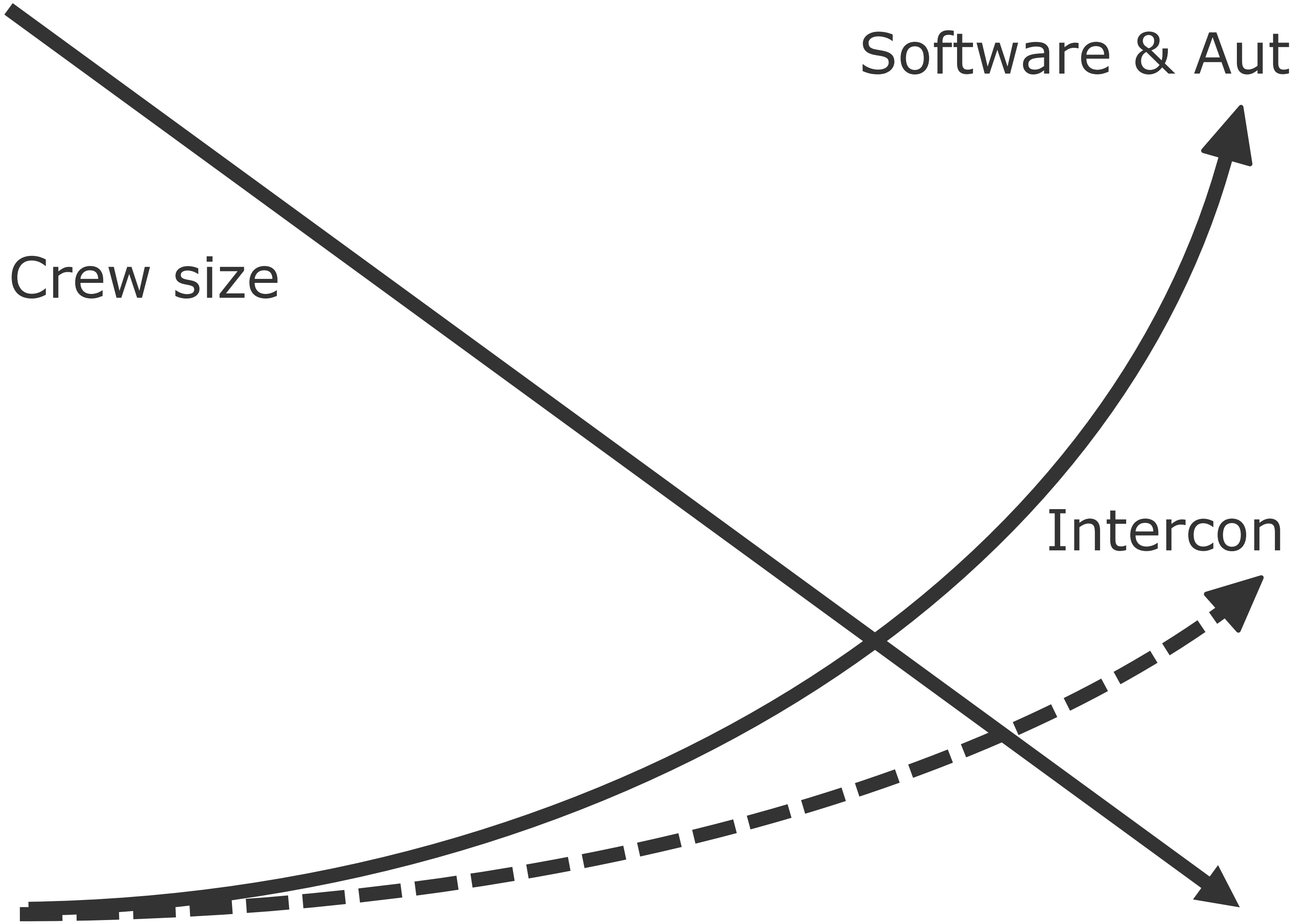
Safe & Secure Ship Design and Operation in a complex Cyber World

DNV GL Maritime

Why is Cyber Security relevant for ship safety?

Maritime & Offshore trends – More complexity

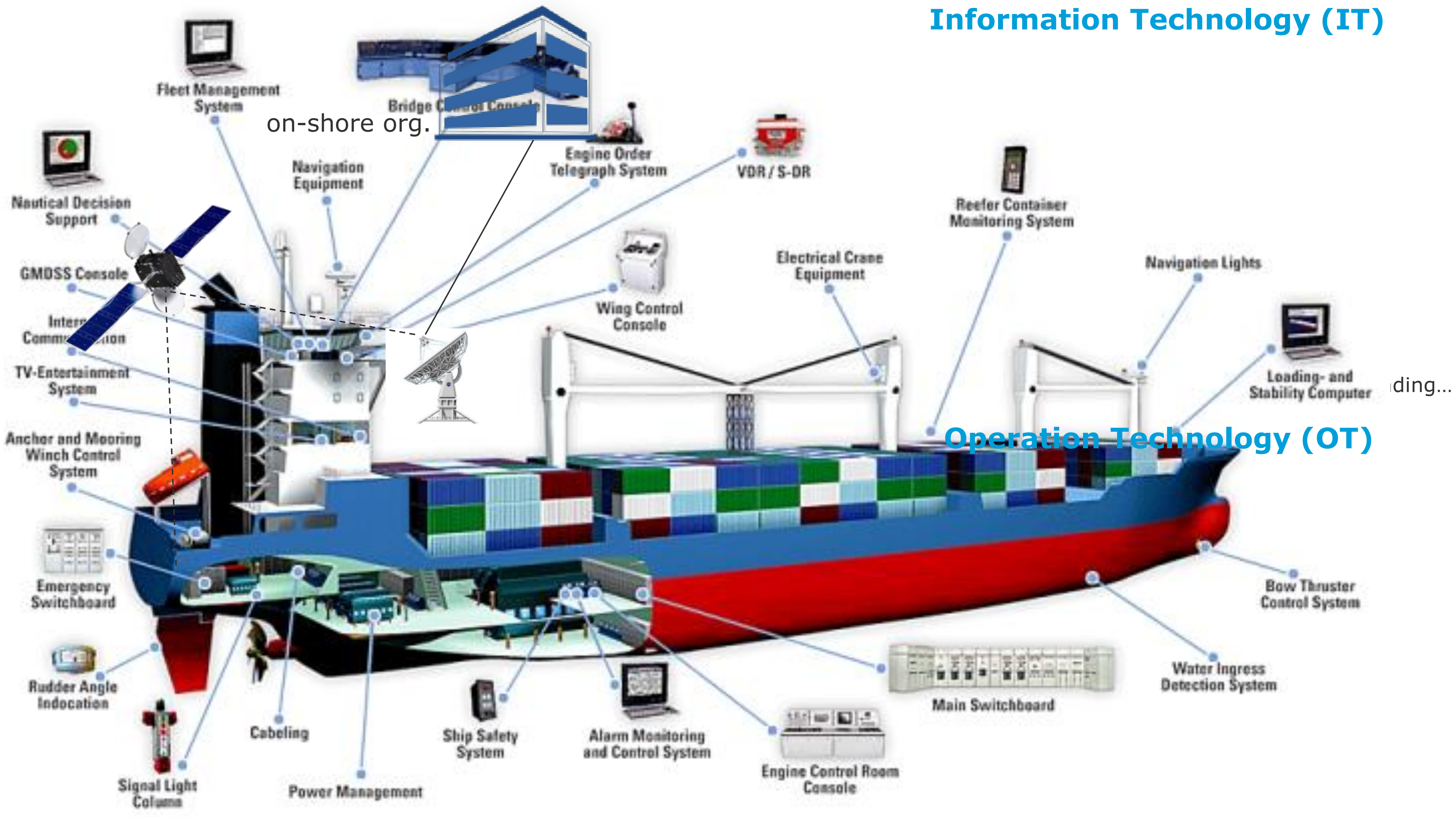


Software & Automation

Crew size

Interconnectivity

Safety in shipping today heavily depends on cyber systems



Information Technology (IT)

At risk:

Mainly finance and reputation

Operation Technology (OT)

At risk:

