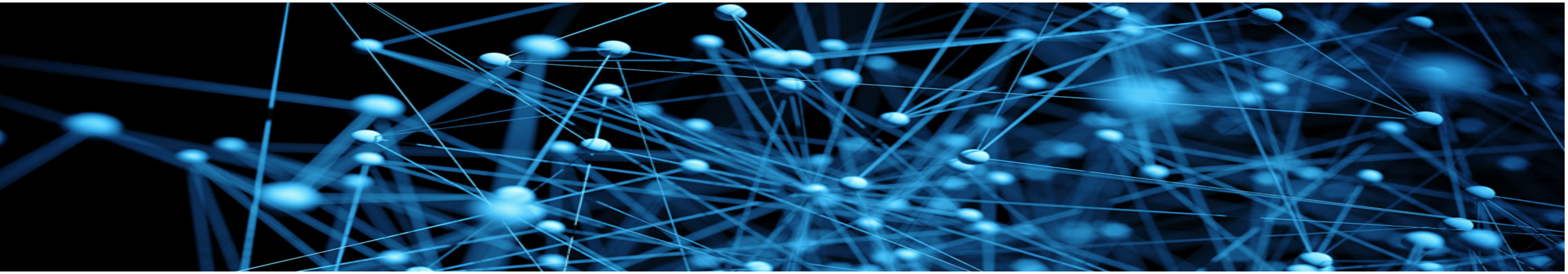
MARITIME

Cyber security threats in maritime industry

DNV GL class notation

17 January 2019



In an ever-more connected and digitized world…

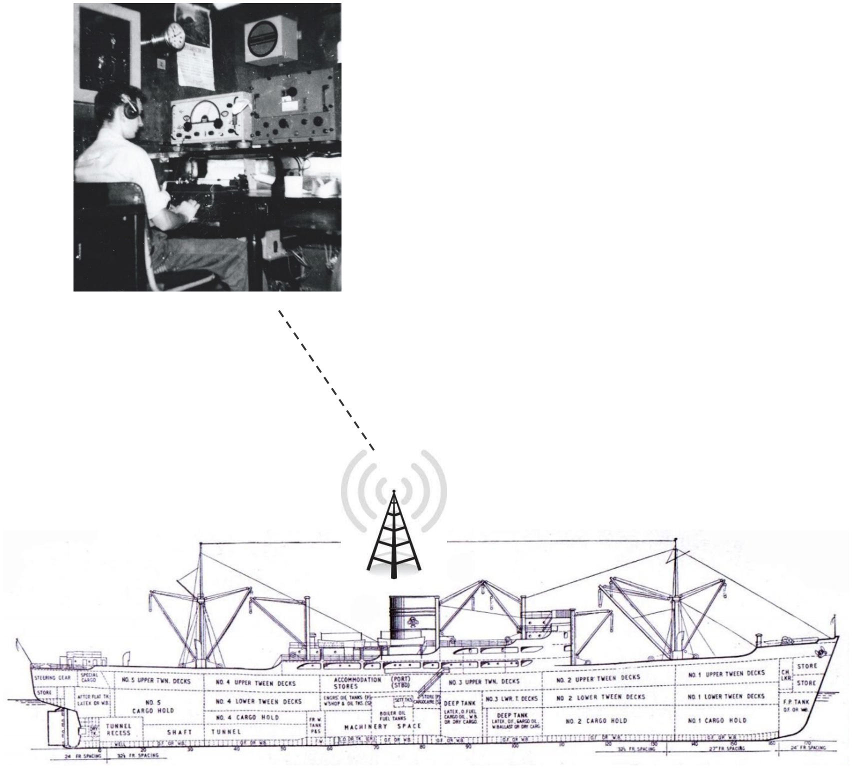
…resilience to cyber incidents becomes increasingly important to address

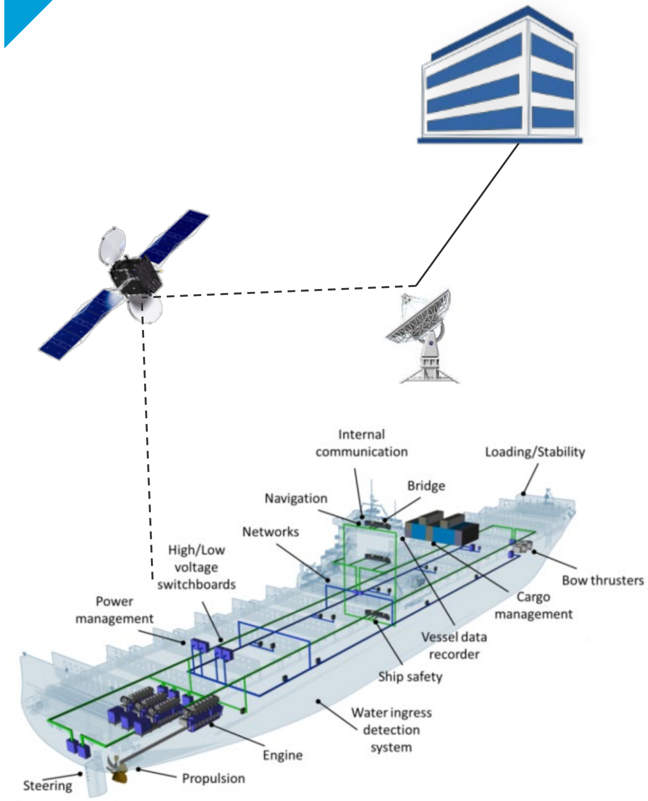
Safety in shipping today heavily depends on cyber systems

1950

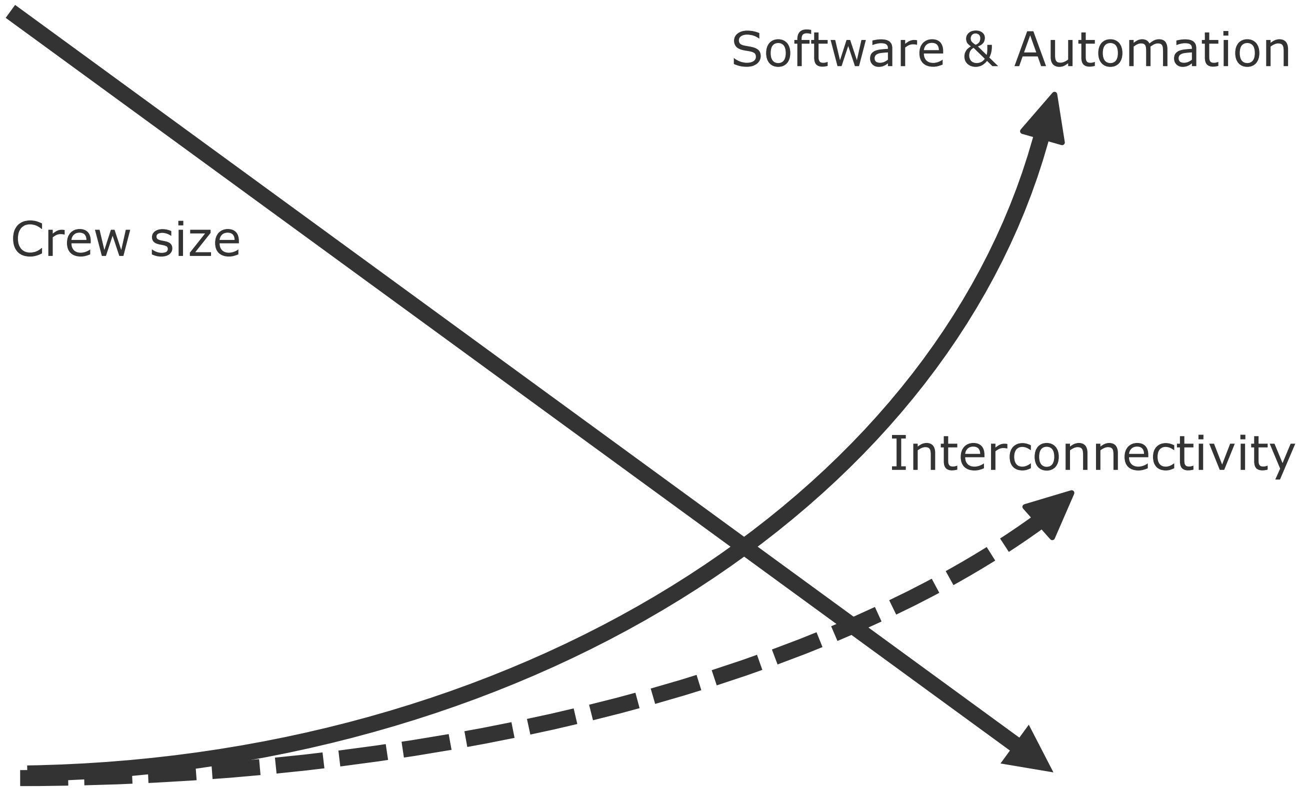
60-70 YEARS

2018



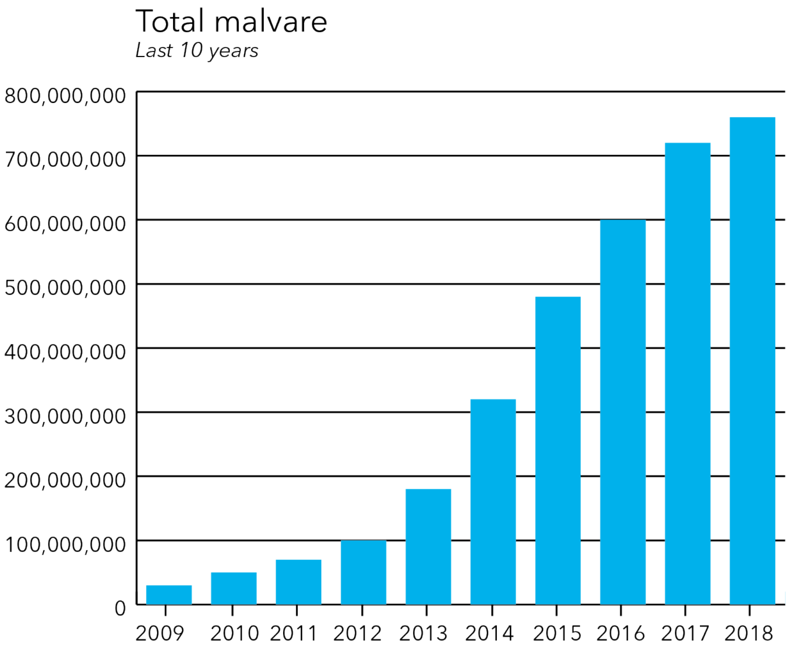


Maritime & Offshore trends – Growing complexity creates new challenges

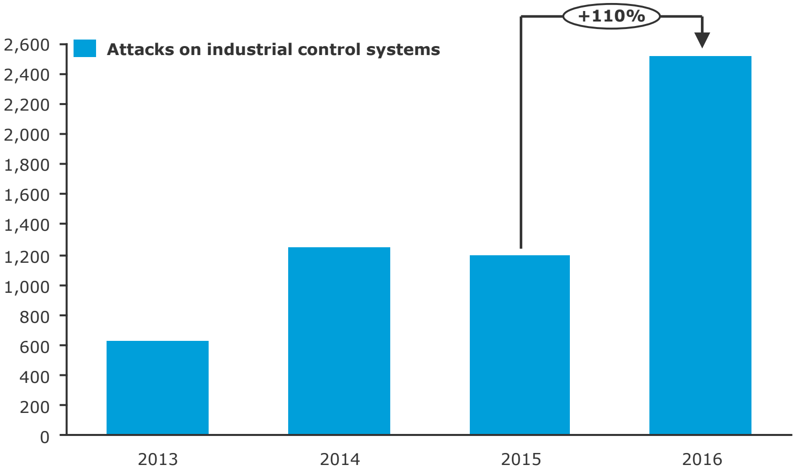


Cyber risk issues are present and migrating to the OT world

Information technology (IT)

