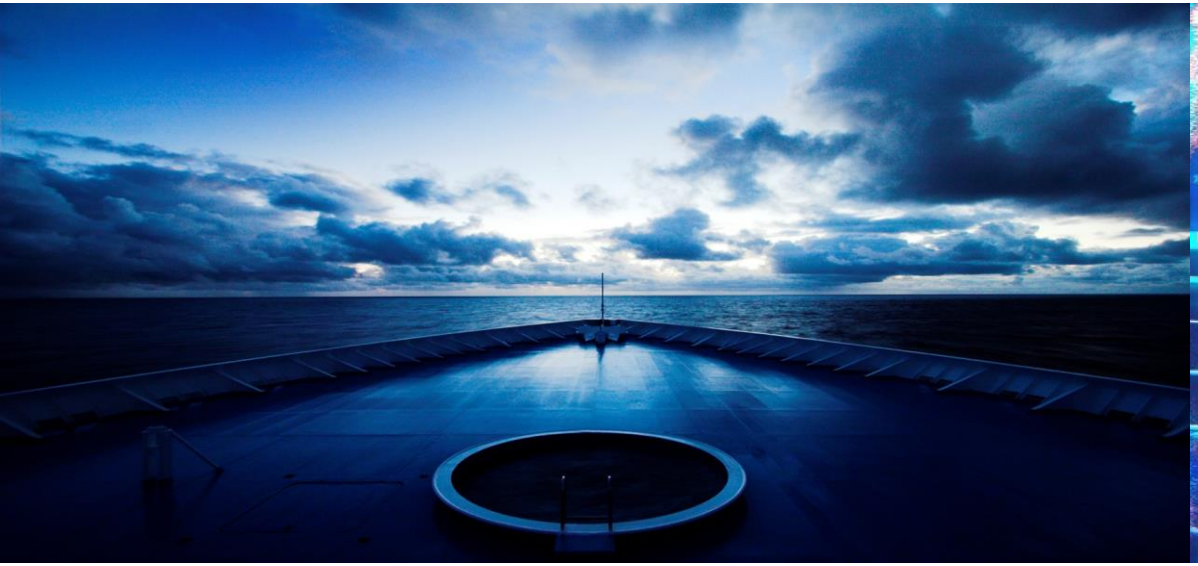
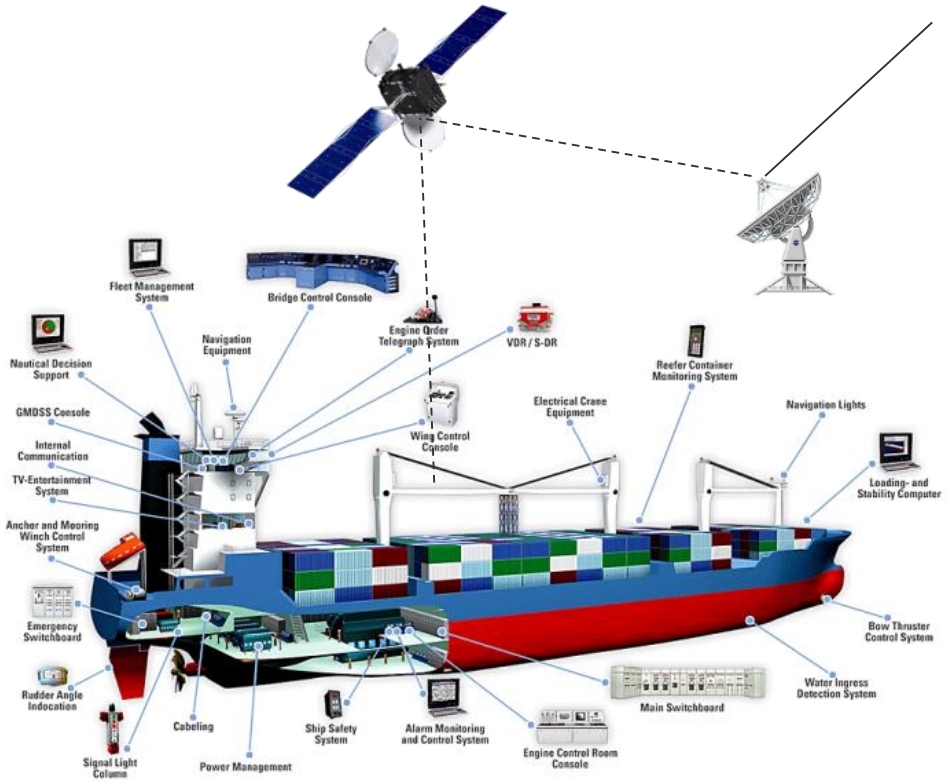


DNV GL Cyber secure class notation

Information Day September 11th 2020

Agenda

- Digital vulnerabilities in the maritime sector
- DNV GL guidelines for cyber security
- The DNV GL Cyber secure class notation
- DNV GL Cyber secure type approval
- DNV GL cyber security certification, testing and advisory services
- Some references



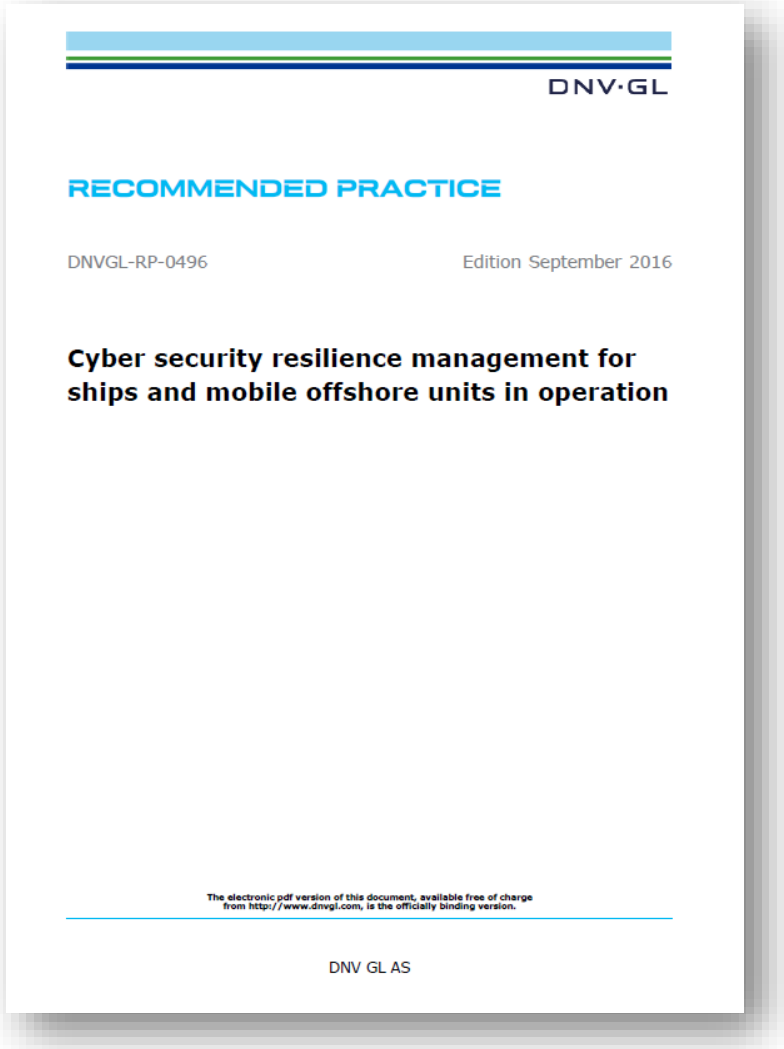
Digital vulnerabilities in the maritime sector

DNV GL assessment for Norwegian Authorities*/ Lysneutvalget , April 2015 *Ministry of Justice and Public Security