Life, property and environment

+

all of the above

Pirates 1.0 → 4.0

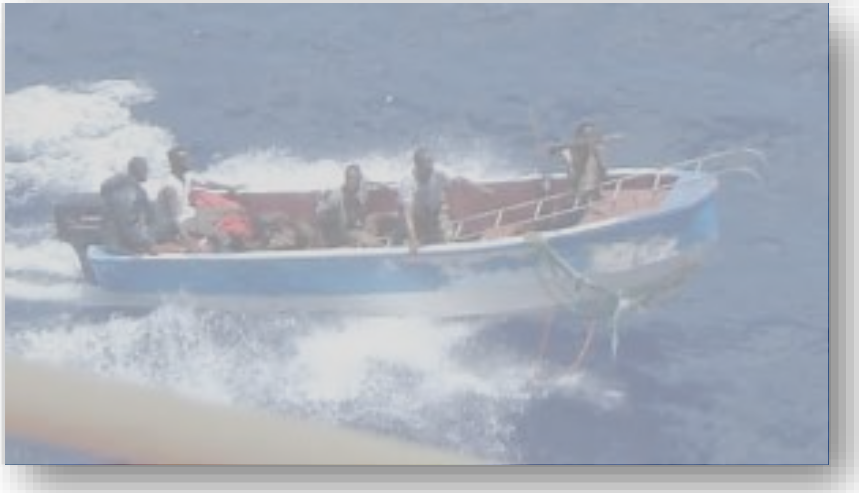


Photo: Shutterstock

WannaCry: Large ransomware attack on IT systems globally

Known affected organisations:

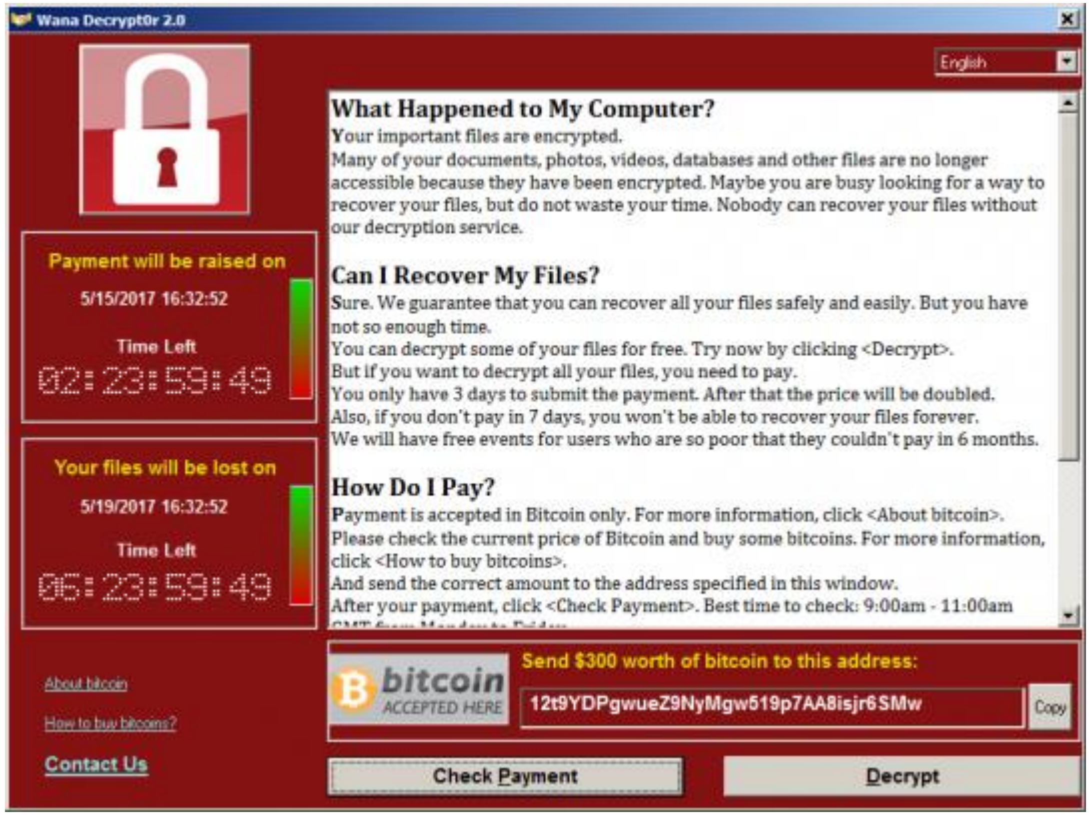
- Spain - Telefonica, power firm Iberdrola, utility provider Gas Natura and more large firms

- USA - FedEx,

- France - Renault,
- Germany - Deutsche Bahn
- Britain's National Health Service
- Nissan car plant

- Jakarta- Two hospitals
- A Russian Ministry

- China – 20,000 gas stations



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

"The latest count is over 200,000 victims in at least 150 countries"

- Rob Wainwright, Europol Executive Director

Reported incidents around the world is increasing

False GPS signals transmitted by attacker
Ballasting
Planned Maintenance Software

Loss of fuel control 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

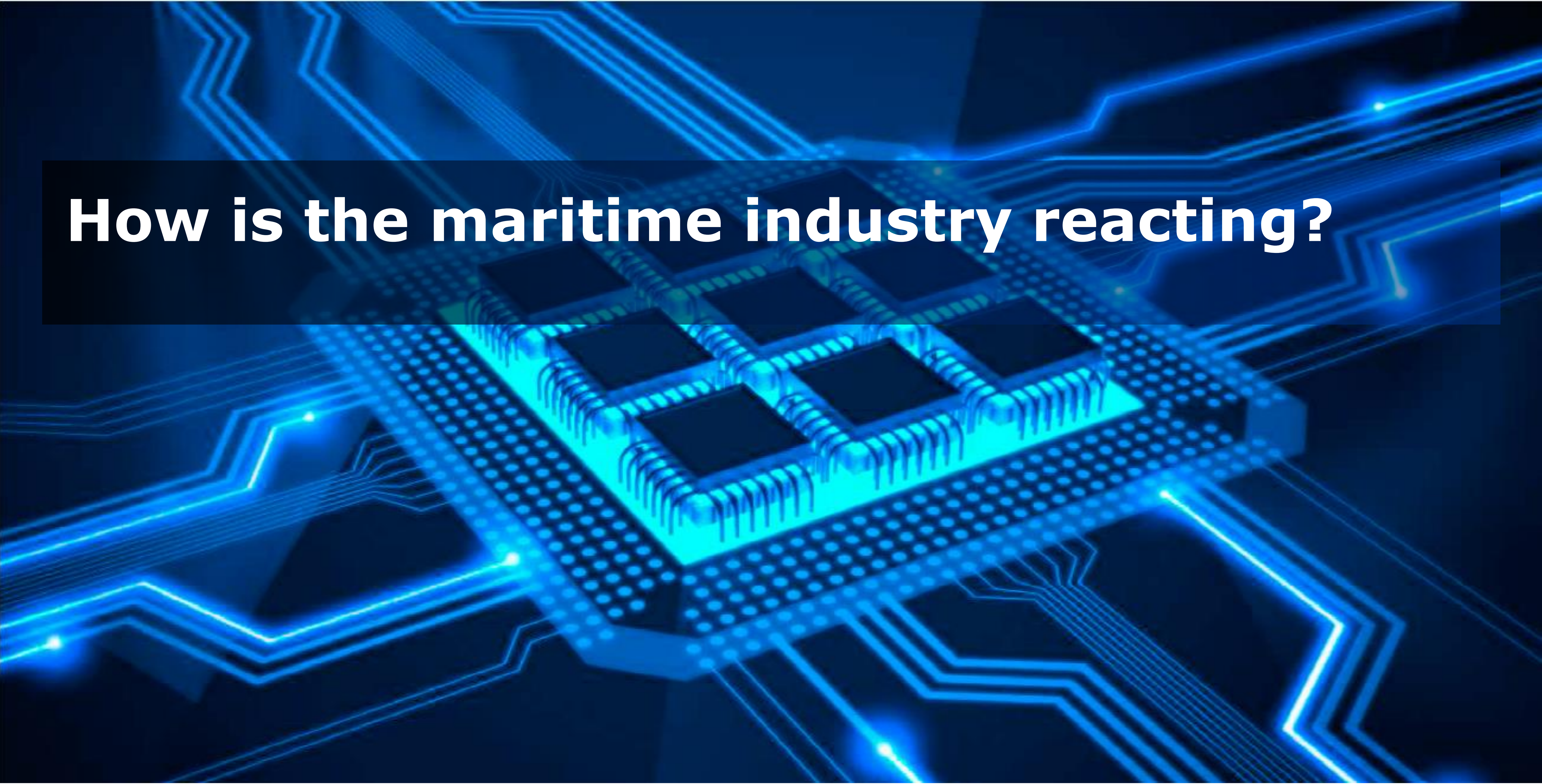
Loss of main switchboard due to ransomware