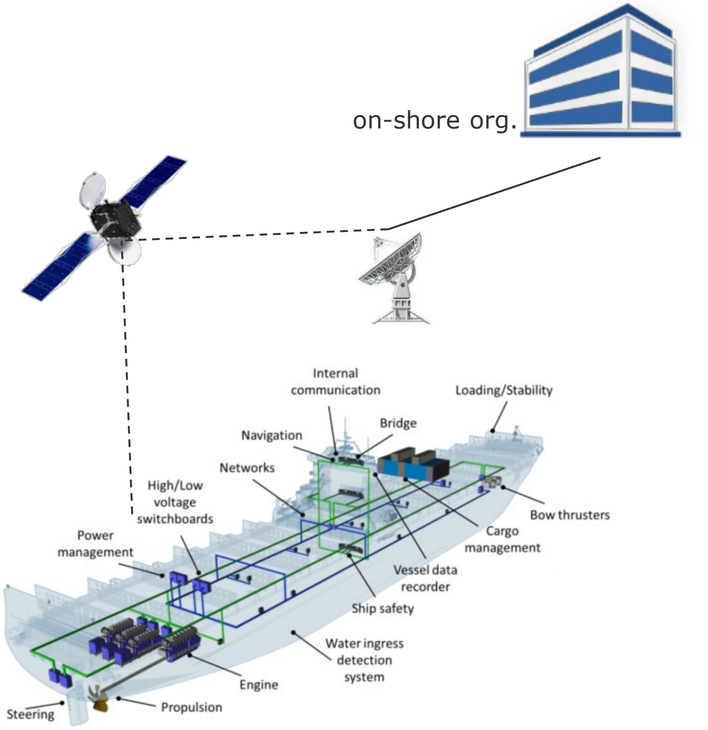


Operational technology (OT)



Source: AV-TEST Institute, Germany & IBM Managed Security Services
OT: Operational Technology such as Industrial Control Systems, SCADA, PLCs, Sensors
SCADA : Supervisory Control and Data Acquisition (Operator control and monitoring systems)

Safety in shipping today heavily depends on cyber systems with potential consequences towards both finance and safety



Information Technology (IT)

- IT networks
- E-mail
- Administration, accounts, crew lists, …
- Planned Maintenance
- Spares management and requisitioning
- Electronic manuals & certificates
- Permits to work
- Charter party, notice of readiness, bill of lading…

Operation Technology (OT)

- PLCs
- SCADA
- On-board measurement and control
- ECDIS, GPS
- Remote support for engines
- Data loggers
- Engine & Cargo control
- Dynamic positioning, …

At risk:

Mainly
finance
and
reputation

At risk:

Life,
property
and
environment
+
all of the above

Cyber risks are increasing rapidly

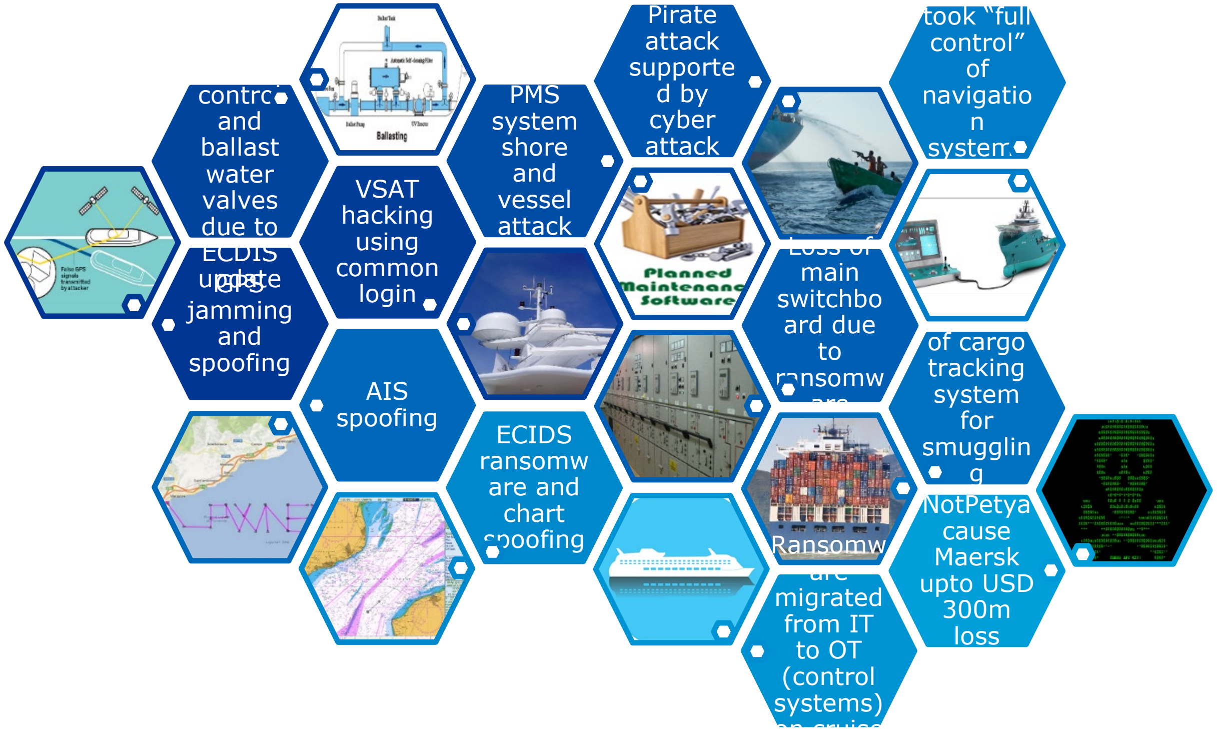
The annual damage to the global economy from cybercrime is estimated to be between 200–400 billion USD.

According to the CSO Alliance, more than 1,000 ships have successfully been hacked in the last five years.

After the NotPetya incident in 2017, Maersk had to reinstall its entire infrastructure including 45,000 PCs, 2,500 applications, and 4,000 servers.

The positive message is: Cyber security is now getting the attention within the maritime industry it deserves – but there is **not enough action yet!**

Reported incidents around is increasing, even with lack of transparency



contrc and ballast water valves due to ECDIS update

GPS jamming and spoofing

VSAT hacking using common login

AIS spoofing

PMS system shore and vessel attack

ECIDS ransomware and chart spoofing

Pirate attack supported by cyber attack

Loss of main switchboard due to ransomware

Ransomware migrated from IT to OT (control systems) on cruise

took "full control" of navigation system

of cargo tracking system for smuggling

NotPetya cause Maersk upto USD 300m loss

Ballasting
Planned Maintenance Software
False GPS signals transmitted by attacker

DNV GL Cyber security class notation and services

Class notation

□ DNV GL Class

□ Approval of systems

□ Approval of CSMS

Verification

□ DNV GL Digital Solutions

□ Test preparation

□ Execution of testing

Advisory

□ DNV GL Maritime advisory

□ GAP assessment

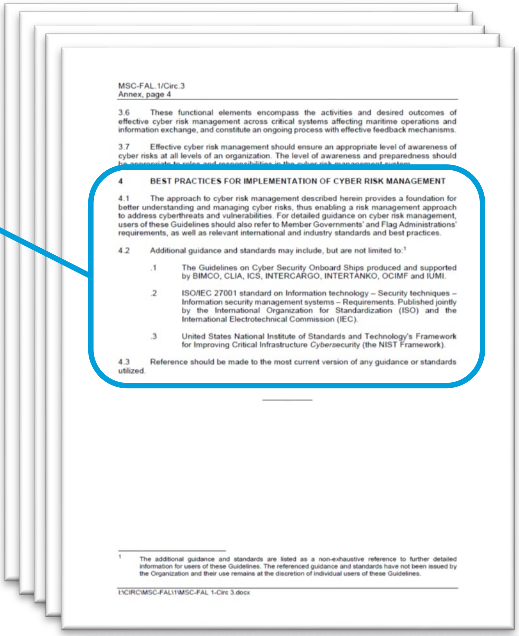
□ Document preparation

Regulatory developments

Cyber security regulations are evolving… i.e. IMO Resolution MSC.428(98)

INTERNATIONAL MARITIME ORGANIZATION

- AFFIRMS that … **safety management system should take into account cyber risk management** in accordance with the … ISM Code.
- Where to start: MSC-FAL.1/Circ.3
  - IT and OT systems
  - Identify – Protect – Detect – Respond – Recover
  - referring to international best practices
- However, not addressing:
  - how to assess the risk,
  - prescriptive or goal-based safety requirements,
  - requirements for incidents management



MSC-FAL.1/Circ.3
Annex, page 4

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

4.2 Additional guidance and standards may include, but are not limited to:[1]

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

.2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

.3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure *Cyber*security (the NIST Framework).

4.3 Reference should be made to the most current version of any guidance or standards utilized.

[1] The additional guidance and standards are listed as a non-exhaustive reference to further detailed information for users of these Guidelines. The referenced guidance and standards have not been issued by the Organization and their use remains at the discretion of individual users of these Guidelines.

I:\CIRC\MSC-FAL\1\MSC-FAL 1-Circ 3.docx

Outcome: MSC 98 adopted the recommendatory MSC-FAL.1/Circ.3 superseding the interim guidelines

Impact: Cyber risks should be addressed in safety management systems no later than the first annual verification of DoC after 1 January 2021. This is a non-mandatory requirement.

EU, USCG and regional regulatory requirements are being introduced

🇪🇺

- Directive (EU)2016/1148 concerning measures for a high common level of security of network and information systems across the Union (May 2016)
  – Applicable for ports but not vessels
- Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR) (April 2016)
  - Applicable for vessels from May 2018

🇺🇸

- USCG develops requirements and guidelines:
  - USCG Cyber Strategy (June 2015)
  - Maritime Bulk Liquids Transfer Cybersecurity Framework Profile (Nov 2016)
  - Draft of Cybersecurity Framework Profile for Offshore Operations (May 2017)
  - Draft of Passenger Operations Cybersecurity Framework Profile (July 2016)
  - Draft navigation and vessel inspection circular no. 05-17 (July 2017)
    Subj: Guidelines for addressing cyber risks at maritime transportation security act (MTSA) regulated facilities
  - Require cyber security incident reporting since (Dec 2016)
    CG-5P Policy Letter 08-16

🇫🇷

- Best Practices for Cyber Security On-board Ships (Oct 2016)
- Recommendations on maritime cyber security (Jan 2017)

🇩🇪

- IT-Sicherheitsgesetz (June 2015) – includes ports but not ships

🇬🇧

- Code of Practice - Cyber Security for Ports and Port Systems (June 2016)
- Code of Practice - Cyber Security for Ships (Sep 2017)

🇳🇴

- Norwegian Maritime Authorities' report "Digital vulnerabilities in
  the maritime sector" by DNV GL (Oct 2015)

🇳🇱

- Data Processing and Cybersecurity Notification Obligation Act (Jan 2016)
  – Applicable for ports and vessels (Dutch Flag)
- ….

