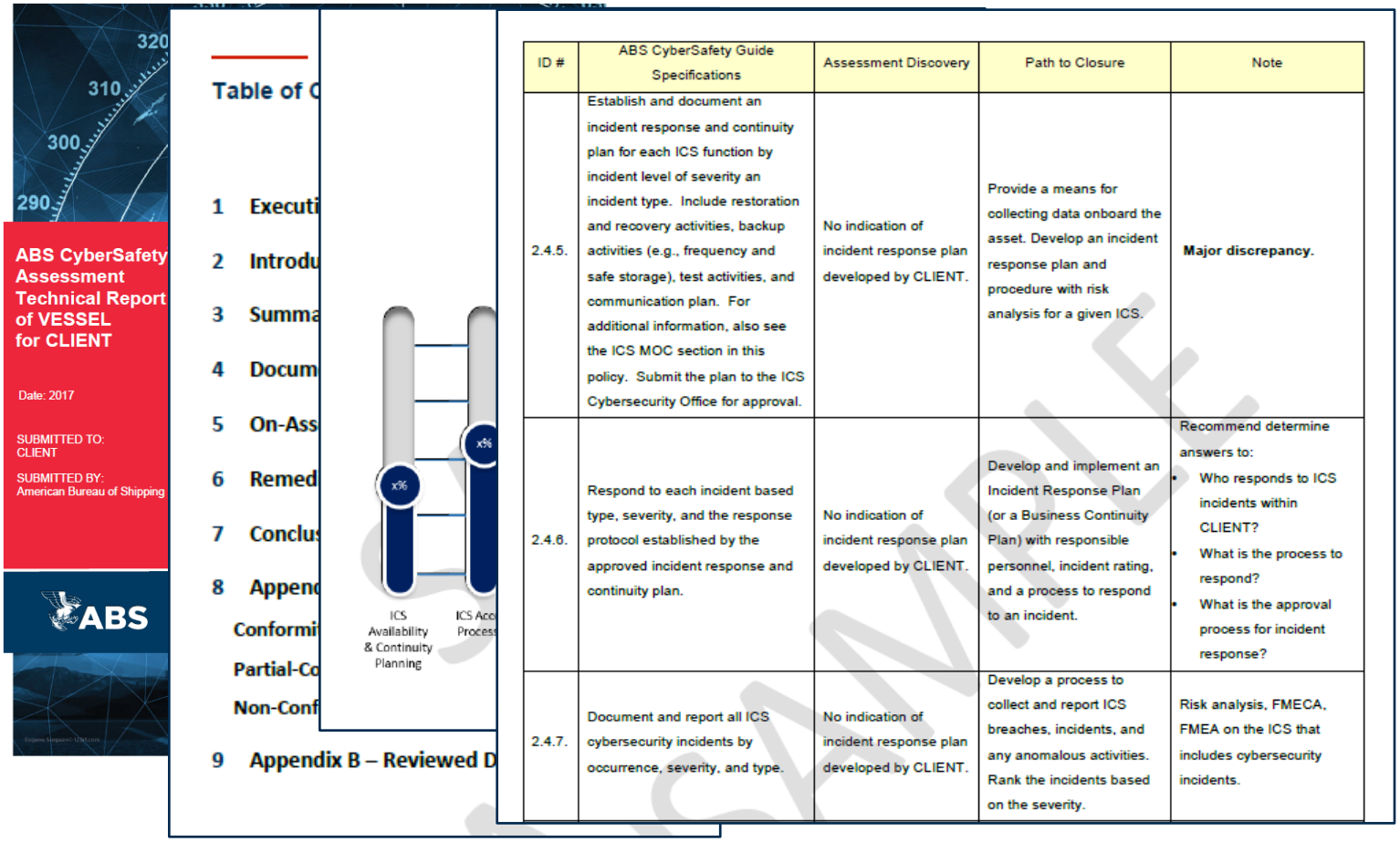
ABS CyberSafety® Approach

- Establish a staffed cybersecurity program for Industrial Control Systems (ICS)
- Develop an incident response capability
- Implement a Cybersecurity Management System
- Establish a formal management of change system
- Develop formal ICS cybersecurity training