Malware allows full access to vessel systems

Hackers took “full control” of navigation systems for 10 h

Hacking of cargo tracking system for smuggling purposes

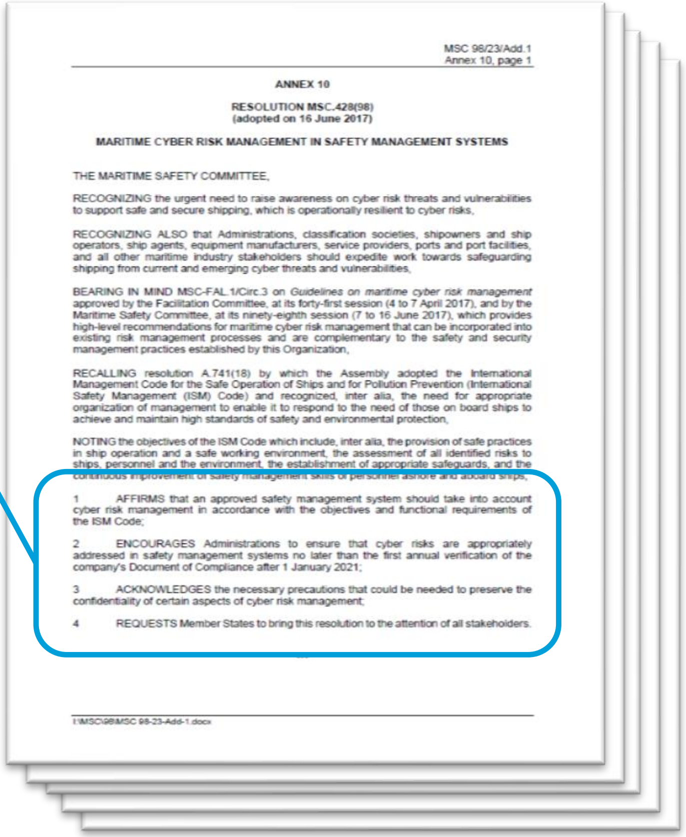
NotPetya cause Maersk upto USD 300m loss



How is the maritime industry reacting?

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

- 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 98/23/Add.1
Annex 10, page 1

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

I:\MSC\98\MSC 98-23-Add-1.docx

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.

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

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 through:

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

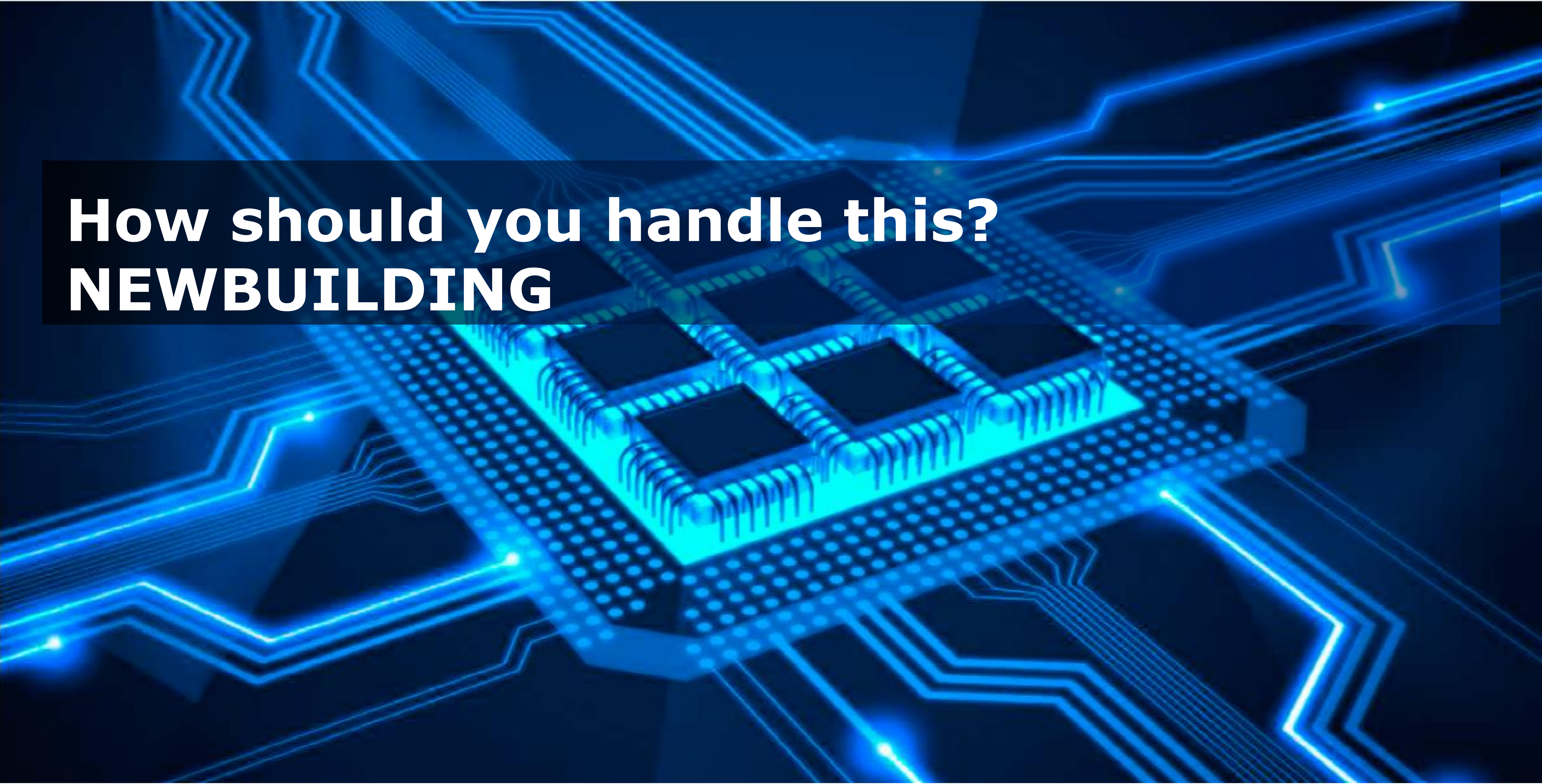
and

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

OCIMF

Oil Companies International Marine Forum

RIGHTSHIP

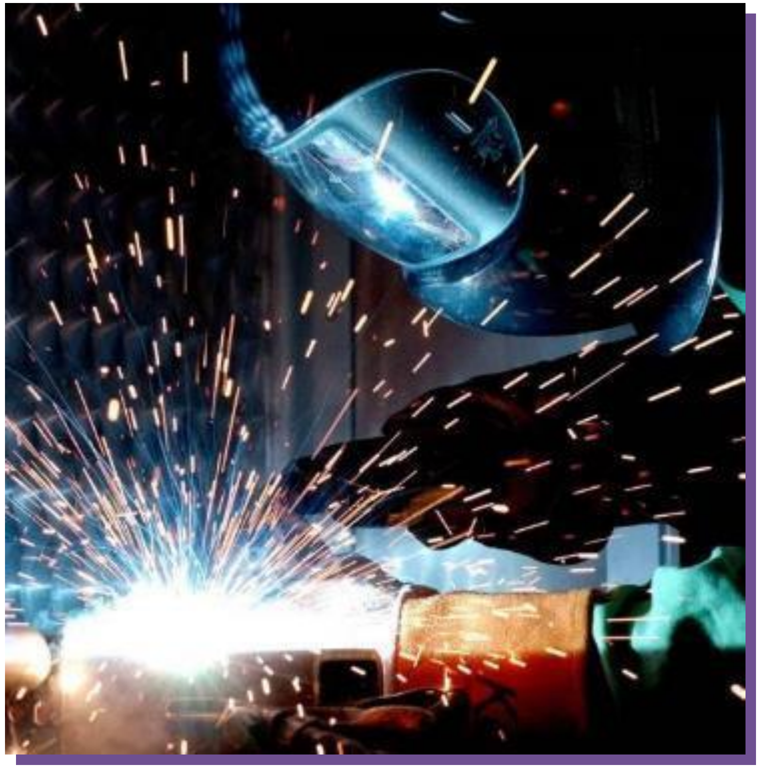


How should you handle this? NEWBUILDING

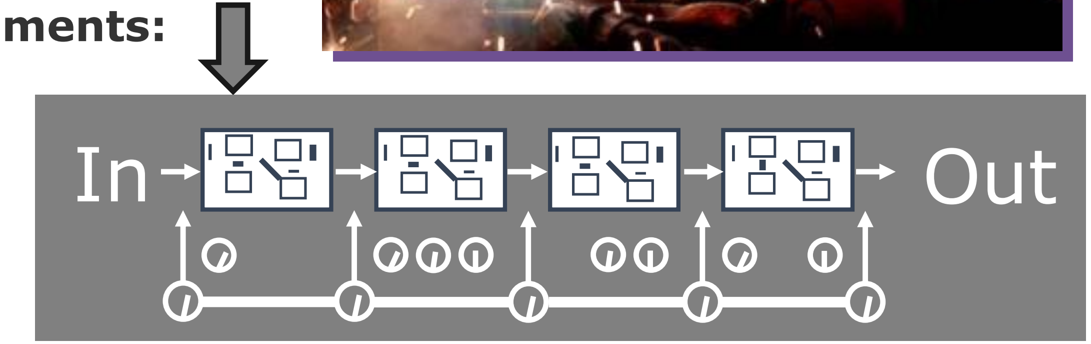
OT track assessments: using a common language for cyber systems engineering

How to control EMERGENT properties?