Insurance companies and shipping organisations are examples of further stakeholder developments

The **cyber security exclusion clause** in insurance (Clause 380) is being challenged:

- Owners expect complete insurance coverage
- Underwriters need to properly manage their risks

Rating by charters though:

- Tanker Management and Self Assessment (TMSA) No. 3

OCIMF

Oil Companies International Marine Forum

and

- Inspection and Assessment Report For Dry Cargo Ships (FOD06) 11

RIGHTSHIP

How DNV GL supports

Cyber security is more then just software and technology

- Cyber security implementation involves three pillars:

Processes

- Management systems
- Governance frameworks
- Policies and procedures
- Vendor/third-party contracts follow-up
- Audit regimes

People

- Training and awareness
- Professional skills and qualifications
- Emergency drills
- Authorizations and authentication
- Physical security

Technology

- System design
- Hardening of connections
- Software configuration
- Encryption protocols
- Jamming and spoofing
- Detection and monitoring

Industry has responded with Cyber Security guidance….
…and DNV GL has follow-up with additional support

OFFSHO

DNVGL-OS-D20

Integrate
(ISDS)

RECOMM

DNVGL-RP-0496

Cyber secu
ships and

RECOMM

DNVGL-RP-G10

Cyber sec
based on

CLASS R

Type appro

DNVGL-CP-023

Cyber sec
componen

DNV·GL

RULES FOR CLASSIFICATION

Ships

Edition July 2018

Part 6 Additional class notations

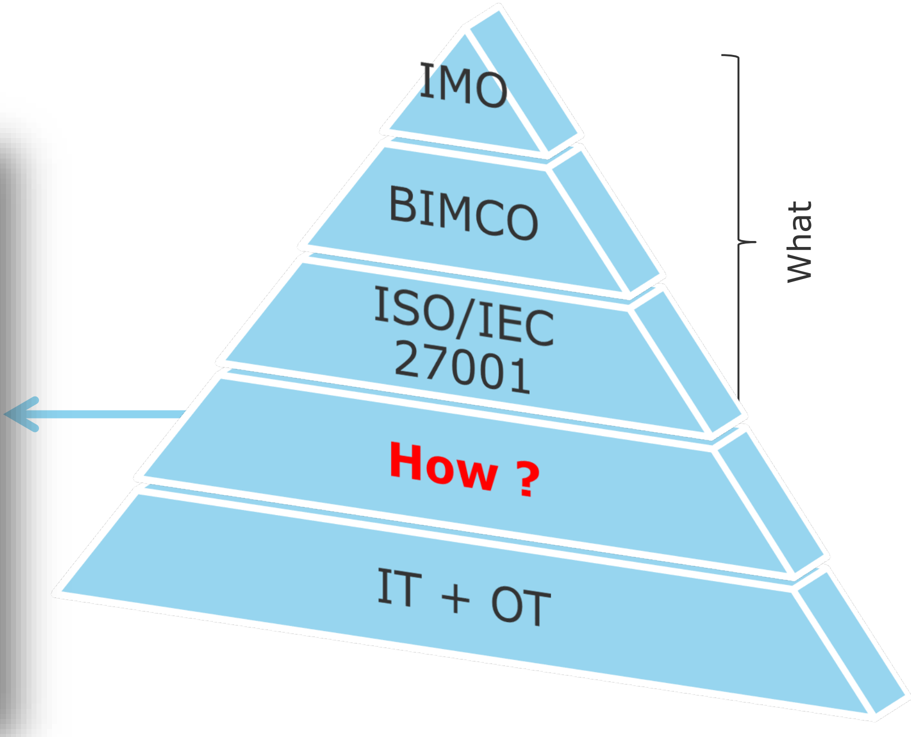
Chapter 5 Equipment and design features

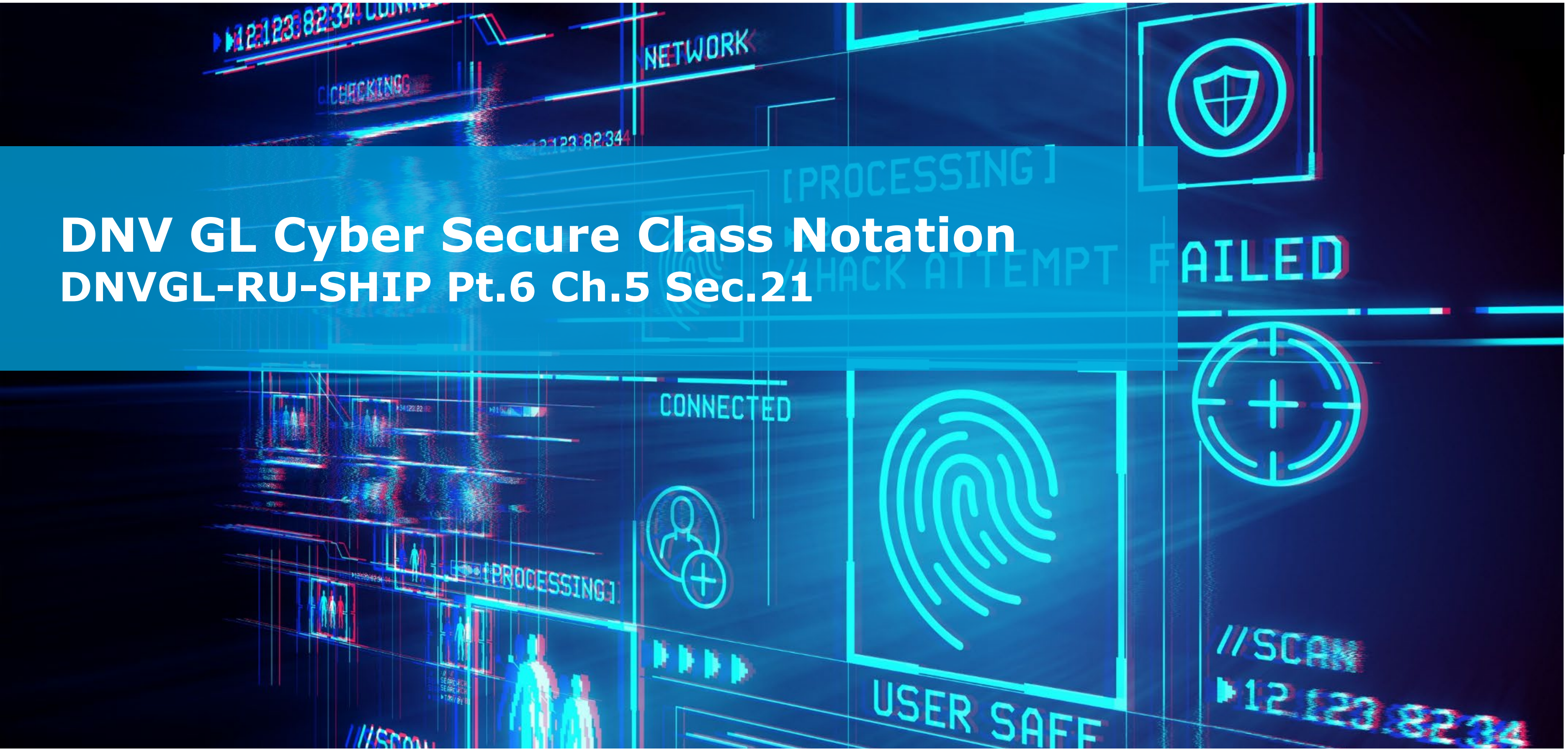
Section 21 Cyber Security

The content of this service document is the subject of intellectual property rights reserved by DNV GL AS ("DNV GL"). The user accepts that it is prohibited by anyone else but DNV GL and/or its licensees to offer and/or perform classification, certification and/or verification services, including the issuance of certificates and/or declarations of conformity, wholly or partly, on the basis of and/or pursuant to this document whether free of charge or chargeable, without DNV GL's prior written consent. DNV GL is not responsible for the consequences arising from any use of this document by others.

The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

DNV GL AS

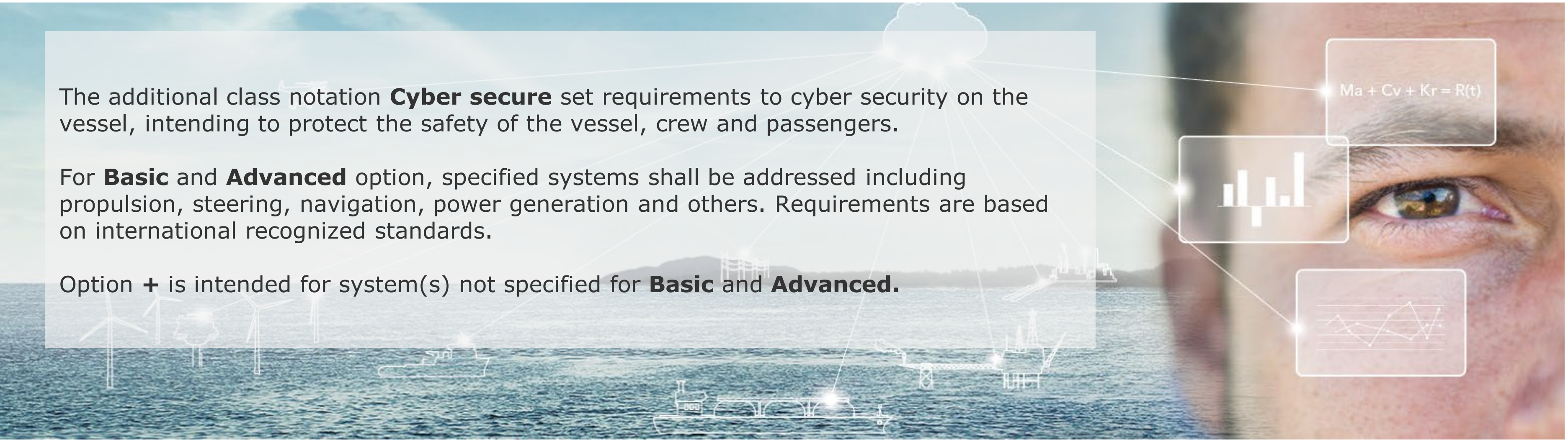




DNV GL Cyber Secure Class Notation

DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21

Cyber secure class notation



The additional class notation **Cyber secure** set requirements to cyber security on the vessel, intending to protect the safety of the vessel, crew and passengers.

For **Basic** and **Advanced** option, specified systems shall be addressed including propulsion, steering, navigation, power generation and others. Requirements are based on international recognized standards.

Option **+** is intended for system(s) not specified for **Basic** and **Advanced.**

Cyber secure(Basic)

Minimum security level

Primarily intended for sailing vessels where security will be implemented in procedures and existing systems

Cyber secure(Advanced)

Higher security level

Primarily intended for new builds, where security will be integrated into the design of the vessel

Cyber secure(+)

Security level based on risk assessment

Target system(s) can be freely selected to address different needs. Can combined with Basic and Advanced

Cyber secure class notation

Cyber secure will bridge security knowledge between information technology and operation technology for systems on-board the vessel

Cyber secure will also:

- Provide baselines for demonstrating vessel’s cyber resilience to charterer and oil majors
- Provide measures reducing the risk of downtime due to cyber security incidents
- Increases the crew’s awareness to cyber threats
- Provide processes for continued focus on cyber security threats

Cyber secure(Basic)

Minimum level of technical measures implemented on-board the vessel

Cyber security management systems addressing a minimum security level

Cyber secure(Advanced)

Higher level of technical measures implemented on-board the vessel

Cyber security management systems addressing a higher level of security

Cyber secure(+)

