



**▶ WEBINAR**

# Maritime Cyber Security for Ship Owners and Managers

 **25TH MAY 2022**

 **11 AM, CET**



**ORGANISED BY:**



**Varuna Marine Services**  
Smart Sustainable Shipping



# MODERATORS



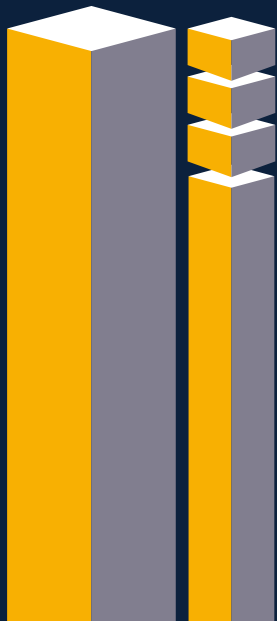
**Ms. Yipaerguli Waili (Ipar)**

Sustainability and Business Development  
Manager – Varuna Marine Services B.V.



**Ms. Richa Dutt Nandan**

Marketing Manager  
– Varuna Marine Services B.V.





# BEFORE WE START...



The webinar will run  
about 1 hour.  
Last 15 mins for Q&A.



This webinar is recorded,  
and we will share the  
recording in a blog article  
after the webinar



Use the Q&A function to  
send you questions anytime  
during the Webinar.

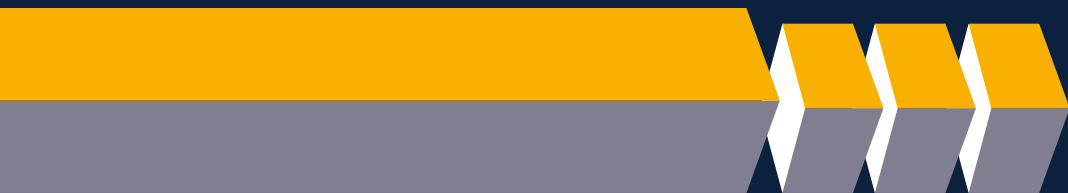




# POLLS QUESTION



The results of the polls will be published along with the in a blog article after the webinar



**WHAT'S NEXT??**

# PANELISTS FOR TODAY



**MR. JONGWOO AHN**

*Senior Surveyor – Korean Register*



**MR. SVANTE EINARSSON**

*Head of Cyber Security Maritime –  
DNV*



**MR. SANJEEV WEWERINKE-SINGH**

*Director – Varuna Marine Services  
B.V.*



**MR. JONGWOO AHN**

*Senior Surveyor – Korean Register*



# Maritime Cybersecurity

2022. 05. 25

AHN, Jongwoo

Cyber Certification Team, Korean Register



# Maritime Cyber Security Status

## States of Maritime Cyberattack



'17 Maersk NotPetya<sup>1)</sup>



'18 COSCO Ransomware<sup>2)</sup>



'20 US-flag Container ship<sup>5)</sup>

### Shipping companies

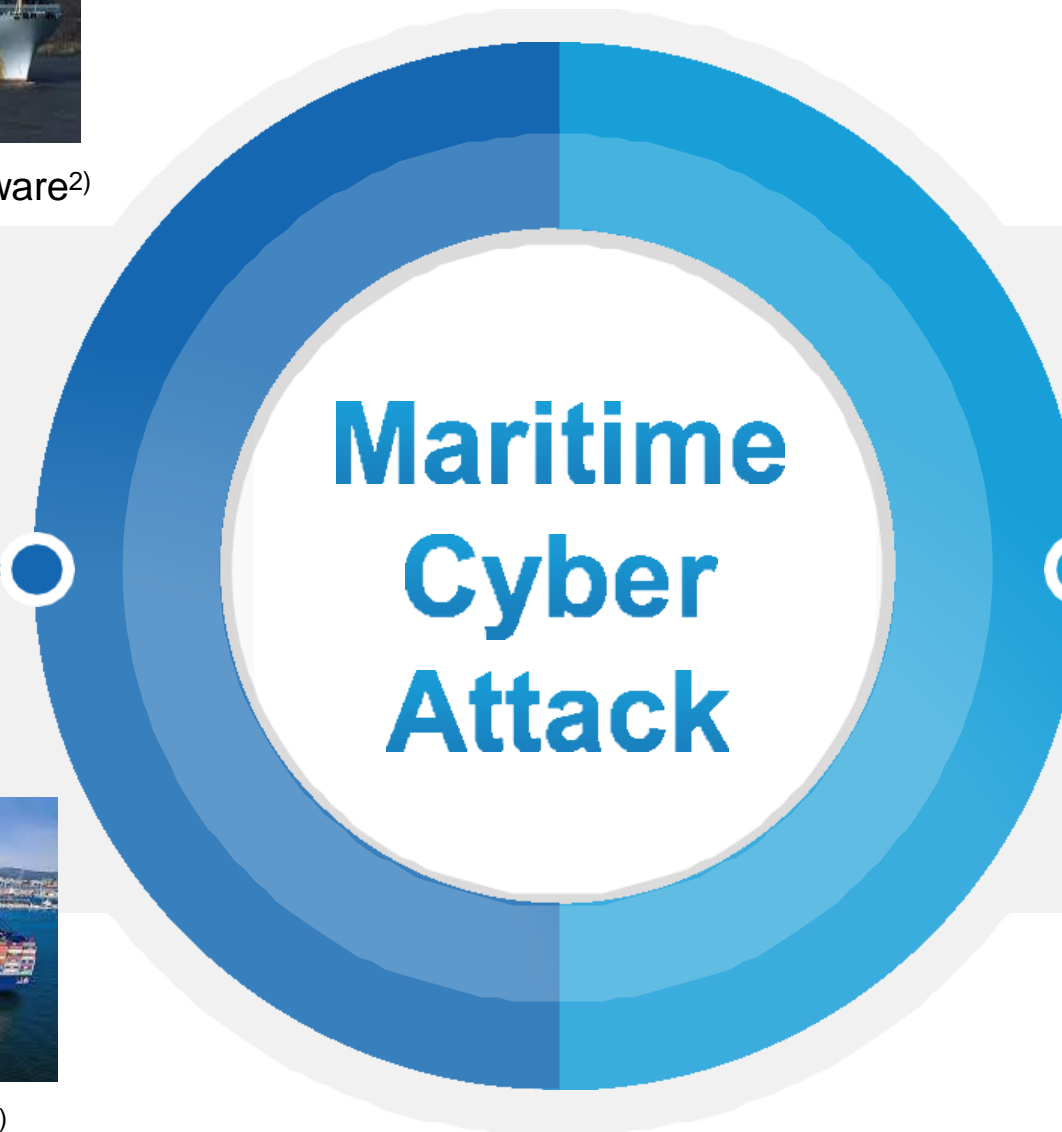
From 2017 to 2021, five major shipping companies have been hit by cyberattacks.



'20 MSC Malware<sup>3)</sup>



'20 CMA Ransomware<sup>4)</sup>



### Ships

IT and OT system in the ship have been attacked by malware, ransomware, etc.



'20 US tugboat<sup>6)</sup>

# Maritime Cyber Security Status

## Development of Cyber Security Requirements



2017 U.K government launched Code :  
Cyber Security for Ships



2016 BIMCO published Guidelines on Cyber Security Onboard Ships  
2017, 2018. 2<sup>nd</sup> and 3<sup>rd</sup> Version of Guidelines on Cyber Security  
Onboard Ships .



2020 4<sup>th</sup> Version of Guidelines on Cyber Security Onboard Ships  
2019 DCSA publishes Implementation Guide for Cyber Security  
on Vessels v1.0.



2017 IMO approved GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.  
2017 IMO has given shipowners and managers until 2021 to incorporate cyber  
risk management into SMS in ISM Code



2018 IACS published 12 recommendations  
2021 URs for new ship and equipment/system onboard are issued.



2020 USCG published Vessel Cyber Risk Management  
Work Instruction (CVC-WI-027(1)).



The Administration asked the shipowners, ship's  
managers, etc. that cyber risks should be  
appropriately addressed in a SMS no later than the  
first annual verification of the company's Document of  
Compliance that occurs after 1 January 2021.

**Note. Over 22 flag states like USCG, Marshall Island,  
Singapore, Australia, Cyprus, Vanuatu decided to  
make it compulsory.**



2017 TMSA3 includes procedure and requirement including threat  
identification related to cyber security.

2018 SIRE VIQ 7.7.14 Cyber Security was added.

**2022 SIRE 2.0.7.5 Cyber Security introduced detailed requirements.**



2017 Rightship revised "Inspection and Assessment Report for Dry  
Cargo Ships" in which check list on risk assessment and  
contingency plan for cyber security is added.

**2021 RightShip Inspection Ship Questionnaire (RISQ) includes  
requirement of cyber security like incorporation of cyber risk  
management in SMS.**

### MSC-FAL.1/Circ.35

#### GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

- Urgent need to raise **awareness on cyber risk threats and vulnerabilities**
- **High-level recommendations on maritime cyber risk management** to safeguard shipping from current and emerging cyber threats and vulnerabilities
- **Five Functional elements** that support effective cyber risk management.

### Resolution MSC.428(98)

#### MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing **safety management systems (as defined in the ISM Code)** no later than the first annual verification of the company's Document of Compliance **after 1 January 2021**.

### Administrations who required CRM\*

- Antigua and Barbuda
- Australia
- Bahamas
- Cyprus
- Faroe Islands
- Georgia
- Germany
- Greece
- India
- Isle of Man
- Liberia
- Malaysia
- Marshall Islands
- Myanmar
- Palau
- Singapore
- St. Kitts and Nevis
- St. Vincent and The Grenadines
- Togo
- Vanuatu
- U.S.A and all ships calling at U.S.A ports

\* Cyber Risk Management

USCG Office of Commercial Vessel Compliance (CG-CVC)  
Mission Management System (MMS) Work Instruction (WI)

Category	Commercial Vessel Compliance (Domestic and Foreign Vessels)		
Title	Vessel Cyber Risk Management Work Instruction		
Serial	CVC-WI-027(1)	Orig. Date	27OCT20
		Rev. Date	N/A
Disclaimer:	This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally binding requirements on any part. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact the Coast Guard Office of Commercial Vessel Compliance (CG-CVC) at <a href="mailto:CG-CVC@uscg.mil">CG-CVC@uscg.mil</a> who is responsible for implementing this guidance.		
References:	(a) Maritime Safety Committee Resolution 428(98), "Maritime Cyber Risk Management in Safety Management Systems" (b) U.S. Coast Guard Cyber Strategy, June 2015 (c) International Safety Management (ISM) Code (d) U.S. Flag Interpretations on the ISM Code, (CVC-WI-004(1))		

1. **Basic Cyber Hygiene.** The MI/PSCO shall identify when basic cyber hygiene procedures are not in place onboard. These include, but not limited to the following:
  - a. Poor cyber hygiene
    - 1) Username / Password openly displayed
    - 2) Computer system appears to require a generic login or no login for access
    - 3) Computer system does not appear to automatically log out after extended period of user inactivity
    - 4) Heavy reliance on flash drive/USB media use
  - b. Shipboard computers readily appear to have been compromised by ransomware/excessive pop-ups
  - c. Officers/crew complain about unusual network issues and reliability impacting shipboard systems
  - d. Unit/vessel screener received potential 'spoofed' email from master/crew onboard.

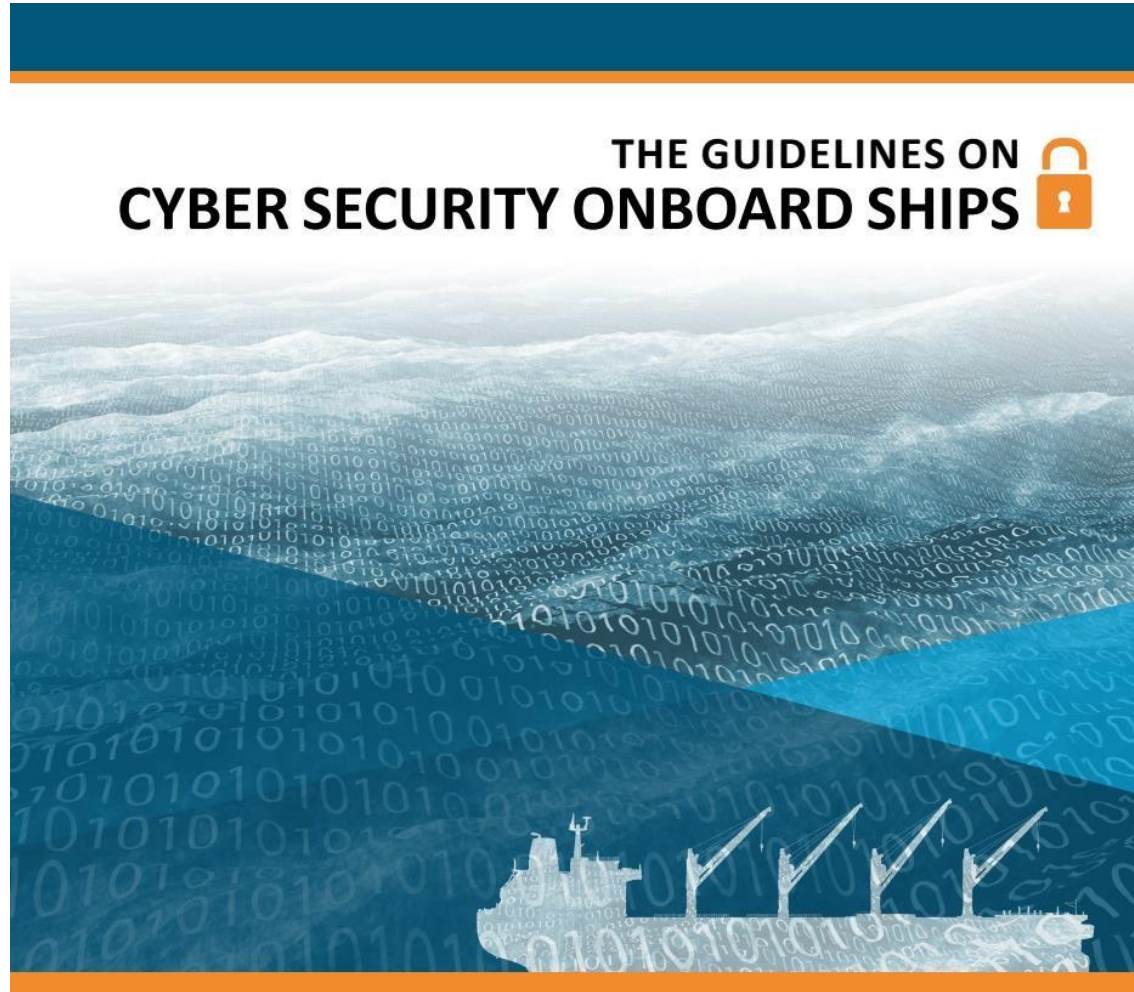
If these observations are not directly linked to statutory requirements or are not technical or operational-related deficiencies, the MI/PSCO does not have clear grounds to conduct a more detailed inspection. However these vulnerabilities should be discussed directly with the master. In addition, these discussions shall be annotated in the MISLE inspection narrative and documented with a deficiency entered into MISLE marked "Worklist Item/Do Not Show in PSIX" for data analysis.

Ref : USCG, CVC-WI-027(1)

If cyber risk management has not been incorporated into SMS or not implemented, a deficiency should be issued with **Action Code 30 – Ship Detained or Code 17 – Rectify Prior to Departure.**

# BIMCO and Classification Society(KR)

Administrative Security for IMO Resolution MSC.428(98)



## THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

### Produced and supported by

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)



## DOC CHECK LIST for Cyber Risk Management(CRM)

This checklist was developed for reference to efficiently implement the cyber risk management in accordance with Res.MSC.428(98), and it is recommended to use this checklist in conjunction with the Checklist for ISM company audit.

※ Mark methods for the each questionnaire in a square box

or  : Verified as sampling basis

: Not Applicable

\* If a check item is identified as a non-conformity on a sampling verification, it shall be recorded in the non-conformity report

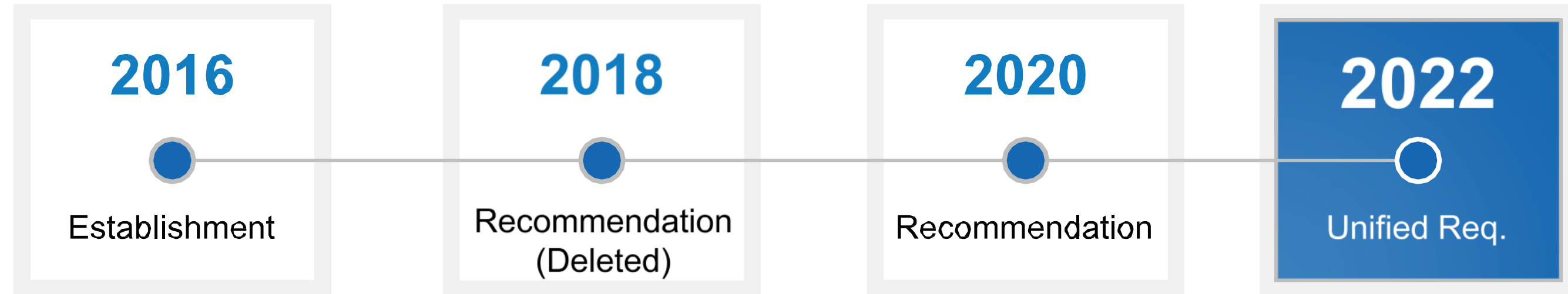
No.	Code	Check items	Result
1	1	<b>Does the company implement cyber risk assessment for cyber assets and establish Cyber Risk Management (CRM) in the approved safety management systems?</b> - Check the CRM in accordance with ISM Code 1.2(objectives) and 1.4(functional requirements) - Check the identification of cyber assets (software, hardware, etc.) - Check the existing controls according to data transmission method provided to the vessel	
2	3	<b>Does the company establish allocation of responsibility and authority for CRM in the SMS?</b> - Check the identification of responsibility, authority and designated PIC.(D.P, Master, etc.)	
3	6	<b>Does the company provide any Cyber risk training with shore staff and crews?</b> - Check the cyber risk awareness training provided to the shore staff and crews - Check the updated information for cyber risk provided to the vessel	
4	6	<b>Does the company provide appropriate support at the request of the vessel?</b> - Hardware, Software, update patches, USB/LAN Blocker, information for Cyber risk, etc.	
5	7	<b>Does the company establish any additional procedure or existing controls in relation to key shipboard operation resulted from cyber risk assessment?</b> - Check the additional procedure or existing controls such as physical security for visitor, list of personal device(For visitors), password-account locks, statement of oath for security and etc.	
6	8	<b>Does the company establish emergency plans/procedures for response of cyber incidents?</b> - Check the emergency plans/recovery procedures, contact details for technical IT support.	
7	6 8	<b>Does the company provide emergency plans/procedures with hard copy for response of cyber incidents?</b> - Check the hard copy of emergency plans/recovery procedures and familiarization of PIC. - Check the measures to prevent cyber incidents from the attacker	
8	10	<b>Does the company establish maintenance procedures for cyber security equipment resulted from cyber risk assessment?</b> - Check the periodical inspection / Maintenance / update / Inventory of spare parts, etc. - Check the designated PIC., records of maintenance	
9	12	<b>Does the company periodically verify/review/assess for the CRM, effectiveness of existing controls and appropriate implementation through internal audit, master review and company review?</b> - Check the results of internal audit, master review and company review - Check the qualification of internal auditors	
10	12	<b>Does the company periodically verify/review/assess the delegated cyber-related tasks and assets?</b> - Check the relevant procedure/records of delegated cyber-related tasks and assets	

Company Name : \_\_\_\_\_ Date : \_\_\_\_\_

Company Representative (with Signature) : \_\_\_\_\_ Auditor (with Signature) : \_\_\_\_\_

# Int. Association of Classification Societies

Technical Security for IMO Resolution MSC.428(98)



## CS System Panel

- All 12 Class Societies
- Communicate with IMO & EU, Industry

## Rec 153~164

- Recommended procedures for software maintenance of computer based systems on board
- Recommendation concerning manual / local control capabilities for software dependent machinery systems
- Contingency plan for onboard computer based systems
- Network Architecture
- Data assurance
- Physical security of onboard computer based system
- Network security of onboard computer based systems
- Vessel System Design
- Inventory List of computer based systems
- Integration
- Remote Update / Access
- Communication and Interface

## Rec 166

- Recommendation on Cyber Resilience

## UR E26, E27

- Cyber Resilience of Ships
- Cyber Resilience of on-board system and equipment
- **Effective to ships contracted for construction on or after 1 January 2024**

# UR E27 Cyber Resilience of on-board systems and equipment

## Overview



E27

---

**E27**  
(Apr 2022) **Cyber resilience of on-board systems and equipment**

**1. General**

**1.1 Introduction**

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

This document specifies unified requirements for cyber resilience of on-board systems and equipment.