Top 10:

- **Lack of attention and training**
- **Navigation Signals from a satellite is normally not protected against modification**
- **System for identification of the vessel is normally not protected against modification**
- **Remote Maintenance**
- **A large number of parties are exchanging a lot of information on unsecured email**
- **Separation of computer networks**
- **Use of mobile storage devices**
- **Booking systems and administration systems are vulnerable**
- **Lack of physical security for server rooms, wiring closets, etc.**
- **Limited user authentication against systems for public reporting**

DNVGL-RP-0496 Cyber Security resilience management for ships and mobile offshore units in operation


DNV·GL

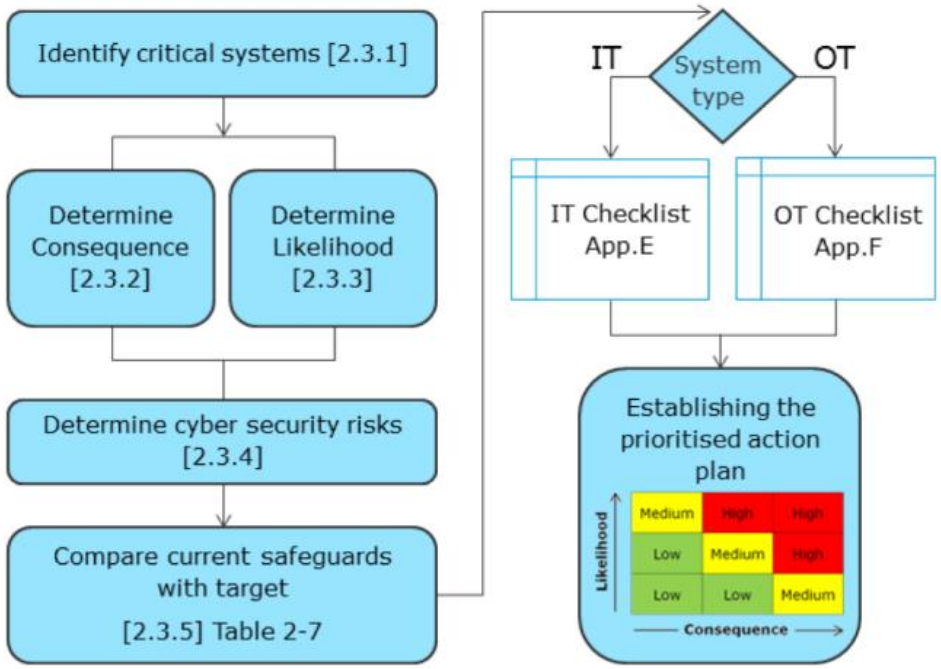
RECOMMENDED PRACTICE

DNVGL-RP-0496 Edition September 2016

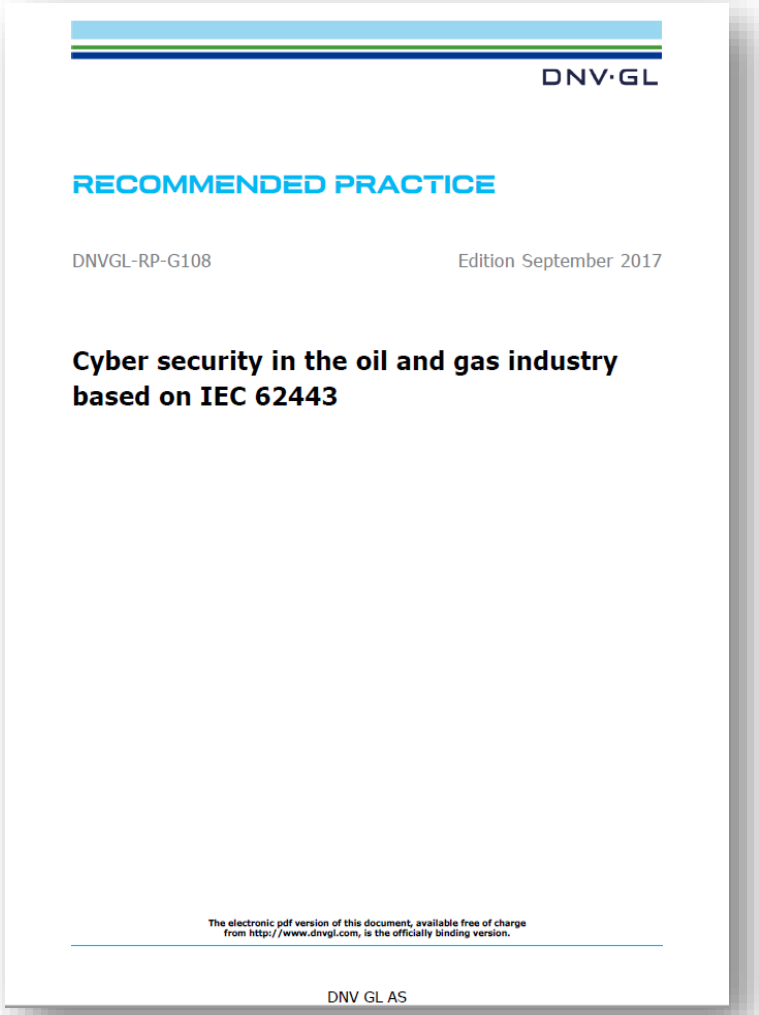
Cyber security resilience management for ships and mobile offshore units in operation

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

DNV GL AS



DNVGL-RP-G108 Cyber security in the oil and gas industry based on IEC 62443


DNV·GL

RECOMMENDED PRACTICE

DNVGL-RP-G108 Edition September 2017

Cyber security in the oil and gas industry based on IEC 62443

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

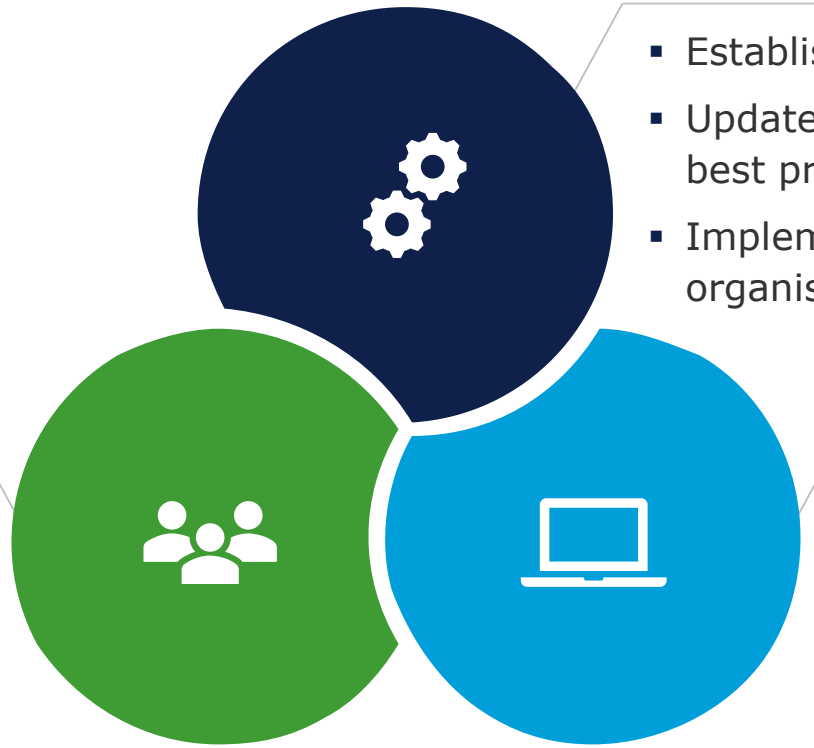
DNV GL AS

- Developed as a Joint Industry project (JIP)
- Participants: ABB, DNV GL, Emerson, Equinor, Honeywell, Kongsberg Maritime, Lundin, PTIL, Shell, Siemens and Woodside
- Started April 2016
- Released the RP at Offshore Europe September 2017