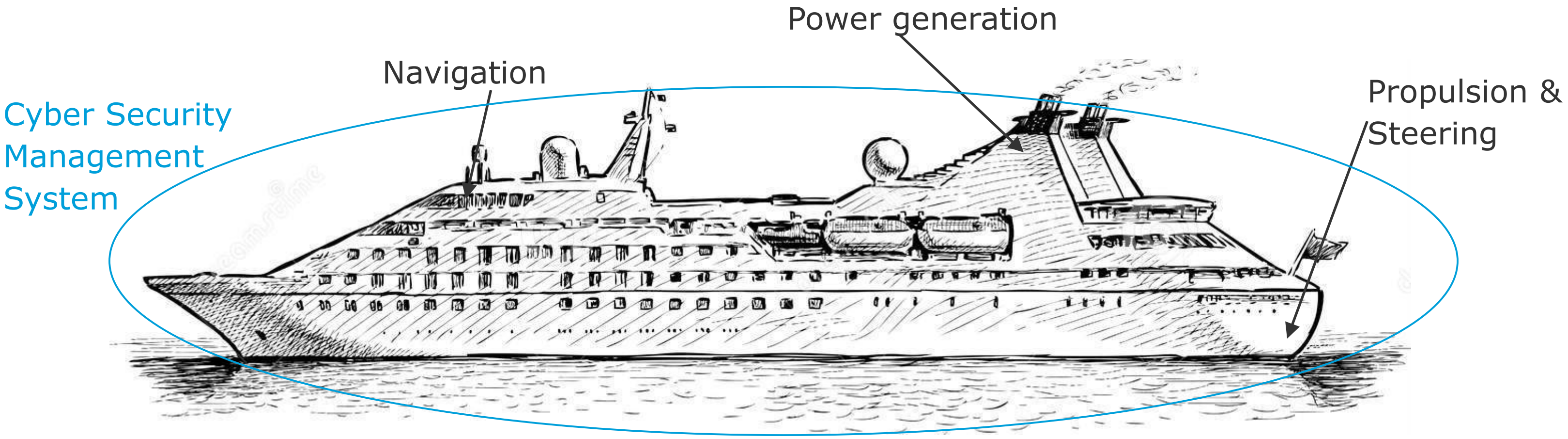
Level of technical measures derived from risk assessment

Cyber security management systems addressing the derived security level

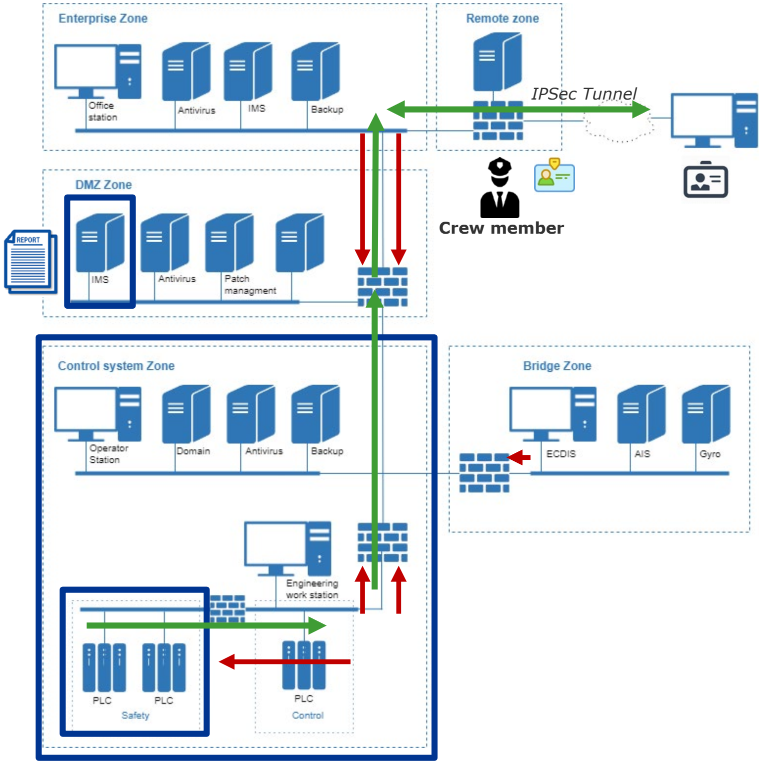
Scope for Cyber secure

- For qualifier **Basic** and **Advanced**, a number of given systems shall be addressed for cyber security. This includes e.g. propulsion, steering, navigation and power generation.
- For qualifier **+**, system(s) to addressed for cyber security can be freely selected. Security level should be determined based on a risk assessment by use of e.g. DNVGL-RP-0496.

- For all qualifiers, a cyber security management system for the vessel is required.



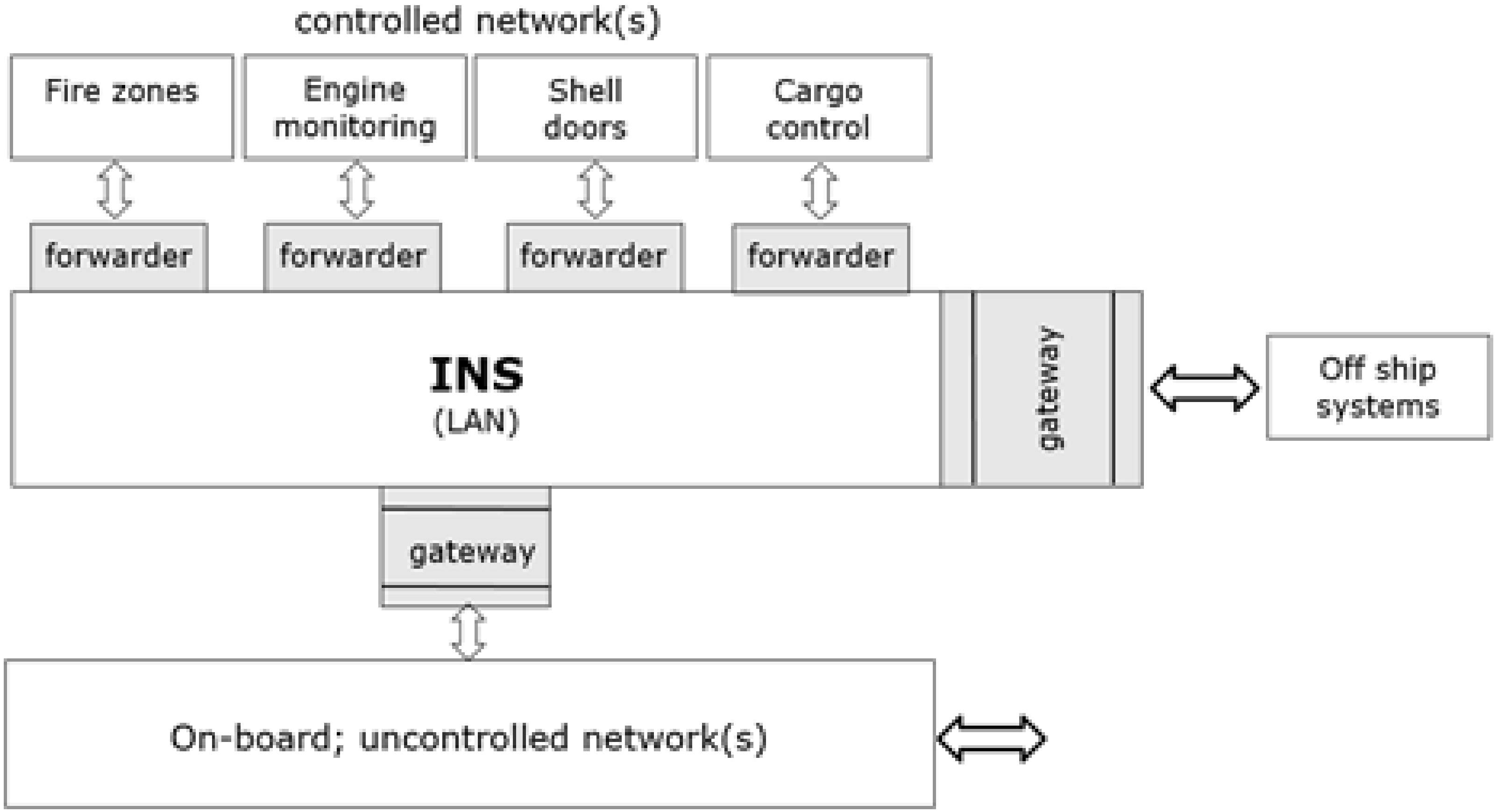
Example of security implementation by use of zones and conduits



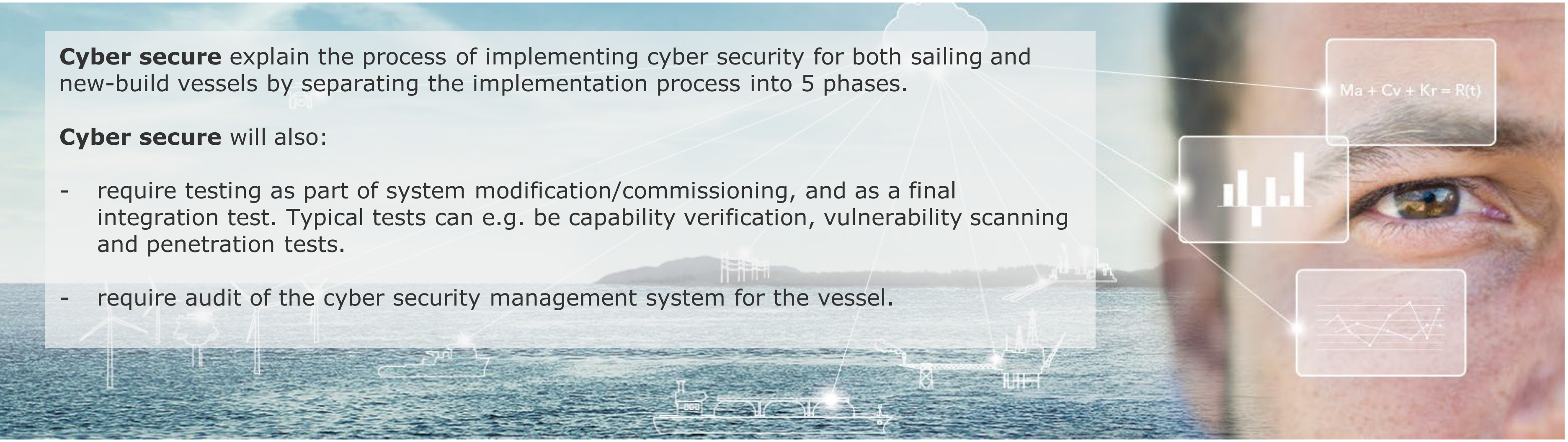
By applying the rules;

- Systems are securely segregated
- Communication between the systems are managed and secured
- Remote access to the vessel are managed and secured

Example of security implementation in bridge INS



Implementation and testing for Cyber secure

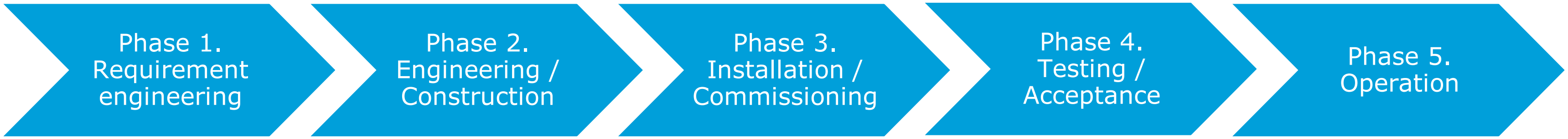


Cyber secure explain the process of implementing cyber security for both sailing and new-build vessels by separating the implementation process into 5 phases.

Cyber secure will also:

- require testing as part of system modification/commissioning, and as a final integration test. Typical tests can e.g. be capability verification, vulnerability scanning and penetration tests.

- require audit of the cyber security management system for the vessel.