**1.2 Limitations**

This UR does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, following URs shall be applied:

- UR E10 for environmental performance for the system hardware
- UR E22 for safety of equipment for the functionality of the software

**1.3 Scope**

The requirements specified in this UR are applicable to computer based systems as defined in UR E26.

Navigation and radiocommunication systems may follow IEC 61162-460 instead of the requirements in this UR. See IACS UR E26 section 1.3

---

Note:

1. This Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance. In order to allow sufficient time for non-mandatory pilot application of this UR, the application date of 1 January 2024 has been selected.
2. The "contracted for construction" date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details regarding the date of "contract for construction", refer to IACS Procedural Requirement (PR) No. 29.

---

Page 1 of 14 IACS Req. 2022



BS IEC 62443-3-3:2013  
*Incorporating corrigendum April 2014*

BSI Standards Publication

## Industrial communication networks — Network and system security

Part 3-3: System security requirements and security levels

**SL4** : Intentional violation, sophisticated means with extended resources

- Duplicated authentication
- Unauthorized change detection
- Confirm security features and operations

**SL3** : Intentional violation, sophisticated means with moderate resources

- Security mechanism based on hardware
- Concurrent user management

**SL2** : Intentional violation, simple means with low resources

- Preventing unauthorized use of the test interface
- Preventing unauthorized software installations
- Equipment communication date authentication

**SL1** : Casual or coincidental violation

- Authorization
- Recovery function
- Human user authentication

# UR E27 Cyber Resilience of on-board systems and equipment

## 17 Requirements of UR E27



### 4.1 Required security capabilities

The following security capabilities are required for all CBSs in the scope specified in section 1.3.

Table 1

SI No	Objective	Requirements
1	Human user identification and authentication	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces
2	Account management	a) Limit the use of portable and mobile devices only to those permitted by design b) Restrict code and data transfer to/from portable and mobile devices Note: Port limits / blockers (and silicone) could be accepted for a specific system (IEC 62443-3-3/SR 3.6)
3	Identifier management	11 Mobile code The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit. (IEC 62443-3-3/SR 4.1)
4	Authenticator management	12 Session lock
		13 Auditable events
5	Wireless access management	14 Audit storage capacity The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel. (IEC 62443-3-3/SR 1.12)
6	Strength of password-based authentication	15 Response to audit processing failures
7	Authenticator feedback	16 Timestamps
8	Authorization enforcement	17 Communication integrity
		18 Malicious code protection
9	Wireless use control	19 Security functionality verification
		20 Input validation
10	Use control for portable and mobile devices	21 Deterministic output
		22 Information confidentiality
		23 Use of cryptography
		24 Audit log accessibility
		25 Denial of service protection
		26 Resource management
		27 System backup
		28 System recovery and reconstitution
		29 Emergency power
		30 Network and security configuration settings
		31 Least Functionality

### 4.2 Additional security capabilities

The following additional security capabilities are required for CBSs with network communication to untrusted networks (i.e. interface to any networks outside the scope of UR E26).

Table 2

SI No	Objective	Requirements
32	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network. (IEC 62443-3-3/SR 1.1, RE 2)
33	Software process and device identification and authentication	The system shall identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
34	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (IEC 62443-3-3/SR 1.11)
35	System use notification	The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel. (IEC 62443-3-3/SR 1.12)
36	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks shall be monitored and controlled. (IEC 62443-3-3/SR 1.13)
37	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (IEC 62443-3-3/SR 1.13, RE1)
38	Remote session termination	The CBS shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session. (IEC 62443-3-3/SR 2.6)
39	Cryptographic integrity protection	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (IEC 62443-3-3/SR 3.1, RE1)
40	Session integrity	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected. (IEC 62443-3-3/SR 3.8)
41	Invalidation of session IDs after session termination	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions). (IEC 62443-3-3/SR 3.8, RE1)



### E26 Cyber resilience of ships

(Apr 2022)

#### 1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

#### 1.1 Structure of this UR

Table 1: Structure of this UR

Introductory Part	1 Introduction
	2 Definitions
	3 Goals and Organization of Requirements
Main Part	4 Requirements
	4.1 Identify
	4.2 Protect
	4.3 Detect
	4.4 Respond
	4.5 Recover
Supplementary Part	5 Test plan for performance evaluation and testing
	5.1 During design and construction phases
	5.2 Upon ship commissioning
	5.3 During the operational life of the ship
	6. Risk assessment for exclusion of CBS from the application of requirements (required only when systems are excluded from application of this UR)
	Appendix: Summary of Actions and Documents

#### Note:

1. This Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance. In order to allow sufficient time for non-mandatory pilot application of this UR, the application date of 1 January 2024 has been selected.
2. The "contracted for construction" date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details regarding the date of "contract for construction", refer to IACS Procedural Requirement (PR) No. 29.

“ ... to be uniformly implemented by IACS

Societies on **ships contracted for construction on**

**or after 1 January 2024** and by used for other

ships as non-mandatory guidance.”

## 1.2 Aim and purpose

To provide a **minimum set of requirements** for

cyber resilience of ships, with the purpose of

providing **technical means** to stakeholders

which lead to cyber resilient ships.

# UR E26 Cyber Resilience of Ships

17 Requirements of UR E26



## Identify

- Inventory of CBSs and networks onboard

## Protect

- Security zone
- Network protection safeguards
- Antivirus, antimalware, antispam and other protections from malicious code
- Access control
- Wireless communication
- Remote access control and communication with untrusted networks
- Use of Mobile and Portable Devices

## Detect

- **Network operation monitoring**
- Diagnostic functions of CBS and networks

## Respond

- Incident response plan
- Local, independent and/or manual operation
- Network isolation
- Fallback to a minimal risk condition

## Recovery

- Recovery plan
- Backup and restore capability
- Controlled shutdown, reset, roll-back and restart

### 4.3.1 Network operation monitoring

#### 4.3.1.1 Requirement:

Network in scope of this UR shall be continuously monitored, and alarms shall be generated if malfunction or reduced / degraded capacity occurs.

#### Function

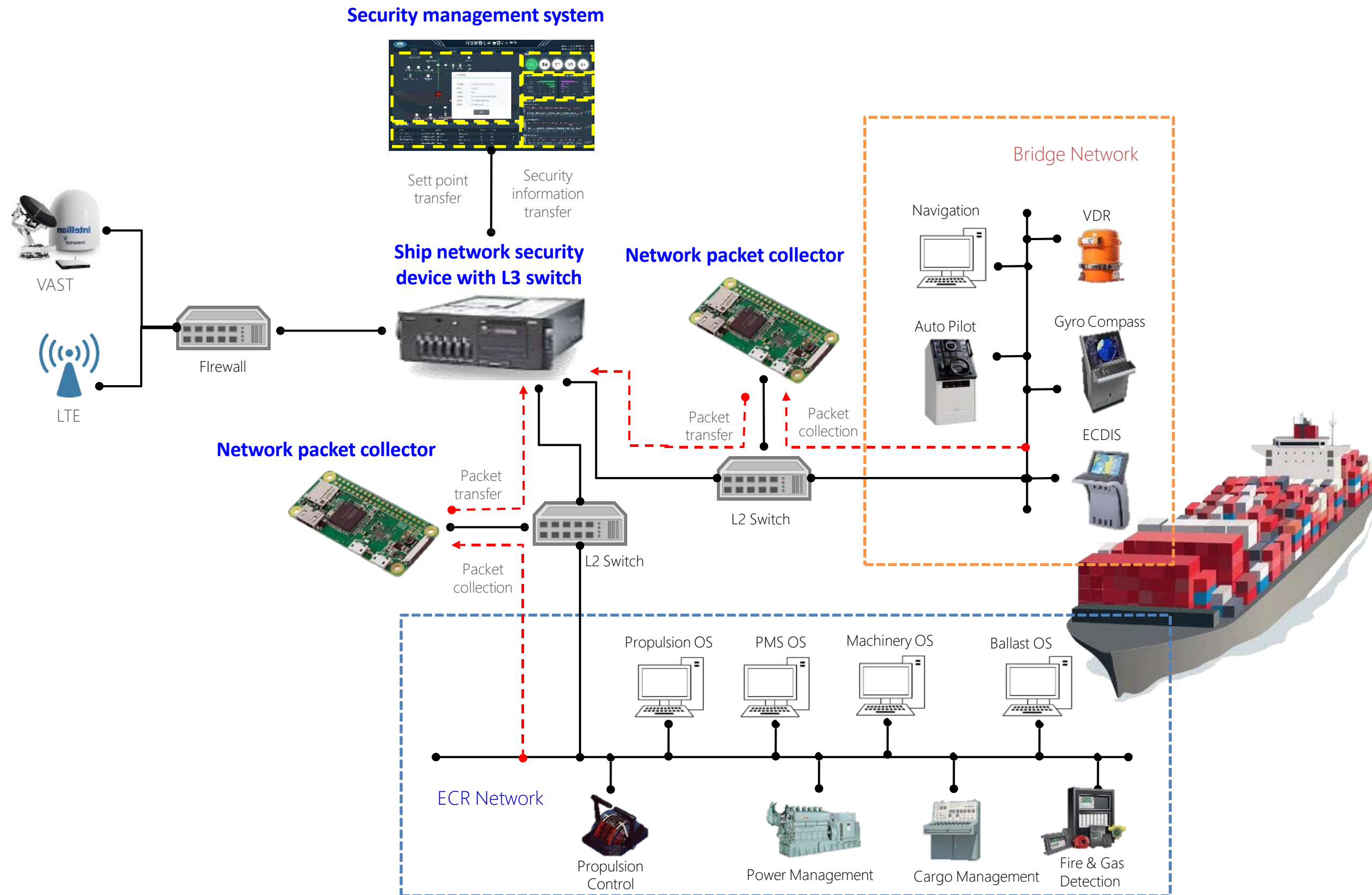
- Monitoring and protection against excessive traffic
- Monitoring of network connections
- Monitoring and recording of device management activities
- Monitoring or protection against connection of unauthorized devices

#### Implementation

- Qualified by the supplier of the respective Computer-based-system(CBS)
- Passive and not activate protection functions that may affect the performance of the CBS
- Relevant personnel should be trained and qualified for use

# UR E26 Cyber Resilience of Ships

## Example of Network Monitoring System



- Cyber security in maritime industry is no longer an option as cyber attacks on ships and shipping companies increase.
- Cyber security can **not be secured by only administrative security**. So IACS published **UR E26 Cyber Resilience of Ships in terms of technical and physical security**.
  - This 2 URs will have experience period for having feedback from the site, especially shipbuilder.
- According to UR E26, network operation monitoring system is required for the new ship after 1 Jan. 2022. KR is conducting the project to develop and verify it through KASS project.



**Thank you for your attention!**  
**Any Questions?**



**Providing the best service, Creating a better  
world**

**POLLS**



**MR. SVANTE EINARSSON**

*Head of Cyber Security Maritime - DNV*





# Overview & Background of DNV Maritime Cyber Safety & Security Services

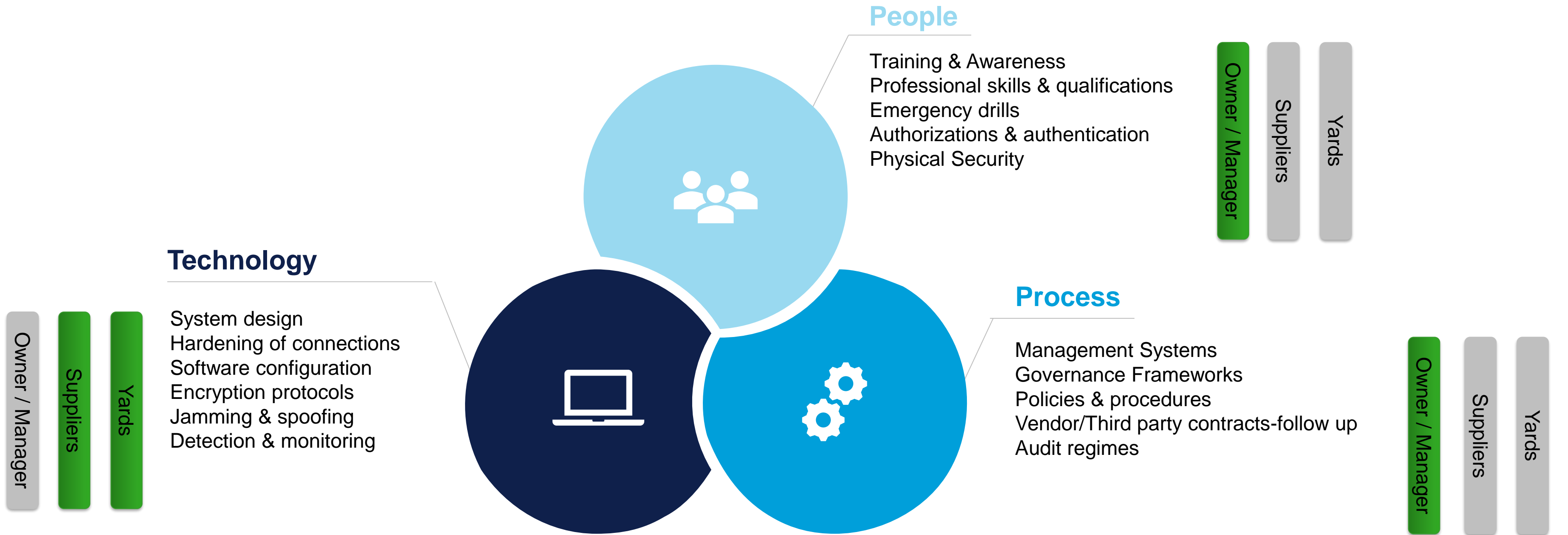
Svante Einarsson, Head of Cyber Security Maritime

2022

# Maritime industry has a wide range of needs when it comes to building Cyber Security resilience of companies and fleets