Cyber Security best practice

Process

- Establish a Cyber Security Management System
- Update your procedures to reflect cyber security best practices
- Implement the management system into your organisation



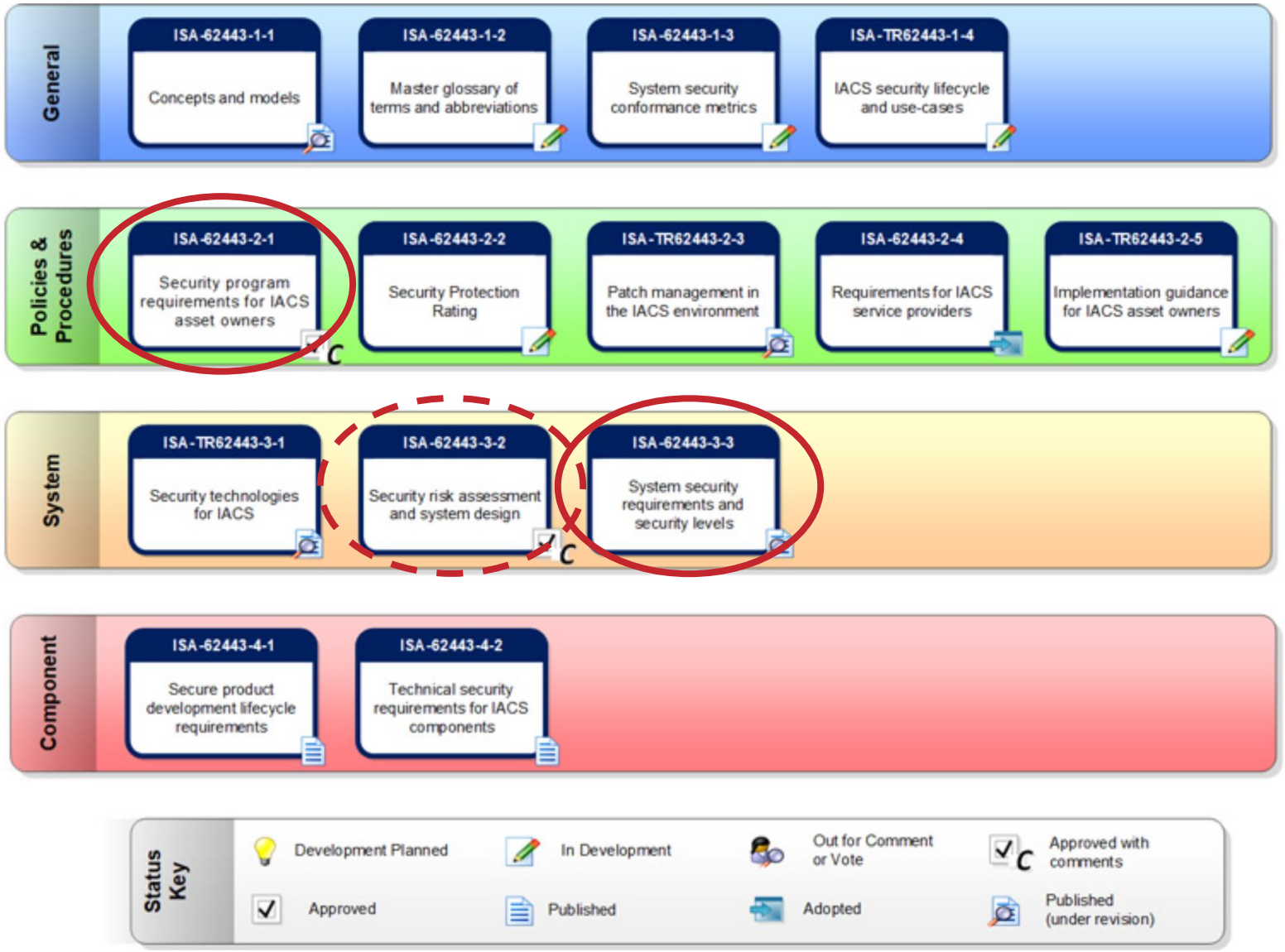
People

- Train your onboard & shore personnel
- Train system responsible personnel
- Perform incident response & recovery training

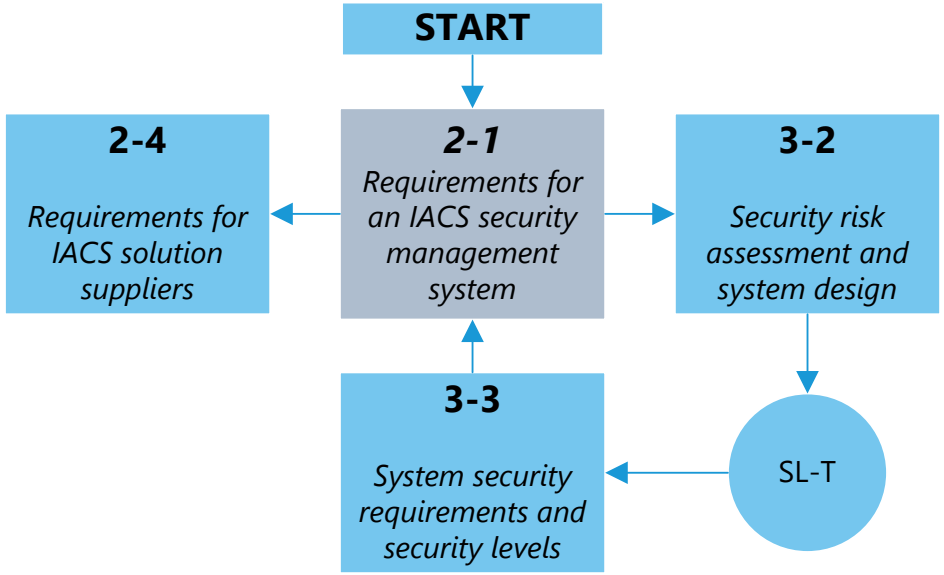
Technology

- Ensure segregation of your networks and secure network boundaries
- Secure systems and components
- Install systems to identify, protect, detect, respond and recover.