Phase 1. Requirement engineering

Phase 2. Engineering / Construction

Phase 3. Installation / Commissioning

Phase 4. Testing / Acceptance

Phase 5. Operation

DNV·GL

MARITIME

Cyber Security type approval programme

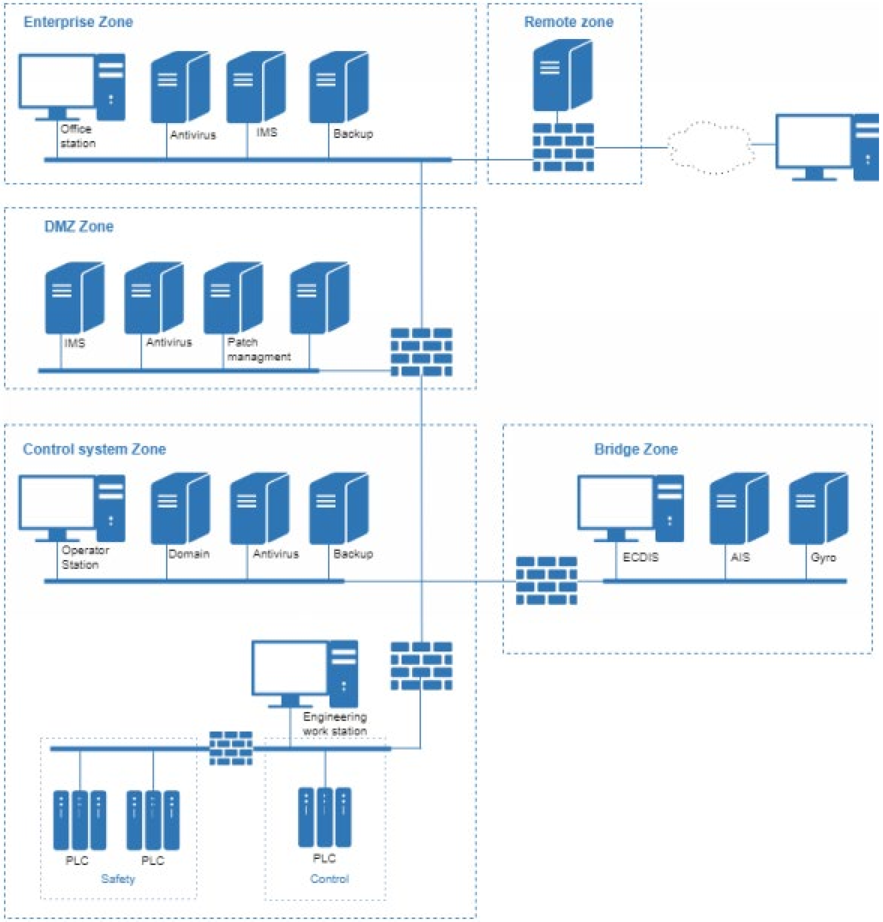
Capabilities of System Components

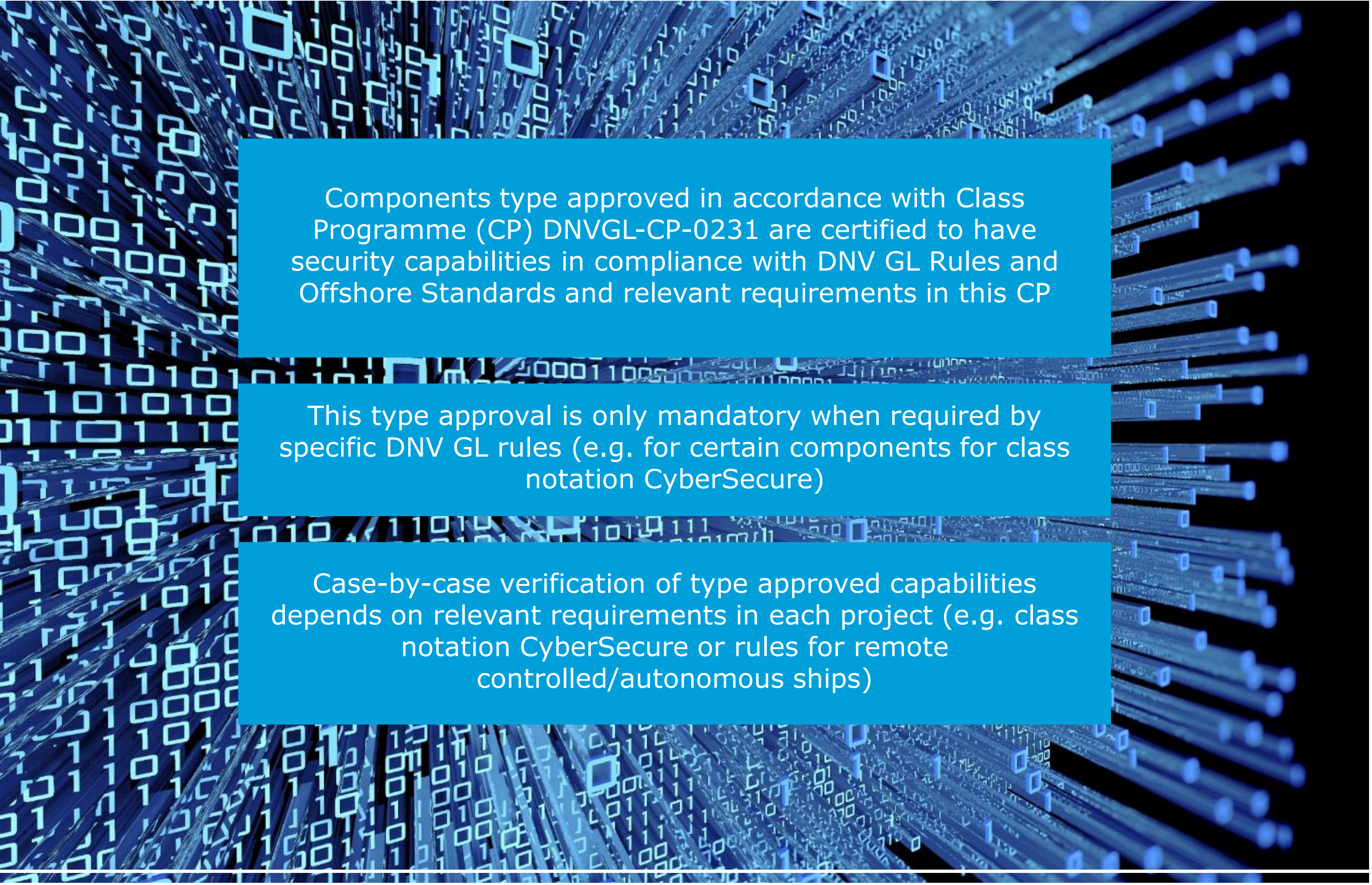
DNVGL-CG-0231

17 January 2019

Typical applications

- Remote access/connection
- Integrated and inter-connected control and monitoring systems
- Safety systems
- Systems supporting essential vessel services
- Other systems subjected to requirements for redundancy and/or separation





Components type approved in accordance with Class Programme (CP) DNVGL-CP-0231 are certified to have security capabilities in compliance with DNV GL Rules and Offshore Standards and relevant requirements in this CP

This type approval is only mandatory when required by specific DNV GL rules (e.g. for certain components for class notation CyberSecure)

Case-by-case verification of type approved capabilities depends on relevant requirements in each project (e.g. class notation CyberSecure or rules for remote controlled/autonomous ships)

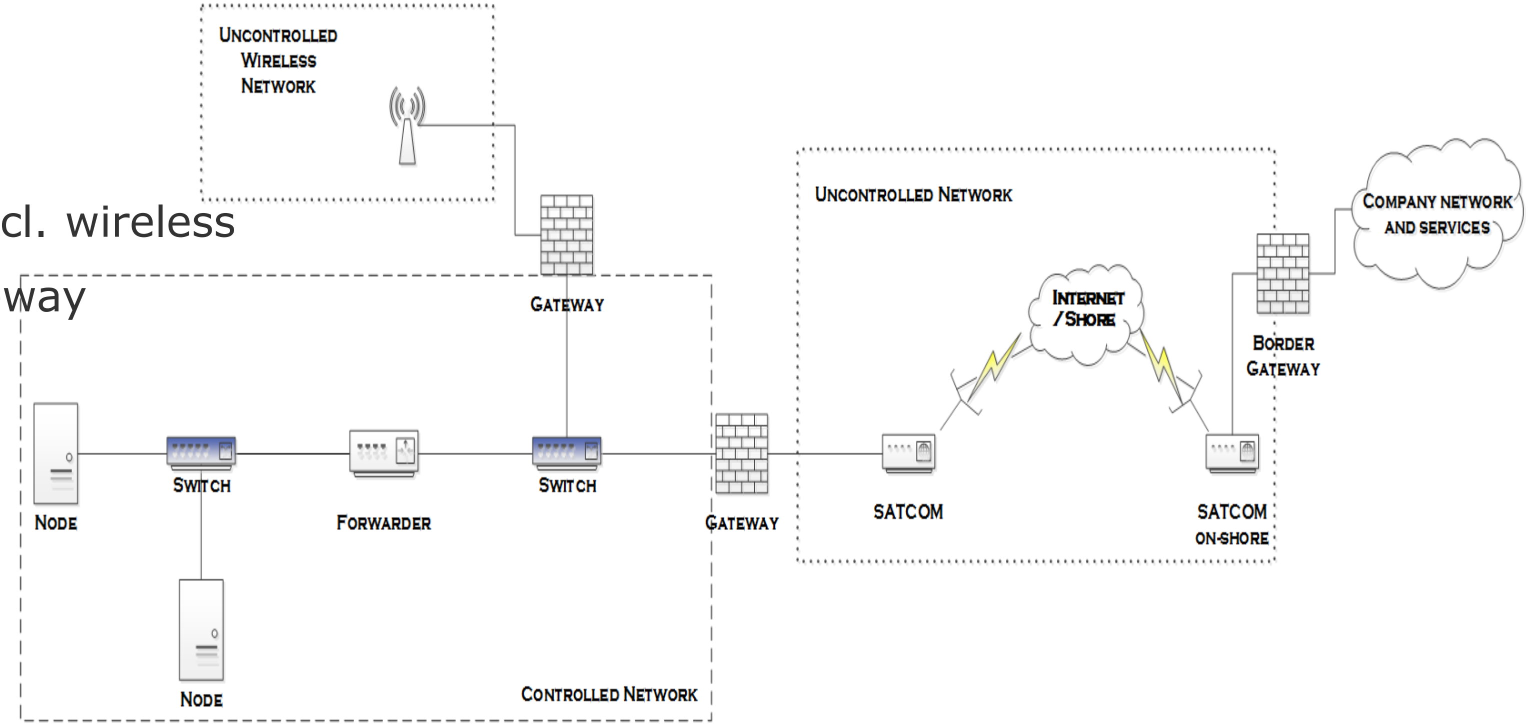
Project Phases

1. Assessment of documentation
   - Verification of compliance with security requirements
2. Type test
   - Witness of test by DNV GL, or
   - Test performed by DNV GL at manufacturer's office or DNV GL's office in Trondheim Norway
3. Issue of certificate