High

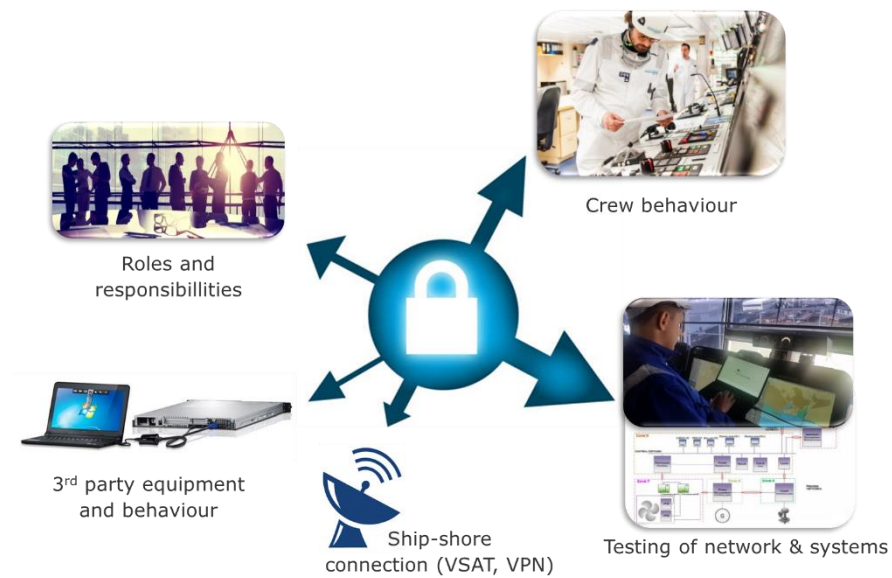
Low



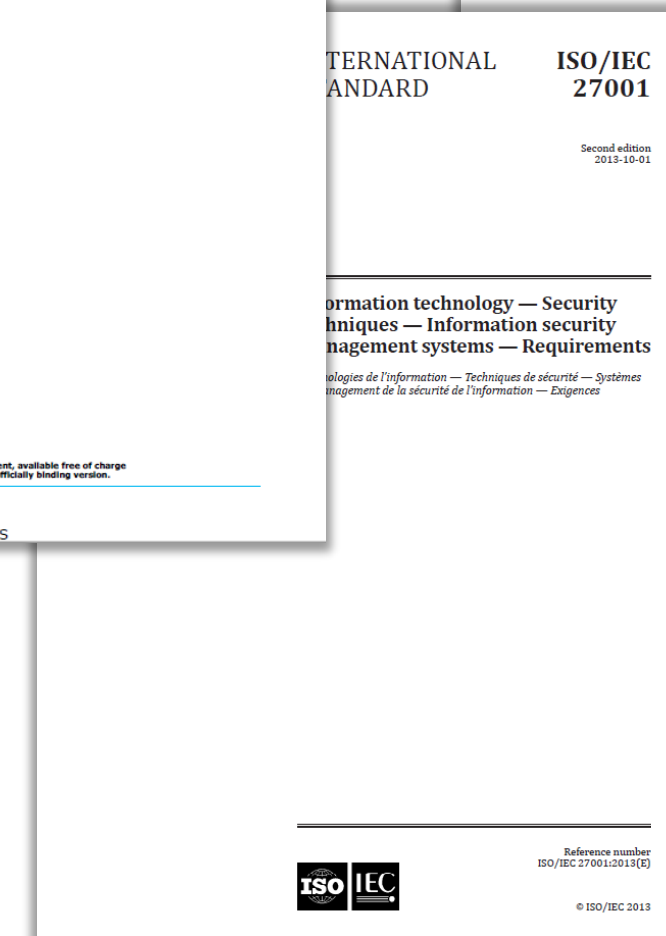
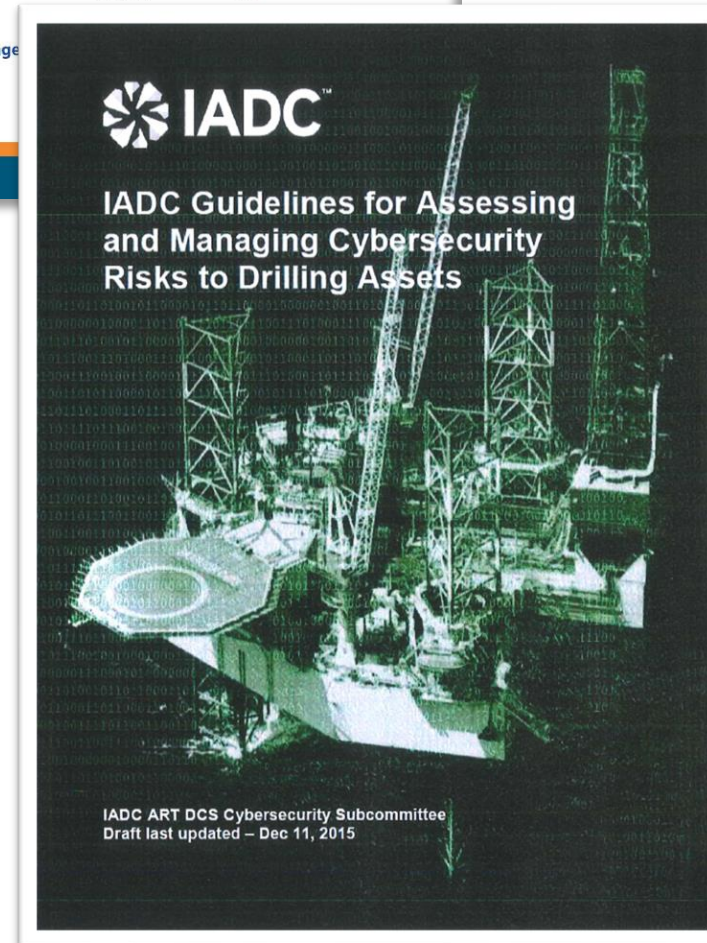
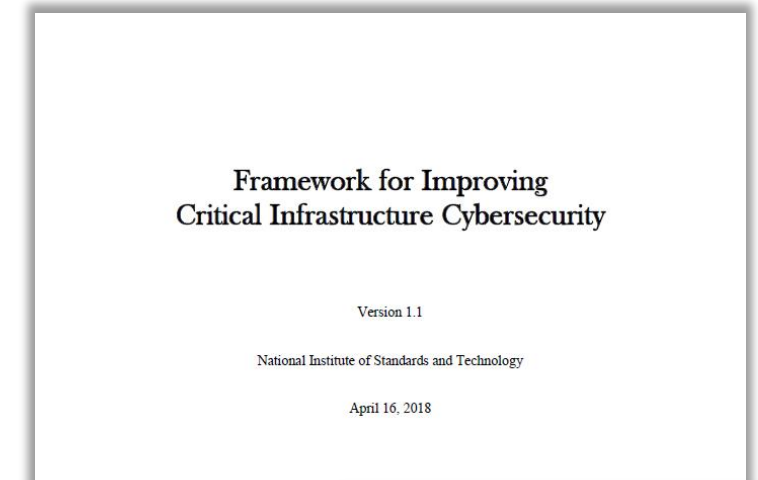
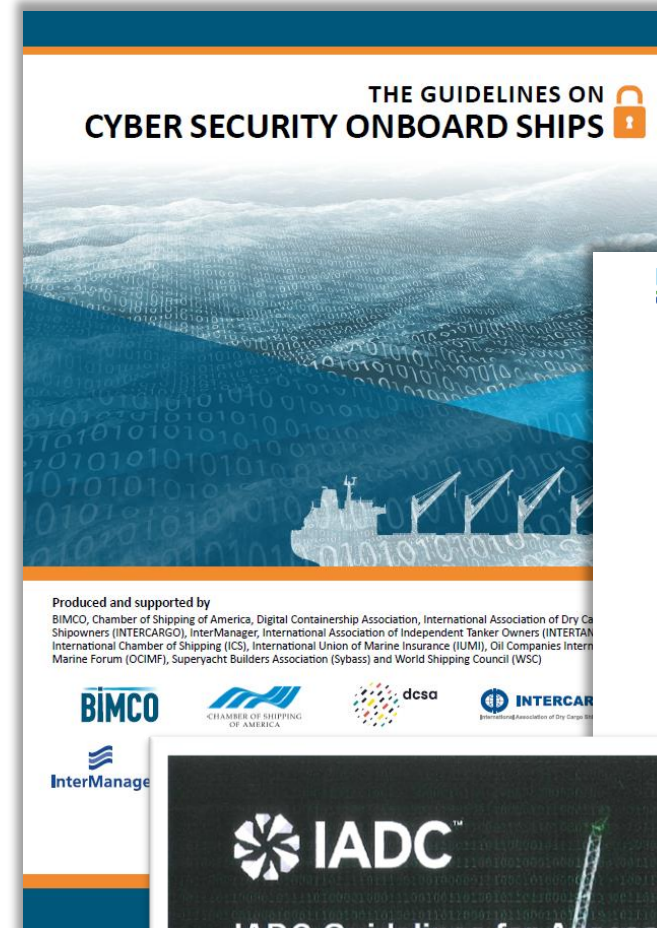
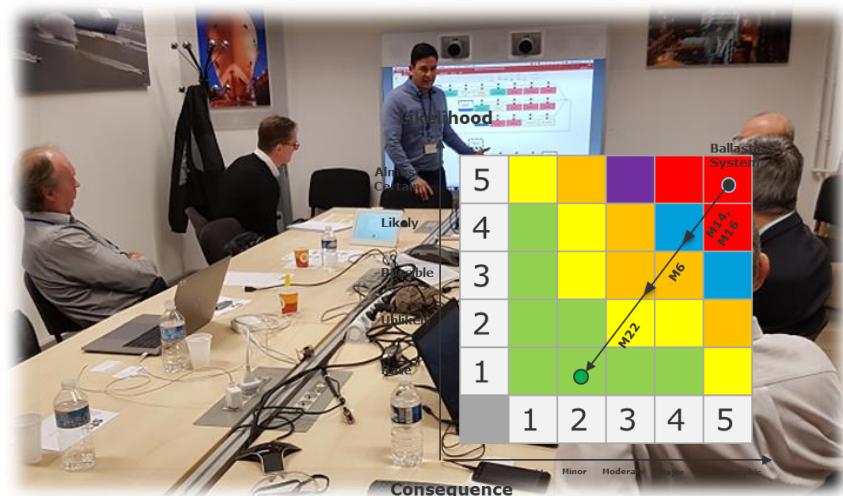
# The needs of the Maritime Industry is developing

## Assess/Test ...2016...

### On-board assessment & testing



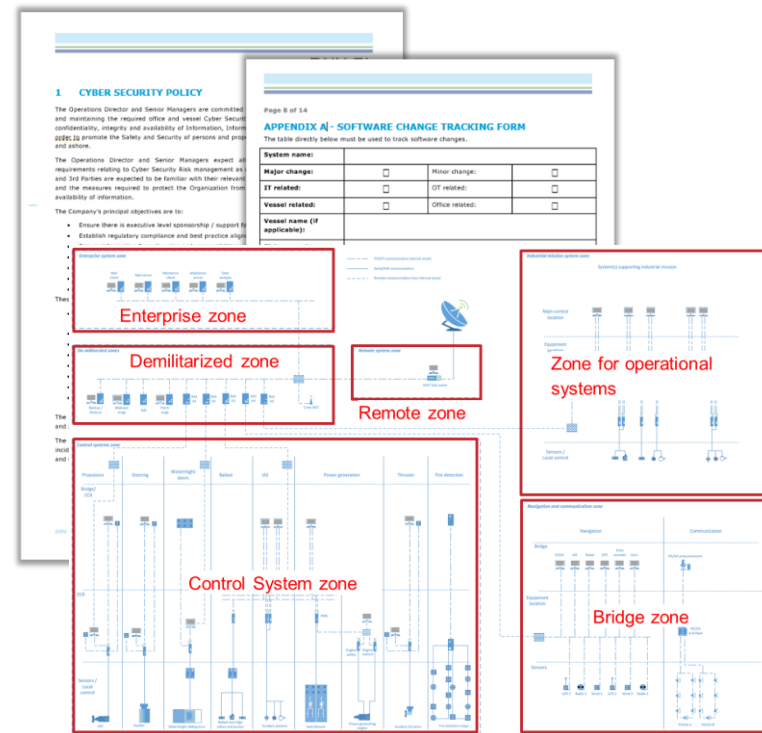
### Cyber risks assessment



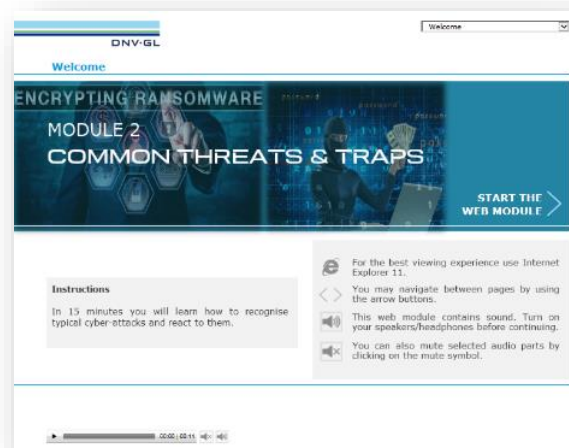
# The needs of the Maritime Industry is developing

Improve  
...2018...

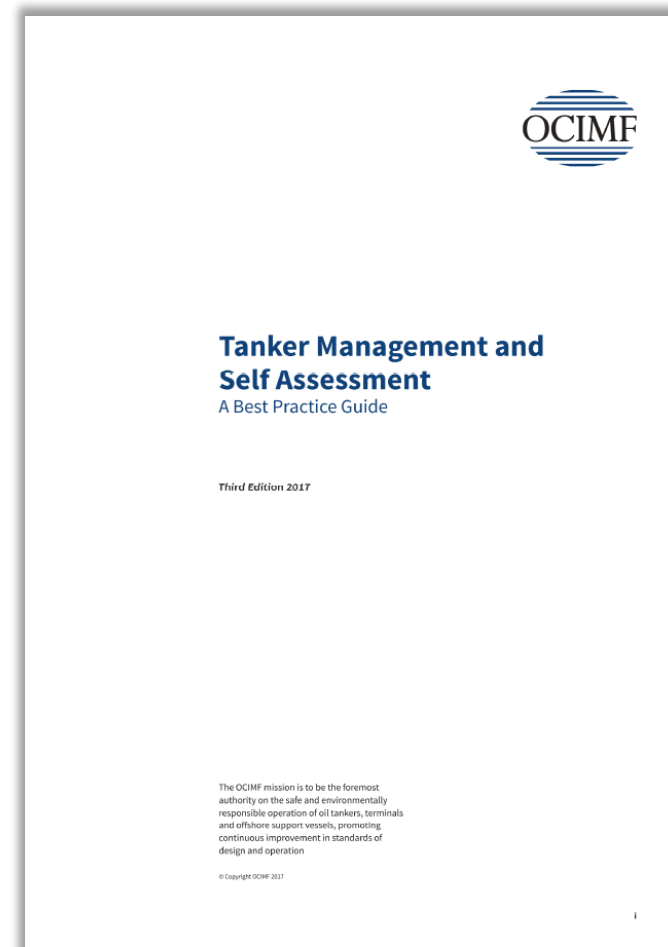
## SMS and Technical Doc. Development



## Training



DNV ©



Deadline: 1st Jan. 2018

## Corporate Earnings Show Impacts of NotPetya Cyber Attack

August 2, 2017 by Reuters

**Transport & Logistics** reiterates the expectation of an underlying profit above USD 1bn, despite expected negative result impact from the June cyber-attack estimated at a level of USD 200-300m, of which the majority relates to lost revenue in July. The vast majority was in Maersk Line.

Interim Report  
Q2 2017

A.P. Moller - Maersk A/S

MAERSK

# The needs of the Maritime Industry is developing

Implement  
...2020...

## On demand Cyber Security Office



## Exercises & Surveys

Scenario 1: Loading incident

• During unloading the loading and stability computer crashes, and the system does not recover after reboot. The crew loses the overview of the operations, as the system is also used to monitor cargo control. Time is lost due to the need to be contacted at the shore.

Cyber Security Awareness - Crew

Importance of cyber security on board

Please select the vessel you are currently sailing on?

In your opinion, how important is cyber security on board?

What makes you feel like that way?

IMO INTERNATIONAL MARITIME ORGANIZATION

4 ALBERT EMBANKMENT  
LONDON SE1 7SR  
Telephone: +44 (0)20 7735 7811 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3/Rev.1  
14 June 2021

**GUIDELINES ON MARITIME CYBER RISK MANAGEMENT**

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 The Maritime Safety Committee, at its 103rd session (5 to 14 May 2021), and the Facilitation Committee, at its forty-fifth session (1 to 7 June 2021), approved an update to the additional guidance and standards included in paragraph 4.2 of the Guidelines.

4 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

5 This circular and any revisions supersede the interim guidelines contained in MSC.1/Circ.1526.

\*\*\*

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

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

Deadline: 1<sup>st</sup> Jan. 2021

# Experiences from DNV's ISM auditors



- IT language too technical
- Gap analysis not utilized effectively
- There is more focus on IT and less on OT
- Less focus on organizational and personnel needs
- No or limited focus on training, exercises and/or competence
- Unclear lines of responsibility and/or charts of authority on cyber
- Inadequate implementation of existing cyber security procedures in SMS
- Difficulties in including cyber security in existing maintenance routines (PMS)