ISA/IEC 62443 Security for Industrial Automation and Control Systems



How to implement 62443



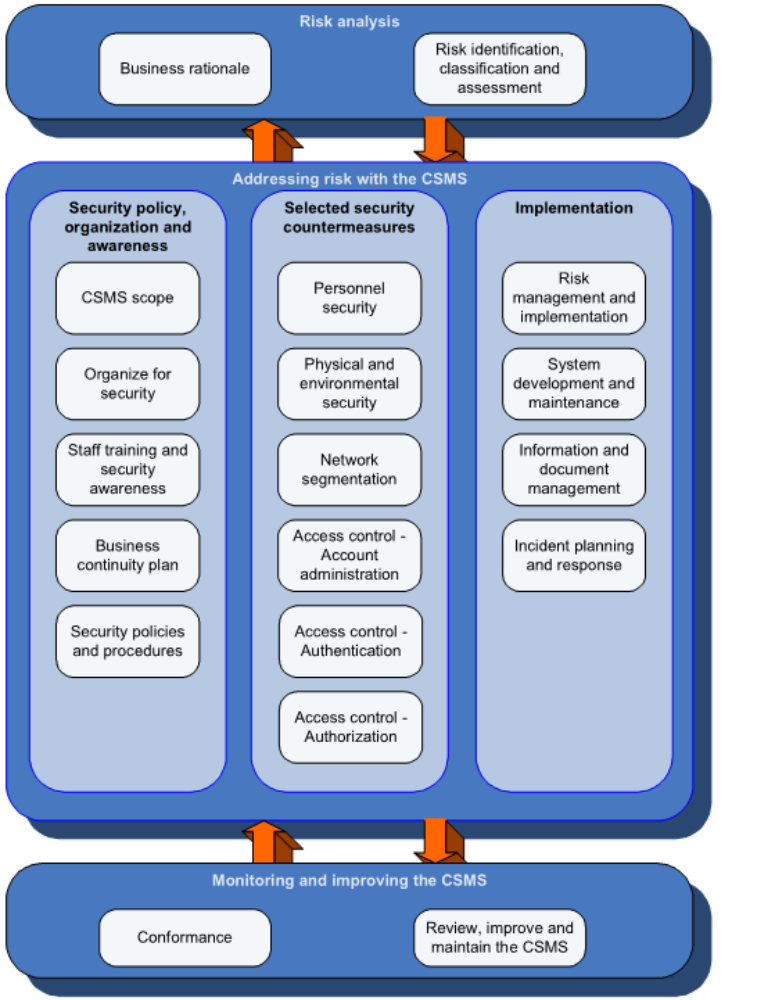
Define System Under Consideration

Do a risk assessment

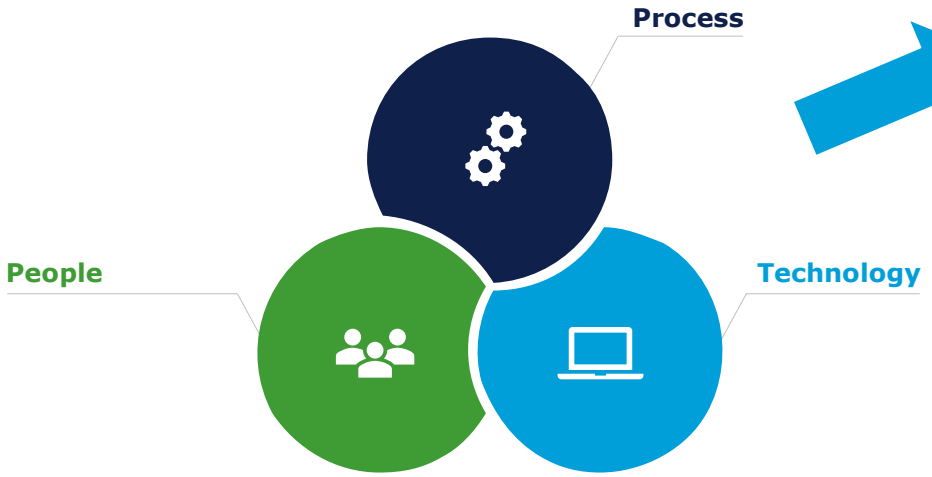
Define zones and conduits

Define Security Level Target

62443-2-1 Cyber Security Management System (owner)

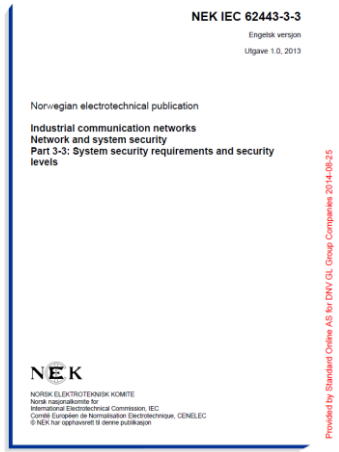


The DNV GL Cyber Security Class Notation



IEC 61162-460

IEC 62443-3-3


NEK IEC 62443-3-3

Engelsk versjon

Utgave 1.0, 2013

Norwegian electrotechnical publication

Industrial communication networks
Network and system security
Part 3-3: System security requirements and security levels

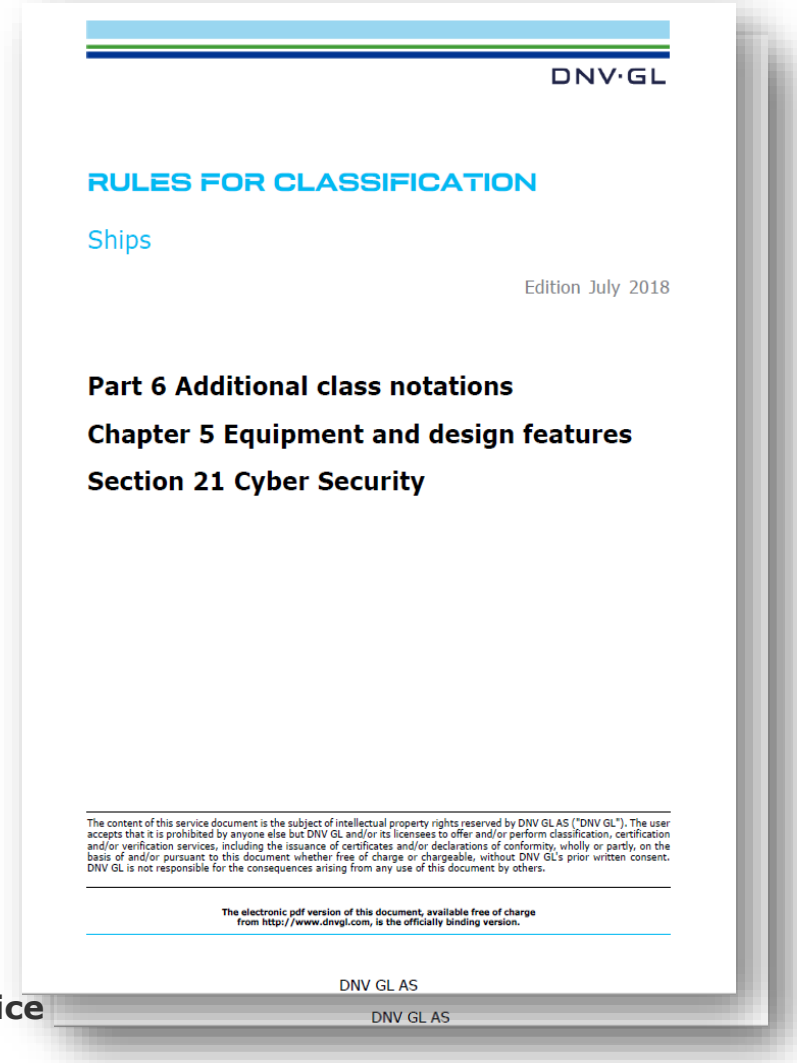
NEK

NORSK ELEKTROTEKNISK KOMITE
Norsk nasjonalkomite for
International Electrotechnical Commission, IEC
Comité Européen de Normalisation Electrotechnique, CENELEC
© NEK har opphavsrett til denne publikasjon

