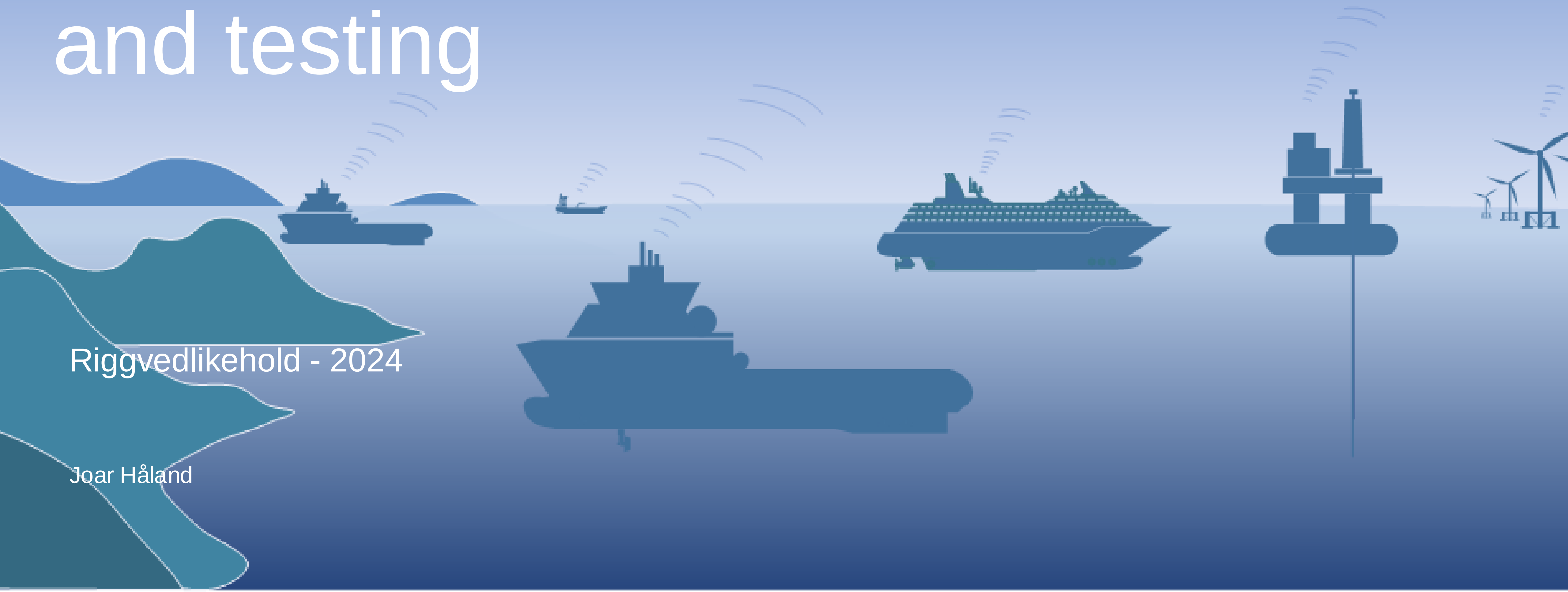
Data-driven maintenance and testing



Riggvedlikehold - 2024

Joar Håland

Topics

How is digitalization effecting maintenance, inspection and testing?

What is condition and data-driven maintenance and testing?

Pilot case: Watertight doors

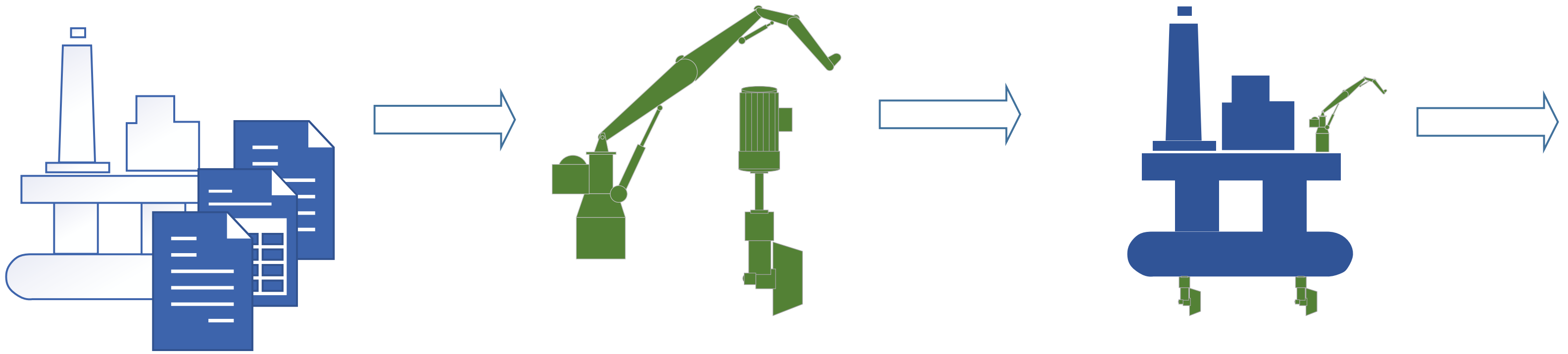
Classification

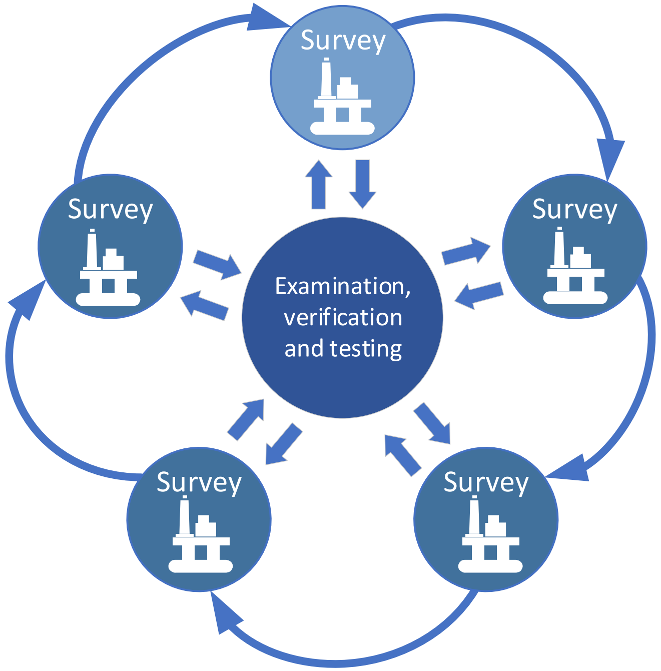
Design

Certification of Components (CMC)