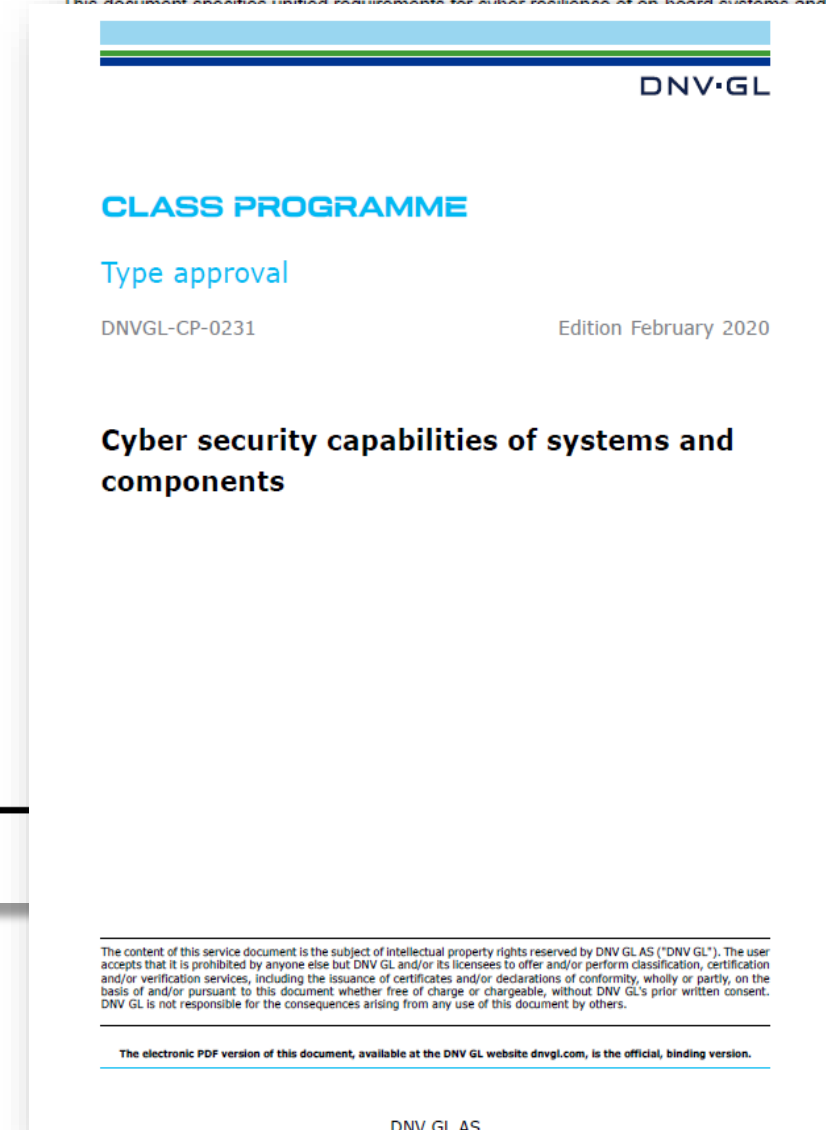
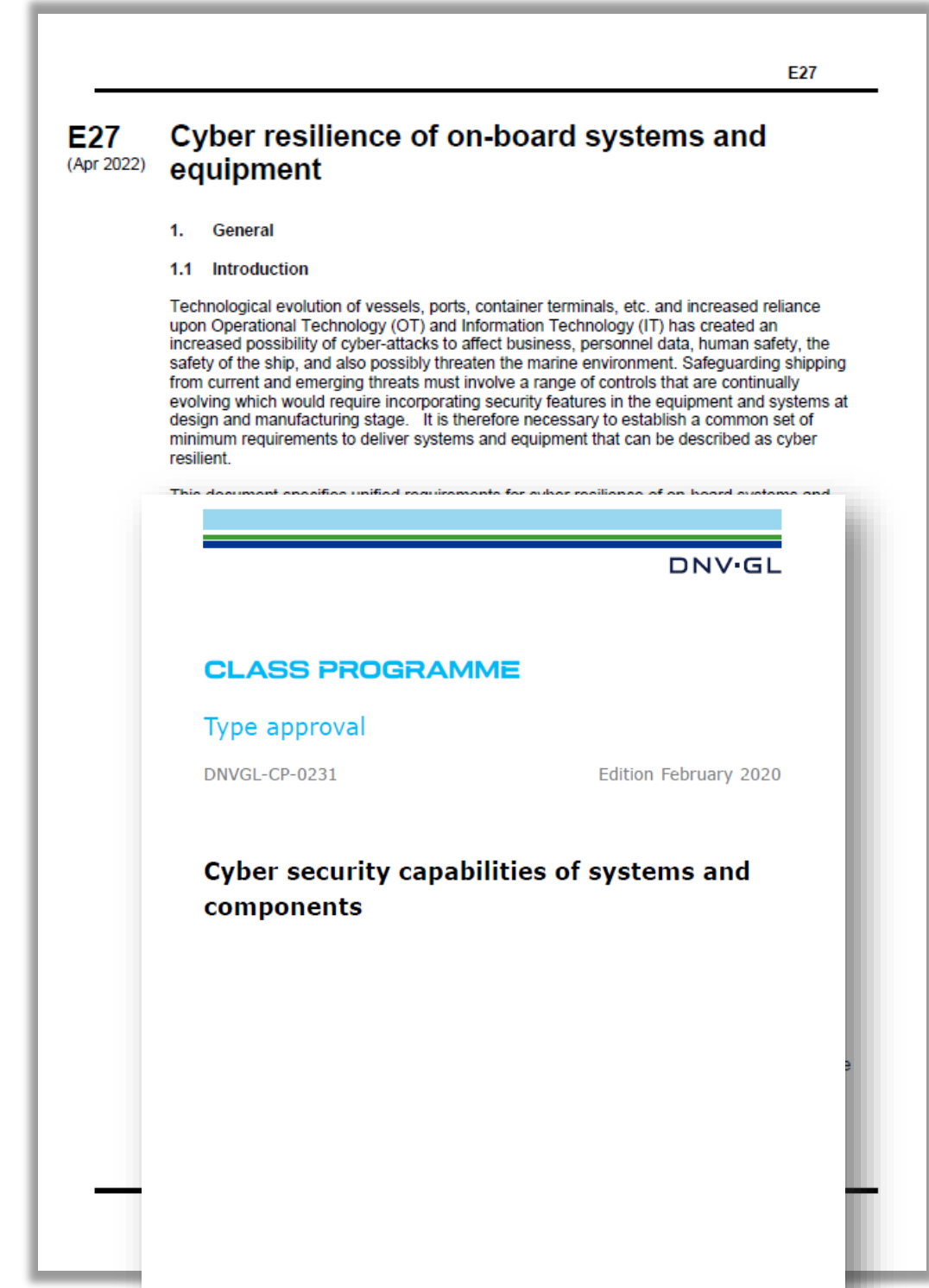
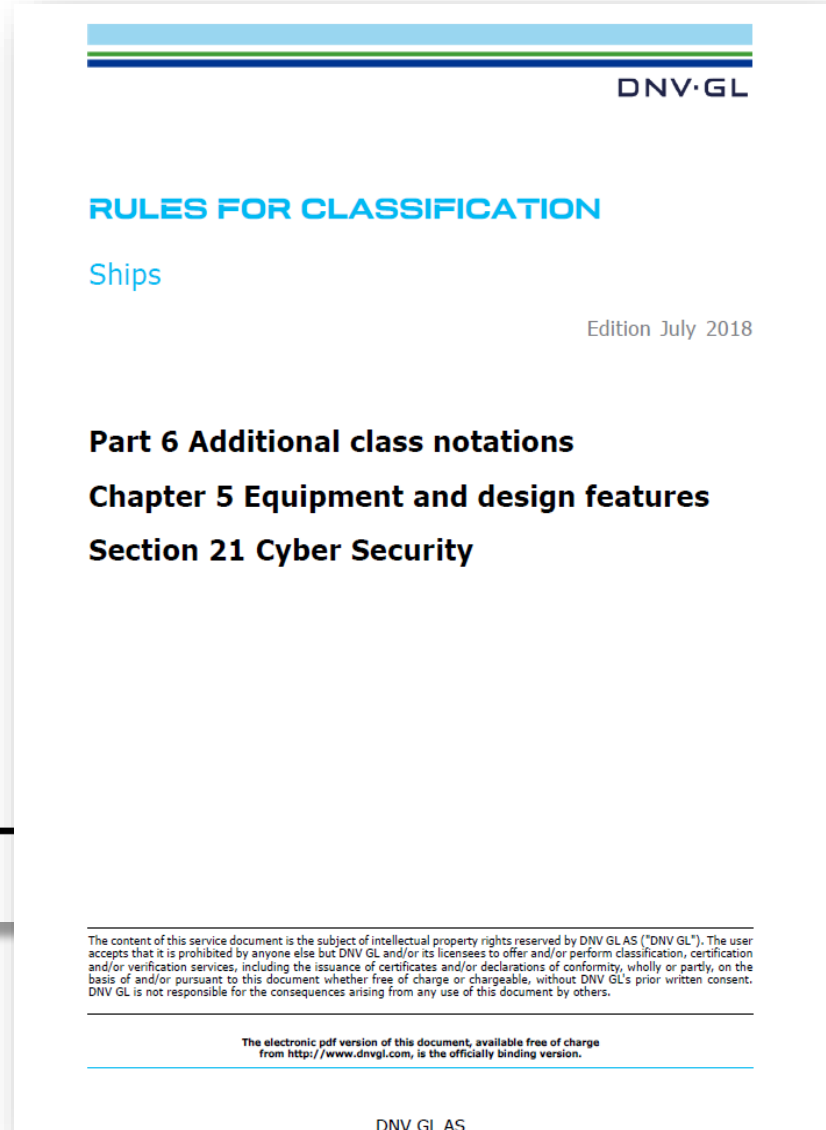
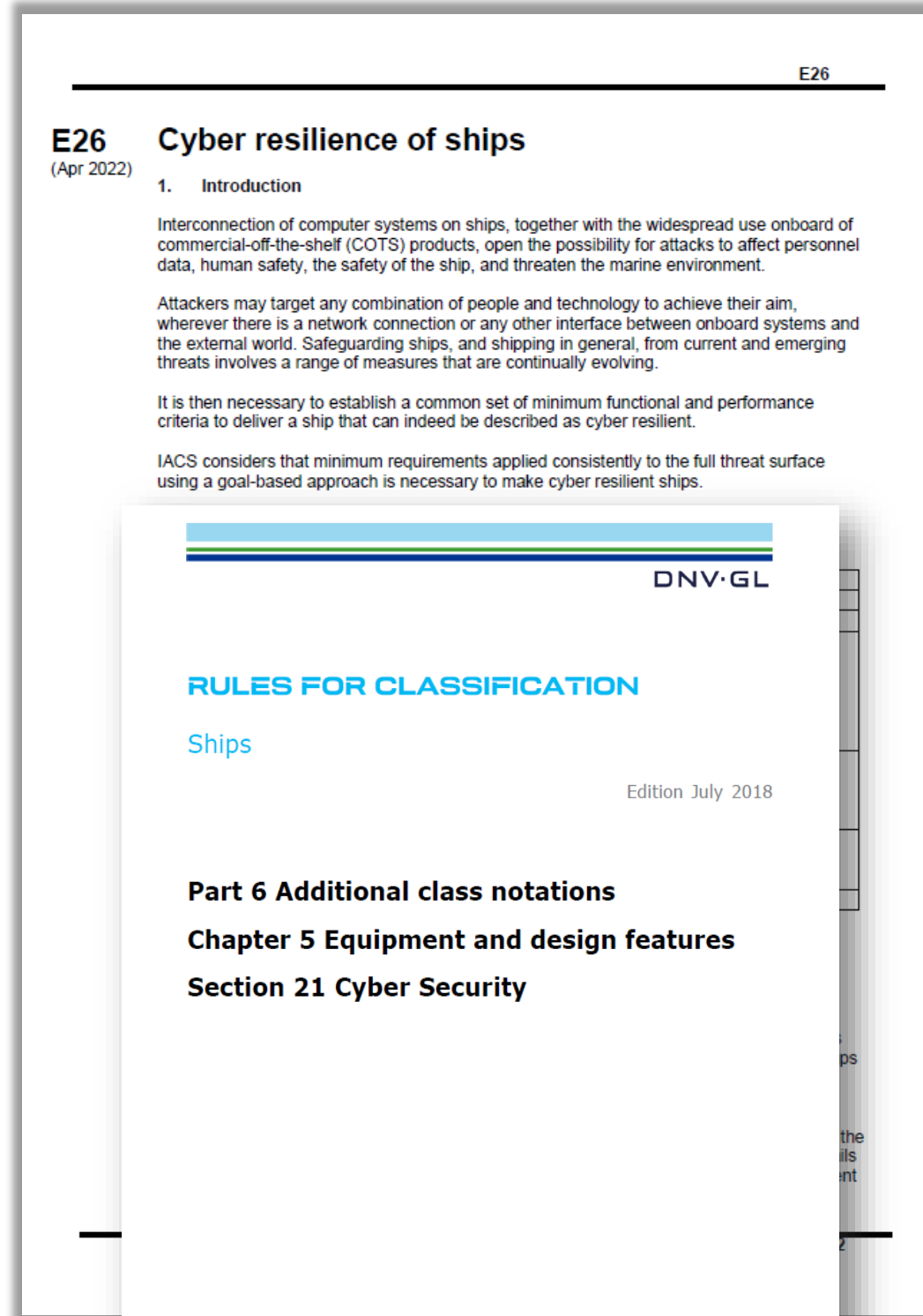
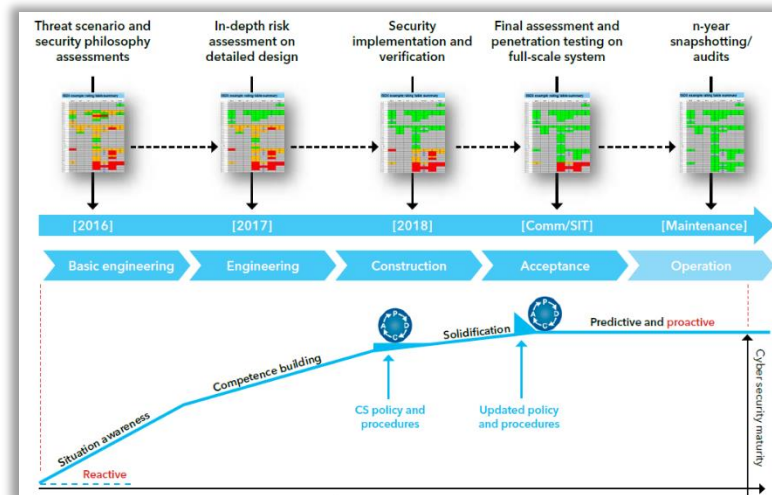
# The needs of the Maritime Industry is developing



## Ship in Operation

RequirementID	RequirementID:Title	Date	Rating
IMO2021-MG-01	Objectives of SMS	5/15/2020	Low
IMO2021-MG-02	Compliance	5/15/2020	Low
IMO2021-MG-03	Cybersecurity policy ar	5/15/2020	Low

## Newbuilding

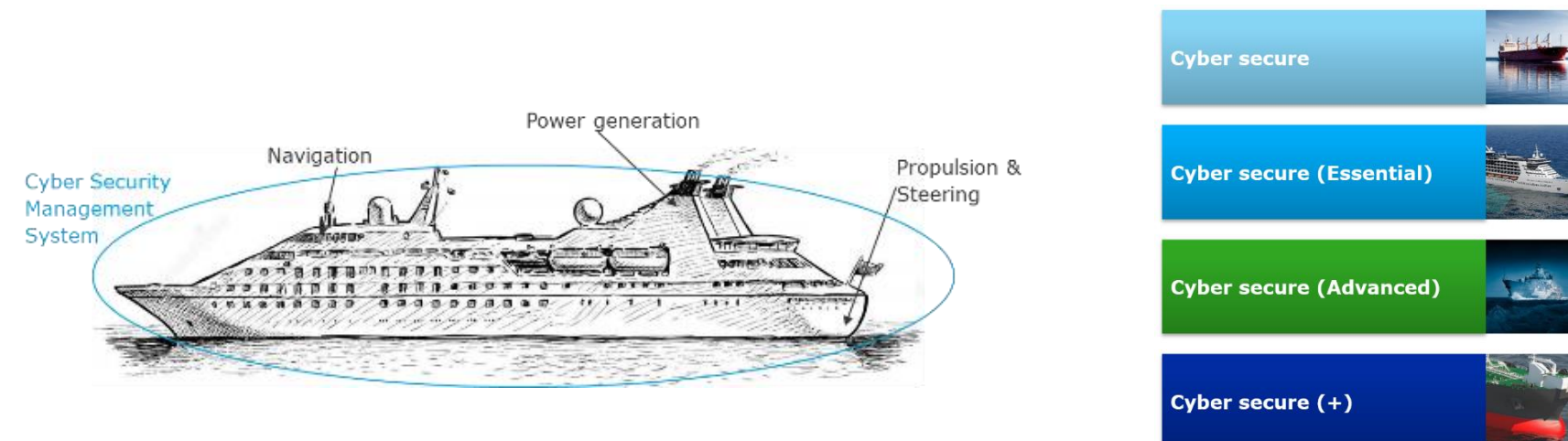


# Cyber Security in the Class scope for ships and offshore units

**Main Class Rules:** For all ships and offshore units in DNV class. Few principle requirements.  
(DNVGL-RU-SHIPS Pt.4 Ch.9 or DNVGL-OS-D202)

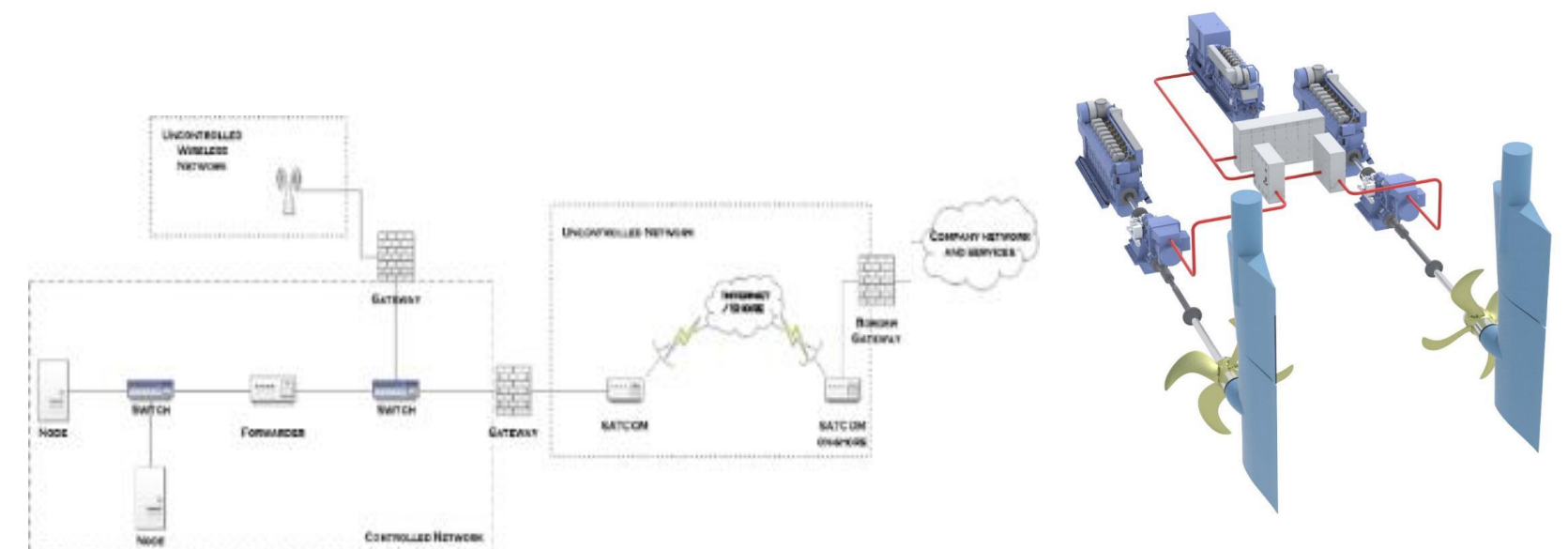
## Cyber Secure Class Notation (DNVGL-RU-SHIPS Pt.6 Ch.5 Sec.21)

- Requirements to **technical security barriers, management system and human behaviour**
- **Pre-defined scope important and essential systems**, and based on recognized standards, **IEC-62443**
- Offers different levels suitable for all vessel segments