Provided by Standard Online AS for DNV GL Group Companies 2014-08-25

IEC 62443-2-1

Fleet in service from 2020


DNV·GL

RULES FOR CLASSIFICATION

Ships

Edition July 2018

Part 6 Additional class notations

Chapter 5 Equipment and design features

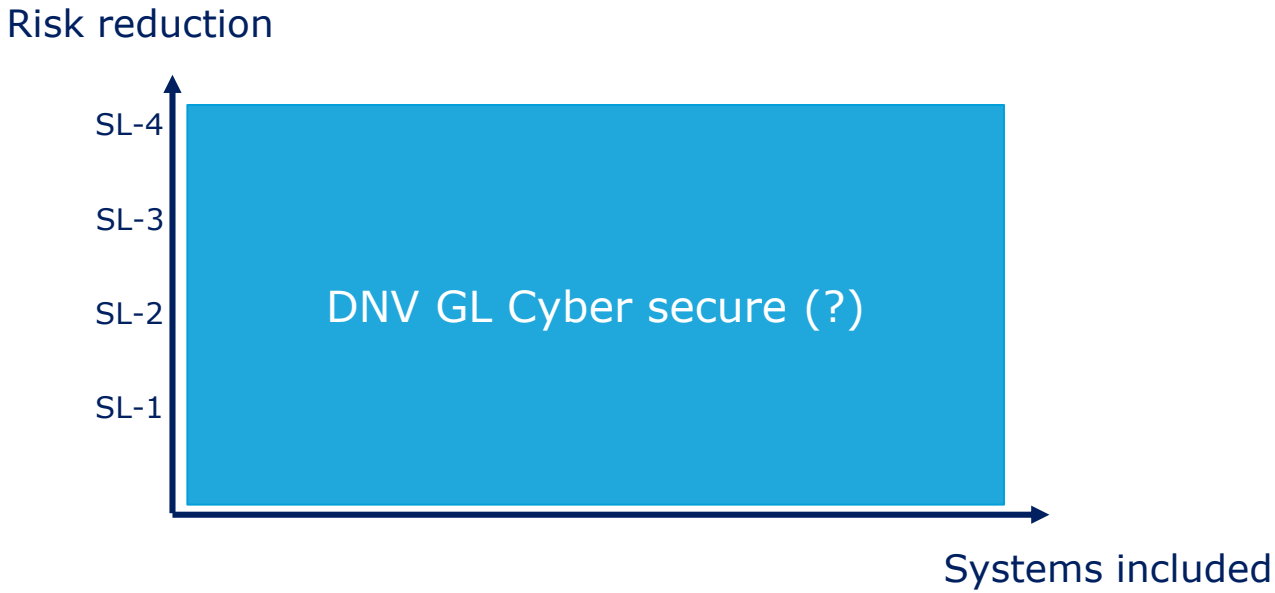
Section 21 Cyber Security

DNV GL AS

DNV GL AS

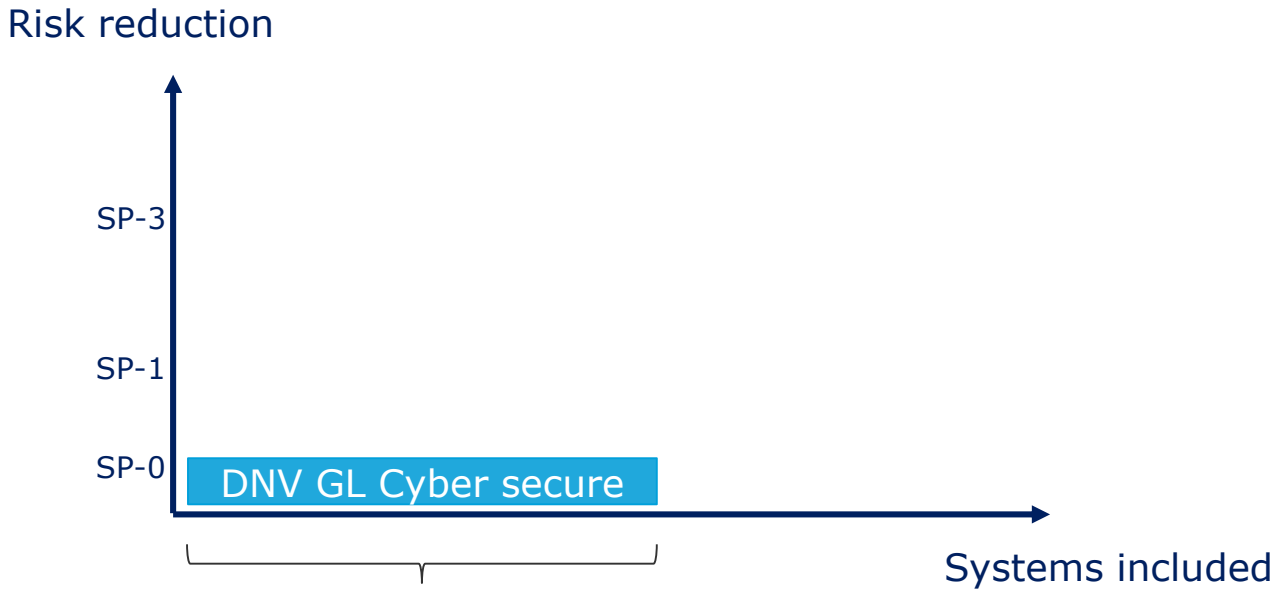
The DNV GL Cyber Security Class Notation “One size fit all”?

- Which systems to include?
- How much risk reduction is wanted/achievable?



The DNV GL Cyber Secure

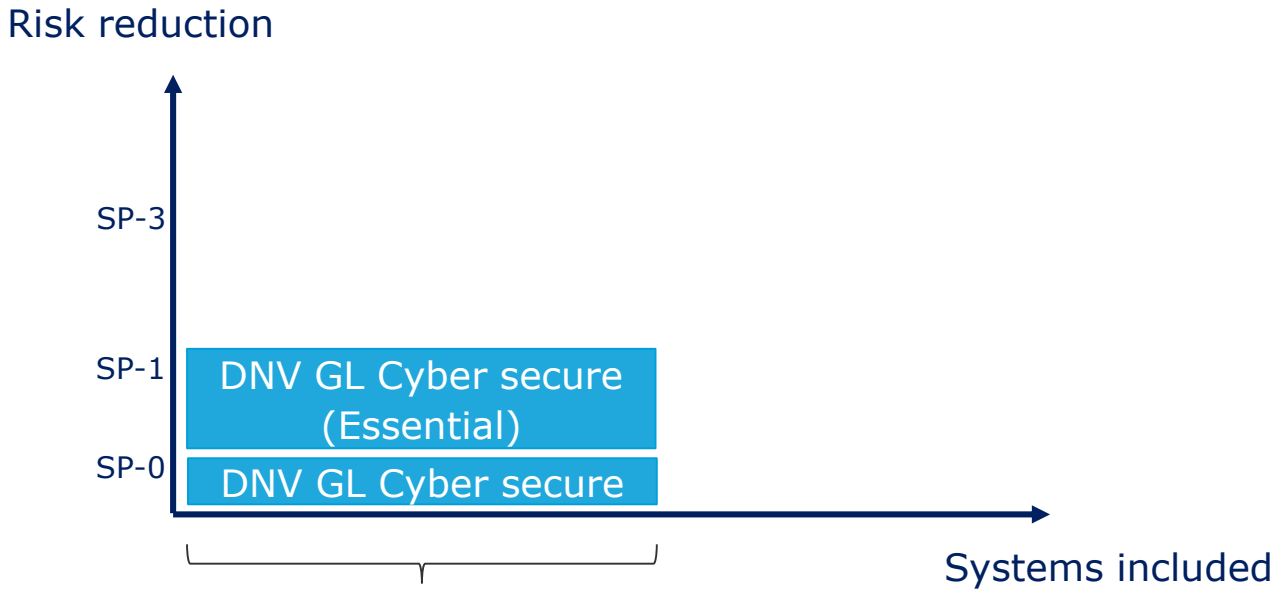
- Intended for NB + FIS
- Cover IMO.428(98) requirements
- Requires management system (CSMS) for FIS
- Focus on external barrier defence:
  - Zones and conduits
  - Remote access
  - Removable devices
  - Malware
  - Incident handling and reporting
- Limited in depth protection SP-0:
  - 8 requirements for 11 systems



Propulsion
Steering
Watertight integrity
Fire detection and mitigation
Ballasting
Thrusters not part of propulsion functions
Power generation supplying essential and important systems
Auxiliary systems for essential and important systems
Ignition source control
Navigation
Communication