When welding is introduced to a structure, how is the reliability of the weld controlled?



There are known quality control steps and expected traceable documents:

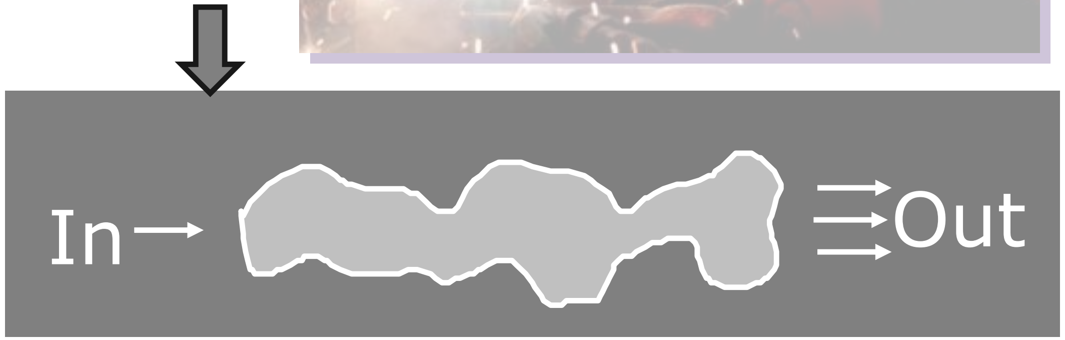


OT track assessments: using a common language for cyber systems engineering

How to control EMERGENT properties?

When welding is introduced to a structure, how is the reliability of the weld controlled?

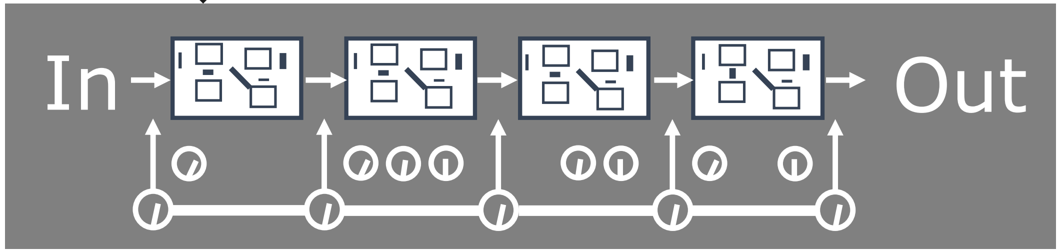
When software is introduced, then what?



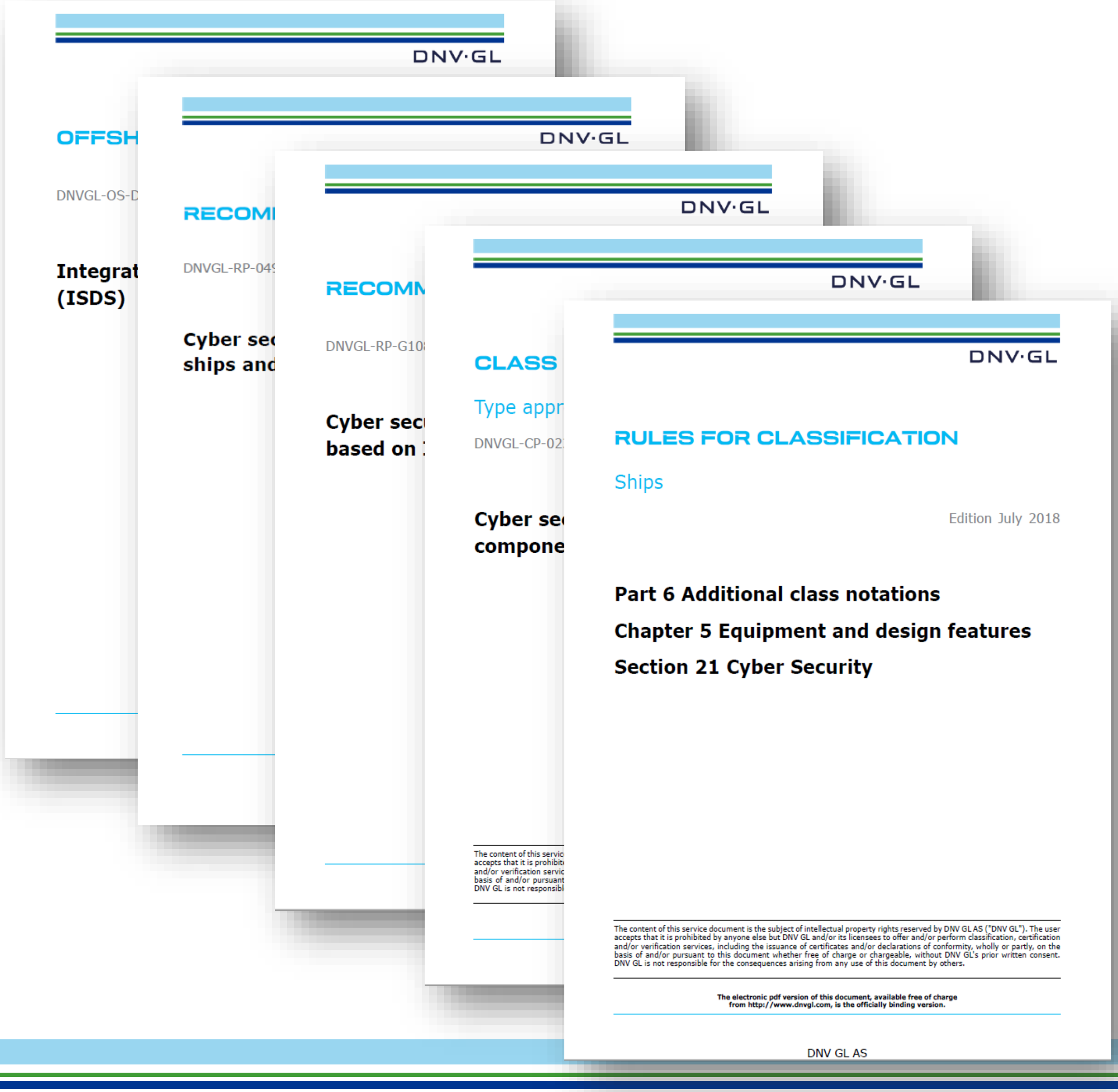
OT track assessments: using a common language for cyber systems engineering

The DNV GL rule set 'ISDS' (Intergraded Software Dependent Systems) is a standard Cyber Systems Engineering framework made for Maritime & Offshore

The trick is to breakdown the cyber process <u>best practices</u> in <u>roles</u> and <u>stages</u>:



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



DNV·GL

OFFSH

DNVGL-OS-D

Integrat
(ISDS)