## Cyber Secure Type Approval (DNVGL-CP-0231)

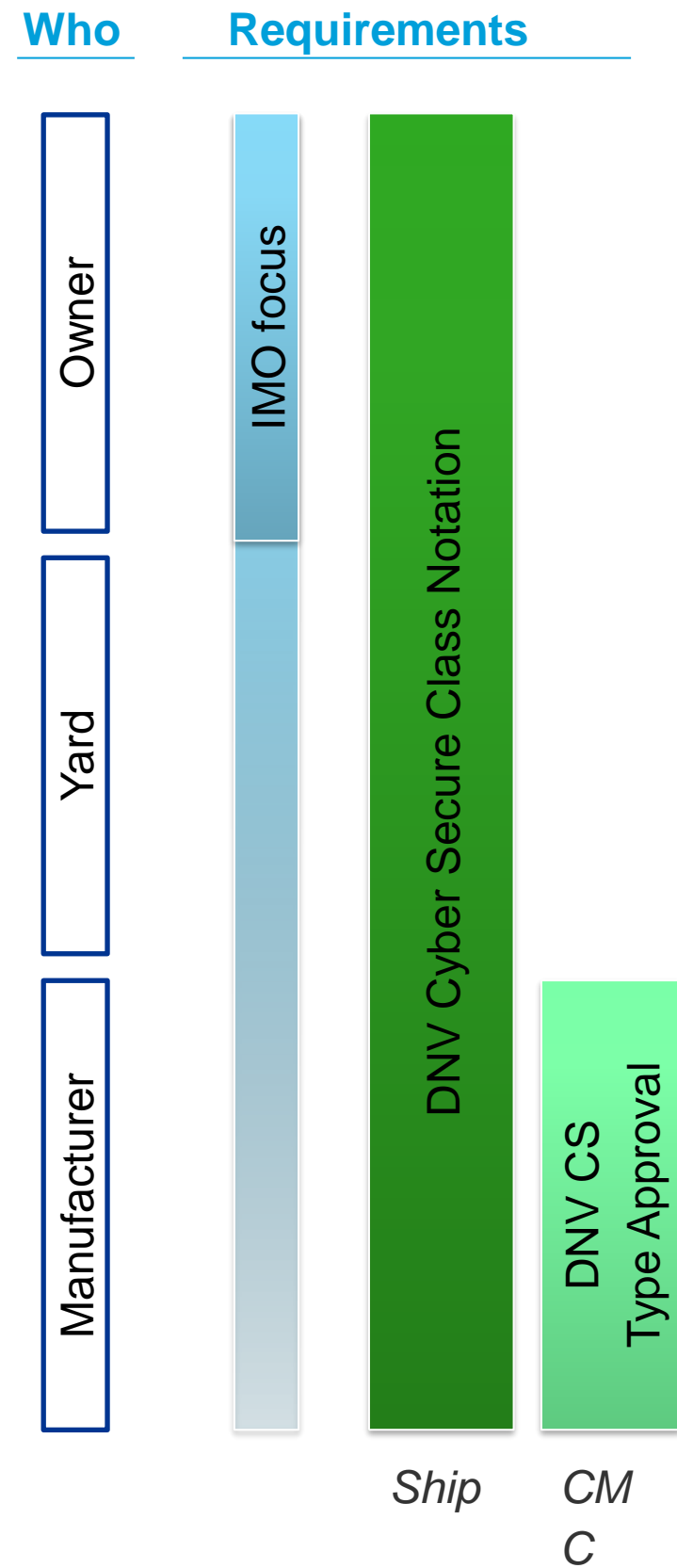
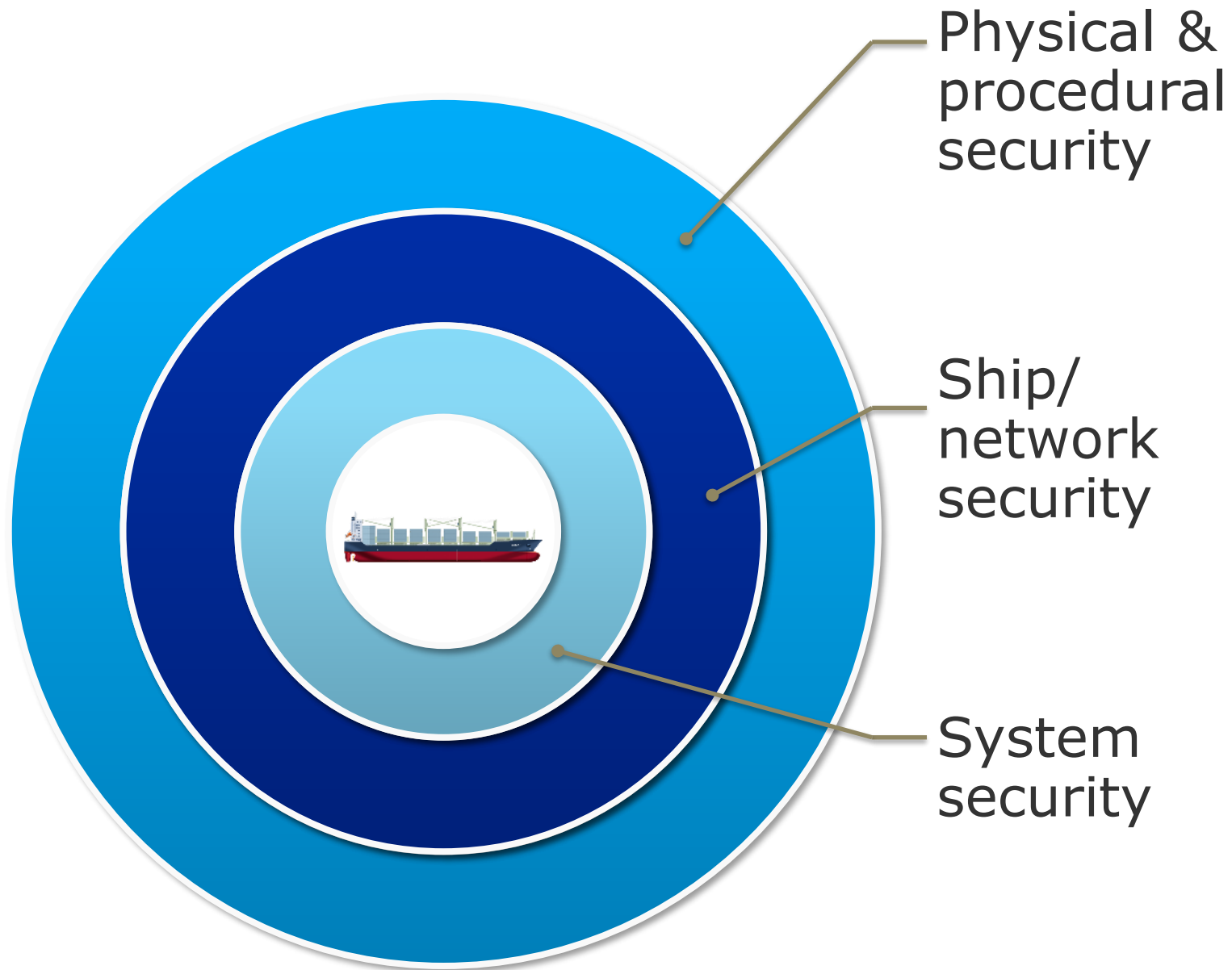
- **Pre-qualify vessel system's or component's** security capabilities using DNVGL-CP-0231
- **Requirements in rules** for class notation Cyber secure accepting recognized standards **IEC62443(control)** and **IEC61162-460(bridge)**





# Effective Cyber security barriers using Defence in Depth concept

## Defence in depth model



## All layers support cyber resilience

- **Physical & procedural barriers** protect vessel systems using physical access and procedures (patching, access cards, locked cabinets, maintenance scans, “human firewall”, ...)
- **Ship barriers** protect connection between zones & systems with remote access (VPN, DMZ, ...), segregation (firewalls, data diodes, ...)
- **System barriers** protect the individual system with barriers such as encryption, user control and authentication, removable devices, event logging, backup and recovery, etc.

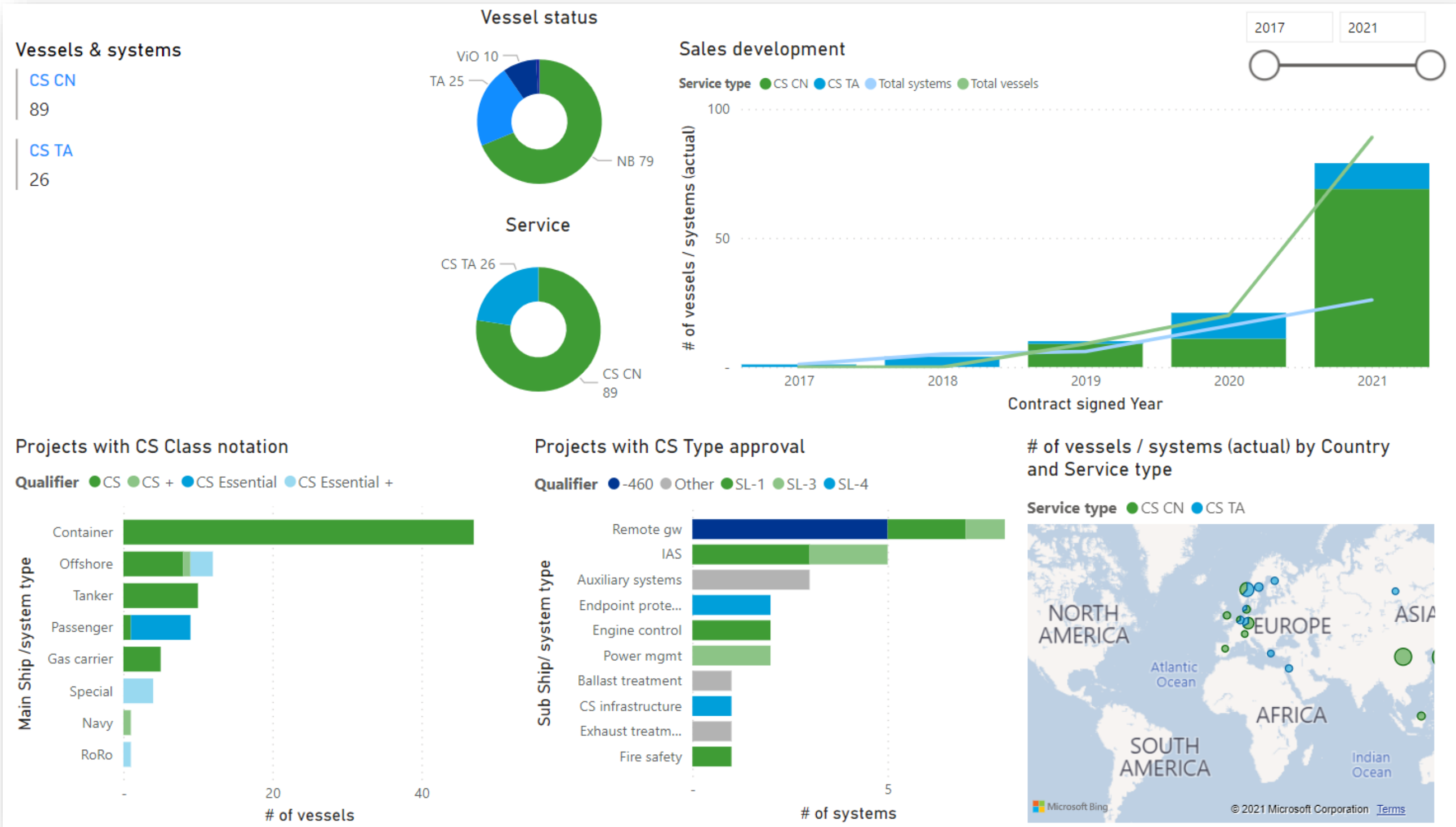
# High uptake of Cyber secure verification among yards & suppliers



SAMSUNG HEAVY INDUSTRIES



...and many more



...and more

# The needs of the Maritime Industry is developing

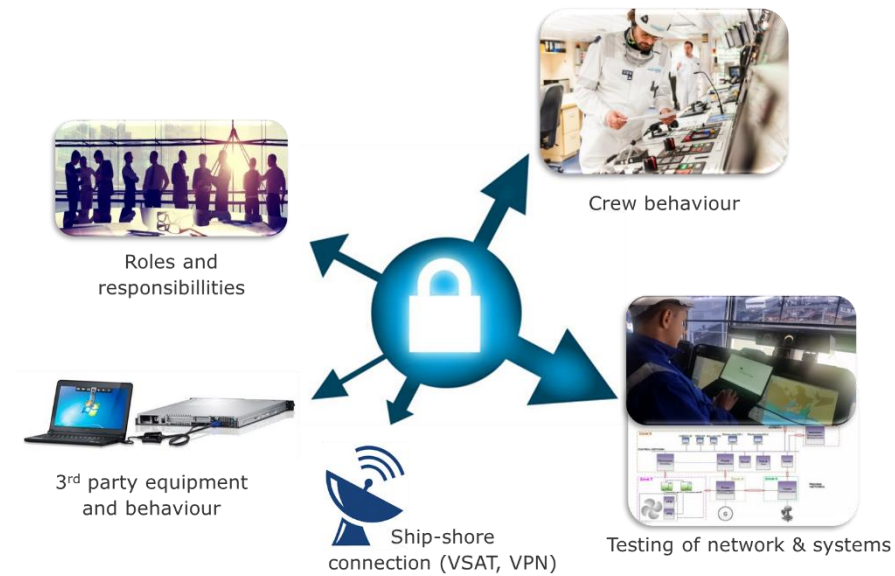
Assess/Test  
...2016...

Improve  
...2018...

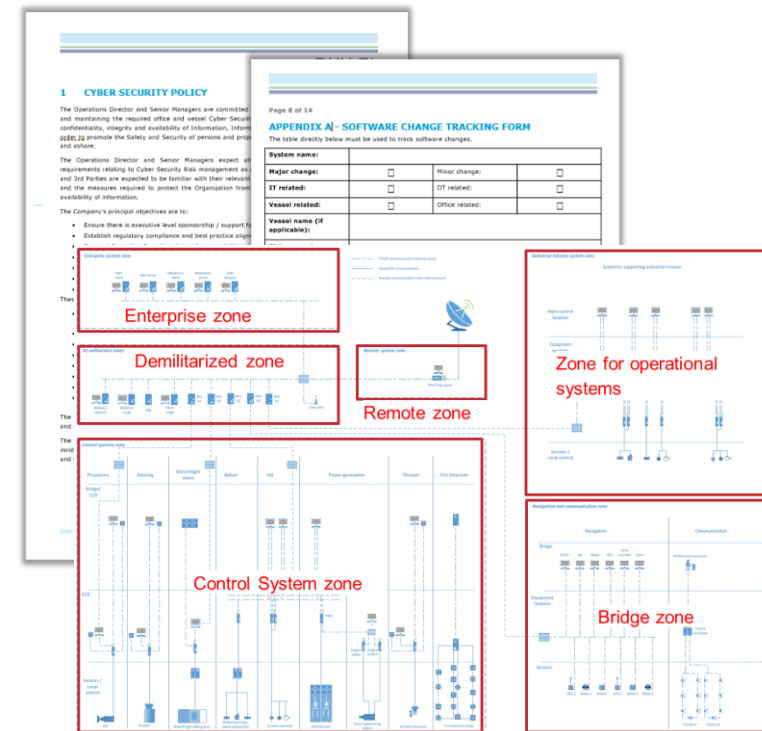
Implement  
...2020...

Manage/Assure  
...2022...

## On-board assessment & testing



## SMS and Technical Doc. Development



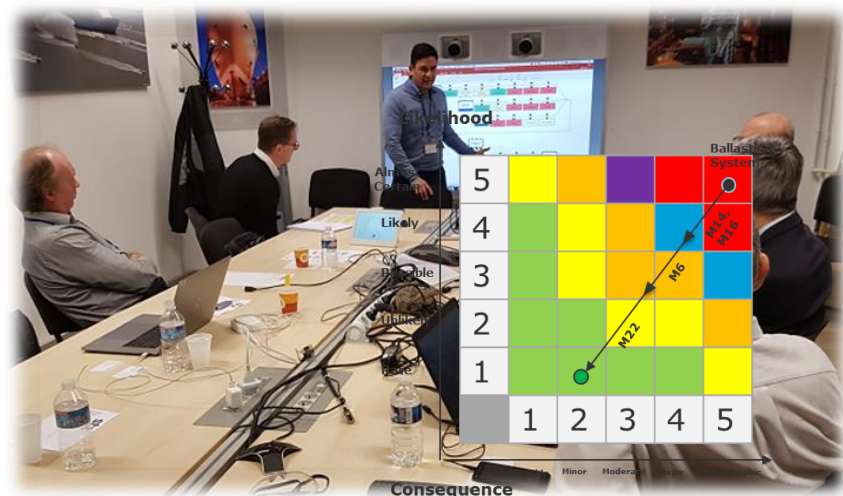
## On demand Cyber Security Office



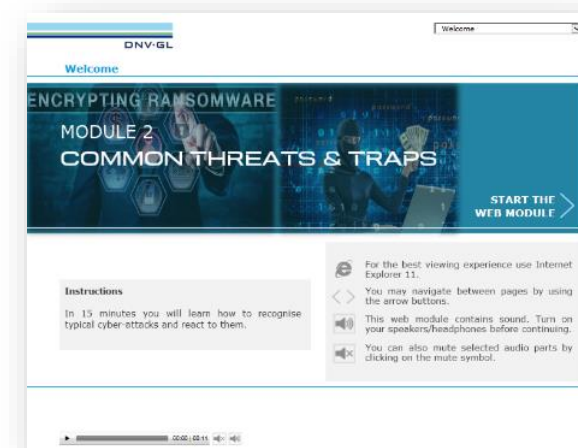
## Ship in Operation

RequirementID	RequirementID:Title	Date	Rating
IMO2021-MG-01	Objectives of SMS	5/15/2020	Low
IMO2021-MG-02	Compliance	5/15/2020	Low
IMO2021-MG-03	Cybersecurity policy ar	5/15/2020	Low

## Cyber risks assessment



## Training



## Exercises & Surveys

### Scenario 1: Loading incident

During unloading the loading and stability computer crashes, and the system does not recover after reboot. The crew loses the overview of the operations, as the system is also used to monitor cargo control. Time is stable until the system is restored at the

DNV GL

Welcome

Cyber Security Awareness - Crew

25%

Importance of cyber security on board

Please select the vessel you are currently sailing on?

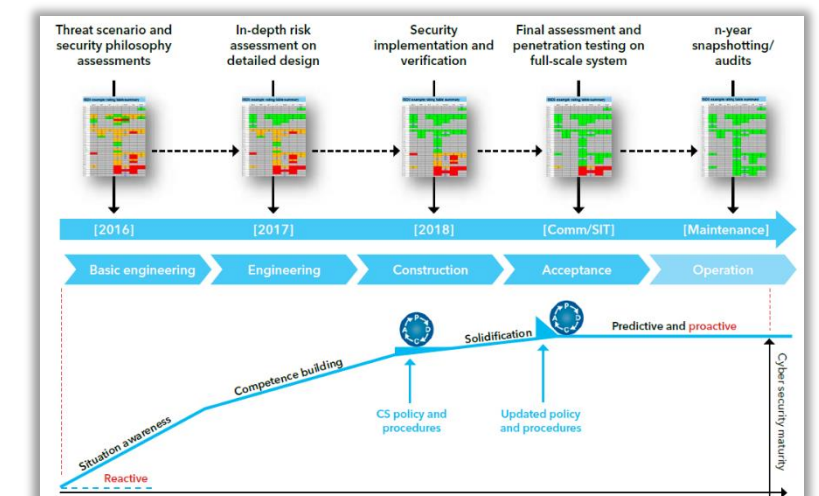
Select

In your opinion, how important is cyber security on board?

1 Not important 4 Highly important

What makes you feel like that way?

## Newbuilding



# Thank you!

[svante.einarsson@dnv.com](mailto:svante.einarsson@dnv.com)

+49 (0)175 49 100 74

[www.dnv.com](http://www.dnv.com)



**MR. SANJEEV WEWERINKE-SINGH**

*Director – Varuna Marine Services B.V.*



**Varuna Marine Services**  
Smart Sustainable Shipping



**Cyber Waves**  
**ROLLING OUT SOLUTIONS**

# WILL IT AFFECT US?

All four of the largest maritime shipping companies have all been hit by a ransomware attack between 2017 and Sept 2020.