The DNV GL Cyber Secure (Essential)

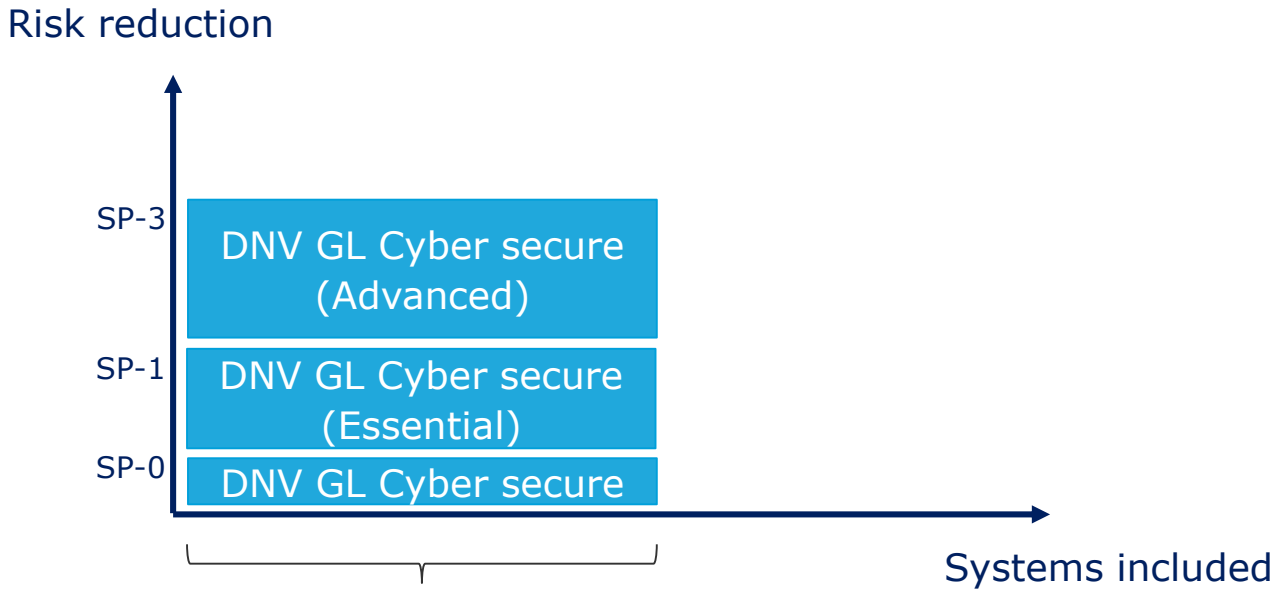
- Intended for NB + FIS
- Cover IMO.428(98) requirements
- Requires management system (CSMS) for FIS
- Barrier defence:
  - Zones and conduits
  - Remote access
  - Removable devices
  - Malware
  - Incident handling and reporting
- Essential in depth protection **SP-1**:
  - 46 requirements for 11 systems



Propulsion
Steering
Watertight integrity
Fire detection and mitigation
Ballasting
Thrusters not part of propulsion functions
Power generation supplying essential and important systems
Auxiliary systems for essential and important systems
Ignition source control
Navigation
Communication

The DNV GL Cyber Secure (Advanced)

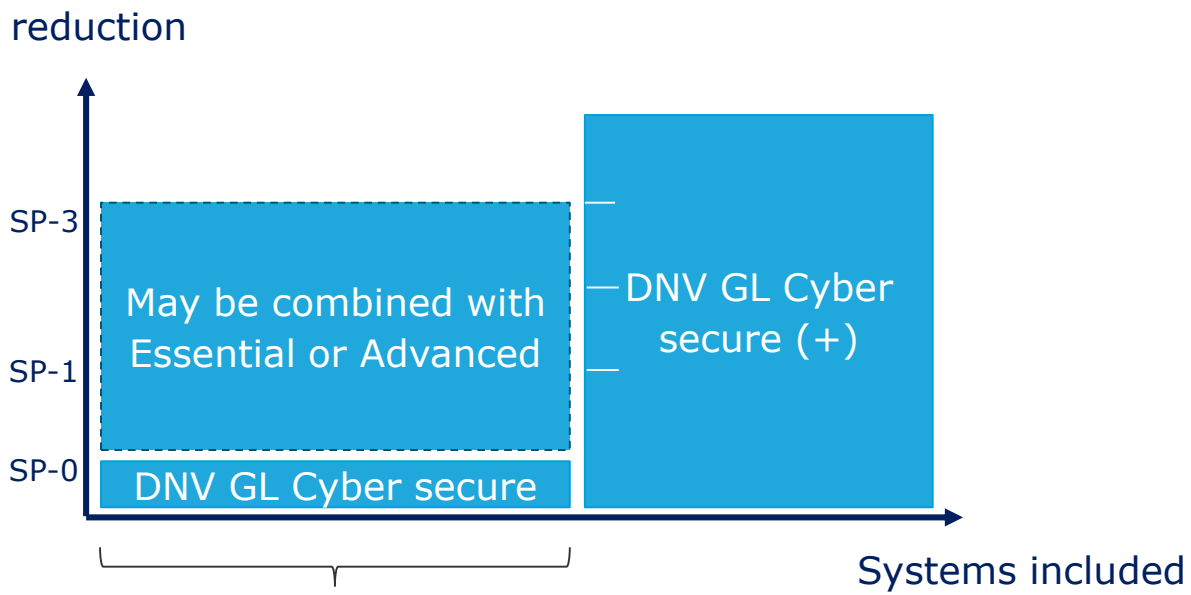
- **Intended for NB**
- Cover IMO.428(98) requirements
- Requires management system (CSMS) for FIS
- Barrier defence:
  - Zones and conduits
  - Remote access
  - Removable devices
  - Malware
  - Incident handling and reporting
- Advanced in depth protection **SP-3**:
  - 88 requirements for 11 systems



Propulsion
Steering
Watertight integrity
Fire detection and mitigation
Ballasting
Thrusters not part of propulsion functions
Power generation supplying essential and important systems
Auxiliary systems for essential and important systems
Ignition source control
Navigation
Communication

The DNV GL Cyber Secure (+)

- Intended for NB + FIS
- Cover IMO.428(98) requirements
- Requires management system (CSMS) for FIS
- Barrier defence:
  - Zones and conduits
  - Remote access
  - Removable devices
  - Malware
  - Incident handling and reporting
- Limited in depth protection SP-0 for 11 systems
- **In depth protection for systems included**
  - **SP 1-4 based on risk assessment**