DNV·GL

RECOM

DNVGL-RP-049

Cyber sec
ships and

DNV·GL

RECOMN

DNVGL-RP-G10

Cyber sec
based on

DNV·GL

CLASS

Type appr

DNVGL-CP-02

Cyber se
compone

DNV·GL

RULES FOR CLASSIFICATION

Ships

Edition July 2018

Part 6 Additional class notations

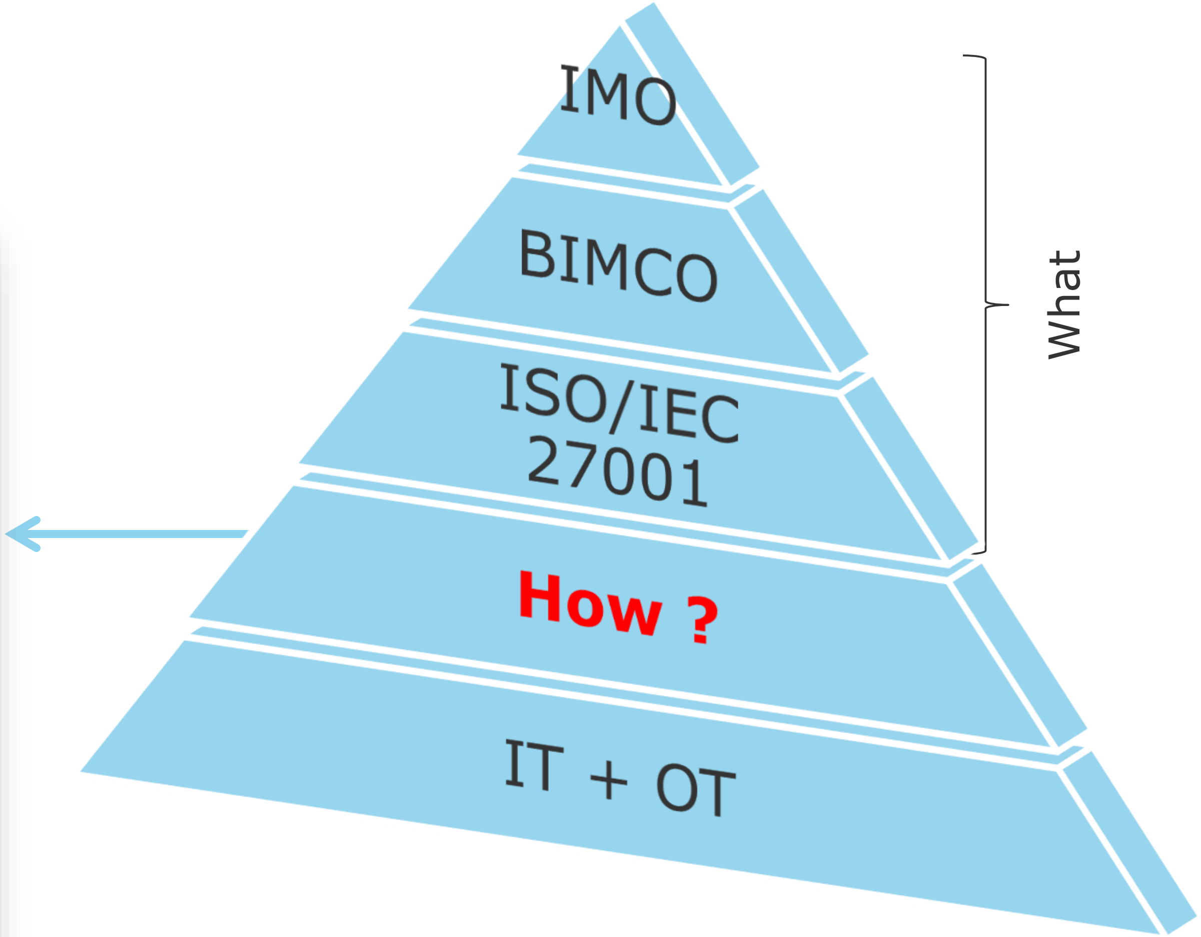
Chapter 5 Equipment and design features

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



IMO

BIMCO

ISO/IEC 27001

How ?

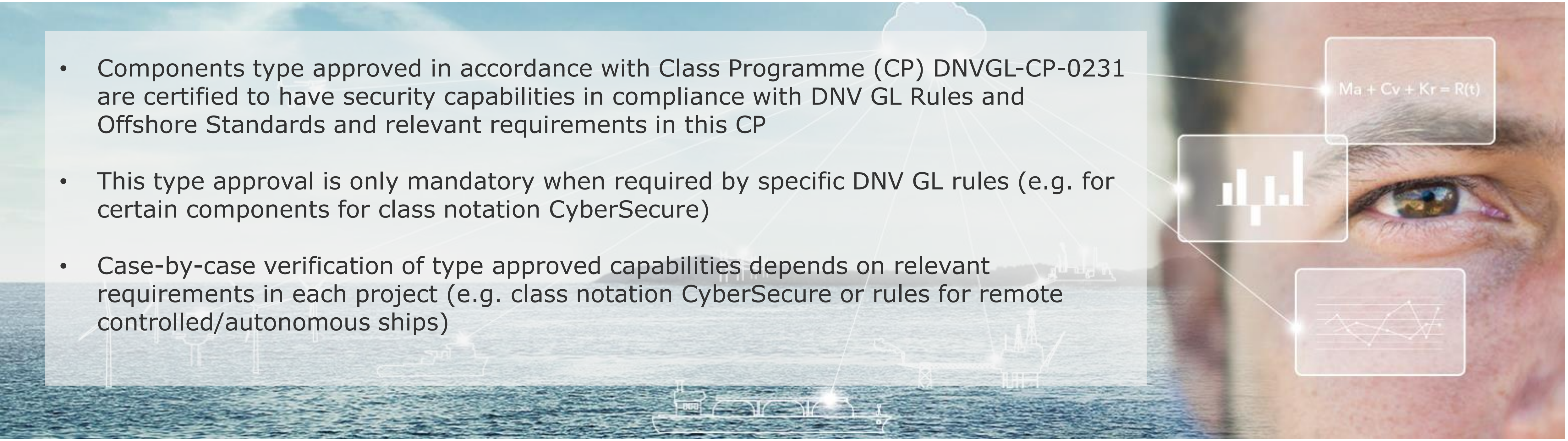
IT + OT

What

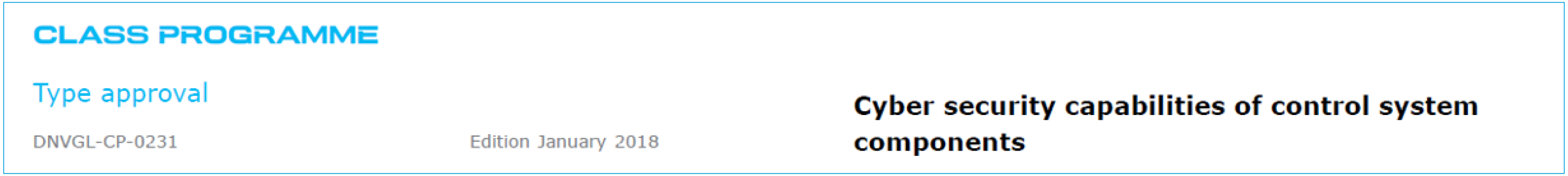
DNV GL Cyber Security Type approval

DNVGL-CP-0231

Cyber security type approval



- 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)


CLASS PROGRAMME

Type approval

DNVGL-CP-0231

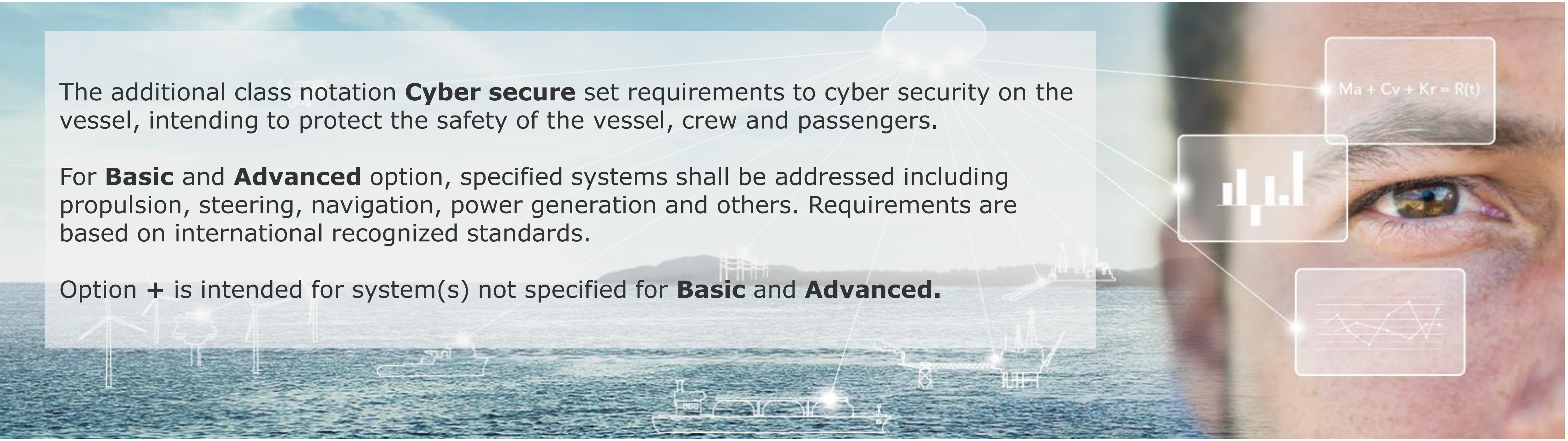
Edition January 2018

Cyber security capabilities of control system components

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

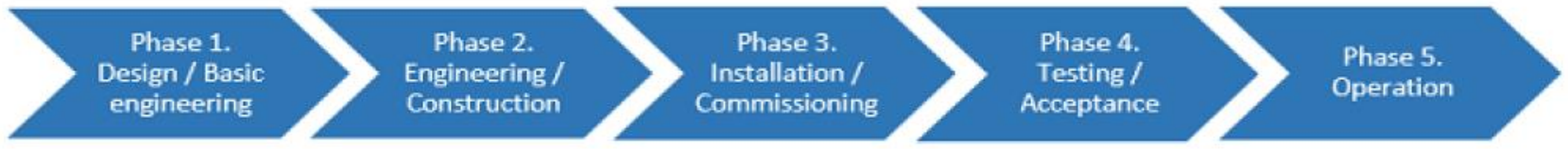
Cyber secure(+)