- French shipping giant CMA CGM has been hit by a ransomware attack Sept 2020.
- Mediterranean Shipping Company - hit in April 2020 by an unnamed malware strain that brought down its data center for days.
- COSCO - brought down for weeks by ransomware in July 2018.
- APM-Maersk - taken down for weeks by the NotPetya ransomware/wiper in 2017.



# WHAT SHALL CYBER RISK MANAGEMENT INCLUDE?

## Respond to and recover from cyber security incidents

Respond to and recover from cybersecurity incidents using the contingency plan. Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

## Establish response plans

Develop contingency plans to effectively respond to identified cyber risks.

## Identify threats

Understand the external cybersecurity threats to the ship.  
Understand the internal cybersecurity the threat posed by inappropriate use and poor cyber security practices.

## Identify vulnerabilities

Develop inventories of onboard systems with direct and indirect communications links. Understand the consequences of a cyber security threat on these systems.  
Understand the capabilities and limitations of existing protection measures.

## Assess risk exposure

Determine the likelihood of vulnerabilities being exploited by external threats.  
Determine the likelihood of vulnerabilities being exposed by inappropriate use.  
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

## Develop protection and detection measures

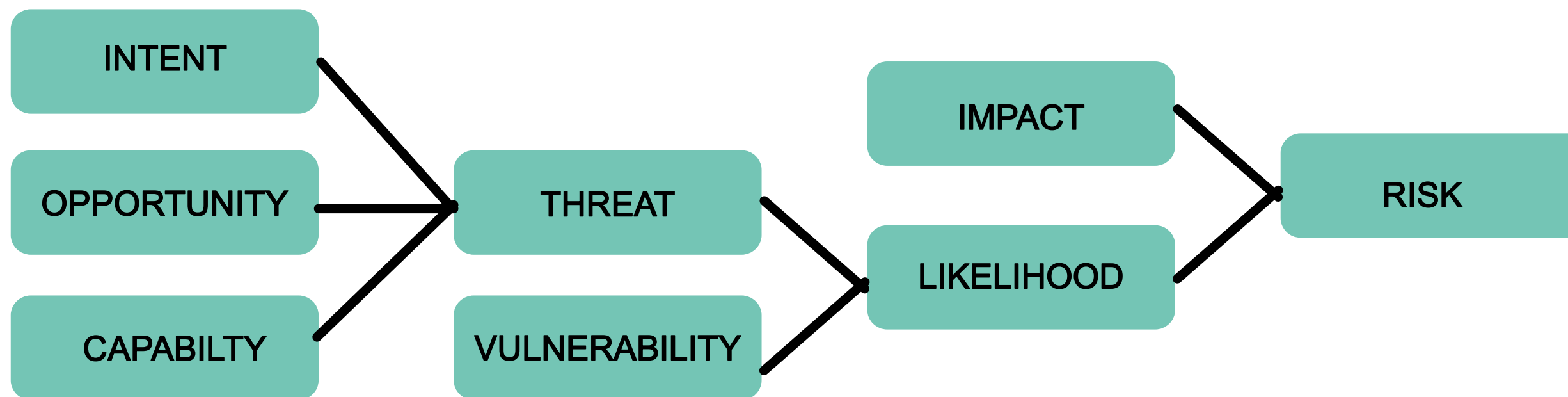
Reduce the likelihood of vulnerabilities being exploited through protection measures.  
Reduce the potential impact of a vulnerability being exploited.





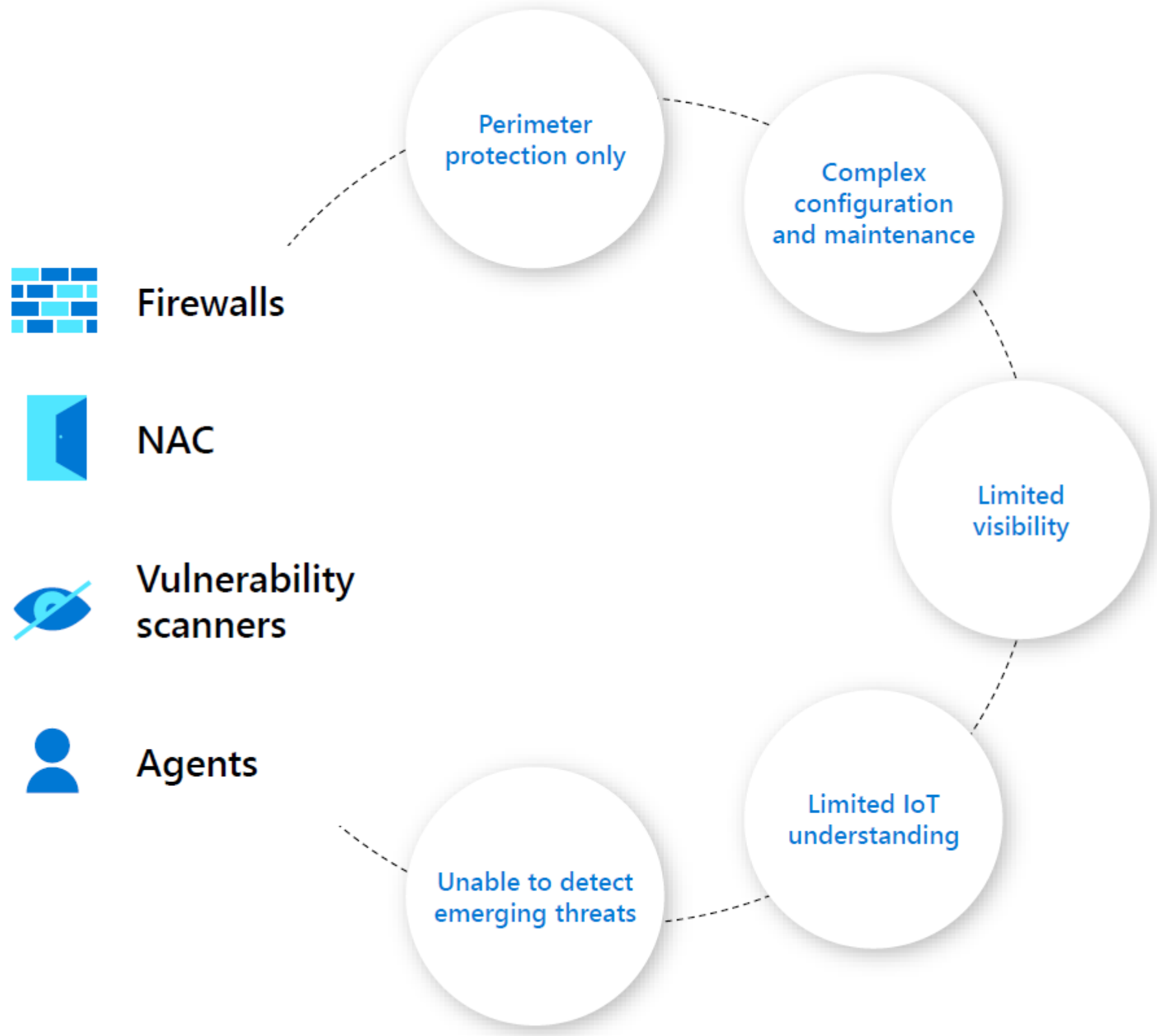
# RISK ASSESSMENT

- Relationship between factors influencing risk



- The four phases of a risk assessment
- Third party risk assessment

# Challenges with existing solutions



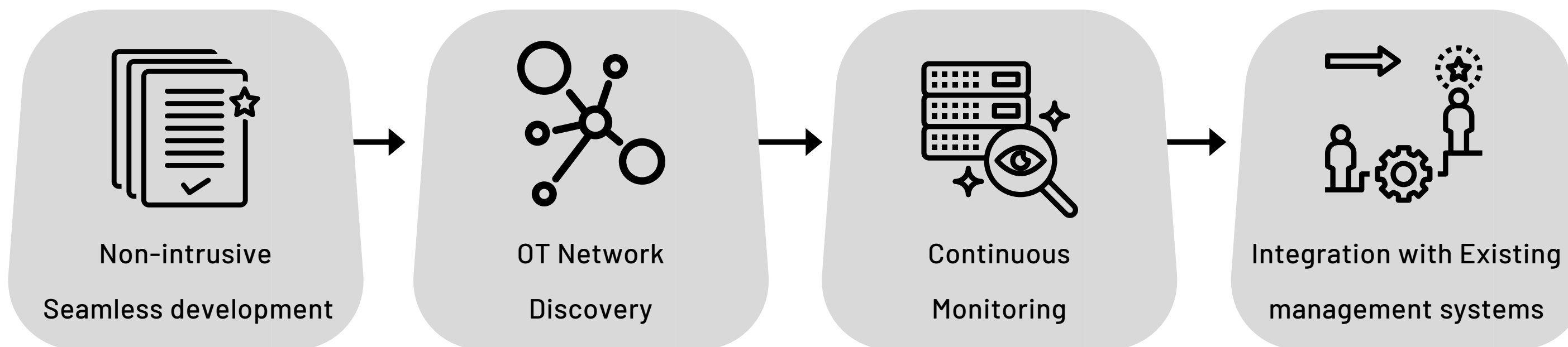


# 24/7 Network Monitoring : CyberShell

It requires a shift in the security mindset from

“How can I air gap or isolate?” to “How can I stay secure while connected?”

How it works:

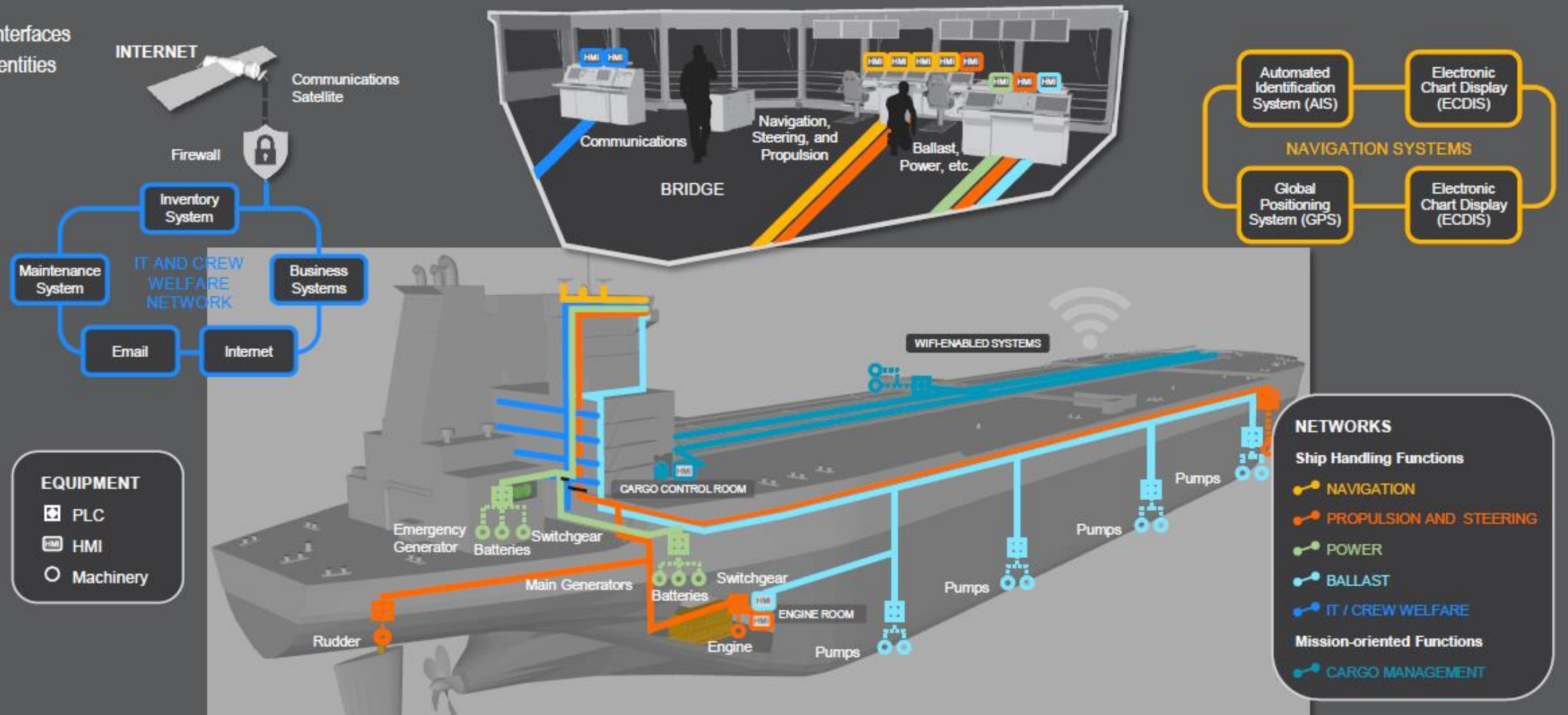


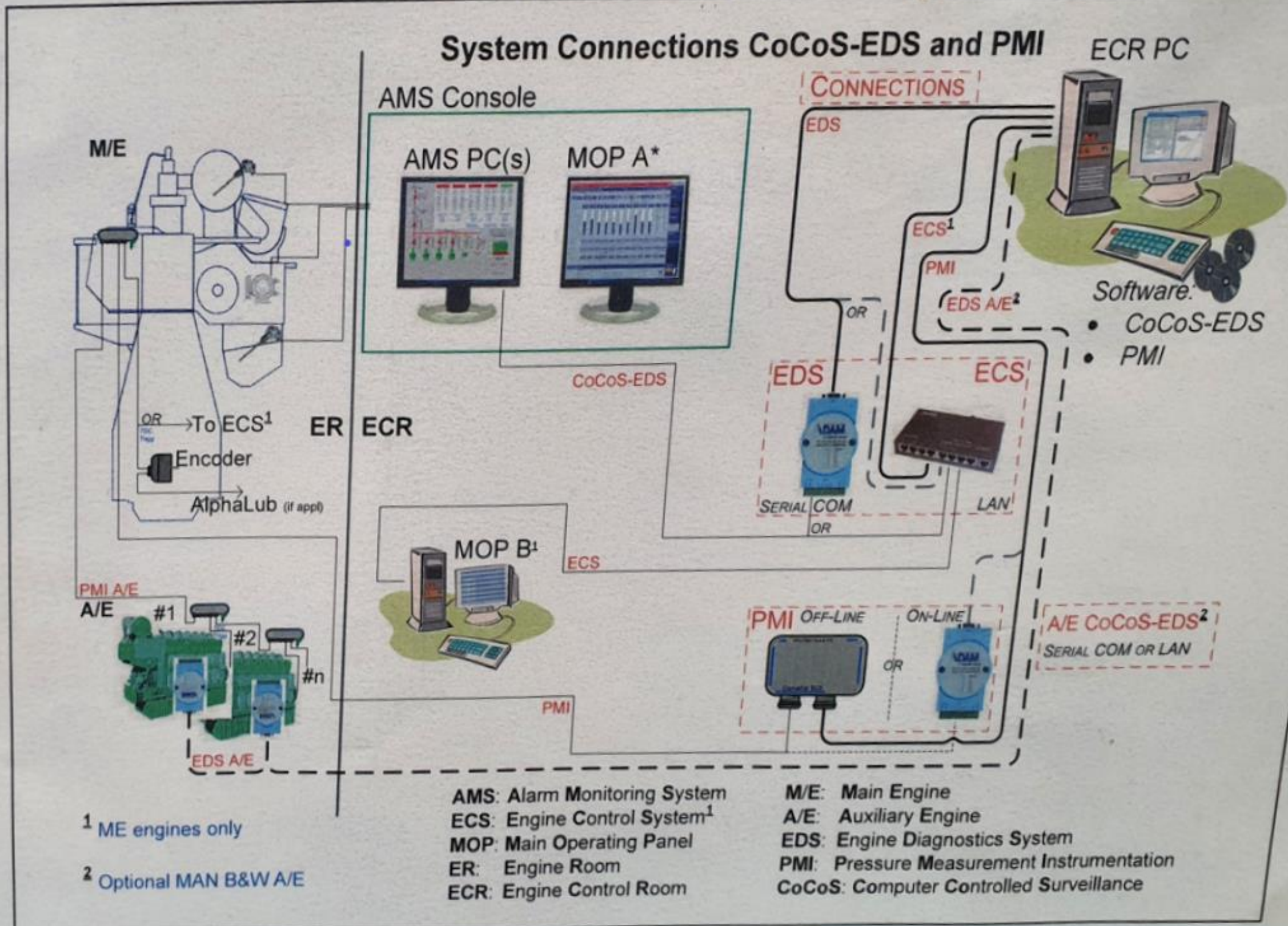
# The Virtual Asset

Maritime assets are designed to perform a specific set of functions. For vessels, these include both ship handling and mission-oriented functions. This diagram illustrates several representative functions for a tanker ship and how they are implemented using various onboard networks.