Component types

- Concept from IEC 61162-460
  - Controlled (secure) network

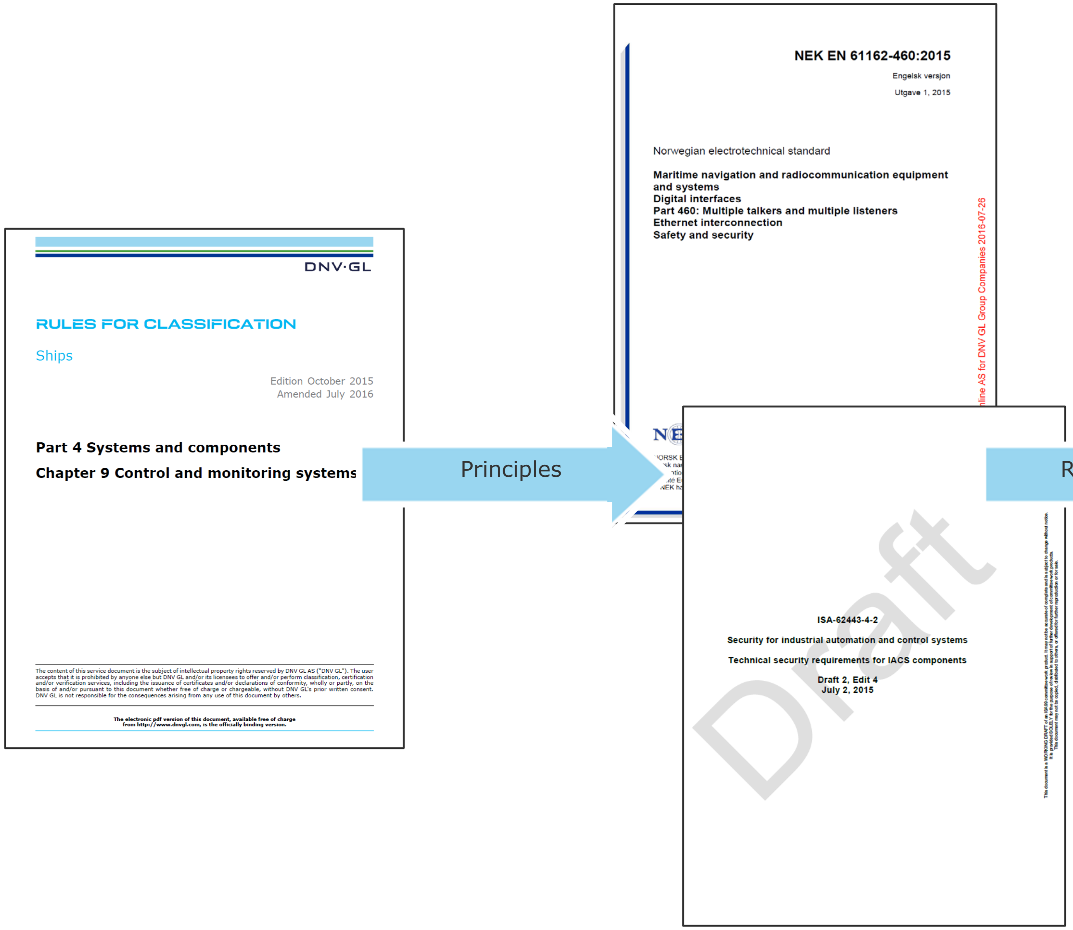
- Node
- Switch
- Forwarder
- Gateway, incl. wireless
- Border gateway



Security requirements

Mainly from ISA 62443-4-2 draft 4 edit 1

Test requirements developed by DNV GL



DNV·GL

RULES FOR CLASSIFICATION

Ships

Edition October 2015
Amended July 2016

Part 4 Systems and components

Chapter 9 Control and monitoring systems

The content of this service document is the subject of intellectual property rights reserved by DNV GL AS ("DNV GL"). The user accepts that it is prohibited by anyone else but DNV GL and/or its licensees to offer and/or perform classification, certification and/or verification services, including the issuance of certificates and/or declarations of conformity, wholly or partly, on the basis of and/or pursuant to this document whether free of charge or chargeable, without DNV GL's prior written consent. DNV GL is not responsible for the consequences arising from any use of this document by others.

The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

Principles

NEK EN 61162-460:2015

Engelsk versjon

Utgave 1, 2015

Norwegian electrotechnical standard

Maritime navigation and radiocommunication equipment and systems
Digital interfaces
Part 460: Multiple talkers and multiple listeners
Ethernet interconnection
Safety and security

ISA-62443-4-2

Security for industrial automation and control systems

Technical security requirements for IACS components

Draft 2, Edit 4
July 2, 2015

This document is a WORKING DRAFT of an ISA99 committee work product. It may not be accurate of complete and is subject to change without notice.
It is provided SOLELY for the purpose of review in support of further development of committee work products.
This document may not be copied, distributed to others, or offered for further reproduction or for sale.

Requirements

CONTENTS

Security Levels (SL)

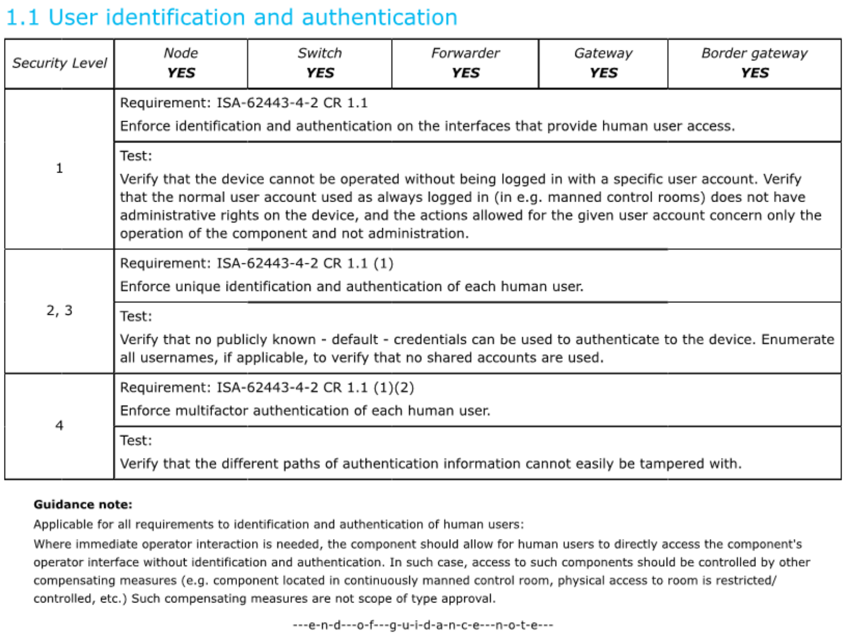
SL1: Protection against casual or coincidental violation

SL2: Protection against intentional violation using simple means, low resources, generic skills, low motivation

SL3: Protection against intentional violation using sophisticated means, moderate resources, OT system specific skills, moderate motivation

SL 4: Protection against intentional violation using sophisticated means, extended resources, OT system specific skills, high motivation

Security Requirements, examples



1.1 User identification and authentication

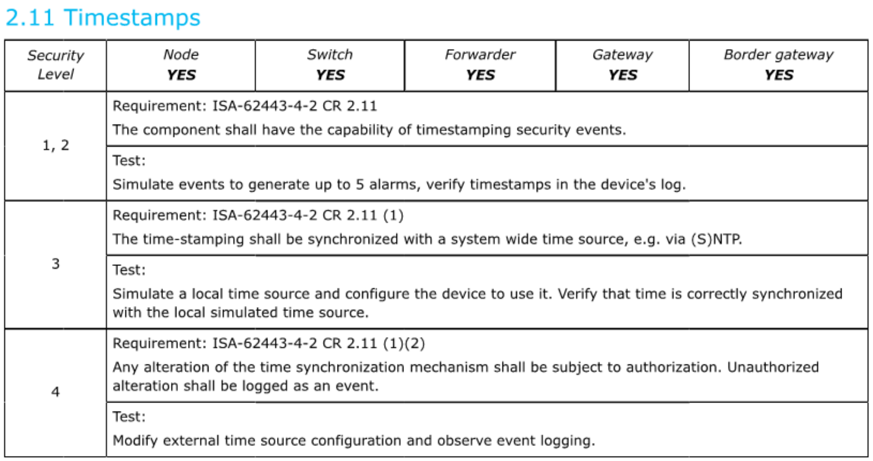
Security Level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Requirement: ISA-62443-4-2 CR 1.1 Enforce identification and authentication on the interfaces that provide human user access.				
	Test: Verify that the device cannot be operated without being logged in with a specific user account. Verify that the normal user account used as always logged in (in e.g. manned control rooms) does not have administrative rights on the device, and the actions allowed for the given user account concern only the operation of the component and not administration.				
2, 3	Requirement: ISA-62443-4-2 CR 1.1 (1) Enforce unique identification and authentication of each human user.				
	Test: Verify that no publicly known - default - credentials can be used to authenticate to the device. Enumerate all usernames, if applicable, to verify that no shared accounts are used.				
4	Requirement: ISA-62443-4-2 CR 1.1 (1)(2) Enforce multifactor authentication of each human user.				
	Test: Verify that the different paths of authentication information cannot easily be tampered with.				

Guidance note:

Applicable for all requirements to identification and authentication of human users:

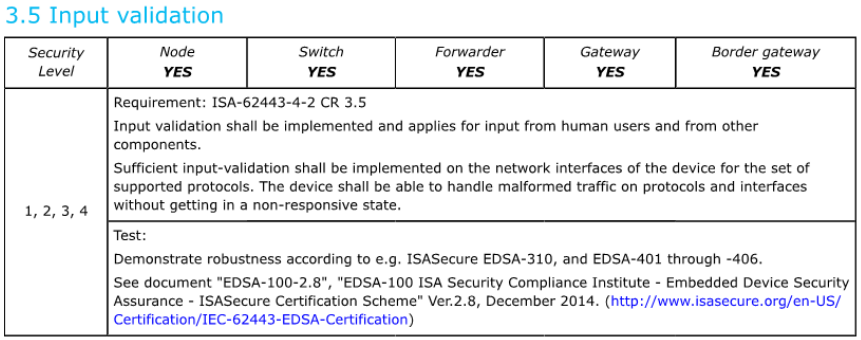
Where immediate operator interaction is needed, the component should allow for human users to directly access the component's operator interface without identification and authentication. In such case, access to such components should be controlled by other compensating measures (e.g. component located in continuously manned control room, physical access to room is restricted/ controlled, etc.) Such compensating measures are not scope of type approval.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---



2.11 Timestamps

Security Level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 CR 2.11 The component shall have the capability of timestamping security events.				
	Test: Simulate events to generate up to 5 alarms, verify timestamps in the device's log.				
3	Requirement: ISA-62443-4-2 CR 2.11 (1) The time-stamping shall be synchronized with a system wide time source, e.g. via (S)NTP.				
	Test: Simulate a local time source and configure the device to use it. Verify that time is correctly synchronized with the local simulated time source.				
4	Requirement: ISA-62443-4-2 CR 2.11 (1)(2) Any alteration of the time synchronization mechanism shall be subject to authorization. Unauthorized alteration shall be logged as an event.				
	Test: Modify external time source configuration and observe event logging.				



3.5 Input validation

Security Level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 3.5 Input validation shall be implemented and applies for input from human users and from other components. Sufficient input-validation shall be implemented on the network interfaces of the device for the set of supported protocols. The device shall be able to handle malformed traffic on protocols and interfaces without getting in a non-responsive state.				
	Test: Demonstrate robustness according to e.g. ISASecure EDSA-310, and EDSA-401 through -406. See document "EDSA-100-2.8", "EDSA-100 ISA Security Compliance Institute - Embedded Device Security Assurance - ISASecure Certification Scheme" Ver.2.8, December 2014. (http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification)				

Benefits

Use of recognized industry standards for cyber security capabilities of components in Industrial Automation and Control Systems

No need to share confidential documentation outside organization with vendors to prove cybersecurity requirements

Third party verification

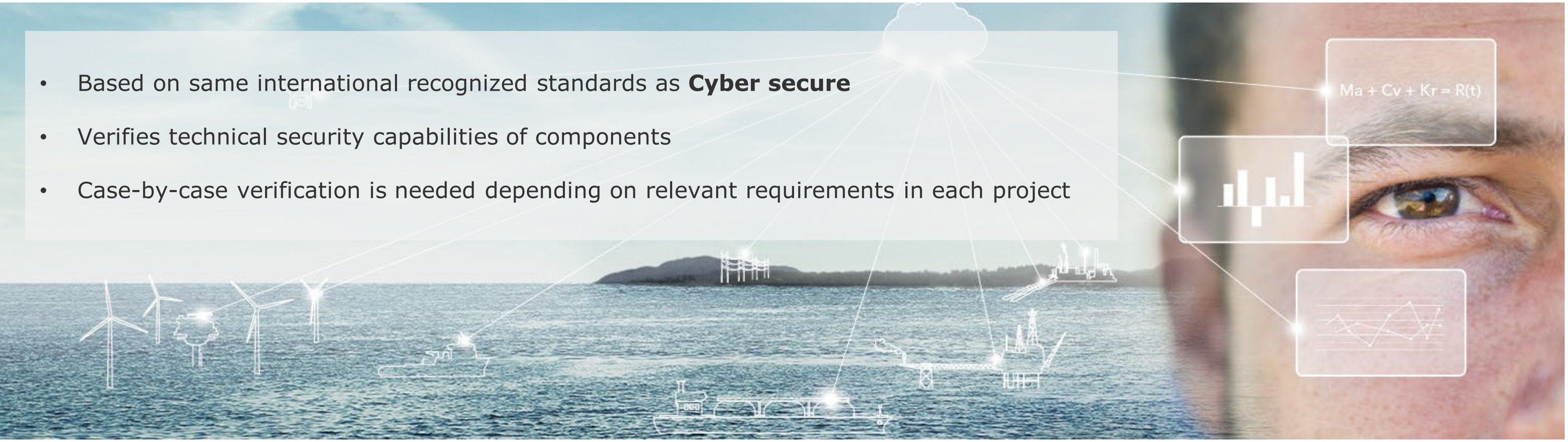
Show to the market how cyber secure your product is

Four security levels. Vendor selects the level.