Construction

In service

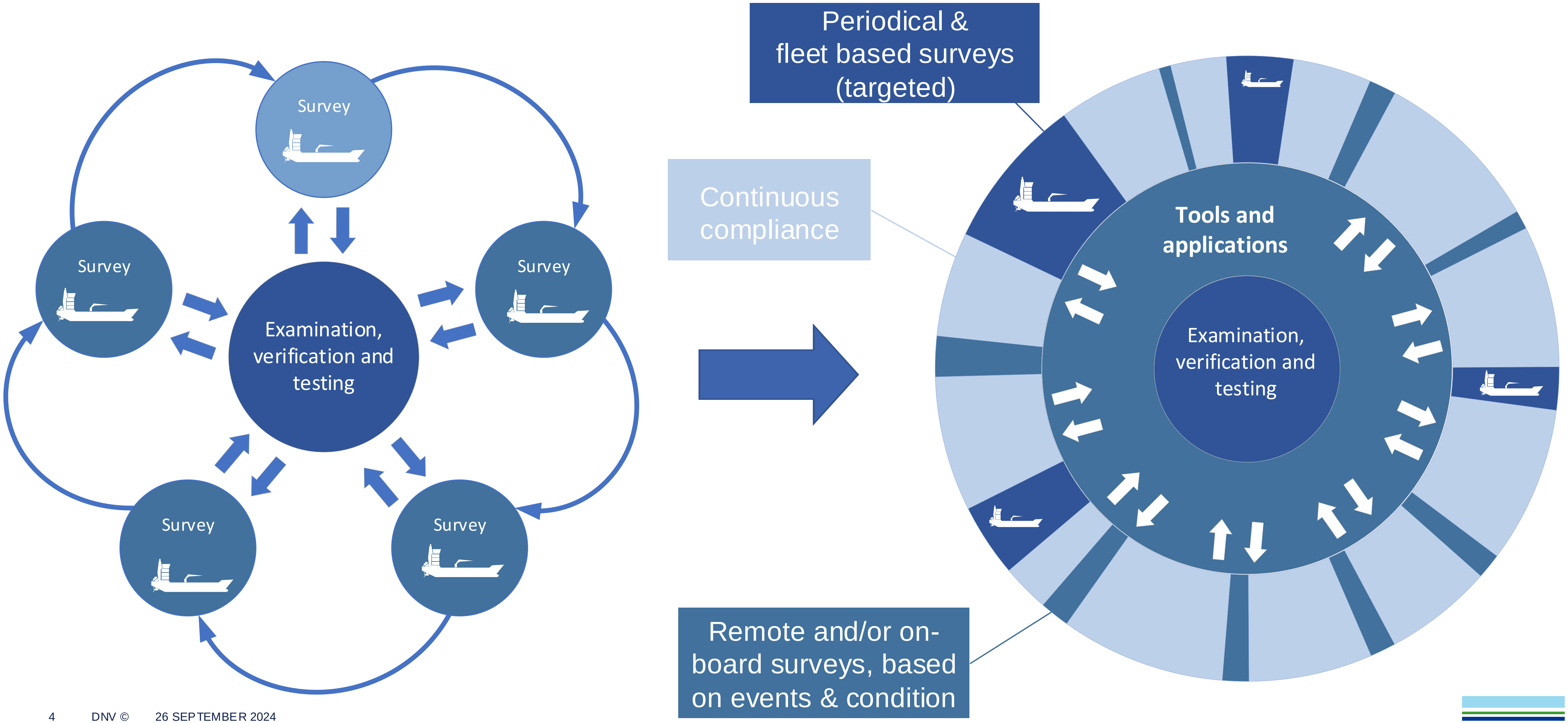




Classification is a life cycle management for a vessel starting from concept and design, followed by construction, and later in-service.

The requirements to obtain and retain classification is described in a framework (rules) structured according to the different life cycle phases and specified according to vessel type, service, features, and operation.