The cyber security risk exposure of an asset is highly dependent on the number of:

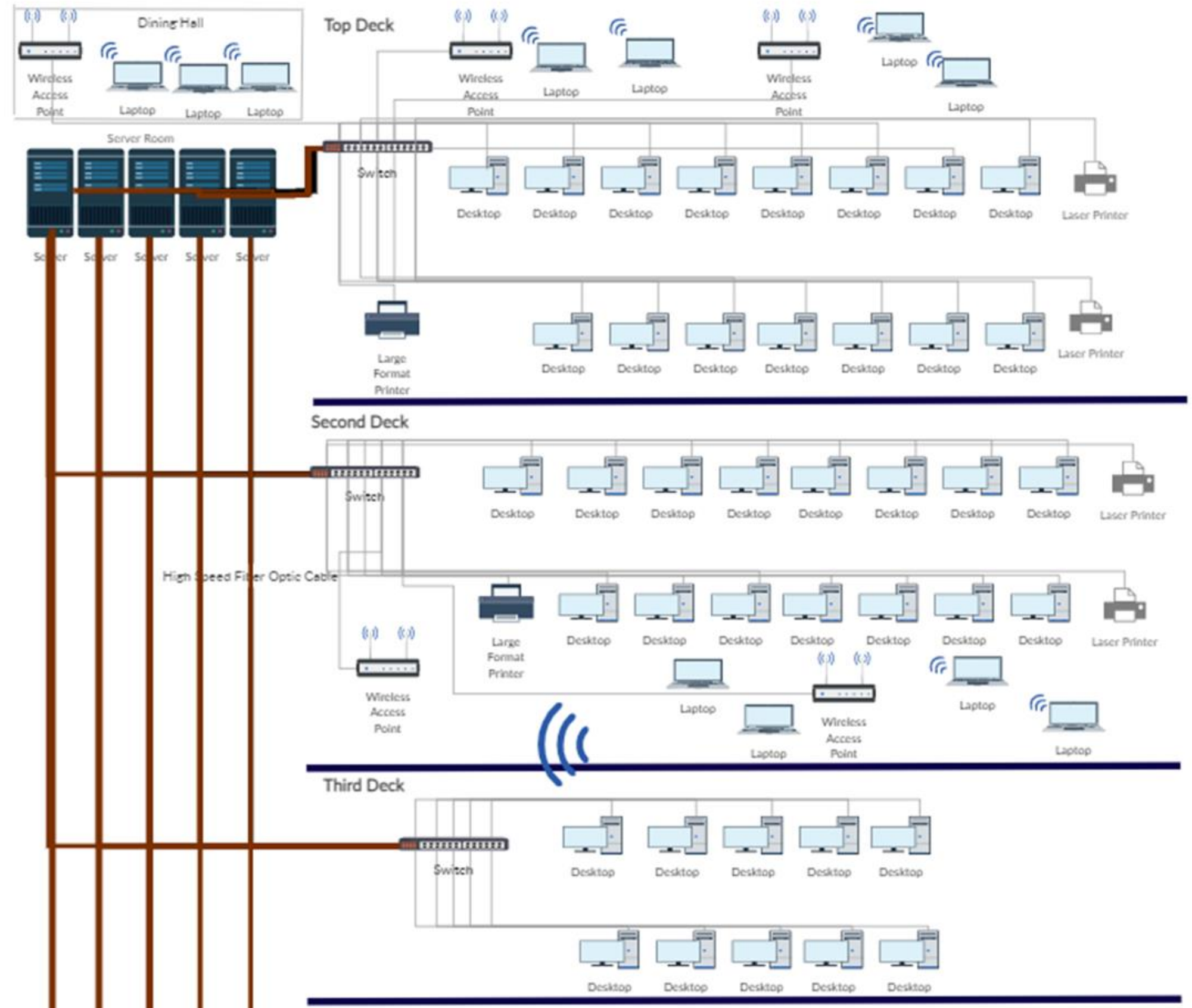
1. Safety-critical functions
2. Network connections and interfaces
3. Authorized/unauthorized identities







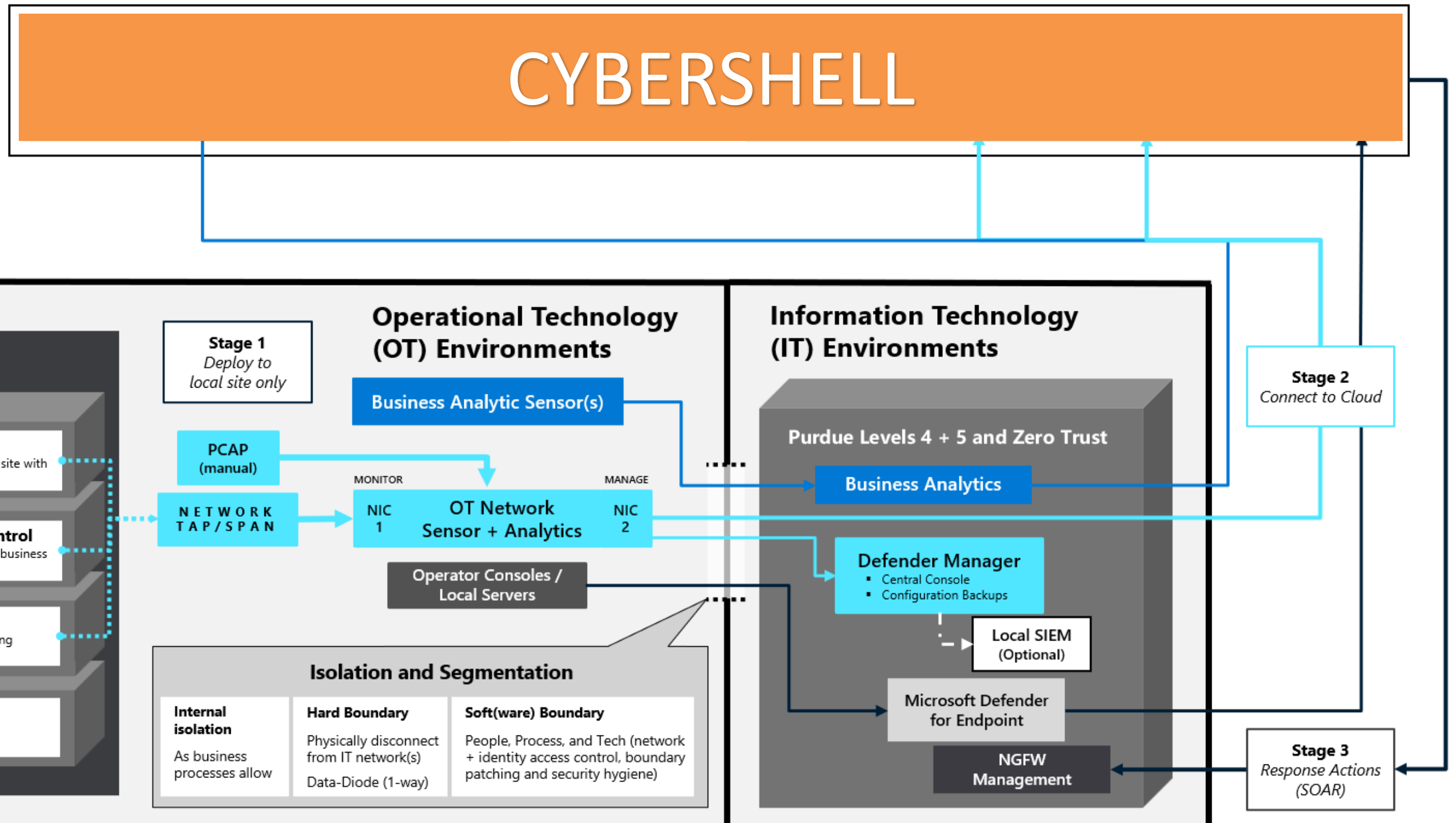
# Network Mapping Sample



# Operational Technology (OT) Deployment Options

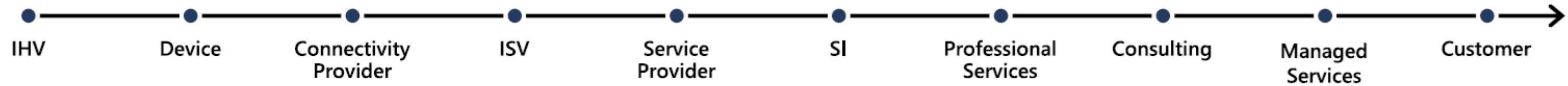
Apply zero trust principles to securing OT and industrial IoT environments

Blended cybersecurity attacks are driving **convergence of IT, OT, and IoT** security architectures and capabilities





# Ecosystem momentum



<p>Microsoft Partners</p>	
<p>OT Landscape</p>	

# Finished Intelligence

Turning raw data into finished, actionable intelligence.

## CyberShell



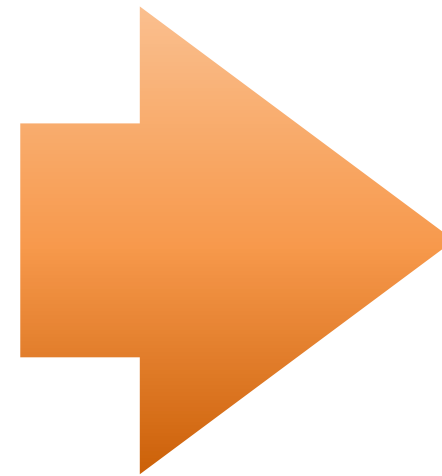
## Remote and Onsite OT Systems

### Coverage

- OT and IT
- Fleet-wide / Company-wide
- Own Fleet
- Managed Fleet
- All Systems, Networks and Devices

### Considerations

- Passive OT Monitoring (agentless)
- Low Bandwidth
- Secure Transmission



## Finished Actionable Intelligence



### Monitoring and Alert Management

- 24/7/365
- Tier 1 & Tier 2
- Explanation and direction



### Analytics and Reporting

- Monthly/quarterly reports
- Insights and analysis
- Summarized and actionable



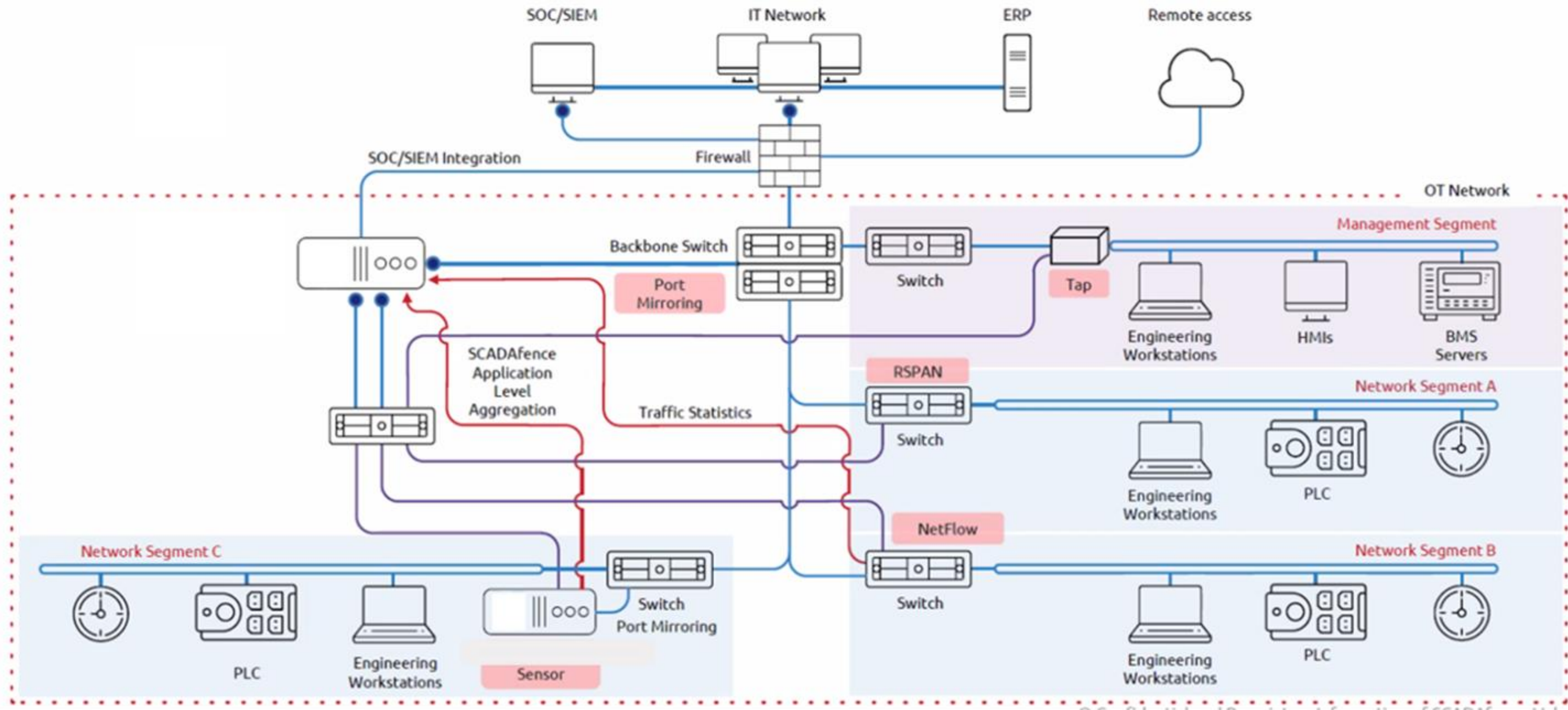
### Threat Hunting

- Proactive searching
- Advanced threats
- Applied threat intelligence

Finished intelligence requires the right tools, technology and domain expertise



# FLEXIBLE DEPLOYMENT OPTIONS



178  
Total Assets

27  
Controllers

10  
HMIs

1.8 GB  
L3 Traffic

8.2 GB  
L2 Traffic

219  
Alerts

28.02 Kb/s  
Current bandwidth



Critical  
Health



Top Alerts

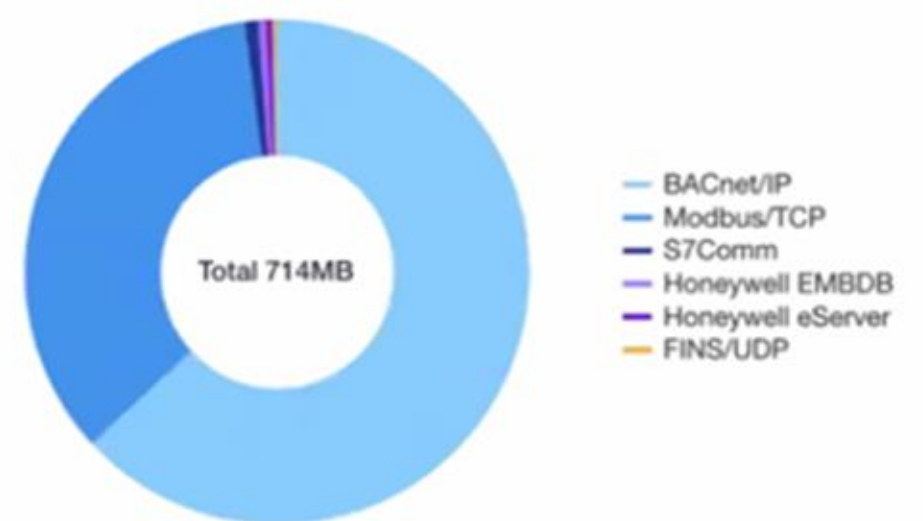
All Categories ▼

- **Group-to-group communication**  
05/26/2020 18:02:25
- **Trickbot trojan communication detected**  
07/18/2020 07:33:16  
192.168.0.102
- **Security Incident Detected**  
05/20/2020 14:07:47  
192.168.0.222
- **SMB exploitation attempt - MS17-10 EternalBlue**  
06/11/2019 15:42:04  
192.168.1.24
- **Vulnerability assessment tool detected - Nessus**  
08/28/2017 11:22:38  
192.168.1.16
- **TeamViewer inbound connection established**  
08/16/2020 07:33:51  
192.168.1.135
- **TeamViewer inbound connection established**  
05/26/2020 16:17:08

Industrial Protocols

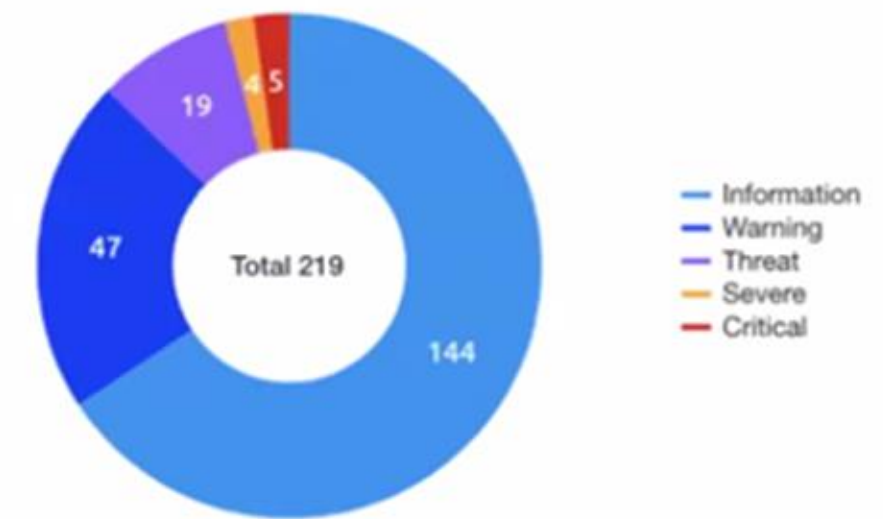
Show Others 🕒 🗨

[Select Protocols](#) [Protocols Report](#)



Alerts

SEVERITY TYPE CATEGORY DAILY



Alerts Pivot by Type

[View Report by Type](#)

Alert Type	Severity..↓	# of Alerts
API	●	2
Vulnerability assessment tool dete...	●	1
Trickbot trojan communication det	●	1

Assets Pivot

Select Dimension Device type

Device type	Total ↓
Others	88
Workstation	24

# Assets Manager

CVE Management WMI Hosts

Select Columns All Types Type exact IP

L3 Assets	L2 Assets	External Hosts	Assets Pivot	Threat Assessment	IP	Hostname	MAC	Vendor	OS	Device types	Alerts	# Int.	# Ext.	Total Traffi... ↓	First seen	Last Seen
					<a href="#">192.168.0.170</a>	Mitsubishi ...	58:52:8A:B7:AB:...	Mitsubishi ...		PLC	1 1	4	0	11.27 MB	03/17/2019 12:29:14	04/24/2019 14:14:53
					<a href="#">192.168.0.125</a>	Eng_STA_6	00:0C:29:8B:18:D6	VMware, Inc.	Windows 7	Engineering...	2 1	2	0	11.21 MB	03/17/2019 13:53:28	03/17/2019 15:21:06
					<a href="#">10.11.0.154</a>		5C:F9:DD:73:FF:...	Dell Inc.	Windows	Engineering...	0	1	0	8.49 MB	08/28/2019 10:48:56	08/28/2019 10:49:52
					<a href="#">192.168.0.155</a>	PLC-9054e	00:24:59:0A:A9:C4	ABB Autom...		PLC	1	3	0	6.86 MB	03/17/2019 12:19:42	04/24/2019 14:09:15
					<a href="#">192.168.0.123</a>	Eng_STA_1	00:0C:29:17:D1:76	VMware, Inc.	Windows 7	Engineering...	1 1	8	0	6.17 MB	03/17/2019 12:19:43	03/17/2019 13:08:03
					<a href="#">192.168.0.140</a>	PLC-TE246	00:80:F4:1B:CD:22	Telemehan...		PLC	1	5	0	5.56 MB	03/17/2019 12:19:50	04/24/2019 14:16:50
					<a href="#">10.11.0.202</a>		F4:54:33:AD:39:7A	Rockwell A...		PLC	1 1	1	0	5.52 MB	05/26/2020 14:56:38	05/26/2020 15:27:04
					<a href="#">192.168.0.107</a>	Eng_STA_4	00:0C:29:58:97:76	VMware, Inc.	Windows 7	Engineering...	2	3	0	5.41 MB	03/17/2019 15:00:43	06/11/2019 15:42:04
					<a href="#">192.168.0.135</a>		AC:64:17:12:5C:51	Siemens AG		PLC	1 2	5	0	4.38 MB	03/17/2019 12:20:09	04/24/2019 14:16:52
					<a href="#">10.117.2.17</a>	xperion_srvb	00:10:18:C8:98:00	Broadcom	Windows S...	Experion eS...	1 1	43	0	3.5 MB	10/19/2020 14:32:02	10/27/2020 15:23:14
					<a href="#">10.212.120.200</a>		00:FF:84:41:5A:19	AP-NordVPN		VPN client	0	0	0	2.72 MB	04/10/2016 07:12:12	04/10/2016 07:33:19
					<a href="#">10.117.1.11</a>	xperion_srv...	00:10:18:C0:86:FC	Broadcom	Windows S...	Experion eS...	1 1	51	0	2.54 MB	10/19/2020 14:32:03	10/27/2020 15:22:14
					<a href="#">192.168.0.141</a>	Schneider_...	00:80:F4:1B:CD:22	Telemehan...			1	46	1	2.54 MB	03/17/2019 12:19:45	04/24/2019 14:09:14
					<a href="#">192.168.0.130</a>		28:63:36:7E:85:49	Siemens AG		PLC	1	6	0	2.48 MB	03/17/2019 12:19:43	04/24/2019 14:16:53
					<a href="#">192.168.0.50</a>	Eng_STA_2	00:0C:29:65:1C:29	VMware, Inc.	Windows 7	VoIP	1	1	0	2.41 MB	03/17/2019 13:23:18	03/17/2019 13:49:24