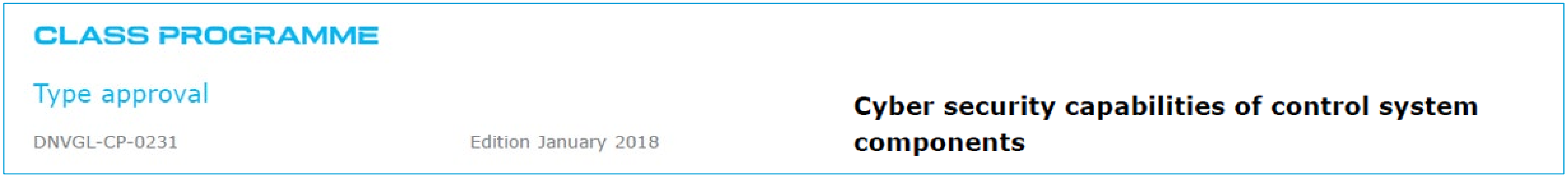
Can be applied on system level

Test requirements included in CP-0231

Our Type Approval program support manufactures, owners and yards ensuring safety through cyber secure components



- Based on same international recognized standards as **Cyber secure**
- Verifies technical security capabilities of components
- Case-by-case verification is needed depending on relevant requirements in each project



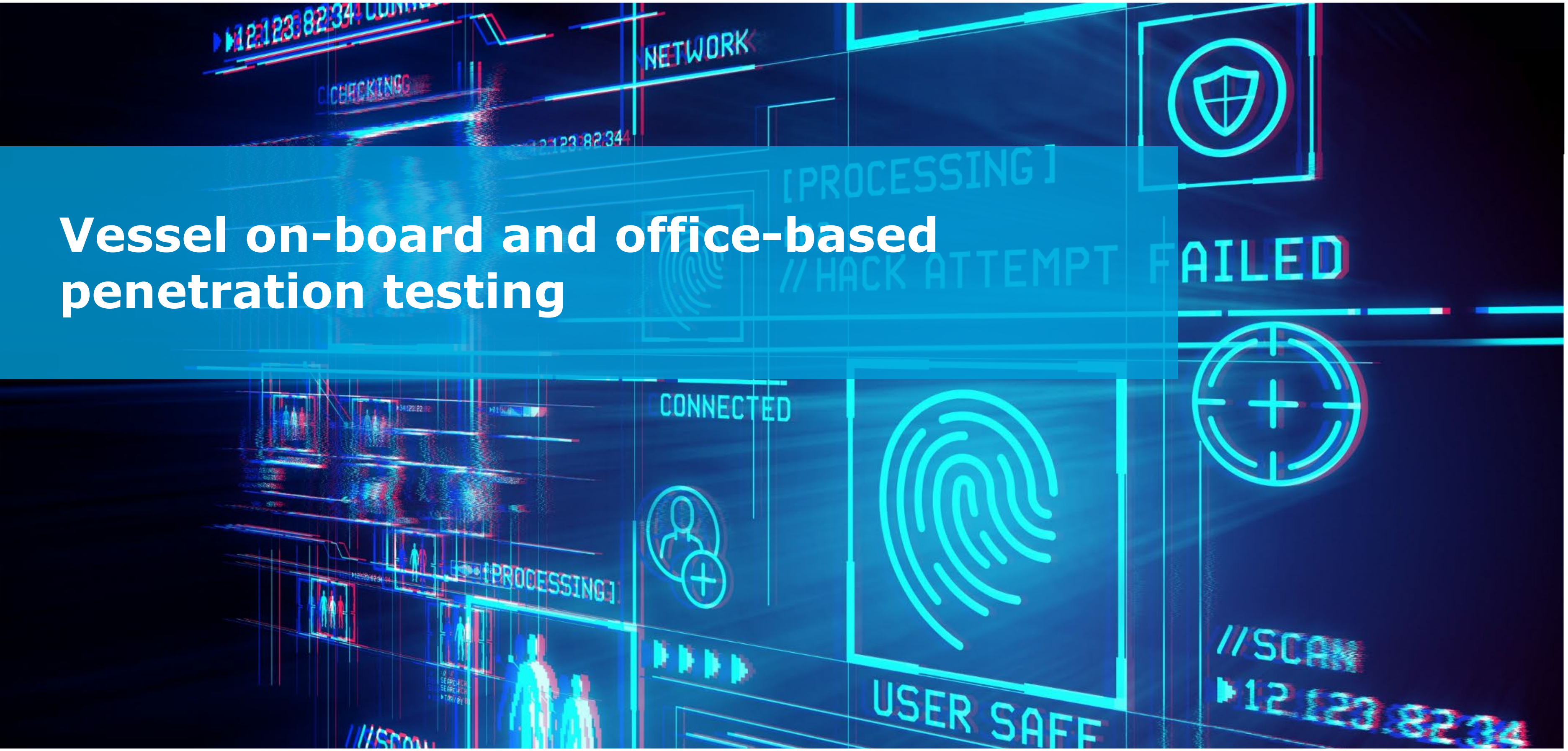
CLASS PROGRAMME

Type approval

DNVGL-CP-0231

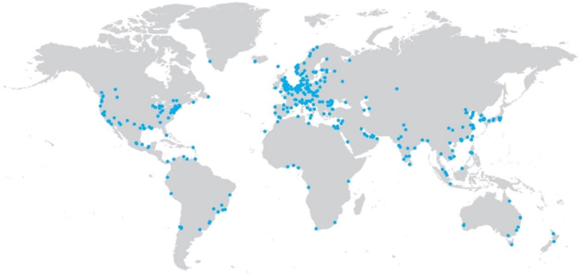
Edition January 2018

Cyber security capabilities of control system components



Vessel on-board and office-based penetration testing

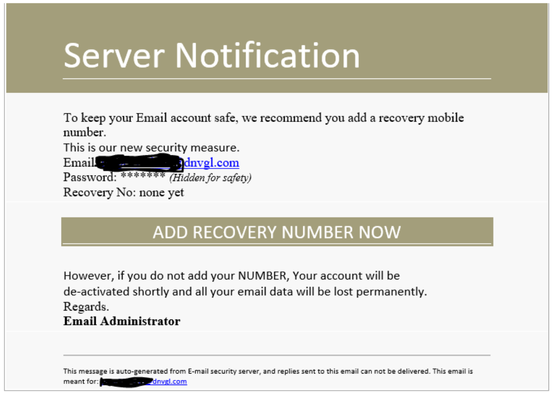
Penetration testing of IT systems, for a typical shipping company



- Global presence, multiple branch offices

- Scanning for remote vulnerabilities
  - Unintentional backdoor IoT devices connected to corporate networks
  - Vulnerable video conferencing systems
  - …

- What happens in case a phish got in?



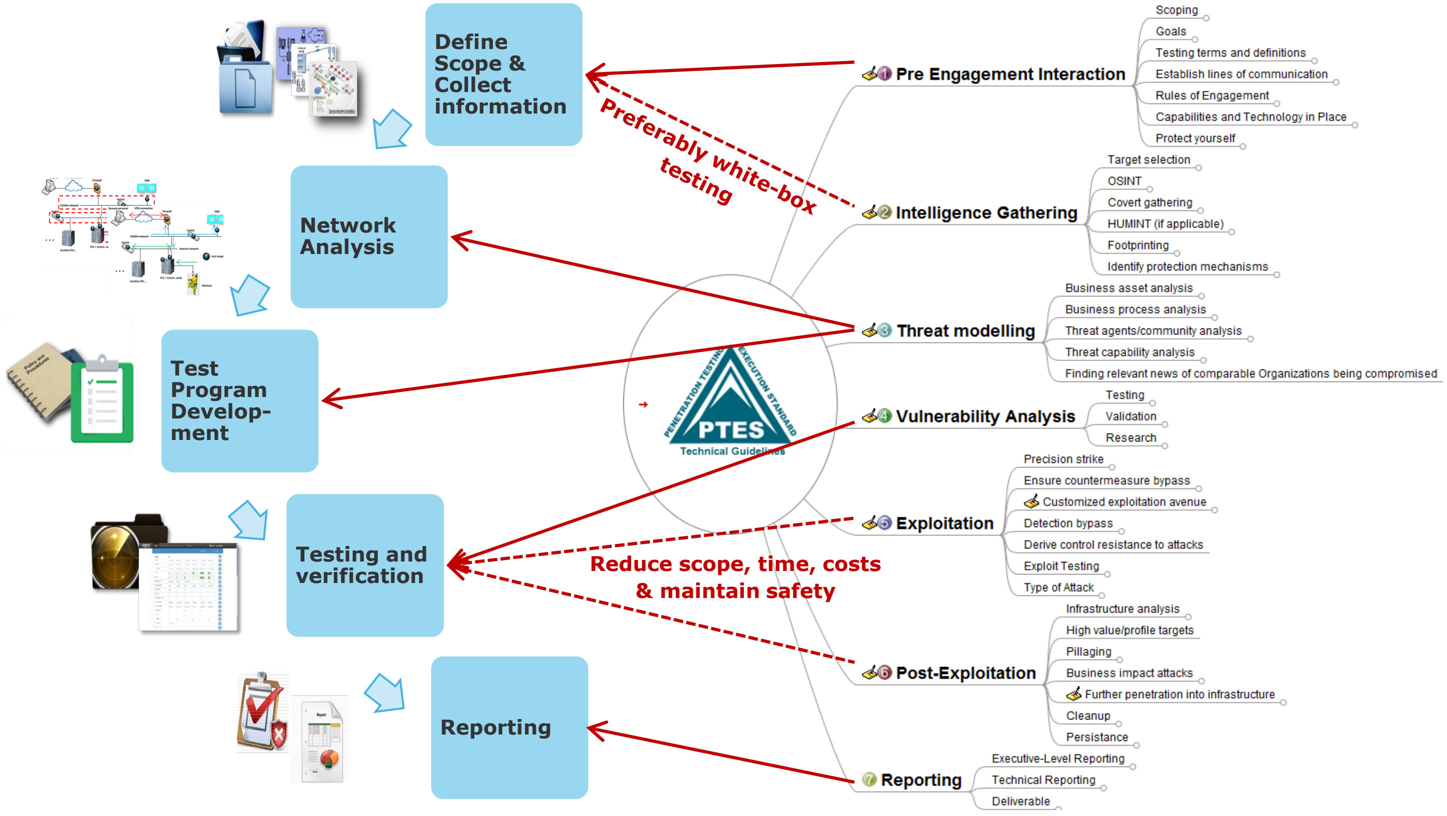
Server Notification

To keep your Email account safe, we recommend you add a recovery mobile number.
This is our new security measure.
Email[redacted]dnvgl.com
Password: ******* *(Hidden for safety)*
Recovery No: none yet