Security level based on risk assessment

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

Design verification and assessment for new building versus sailing vessel

Phases for implementing cyber security for a new build vessel



Phase 1. Design / Basic engineering

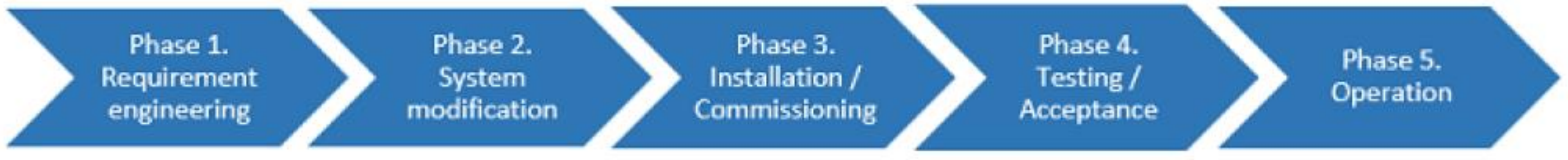
Phase 2. Engineering / Construction

Phase 3. Installation / Commissioning

Phase 4. Testing / Acceptance

Phase 5. Operation

Phases for implementing cyber security on a sailing vessel



Phase 1. Requirement engineering

Phase 2. System modification

Phase 3. Installation / Commissioning

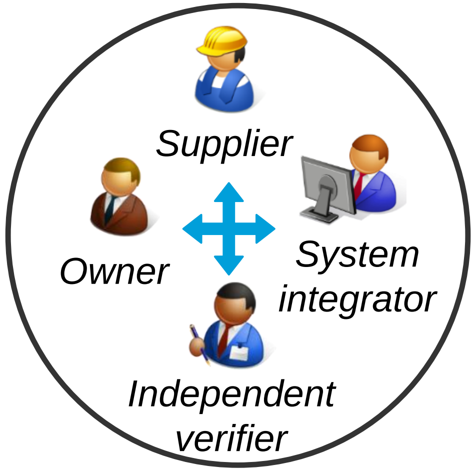
Phase 4. Testing / Acceptance

Phase 5. Operation

Cyber Security verification project of RCL mega cruise ships

Symphony of the Seas

Celebrity Edge



"Using the proposed methodology, we can address cyber security threats together with the vendors, and that is something we were never able to do before. ***This is the first time in this industry*** *that we can achieve this level of* ***communication and collaboration from the yard and the vendors to effectively resolve cyber-security-related*** *questions and issues during newbuilding, and do this as an integrated team."*

Will Perez, Cyber Security Director for Royal Caribbean Cruises

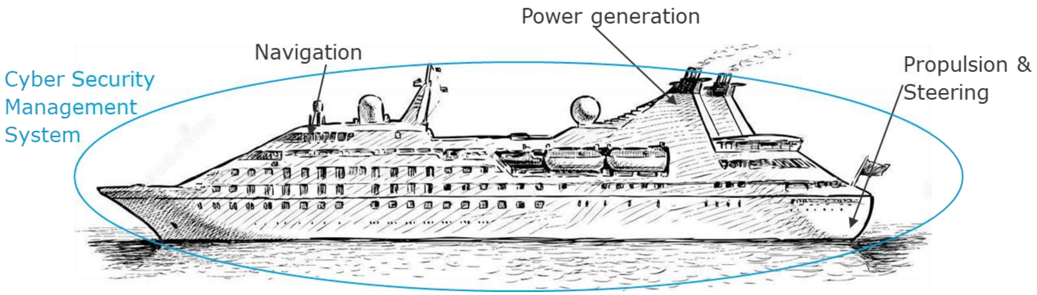
"The on-board penetration testing executed by DNV GL's ethical hackers has not only allowed us to detect cyber security weaknesses that we could fix in time, but once fixed, ***it has also helped with the troubleshooting of other unrelated network issues we were having****, so this has actually saved us a lot of time."*

Thierry Gambier, Fire & Safety System Engineer for STX France

Where to start in newbuilding: Cyber secure class notation for ships & Cyber Secure Type Approval for components

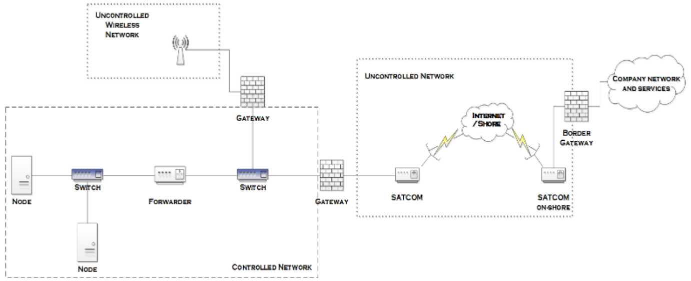
Cyber Secure Class Notation

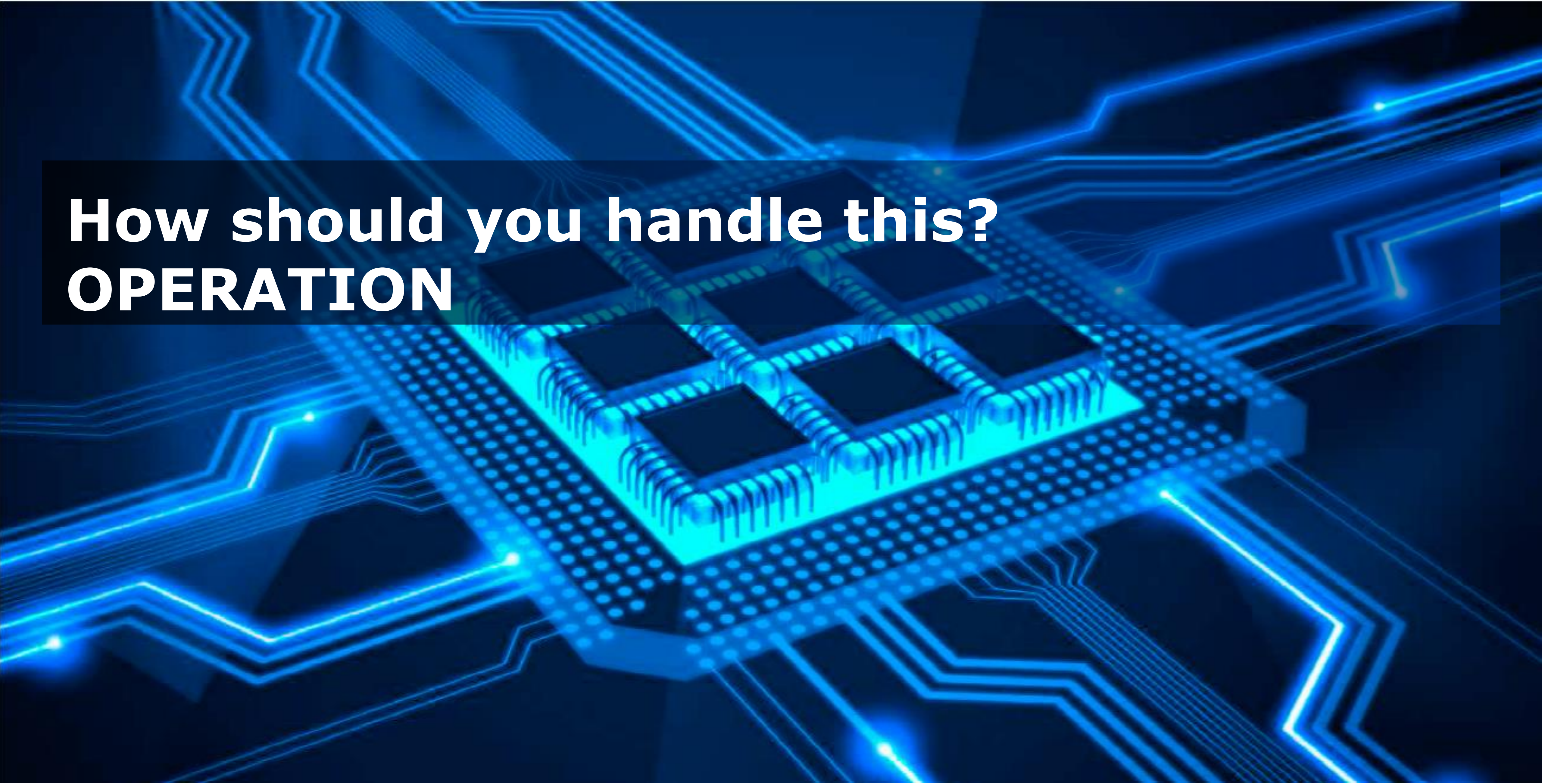
- Notations build on the **DNV GL Recommended Practices** on cyber security, which provide guidance on how to apply ISO/IEC-27001 and ISA-99/IEC-62443 standards in shipping
- **Cyber Secure Basic** is for **ships in operation**
- **Cyber Secure Advanced** is for **newbuilds**
- **Cyber secure (+)** is intended for additional systems beyond navigation, power generation, propulsion and steering