Direction for a new in-service model



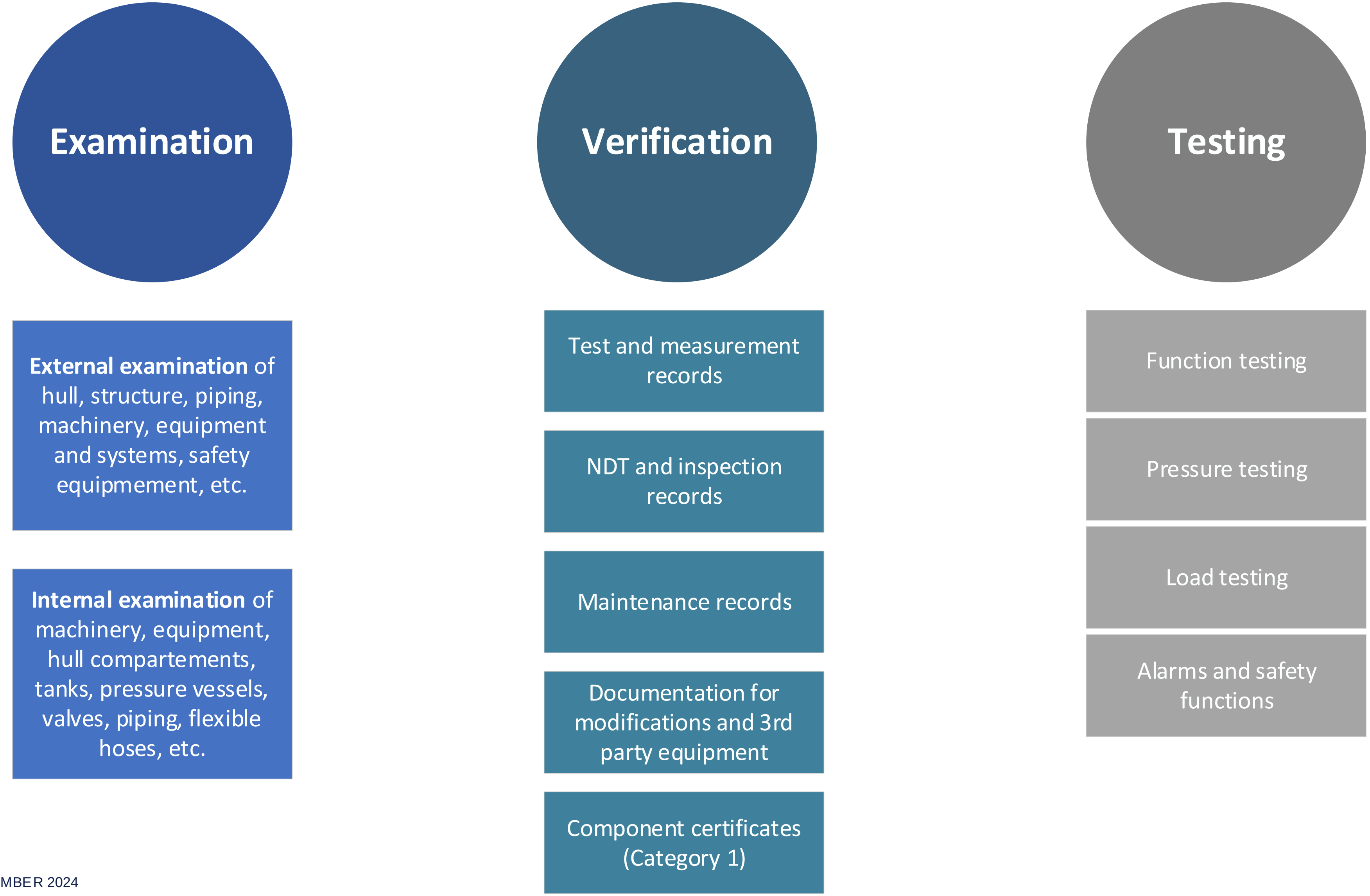
Periodical & fleet based surveys (targeted)

Continuous compliance

Remote and/or on-board surveys, based on events & condition

Survey
Survey
Survey
Survey
Survey
Examination, verification and testing
Tools and applications
Examination, verification and testing

Typical classification scope



Examination

- **External examination** of hull, structure, piping, machinery, equipment and systems, safety equipmement, etc.
- **Internal examination** of machinery, equipment, hull compartements, tanks, pressure vessels, valves, piping, flexible hoses, etc.

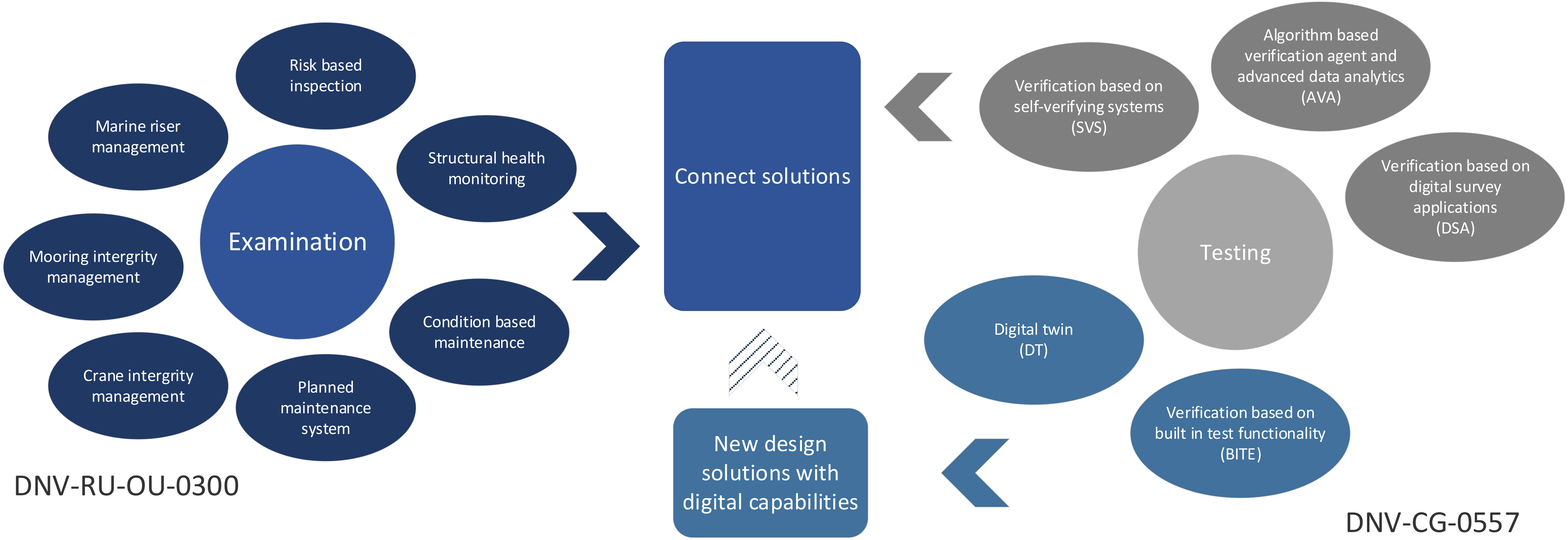
Verification

- Test and measurement records
- NDT and inspection records
- Maintenance records
- Documentation for modifications and 3rd party equipment
- Component certificates (Category 1)

Testing

- Function testing
- Pressure testing
- Load testing
- Alarms and safety functions

Data-driven inspection, maintenance and testing



Risk based inspection

Marine riser management

Structural health monitoring

Examination

Mooring intergrity management

Condition based maintenance

Crane intergrity management

Planned maintenance system

DNV-RU-OU-0300

Connect solutions

New design solutions with digital capabilities

Verification based on self-verifying systems (SVS)

Algorithm based verification agent and advanced data analytics (AVA)