ABS CyberSafety Engagement Options

- Policies and Procedures review
  - Incident response team members & associated responsibilities
  - Software Management of Change policy
  - Description of cybersecurity training policy and procedures
- Formal Vessel Assessment
  - Pre-Assessment Phase including data collection and information sharing
  - Office and Vessel visit applying 200+ point criteria
  - Formal report including findings, recommendation & CS1 gap analysis
- ABS CyberSafety Notation
  - Verification of policies & procedures, Cybersecurity Management System, crew awareness, documentation, etc
  - Vessel visit…confirmation (or gap analysis) of a CSx notation
- Annual/Renewal Survey of CSx Notation
  - Verification during normal Survey window (2-3 hrs. of surveyor time)

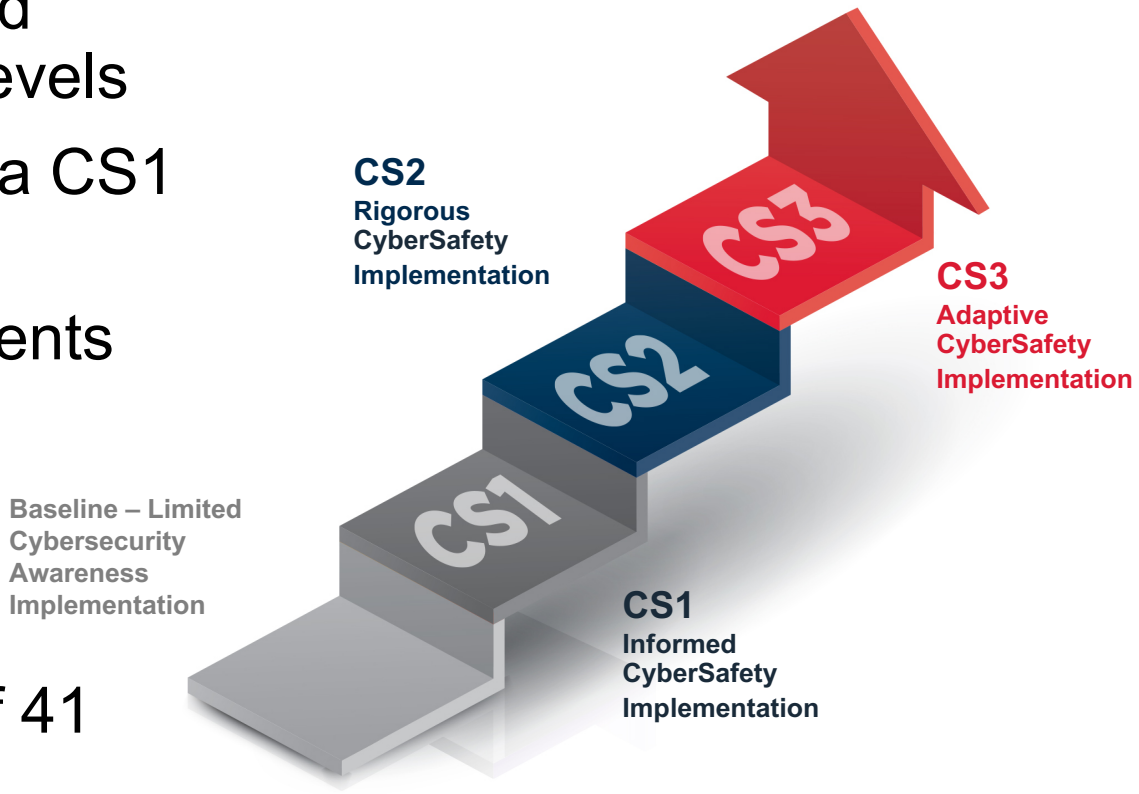
ABS CyberSafety Assessment Reporting



ID #	ABS CyberSafety Guide Specifications	Assessment Discovery	Path to Closure	Note
2.4.5.	Establish and document an incident response and continuity plan for each ICS function by incident level of severity an incident type. Include restoration and recovery activities, backup activities (e.g., frequency and safe storage), test activities, and communication plan. For additional information, also see the ICS MOC section in this policy. Submit the plan to the ICS Cybersecurity Office for approval.	No indication of incident response plan developed by CLIENT.	Provide a means for collecting data onboard the asset. Develop an incident response plan and procedure with risk analysis for a given ICS.	**Major discrepancy.**
2.4.6.	Respond to each incident based type, severity, and the response protocol established by the approved incident response and continuity plan.	No indication of incident response plan developed by CLIENT.	Develop and implement an Incident Response Plan (or a Business Continuity Plan) with responsible personnel, incident rating, and a process to respond to an incident.	Recommend determine answers to: • Who responds to ICS incidents within CLIENT? • What is the process to respond? • What is the approval process for incident response?
2.4.7.	Document and report all ICS cybersecurity incidents by occurrence, severity, and type.	No indication of incident response plan developed by CLIENT.	Develop a process to collect and report ICS breaches, incidents, and any anomalous activities. Rank the incidents based on the severity.	Risk analysis, FMECA, FMEA on the ICS that includes cybersecurity incidents.