Cyber Secure Type Approval

- Components type approved in DNVGL-CP-0231 are certified to have security capabilities
  - 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





How should you handle this?
OPERATION

Three pillars of Cyber Security all crucial to ensure an holistic cyber resilience

Process

- Management Systems
- Governance Frameworks
- Policies & procedures
- Vendor/Third party contracts-follow up
- Audit regimes

People

- Training & Awareness
- Professional skills & qualifications
- Emergency drills
- Authorizations & authentication
- Physical Security

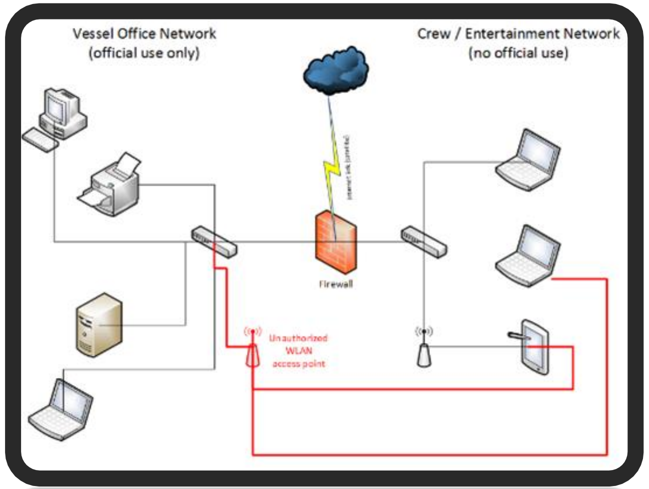
Technology

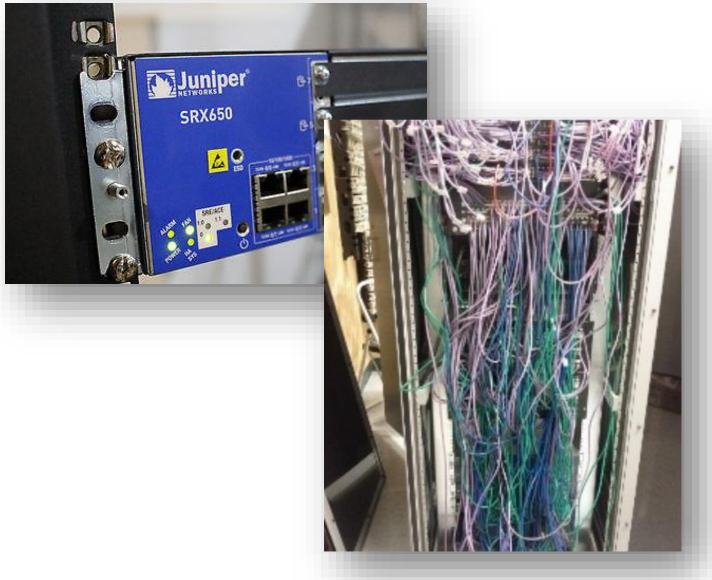
- System design
- Hardening of connections
- Software configuration
- Encryption protocols
- Jamming & spoofing
- Detection & monitoring

An On-board Cyber Security Assessment is a good starting point for uncovering gaps toward best practice cyber resilience

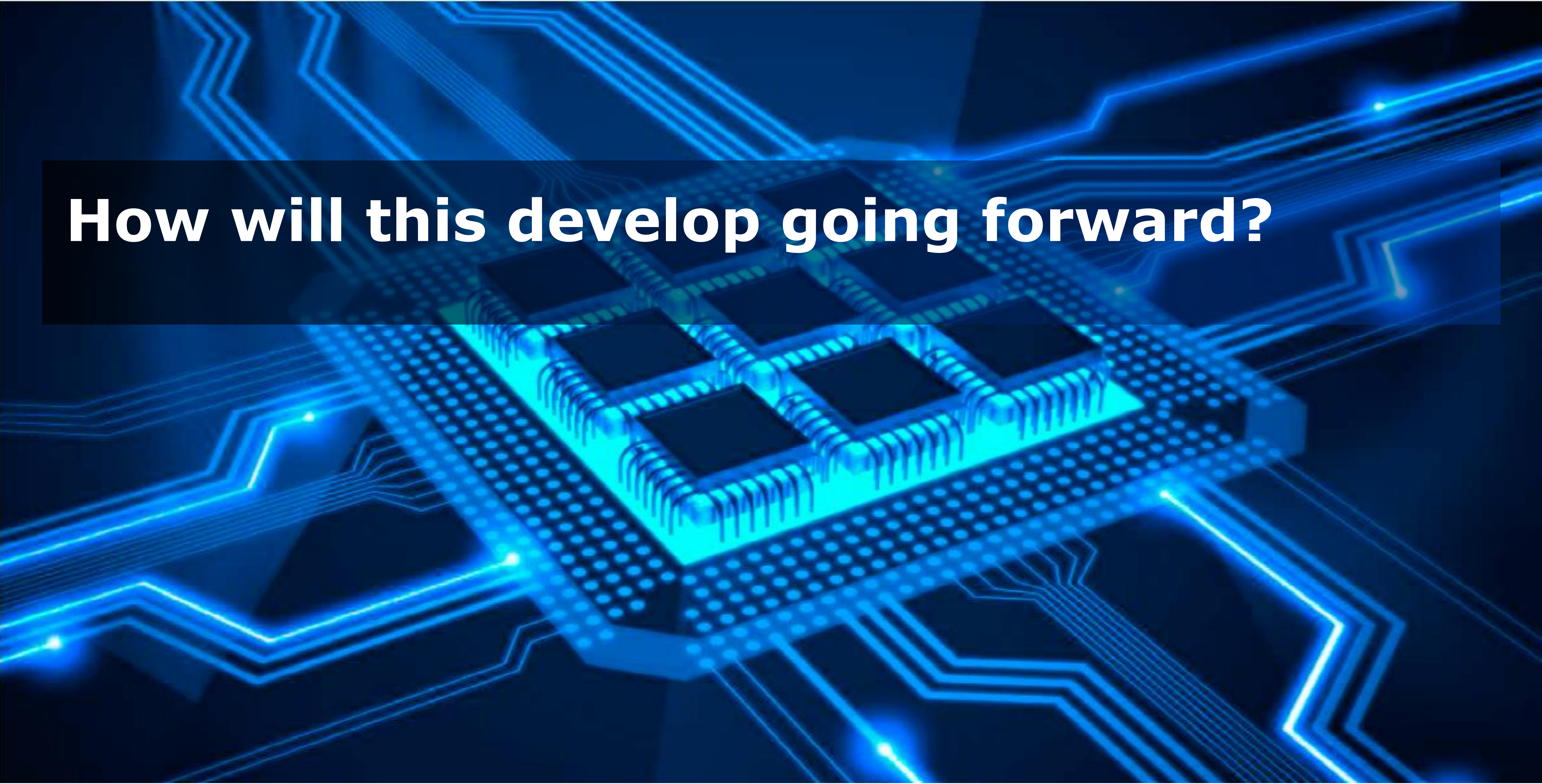
Interviews and spot checking (comparing the current safeguards with target protection levels):

- against policy, procedures, responsibilities and competence
- existence of controls and barriers





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



How will this develop going forward?