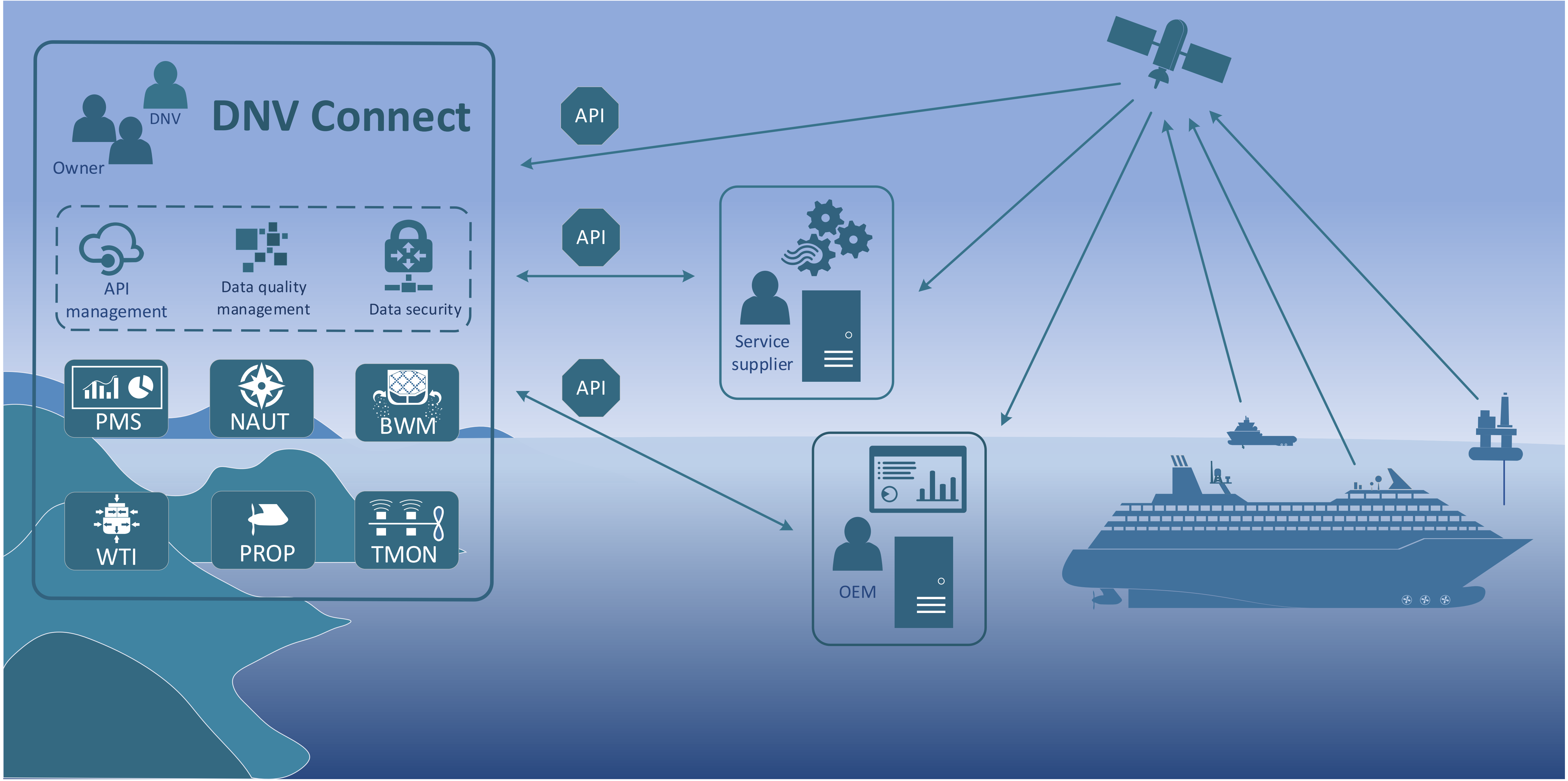
Verification based on digital survey applications (DSA)

Testing

Digital twin (DT)

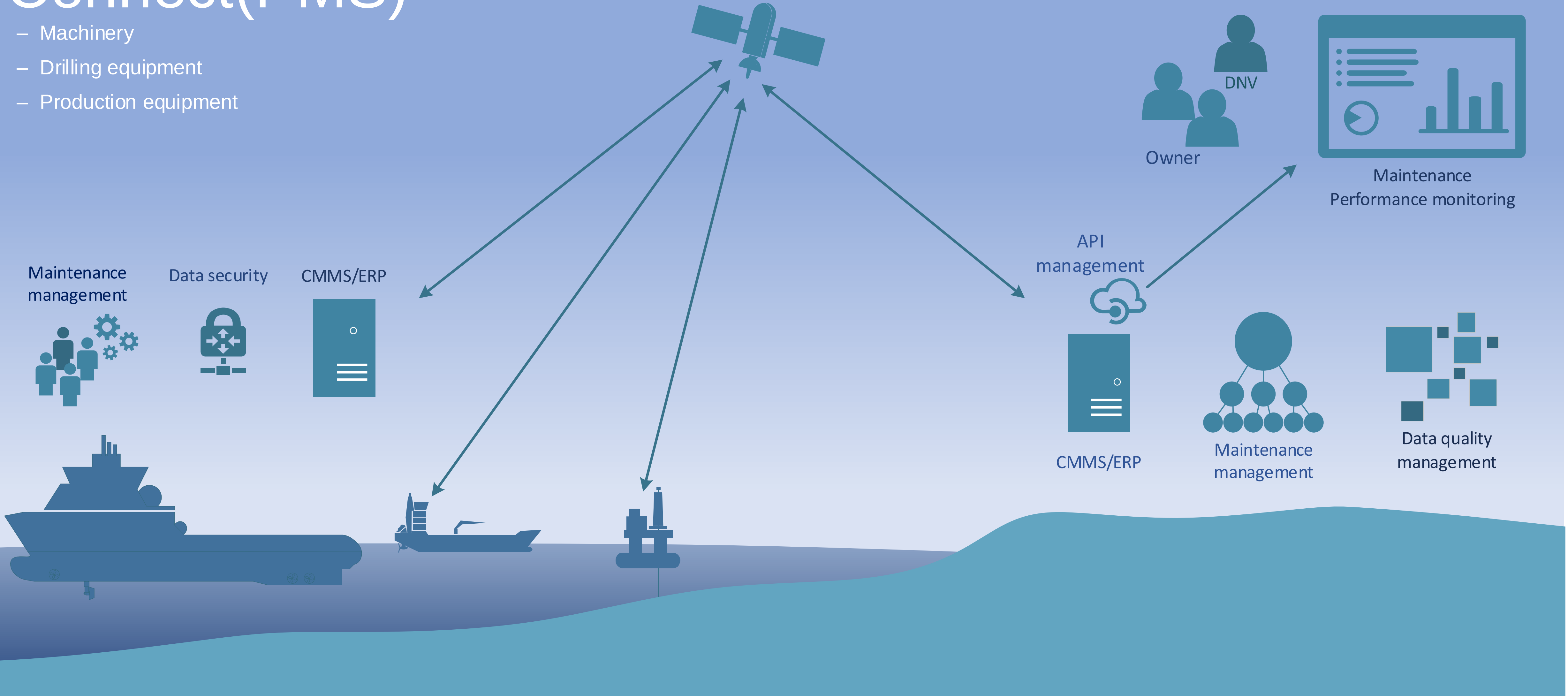
Verification based on built in test functionality (BITE)