ABS Cybersafety Notations

- Vessels are assessed against all notation levels
- Two vessels earned a CS1 notation
- Completed assessments show an average conformity level of 35% to CS1 requirements
- OK approx. 14 out of 41 Requirements (CS1)



ABS CyberSafety® Notations/Certificates

Common Industry Challenges – Versus CS1 Notation

88%

Missing or inadequate Management of Change policies and procedures

63%

Missing or inadequate Incident Response Capability

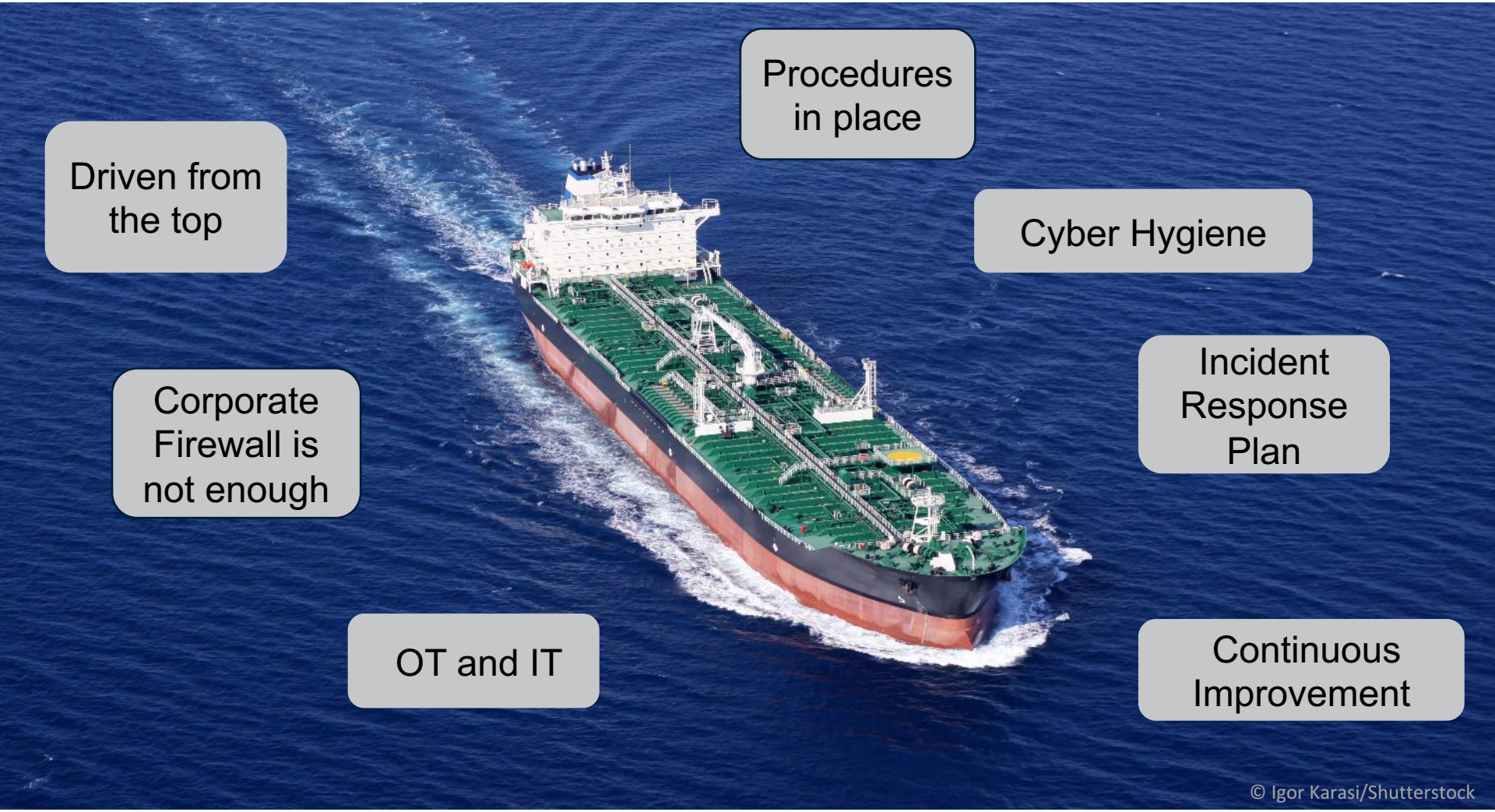
63%

Vessel's crew lacked cyber hygiene awareness

50%

Lack of OT network activity monitoring

…. success implementation of cyber protection