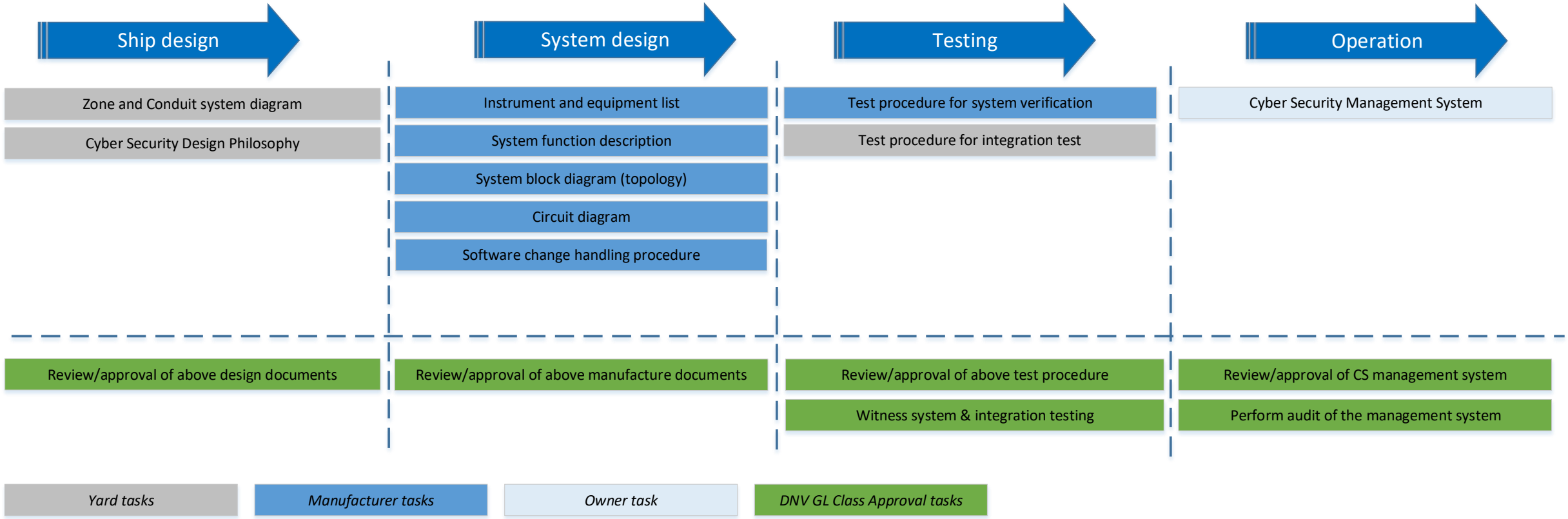


Propulsion
Steering
Watertight integrity
Fire detection and mitigation
Ballasting
Thrusters not part of propulsion functions
Power generation supplying essential and important systems
Auxiliary systems for essential and important systems
Ignition source control
Navigation
Communication

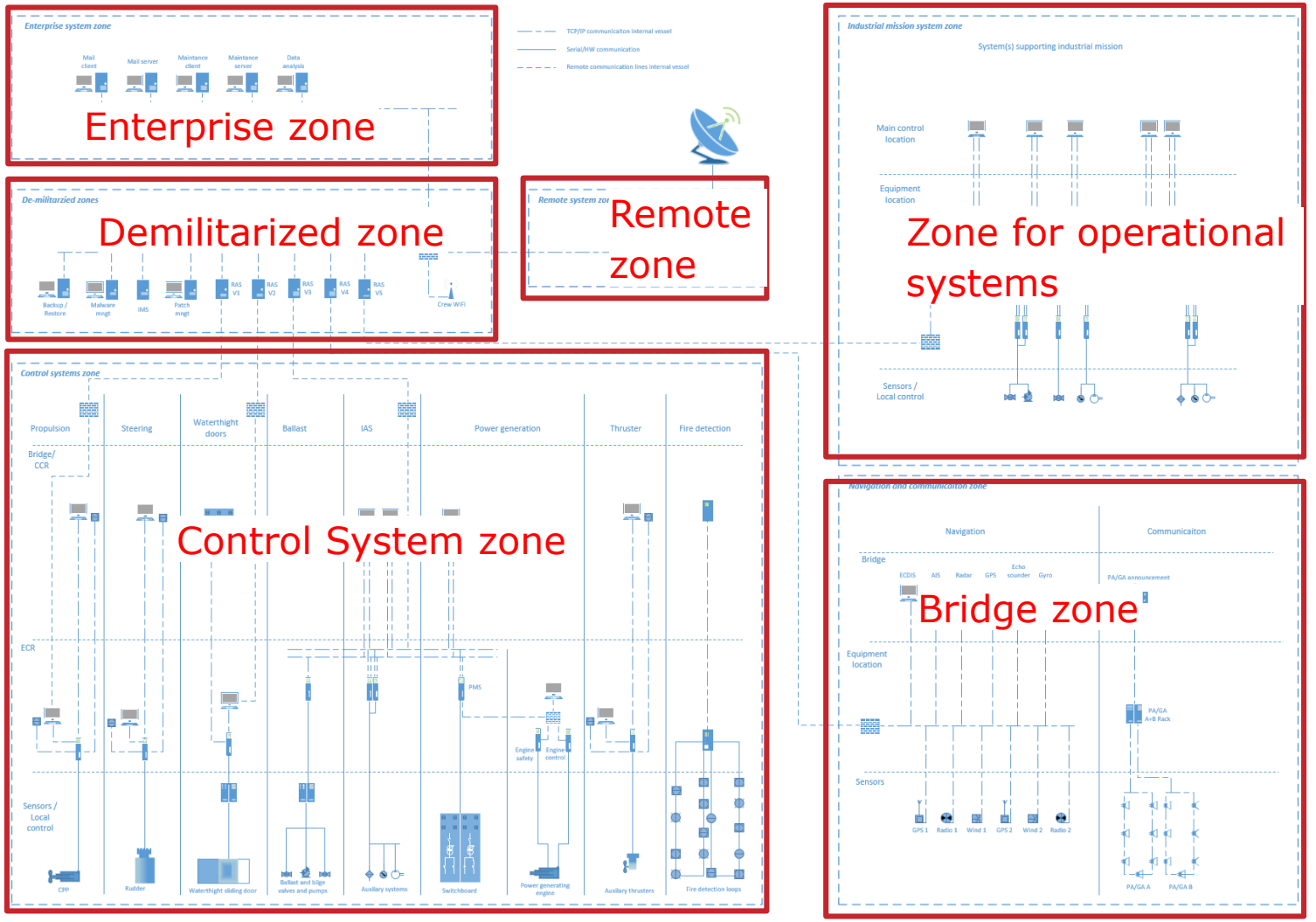
E.g.:

- **Cargo management system on tanker**
- **Oil production systems on FPSO**
- **Drill systems on drill-ship**
- **Passenger network on cruise-vessel**
- **….**

Required documentation/verification to obtain the DNV GL Cyber secure class notation



An example of a Zone and conduit drawing

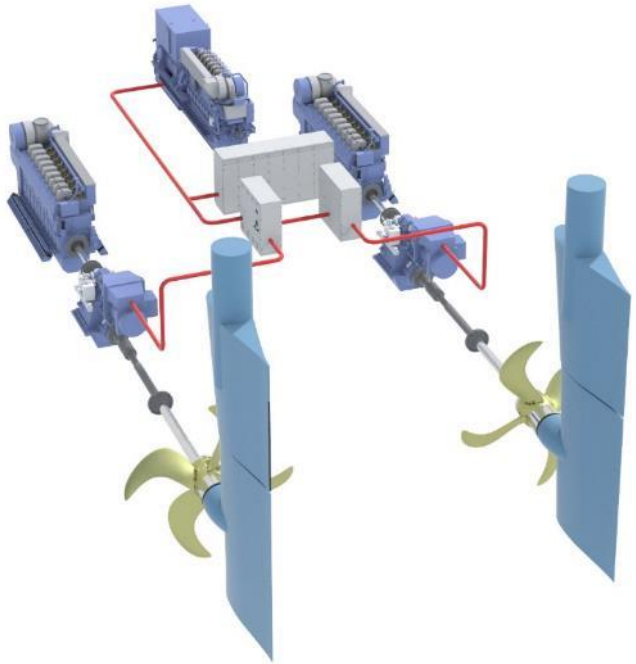


When defining system inventory, systems may be taken out of scope if "no attack surface":

5.2 Initial system selection

Cyber physical systems in [5.3] to [5.5] that possess any of the following capabilities, shall be subject t verification of security capabilities in these rules.

- remote connection (from outside the vessel)
- connected and/ or integrated (with other systems)
- possibility for software updates (of application and/ or operating systems).