DNV-CG-0557

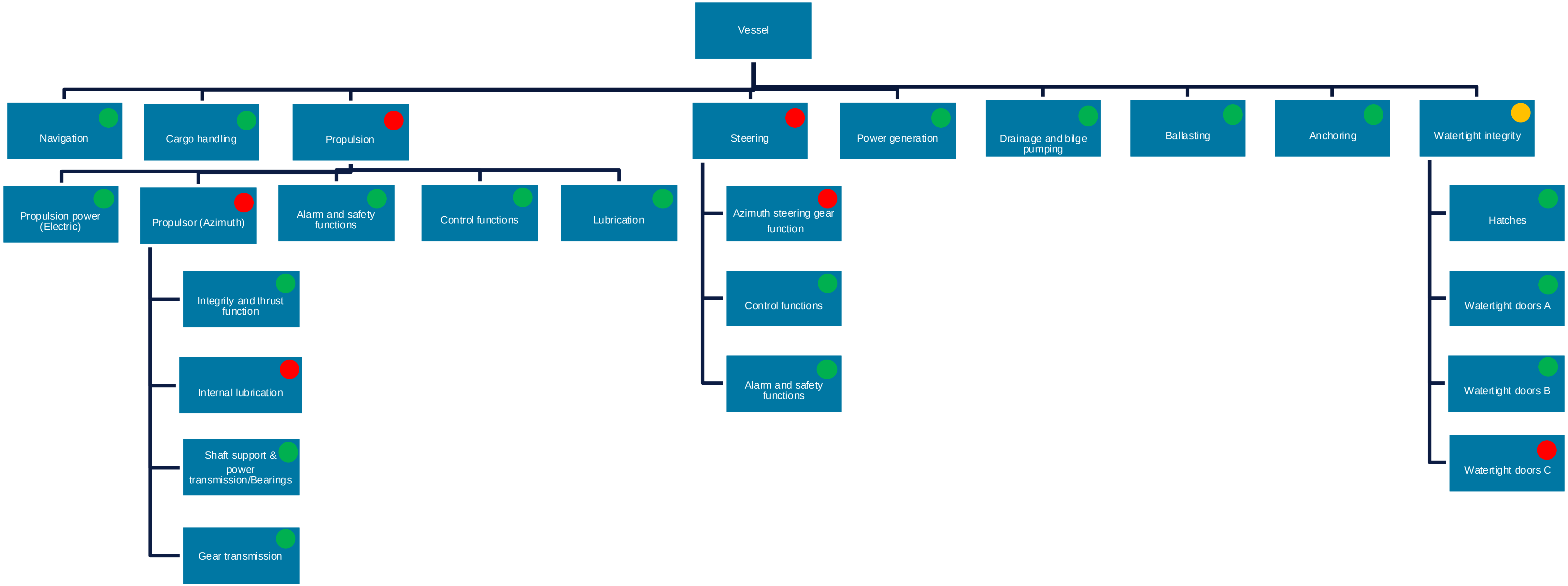

DNV
Owner
DNV Connect
API
management
Data quality
management
Data security
PMS
NAUT
BWM
WTI
PROP
TMON
API
API
API
Service
supplier
OEM

Connect(PMS)

- Machinery
- Drilling equipment
- Production equipment



Compliance dashboard – on a high level pointing at where ship main functions is not compliant



- Vessel
  - Navigation 🟢
  - Cargo handling 🟢
  - Propulsion 🔴
    - Propulsion power (Electric) 🟢
    - Propulsor (Azimuth) 🔴
      - Integrity and thrust function 🟢
      - Internal lubrication 🔴
      - Shaft support & power transmission/Bearings 🟢
      - Gear transmission 🟢
    - Alarm and safety functions 🟢
    - Control functions 🟢
    - Lubrication 🟢
  - Steering 🔴
    - Azimuth steering gear function 🔴
    - Control functions 🟢
    - Alarm and safety functions 🟢
  - Power generation 🟢
  - Drainage and bilge pumping 🟢
  - Ballasting 🟢
  - Anchoring 🟢
  - Watertight integrity 🟡
    - Hatches 🟢
    - Watertight doors A 🟢
    - Watertight doors B 🟢
    - Watertight doors C 🔴

With access to more data and information, how do we define compliance levels

- 🔴 Class acceptance criteria are exceeded
- 🟡 Performance/health criteria from manufacturer/owner are exceeded
- 🟢 Performance/health is good

Ongoing pilot projects:

Objective: Establish alternatives to today's survey regime using data driven verification (DDV) methods to replace physical surveys and testing on board

- **Main engines (ME):**
  - For vessels with main engines for 2-stroke applications
  - Seamless performance management support and compliance verification of engine condition
  - Better support for the planned maintenance and alarm data Continuous view of performance/compliance status.

- **Propulsion (Azimuth thrusters):**
  - For vessels with high-end thruster makers with Condition based maintenance (CBM)
  - Monitoring of condition and functionality/performance for components and system
  - 21 physical surveys replaced, and 4 physical surveys moved to bottom survey.