However, if you do not add your NUMBER, Your account will be de-activated shortly and all your email data will be lost permanently.
Regards.
Email Administrator

This message is auto-generated from E-mail security server, and replies sent to this email can not be delivered. This email is meant for: [redacted]dnvgl.com

Penetration testing – main activities



Define Scope & Collect information

Network Analysis

Test Program Develop-ment

Testing and verification

Reporting

Preferably white-box testing

Reduce scope, time, costs & maintain safety

PENETRATION TESTING EXECUTION STANDARD PTES Technical Guidelines

1 Pre Engagement Interaction
- Scoping
- Goals
- Testing terms and definitions
- Establish lines of communication
- Rules of Engagement
- Capabilities and Technology in Place
- Protect yourself

2 Intelligence Gathering
- Target selection
- OSINT
- Covert gathering
- HUMINT (if applicable)
- Footprinting
- Identify protection mechanisms

3 Threat modelling
- Business asset analysis
- Business process analysis
- Threat agents/community analysis
- Threat capability analysis
- Finding relevant news of comparable Organizations being compromised

4 Vulnerability Analysis
- Testing
- Validation
- Research

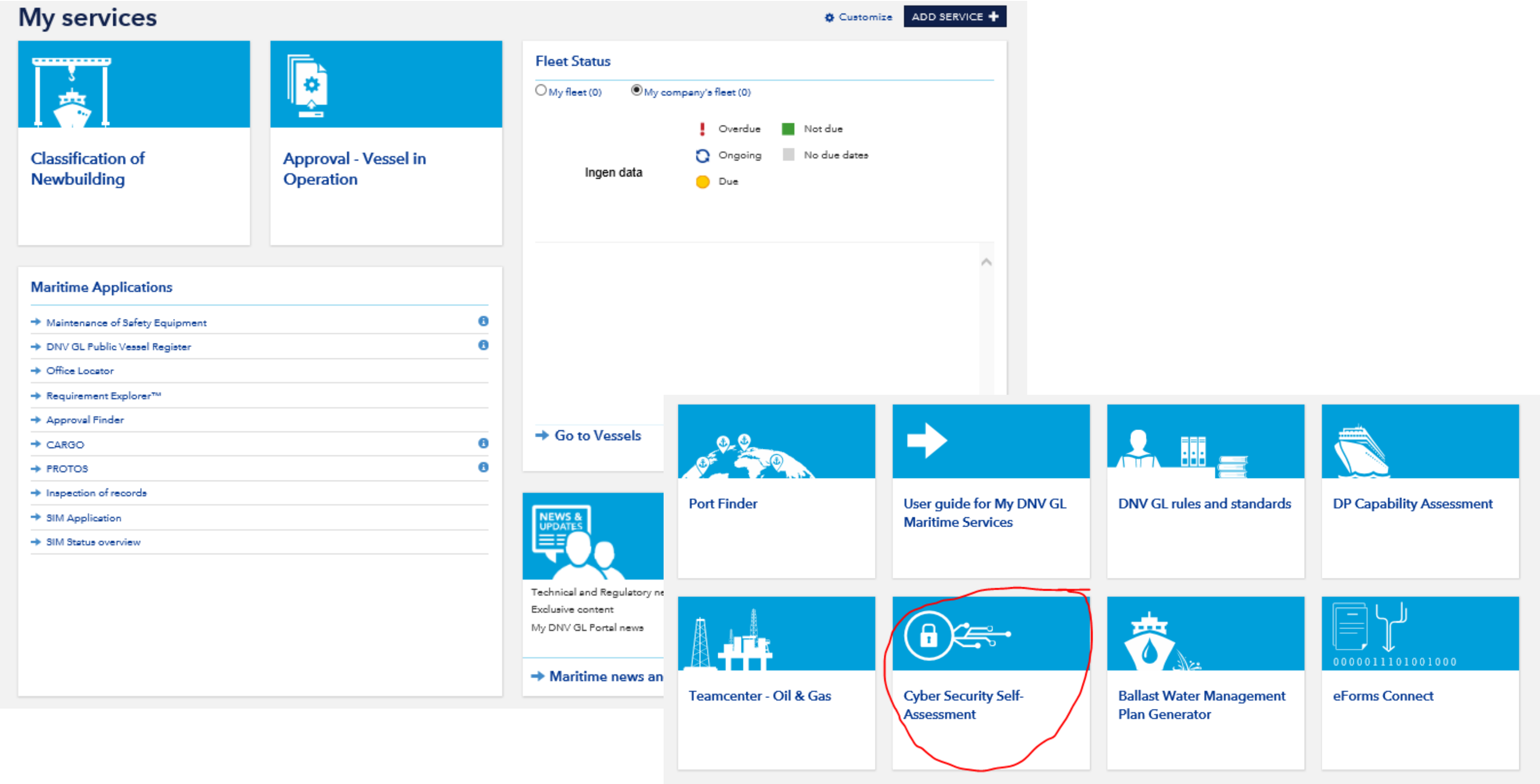
5 Exploitation
- Precision strike
- Ensure countermeasure bypass
- Customized exploitation avenue
- Detection bypass
- Derive control resistance to attacks
- Exploit Testing
- Type of Attack

6 Post-Exploitation
- Infrastructure analysis
- High value/profile targets
- Pillaging
- Business impact attacks
- Further penetration into infrastructure
- Cleanup
- Persistance

7 Reporting
- Executive-Level Reporting
- Technical Reporting
- Deliverable

*PTES is a (not yet formal) standard designed to provide a common language and scope for performing a pentest.

First step



My services

Customize ADD SERVICE +

Classification of Newbuilding

Approval - Vessel in Operation

Fleet Status

○ My fleet (0) ● My company's fleet (0)

Ingen data

! Overdue 🟩 Not due

Ongoing ▨ No due dates

● Due

→ Go to Vessels

Maritime Applications

- → Maintenance of Safety Equipment
- → DNV GL Public Vessel Register
- → Office Locator
- → Requirement Explorer™
- → Approval Finder
- → CARGO
- → PROTOS
- → Inspection of records
- → SIM Application
- → SIM Status overview

NEWS & UPDATES

Technical and Regulatory ne
Exclusive content
My DNV GL Portal news

→ Maritime news an

Port Finder

User guide for My DNV GL Maritime Services

DNV GL rules and standards

DP Capability Assessment

Teamcenter - Oil & Gas

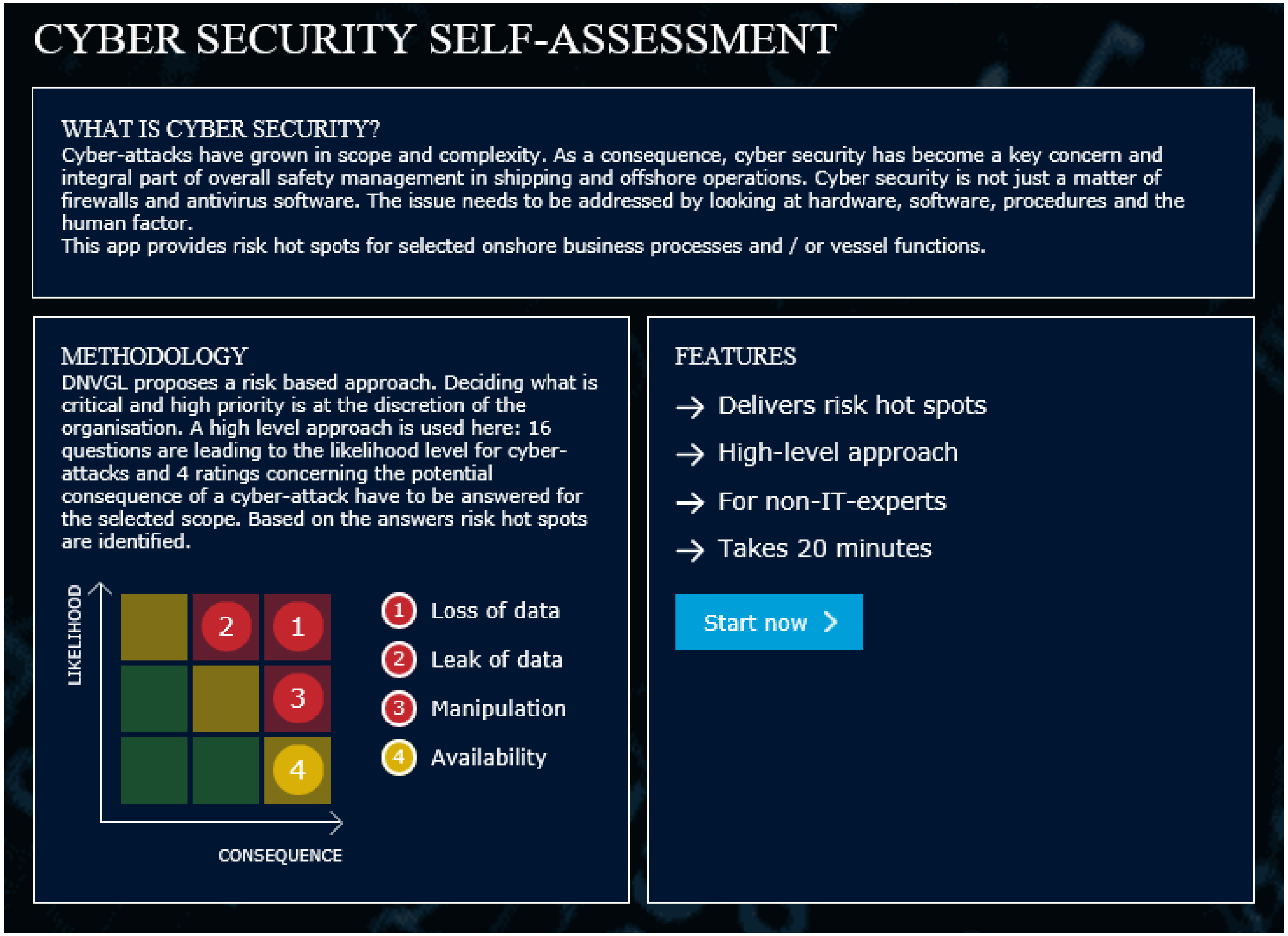
Cyber Security Self-Assessment

Ballast Water Management Plan Generator

eForms Connect

https://services.veracity.com/

Second step- self check



CYBER SECURITY SELF-ASSESSMENT

WHAT IS CYBER SECURITY?

Cyber-attacks have grown in scope and complexity. As a consequence, cyber security has become a key concern and integral part of overall safety management in shipping and offshore operations. Cyber security is not just a matter of firewalls and antivirus software. The issue needs to be addressed by looking at hardware, software, procedures and the human factor.

This app provides risk hot spots for selected onshore business processes and / or vessel functions.

METHODOLOGY

DNVGL proposes a risk based approach. Deciding what is critical and high priority is at the discretion of the organisation. A high level approach is used here: 16 questions are leading to the likelihood level for cyber-attacks and 4 ratings concerning the potential consequence of a cyber-attack have to be answered for the selected scope. Based on the answers risk hot spots are identified.

1 Loss of data

2 Leak of data

3 Manipulation

4 Availability

FEATURES

- → Delivers risk hot spots
- → High-level approach
- → For non-IT-experts
- → Takes 20 minutes

Thank you for your attention

Jan Tore Grimsrud
Jan.tore.grimsrud@dnvgl.com
+47 930 30449

www.dnvgl.com

SAFER, SMARTER, GREENER