Systems	Remote Connection	Connected /Integrated	Software Updates
Propulsion – CPP control system	X	N/A	X
Propulsion – RPM control system	X	N/A	X
Propulsion – Electrical propulsion thruster control system	X	N/A	X
Propulsion – Electrical propulsion drives (PTI/PTO)	X	N/A	X
Steering – Rudder control system	N/A	N/A	X
Steering – Azimuth thrusters control system	N/A	N/A	N/A
Steering – Electrical azimuth thruster drive	N/A	N/A	N/A
Power generation – Main engine control system	X	N/A	X
Power generation – Aux engine control system	X	X	X
Power generation – Aux generator control system	X	X	X
Power generation – Power management system	X	X	X

Classification – product certificate/type approval

- Classification of control, monitoring, alarm and safety systems consist of the following activities

1. Plan approval
2. Manufacturing survey/FAT

Product Certificate

3. New-building inspection
4. FIS survey

DNV·GL

REPORT FOR INCOMPLETE CERTIFICATION

Our ref: A0056120

Report of pending items to allow certification of the fo

Particulars of Product

Product Name: 4 x Control s

Type designation:

Application/context: Two Remote control syste

Serial/Tag no: N.A.

The product is intended for: MEYER WERI 34079

Requirements are based on: DNV Rules fo

The product / material has been marked: N1416R2S o

Particulars of Vendor and Purchaser

Vendor: ABB Oy, Mar

Vendor reference: CVX-003122

Purchaser: Meyer Werft

Purchaser reference:

Pending and / or non-conforming items are reported shall be followed up before DNV GL can issue a Produ

It is the responsibility of the vendor to take appropriate acti the pending / nonconforming items.

Form code: 71.04a Revision: 2015-10

© DNV GL 2014. DNV GL and the Horizon Graphic are trademarks of DNV GL AS.

DNV·GL

TYPE APPROVAL CERTIFICATE

Certificate No: TAA000026G
Revision No: 1

This is to certify:

That the Peripheral Equipment

with type designation(s)
CP604, CP607, CP610

Issued to
ABB Automation Products GmbH
Heidelberg, Baden-Württemberg, Germany

is found to comply with
DNV GL rules for classification – Ships, offshore units, and high speed and light craft

Application :

Product(s) approved by this certificate is/are accepted for installation on all vessels classed by DNV GL.

Type	Temperature	Humidity	Vibration	EMC	Enclosure
CP604	A	B	A	B	B - IP66 (front) / IP20 (rear)
CP607	A	B	A	B	B - IP66 (front) / IP20 (rear)
CP610	A	B	A	B	B - IP66 (front) / IP20 (rear)

Issued at Hamburg on 2019-02-01
This Certificate is valid until 2024-01-16.
DNV GL local station: Augsburg

for DNV GL

Approval Engineer: Marco Rinkel

Joannis Papanuskas
Head of Section

This Certificate is subject to terms and conditions overleaf. Any significant change in design or construction may render this Certificate invalid.
The validity date relates to the Type Approval Certificate and not to the approval of equipment/systems installed.

Form code: TA 251 Revision: 2016-12 www.dnvgl.com Page 1 of 4

© DNV GL 2014. DNV GL and the Horizon Graphic are trademarks of DNV GL AS.

Overview of Advisory Services – Assessment

On-board assessment

Crew behaviour

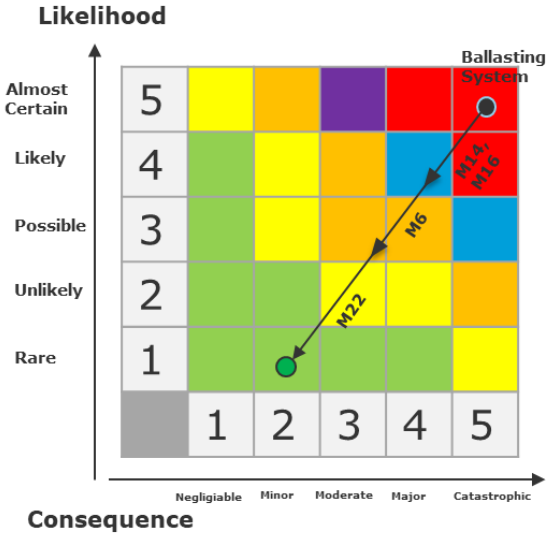
Roles and responsibillities

Testing of network & systems

3rd party equipment and behaviour

Ship-shore connection (VSAT, VPN)

Cyber risks assessment

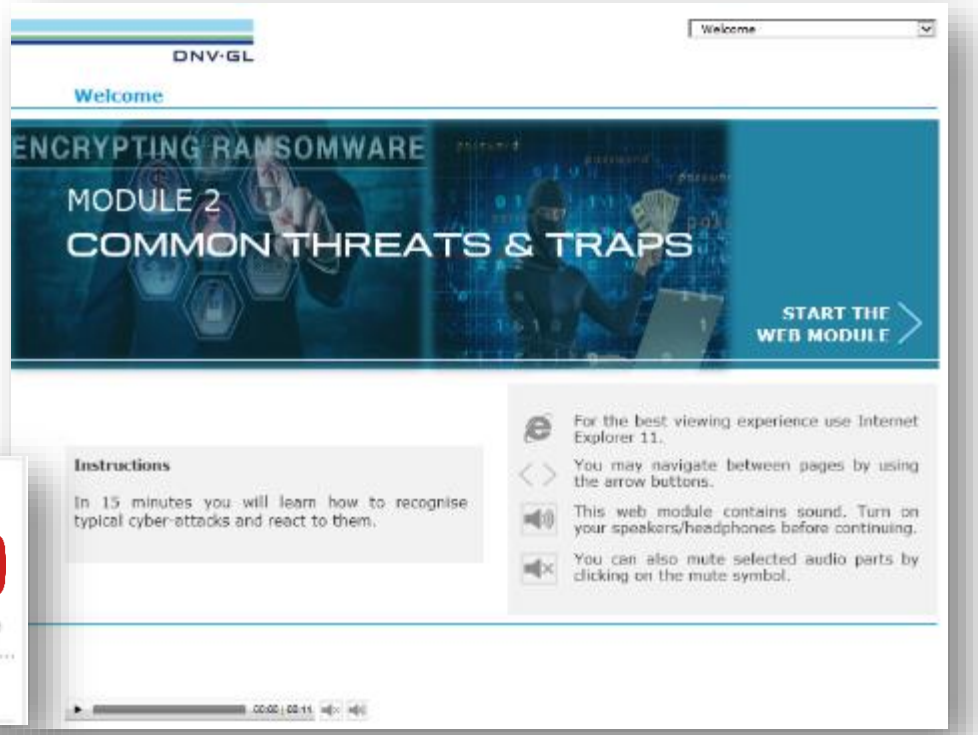


System group	R
Ballasting system	25
Propulsion & steering system	25
Power generation systems	20
Navigation planner	20
Stability Monitoring system	20
Man overboard system/CCTV	16
Muster Evacuation Monitoring	16
Energy management system	16
Environmental systems	16
Position fixing and navigation systems	16
Hospitality management	16
Security systems	16
Security Incident Report Platform	16
Emergency power systems	15
Inventory system	12

Promoting Cyber Security awareness is easy through e-learning

- Module 1: How you can help protect yourself and your organisation (10min)
- Module 2: Common threats & traps (15min)
- Module 3: Best practices (15min)
- Module 4 : Advanced defence in depth course (20min)

Available through our on board solution distributor Seagull



Penetration testing of OT systems

Vulnerability spot-checking of most critical IT/OT systems using white/grey box testing

OT penetration testing:

- Deep system and domain knowledge necessary
- Tailored configurations and bespoke protocols
- Often fragile and safety critical systems