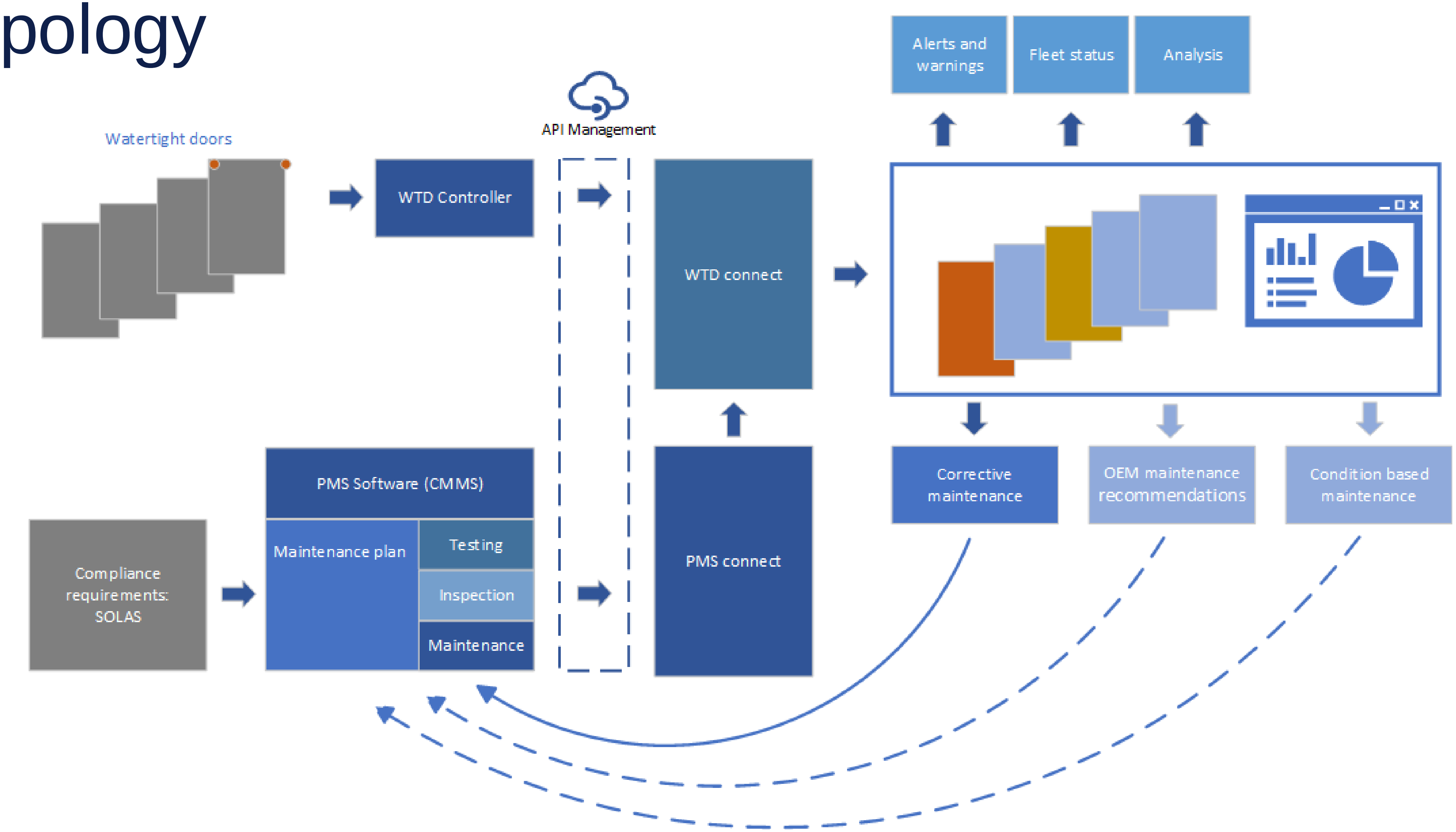
Pilot: Watertight doors

- Objective: to establish a “Connect solution” for data export from watertight door control system, with potential for further expansion to fire doors.
- Scope: hydraulic and electrical doors for watertight integrity. Focus on monitoring according to compliance requirements (not performance).
- Application: the solution is intended to be implemented in “DNV Connect” as part of main function watertight integrity (WTI).
- Project team:

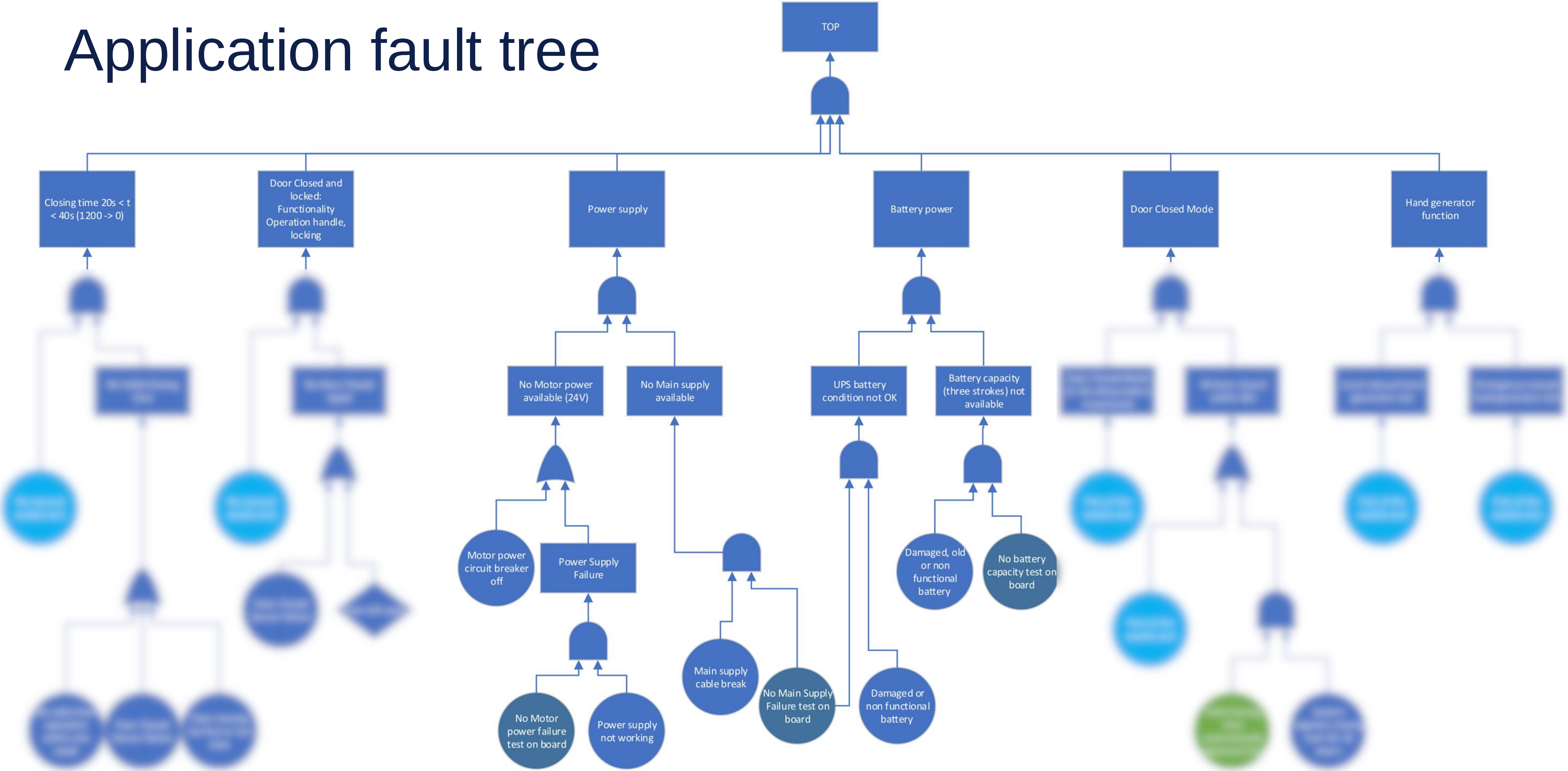
IMS DNV

+ 1 ship owner + 1 MOU owner (TBA)

Topology


Alerts and warnings
Fleet status
Analysis
API Management
Watertight doors
WTD Controller
WTD connect
PMS Software (CMMS)
Maintenance plan
Testing
Inspection
Maintenance
Compliance requirements: SOLAS
PMS connect
Corrective maintenance
OEM maintenance recommendations
Condition based maintenance

Application fault tree


TOP
Closing time 20s < t < 40s (1200 -> 0)
Door Closed and locked: Functionality Operation handle, locking
Power supply
Battery power
Door Closed Mode
Hand generator function
No Motor power available (24V)
No Main supply available
UPS battery condition not OK
Battery capacity (three strokes) not available
Motor power circuit breaker off
Power Supply Failure
Main supply cable break
Damaged, old or non functional battery
No battery capacity test on board
No Motor power failure test on board
Power supply not working
No Main Supply Failure test on board
Damaged or non functional battery

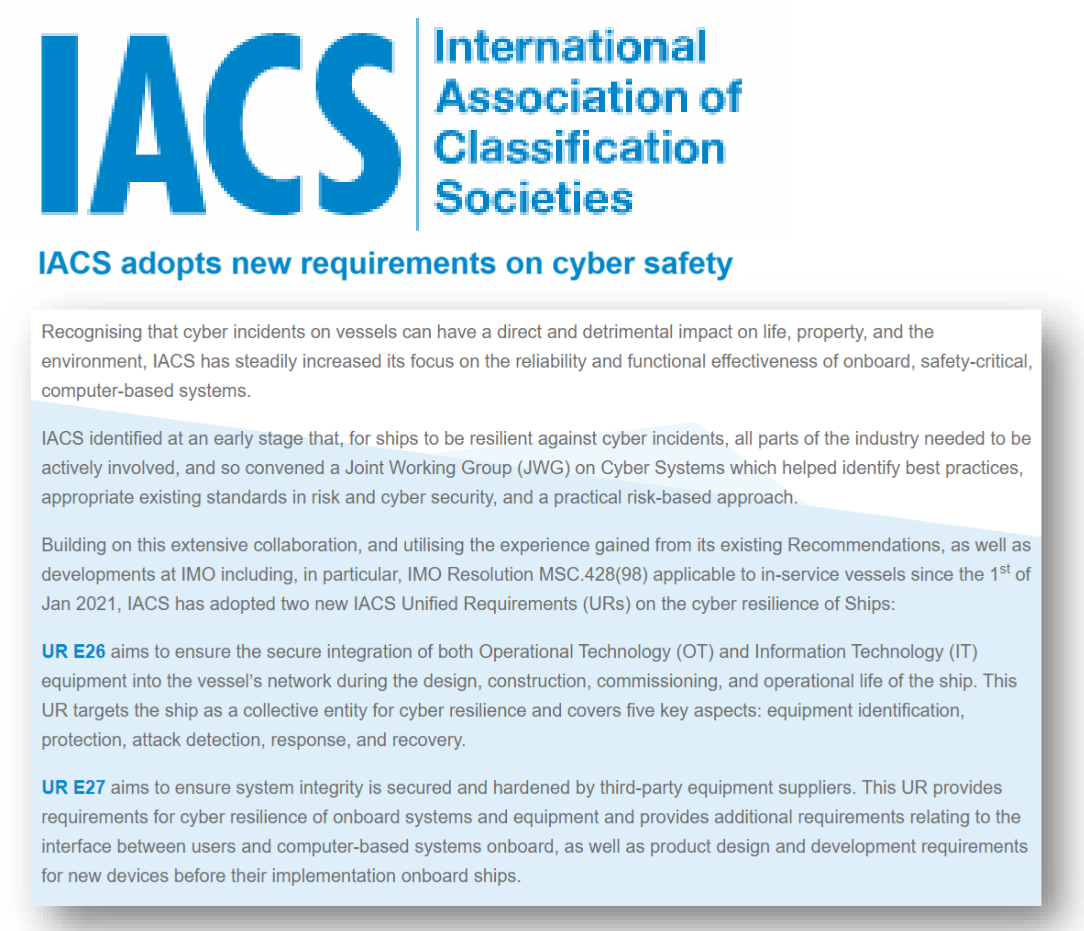
New IACS Unified Requirements on Cyber Security supports Classification Societies' role in safeguarding life and vessels

New vessels contracted after 1st of July 2024 will need to be approved according to Cyber security

The requirements come to yards, designers and owners (UR E26) as well as suppliers (UR E27)

Majority of merchant vessels above 500GT in international trade will be impacted

Safety related systems such as automation, navigation, fire and communication to be approved



IACS International Association of Classification Societies

IACS adopts new requirements on cyber safety

Recognising that cyber incidents on vessels can have a direct and detrimental impact on life, property, and the environment, IACS has steadily increased its focus on the reliability and functional effectiveness of onboard, safety-critical, computer-based systems.