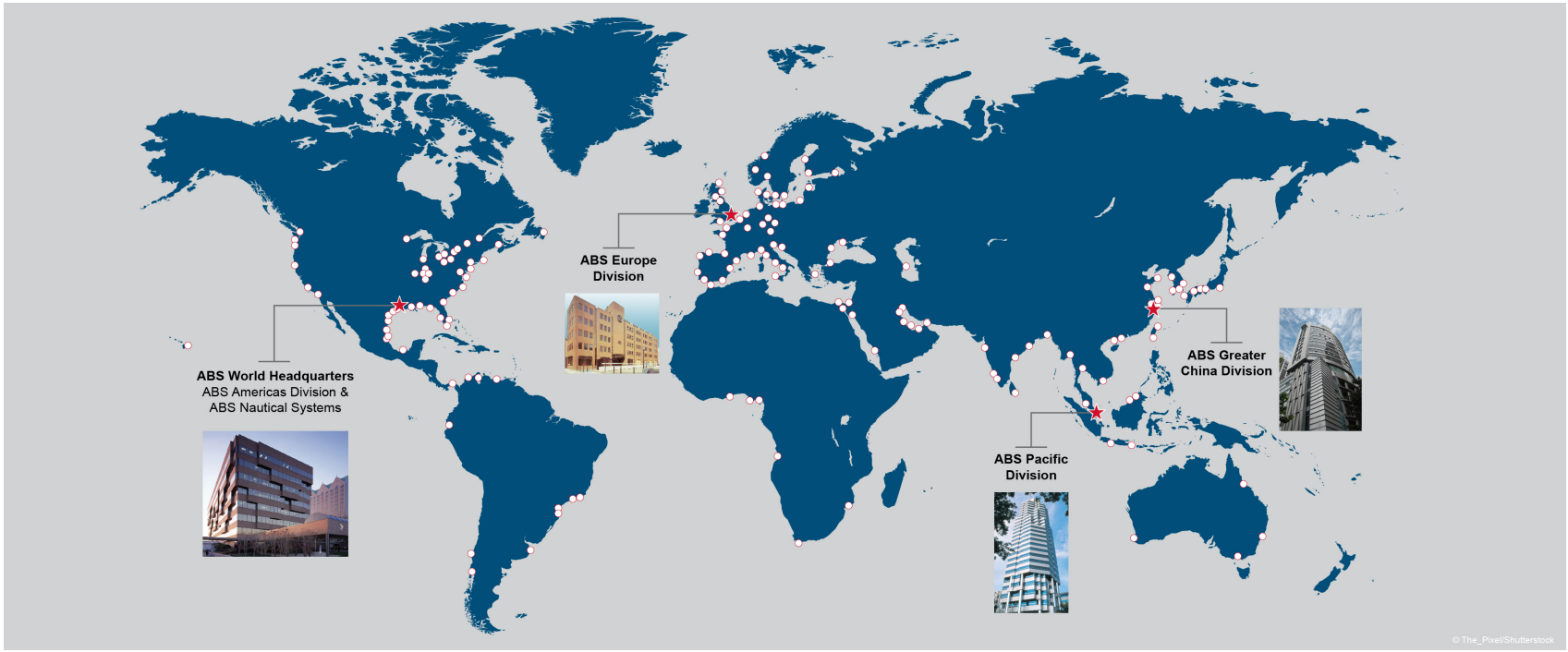


Some considerations…

- The goals are not smarter ships or digital operation per se, the goals are a safer and more efficient shipping industry and smarter ways to operates
- Assets get smarter, the future is data-centric and the management of data integrity is a key
- Cyber Safety and Cyber Security protection are fundamental
- An adequate Cyber Protection culture aims to build the human understanding of how this risk works

Global Reach and Support

- Dedicated ABS CyberSafety team
- Recognized by industry and government
- ABS CyberSafety® Laboratory provides research and development to support a global team



Thank You

www.eagle.org