The “next” future holds more… with further increase of the attack surfaces

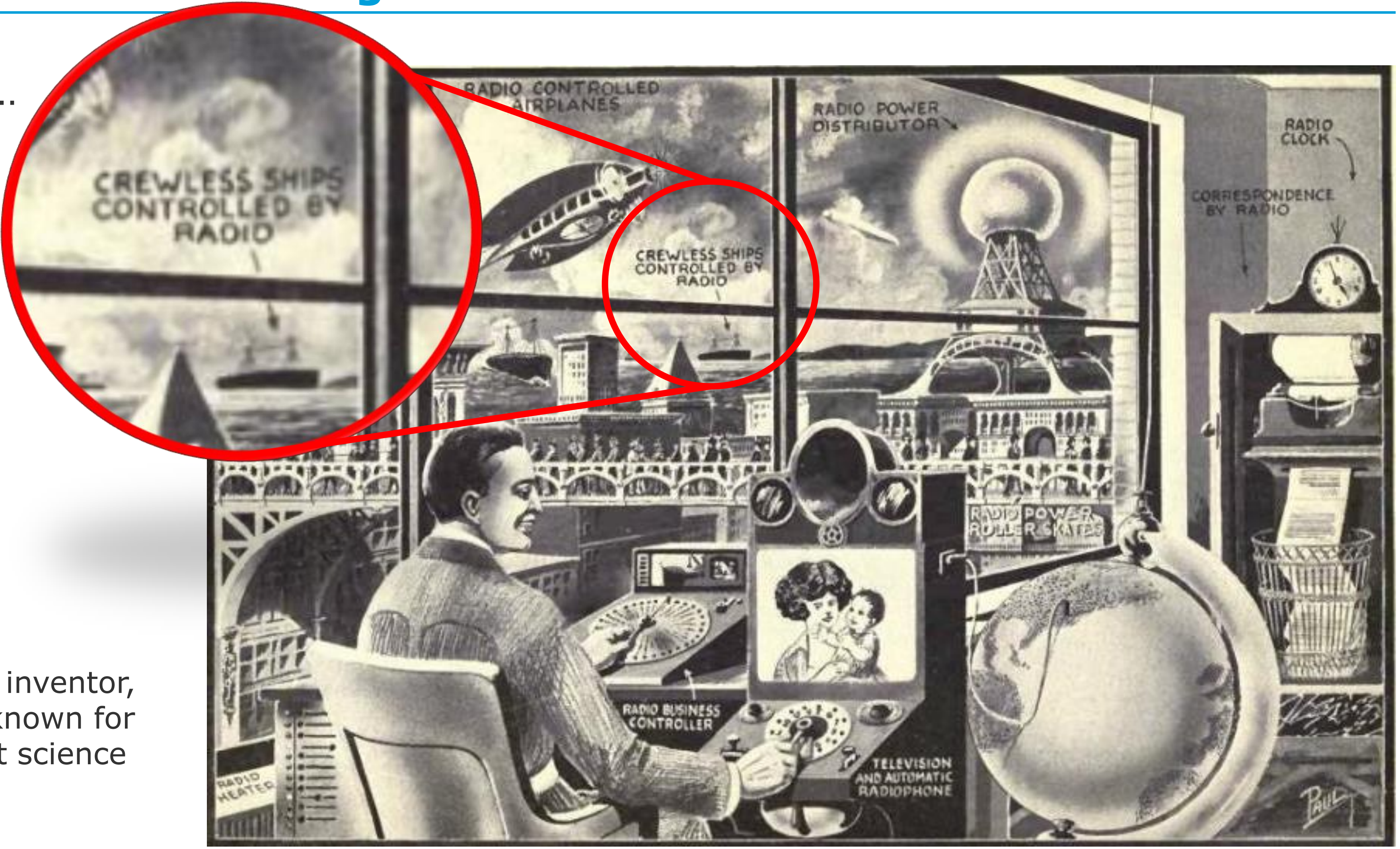
Digital wearables for crew

Crew members receive relevant alerts and notifications on their mobile devices in real time. The same data is available to the company’s shore-based staff.

Enhancing passenger experience

How did the future look like 100 years ago…
…future is here and need to be managed!

Notice what has come true…


CREWLESS SHIPS CONTROLLED BY RADIO
RADIO CONTROLLED AIRPLANES
RADIO POWER DISTRIBUTOR
RADIO CLOCK
CORRESPONDENCE BY RADIO
CREWLESS SHIPS CONTROLLED BY RADIO
RADIO POWER ROLLER SKATES
RADIO BUSINESS CONTROLLER
TELEVISION AND AUTOMATIC RADIOPHONE
RADIO HEATER
PAUL

Hugo Gernsback (1884-1967) inventor, writer, editor, publisher, best known for publications including the first science fiction magazine.

DNVGL’s recommendation to build cyber security defences

Based on our experience the owners/operators should address:

- **Technology**: Network segregation, Access control, Hardening of systems, Back-up, Malicious Software Prevention, Threat intelligence and Intrusion detection
- **People**: Awareness, Behaviour, Tasks, Responsibilities, Training & Drills
- **Process**: Cyber risk policy and objectives, Risk assessment, Management of Change (software and hardware), Software configuration, Incident management

- For more guidance see DNV GL Cyber Secure Class Notation and our Class Programme for type approval

Process
People
Technology

DNV·GL

CLASS

Type appr

Cyber se
compone

DNV·GL

RULES FOR CLASSIFICATION

Ships

Edition July 2018

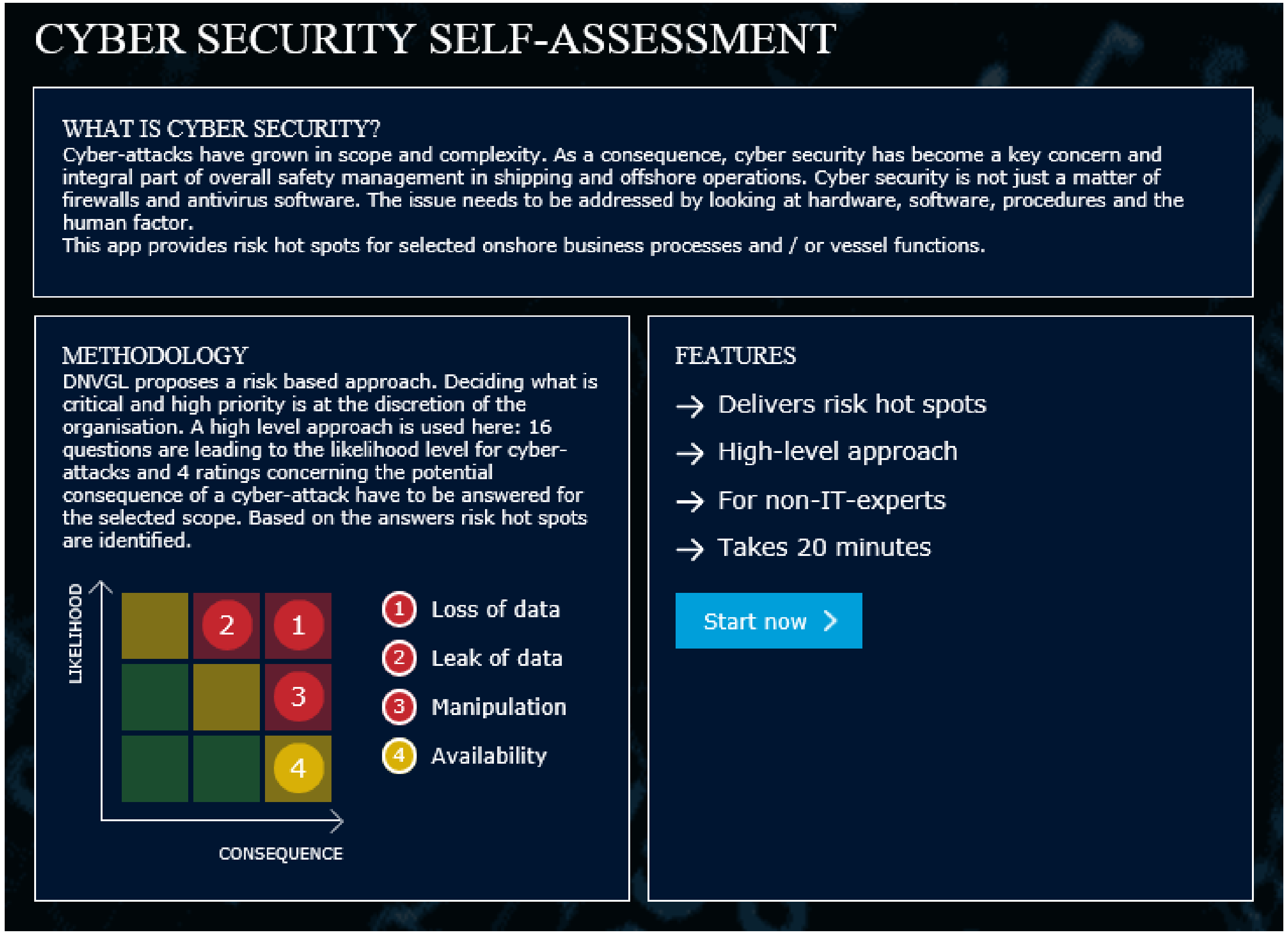
Part 6 Additional class notations

Chapter 5 Equipment and design features

Section 21 Cyber Security

DNV GL AS

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

Start now >

Self assessment can be found here:

https://www.dnvgl.com/maritime/cyber-security-self-assessment.html

Follow instructions

Thank you very much for you attention!

Jan Tore Grimsrud

Head of Section

Control & Bridge Systems/Cyber Safety & security

DNV GL Maritime

Jan.Tore.Grimsrud@dnvgl.com

+47 930 30449

www.dnvgl.com

SAFER, SMARTER, GREENER