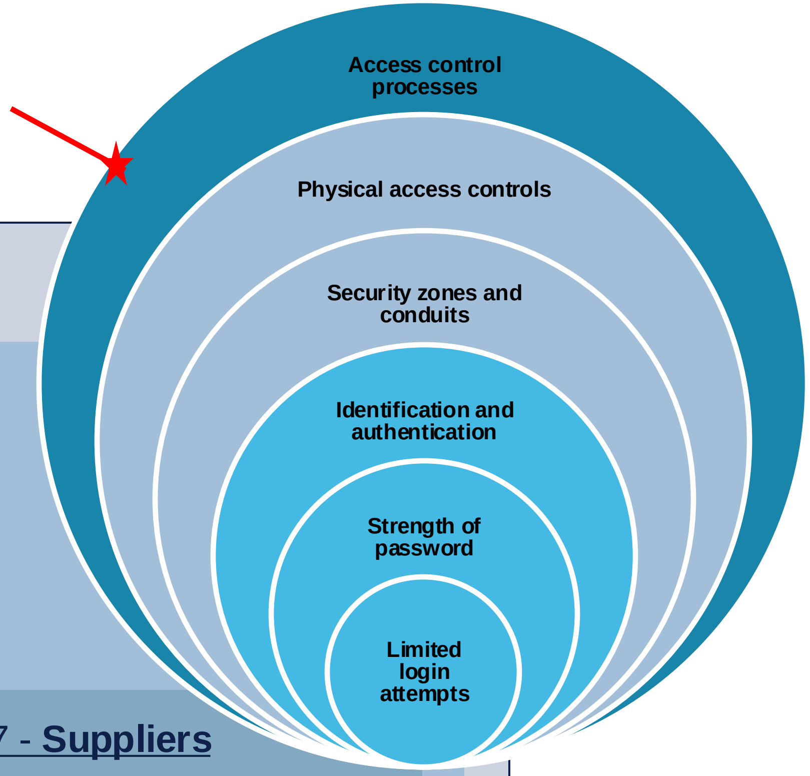
IACS identified at an early stage that, for ships to be resilient against cyber incidents, all parts of the industry needed to be actively involved, and so convened a Joint Working Group (JWG) on Cyber Systems which helped identify best practices, appropriate existing standards in risk and cyber security, and a practical risk-based approach.

Building on this extensive collaboration, and utilising the experience gained from its existing Recommendations, as well as developments at IMO including, in particular, IMO Resolution MSC.428(98) applicable to in-service vessels since the 1st of Jan 2021, IACS has adopted two new IACS Unified Requirements (URs) on the cyber resilience of Ships:

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 five key aspects: equipment identification, protection, attack detection, response, and recovery.

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 and provides additional requirements relating to the interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard ships.

Introduction - Defence in depth



Ex. threat: Unauthorized access

Management of cyber security - E26 – **Vessel owner**

- Scope of applicability
- Cyber risk management
- Change management
- Patch management
- Classification of information
- Access control
- Management of firewalls
- Malware protection
- Remote access
- Use of mobile devices
- Detection of anomalies
- Verification of security functions
- Incident response
- Incident recovery
- Backup and restore

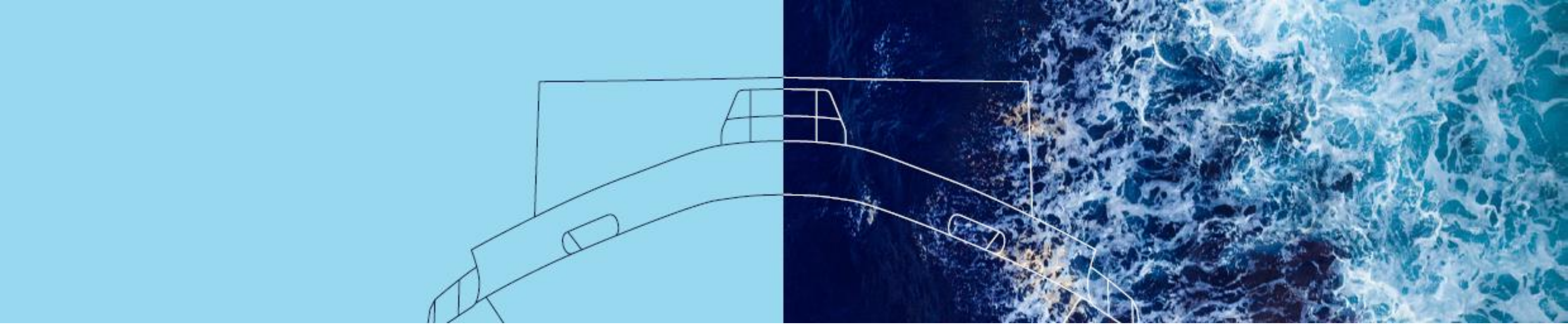
Security zones and conduits - E26 - **Yard**

- Security zones and conduits
- Network segmentation
- Control of zone boundaries/conduits
- Implementation, integration, physical security

Certification of system security capabilities - E27 - **Suppliers**

- 30 + 11 security capabilities based on **IEC 62443-3-3** (System security requirements and security levels)
- Implementation/configuration of security capabilities
- Hardening
- SDL process

Development and certification of components:
IEC 62443-4-1: Secure Product Development Lifecycle Requirements
IEC 62443-4-2: Technical Security Requirements for IACS Components



Thank you.