● 192.168.0.170 (Mitsubishi R04) ● 1 Information ● 1 Threat **Connections:** 4 Internal

5 Exposure Groups

<b>Device types:</b>	PLC	
<b>OS:</b>		
<b>Hostname:</b>	Mitsubishi R04	 
<b>Vendor:</b>	Mitsubishi Electric Corporation	
<b>MAC:</b>	58:52:8A:B7:AB:EC	
<b>First seen:</b>	March 17th 2019, 12:29:14	
<b>Last Seen:</b>	April 24th 2019, 14:14:53	
<b>NIC Type:</b>	Ethernet	

**Additional Details****Module name:** R04CPU**Organization Details**

<b>Criticality:</b>	High	 
<b>OU:</b>	Substation_12	 
<b>Owner:</b>	Harry D.	 
<b>Physical Location:</b>		 
<b>Comment:</b>		 
<b>Product for CVE:</b>		 
<b>Version for CVE:</b>		 

## ▲ Open Alerts



ID	Severity ↓	Description	Status	Details	MITRE ATT&CK	Alert Time	
190	●	PLC start command issued	In Progress	<a href="#">192.168.0.125 (Eng_STA_6)</a> sent a PLC start command to PLC on <a href="#">192.168...</a>	Execution > Change Pr...	03/17/2019 14:06:47	
116	●	New host detected	Created	New host detected: <a href="#">192.168.0.170 (Mitsubishi R04)</a> from source: ARP Packet.		03/17/2019 12:29:14	

⏪ &lt; 1 &gt; ⏩

1 - 2 of 2 items

Connections

Exposure Map

Layered Map

Subnet  
Topology

All Types

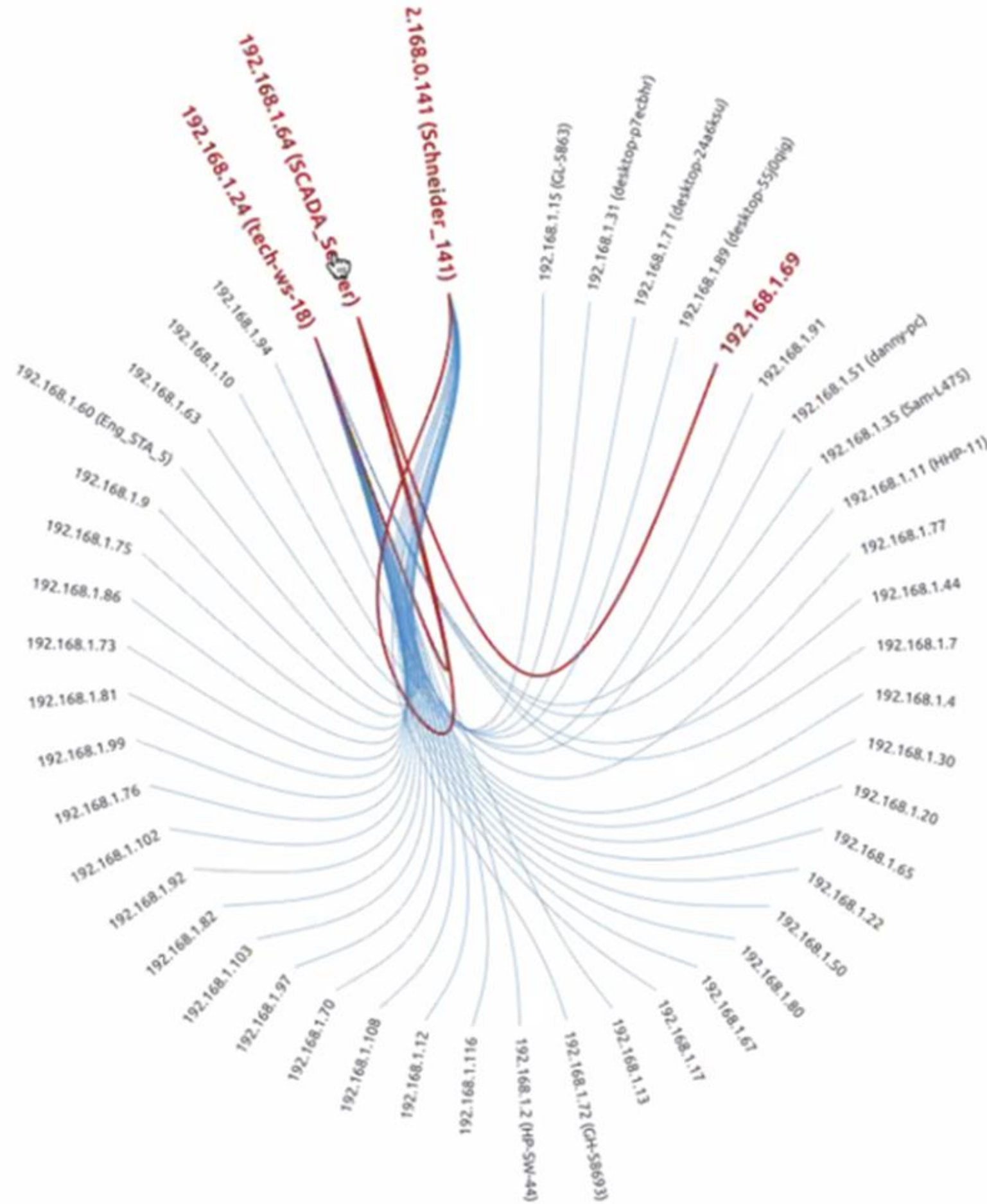
Search IP/Hostname

Hostname & IP address

All data



YES  Connections only



# Network Maps

Logical Groups

Connections

Exposure Map

Layered Map

Subnet Topology

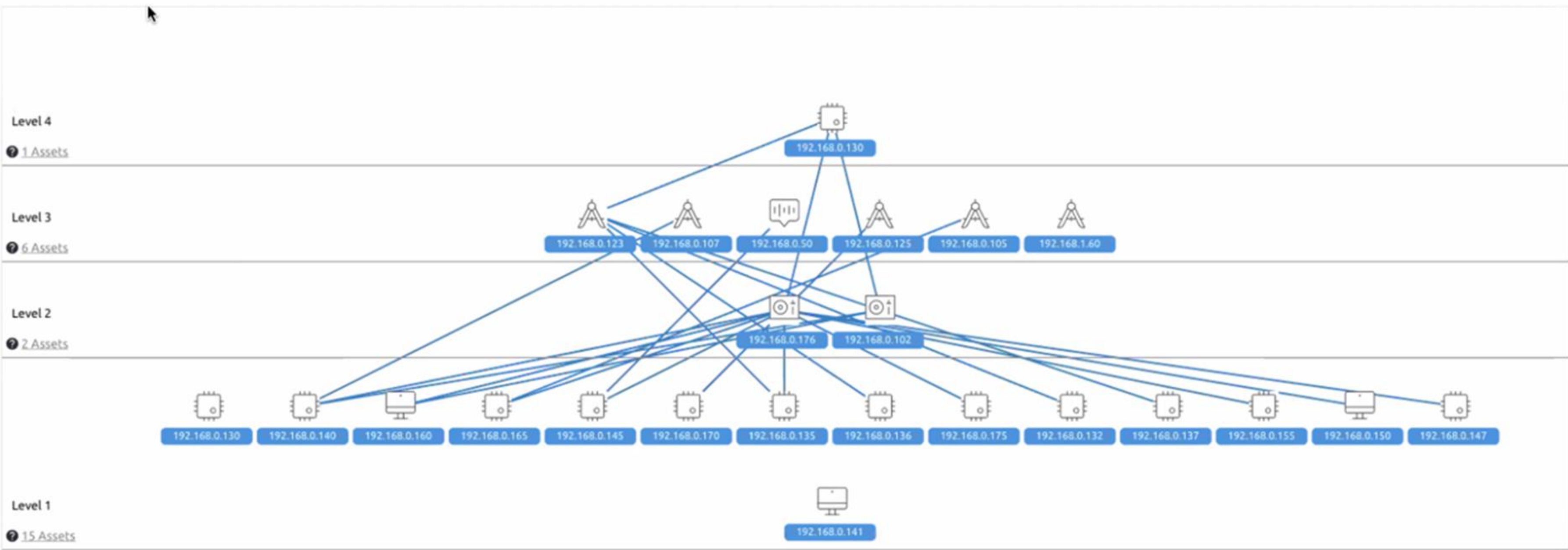
IP labels

All data



Layered Map Purdue Model

Direction





# Traffic Analyzer

Protocols over Time

< IP Conversations

TCP/UDP Conversations

Protocols

Industrial Protocols

Industrial Layer 2 >

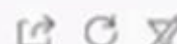
All Protocols

Type Port

All data



Protocol	Dest. Port	Trans...	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total ↓
BACnet/IP	47808	UDP	836.77K	831.72K	197.35 MB	253.34 MB	450.68 MB



Conv...	Source IP	Src. Port	Dest. IP	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total ↓	In...
1	<a href="#">10.15.5.102</a>	generic	<a href="#">10.15.5.111</a>	124.44K	124.46K	82.2 MB	125.65 MB	207.85 MB	
1	<a href="#">10.15.5.111</a>	47808	<a href="#">10.15.5.127</a>	364.05K	364.03K	58.4 MB	45.79 MB	104.18 MB	
6	<a href="#">10.15.5.100</a>	47809	<a href="#">10.15.5.111</a>	107.59K	105.12K	19.92 MB	28.19 MB	48.1 MB	
1	<a href="#">10.15.5.102</a>	generic	<a href="#">10.15.5.112</a>	62.57K	62.53K	13.16 MB	20.02 MB	33.17 MB	
1	<a href="#">10.15.5.102</a>	generic	<a href="#">10.15.5.113</a>	61.91K	61.84K	13.12 MB	19.98 MB	33.1 MB	
6	<a href="#">10.15.5.100</a>	47809	<a href="#">10.15.5.112</a>	93.42K	91.8K	7.3 MB	8.89 MB	16.2 MB	
5	<a href="#">10.15.5.100</a>	47809	<a href="#">10.15.5.113</a>	16.86K	15.28K	2.71 MB	4.14 MB	6.85 MB	
2	<a href="#">192.168.0.180</a>	47808	<a href="#">192.168.0.181</a>	5.36K	5.98K	498.59 KB	629.29 KB	1.13 MB	
1	<a href="#">192.168.0.176</a>	47808	<a href="#">192.168.0.180</a>	444	444	32.76 KB	39.75 KB	72.5 KB	
1	<a href="#">192.168.0.20</a>	65536	<a href="#">192.168.0.181</a>	112	233	7.06 KB	16.64 KB	23.7 KB	

1 2

1 - 10 of 11 items

+	Modbus/TCP	502	TCP	2.28M	2.06M	135.72 MB	123.01 MB	248.54 MB
+	iPulse-ICS	20222	TCP	49.17K	85.17K	3.01 MB	101.41 MB	104.42 MB
+	HTTPS	443	TCP	102.99K	80.75K	12.69 MB	88.81 MB	101.5 MB
+	MS-SQL-s	1433	TCP	638.64K	637.78K	40.64 MB	41.37 MB	82.01 MB

# Alerts Manager

Alerts Policy Firewall Rules Logs

Open 219

Resolved 97

Don't show 1

Stale 90

All 316

Alerts Pivot

Select Columns

All Types

All Severities



Mark 0 selected as Resolved

<input type="checkbox"/>	ID	Severity ↓	Description	Status	IP	Hostname	Details	Last Event Time
<input type="checkbox"/>	50100	●	Group-to-group communication	In Progress			User rule "Unauthorized Traffic": Communication between group "DMZ_Plant...	05/26/2020 18:02:25
<input type="checkbox"/>	1446	●	Trickbot trojan communication detected	In Progress	<a href="#">192.168.0.102</a>	desktop-cs7vbmu	<a href="#">192.168.0.102 (desktop-cs7vbmu)</a> is communicating with a Trickbot C&C ser...	07/18/2020 07:33:16
<input type="checkbox"/>	554	●	Security Incident Detected	In Progress	<a href="#">192.168.0.222</a>	WSTA_4	Multiple alerts on this IP.	05/20/2020 14:08:03
<input type="checkbox"/>	465	●	SMB exploitation attempt - MS17-10 Ete...	In Progress	<a href="#">192.168.1.24</a>	tech-ws-18	SMB exploit detected - device <a href="#">192.168.1.24 (tech-ws-18)</a> sent an exploit to d...	02/19/2020 16:18:14
<input type="checkbox"/>	10	●	Vulnerability assessment tool detected - ...	In Progress	<a href="#">192.168.1.16</a>	scadafence-pc	Nessus communication detected from <a href="#">192.168.1.16 (scadafence-pc)</a> to target...	02/12/2020 13:31:08
<input type="checkbox"/>	50103	●	TeamViewer inbound connection establis...	In Progress	<a href="#">192.168.1.135</a>	scadafence-rbi10d	TeamViewer inbound connection was established from device 213.227.181.1...	08/16/2020 07:34:08
<input type="checkbox"/>	51888	●	TeamViewer inbound connection establis...	In Progress	<a href="#">10.11.0.200</a>	powersvr1	TeamViewer inbound connection was established from device <a href="#">192.168.1.135 (...)</a>	08/16/2020 07:34:08
<input type="checkbox"/>	559	●	Communication with vulnerable device	In Progress	<a href="#">192.168.0.132</a>	plc_32	Industrial device 192.168.0.132 (plc_31) has communicated with device 192.1...	11/05/2020 13:12:37
<input type="checkbox"/>	518	●	Domain reputation alert	In Progress	<a href="#">192.168.0.101</a>	WS-yk75	Device <a href="#">192.168.0.101 (WS-yk75)</a> tried to resolve a known malicious domain n...	02/12/2020 13:31:08
<input type="checkbox"/>	50102	●	New Source IP Connecting to industrial ...	In Progress	<a href="#">10.11.0.202</a>		Unexpected conversation detected between IP address <a href="#">10.11.0.154 (Enginee...</a>	05/22/2020 08:22:29
<input type="checkbox"/>	50101	●	Industrial parameter value out of range	In Progress	<a href="#">10.11.38.100</a>		User rule Analog Value Validation (profile-based): Device <a href="#">10.11.38.100</a> , report...	08/29/2017 02:59:23
<input type="checkbox"/>	51867	●	Programming read command detected	In Progress	<a href="#">10.11.0.202</a>		<a href="#">10.11.0.200 (powersvr1)</a> sent a programming read sequence to PLC on <a href="#">10.11...</a>	05/26/2020 15:07:34
<input type="checkbox"/>	50042	●	Programming write command detected	In Progress	<a href="#">10.77.60.131</a>	PLC_131	<a href="#">10.77.1.60 (win-k4tva753kkg)</a> sent a programming write sequence to PLC on ...	07/29/2018 10:44:20
<input type="checkbox"/>	50019	●	PLC stop command issued	In Progress	<a href="#">10.77.0.140</a>	PLC_140	<a href="#">10.77.1.60 (win-k4tva753kkg)</a> sent a PLC stop command to PLC on <a href="#">10.77.0.1...</a>	01/16/2019 13:30:38
<input type="checkbox"/>	50001	●	PLC stop command issued	In Progress	<a href="#">192.168.60.150</a>		<a href="#">192.168.60.11</a> sent a PLC stop command to PLC on <a href="#">192.168.60.150</a> , using ...	05/17/2020 16:58:10

NIST-CSF

Production Lines: 1-3

Max IPs (max 50) 50

Display only relevant alerts

Generate


Export

- NERC-CIP
- ISO-27001
- NIST-1800-23
- NCSC-CAF
- CMMCS
- CMMC2
- CMMC Level 1

## Compliance Governance Report

Site: Production Lines: 1-3

Standard: NIST-CSF

 Report issued on: Jun 15, 2021  
Issued by: admin

## Security Report Configuration



DISPLAY PARAMETERS

SECTION VISIBILITY

MAPS CONFIGURATION

- Analysis Summary
- Top IPs at Risk
- Asset Inventory
- Network Map
- Exposure Models
- Layered Maps
- Protocol Statistics
- Bandwidth Usage
- Subnets Discovered
- Open Security Alerts
- Network Anomalies
- Open CVEs
- About SCADAfence

Cancel

Update Report

# THANK YOU!

You can reach us at:

- [info@varunamarine.eu](mailto:info@varunamarine.eu)
- [technical@varunamarine.eu](mailto:technical@varunamarine.eu)

OR [tech@cyberwaves.eu](mailto:tech@cyberwaves.eu)

Visit our website for more information:  
[www.varunamarine.eu](http://www.varunamarine.eu)



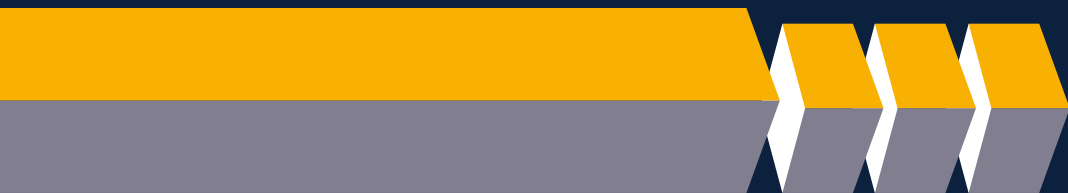
# POLLS







# POLLS





# Conclusion




# Thank You




**Varuna Marine Services**  
Smart Sustainable Shipping

## CONTACT US AT:

 info@varunamarine.eu  
marketing@varunamarine.eu

 www.varunamarine.eu

 + 31 107 640 935

## FOLLOW US ON:

 @Varunamarine

 @varunamarineservices