Dr. Theodoros Ntouskas

Managing Director, ictPROTECT

Vessel OT & IT Risk Assessment Challenges

Digital Ship

23rd ATHENS CONFERENCE

ict PROTECT

INFORMATION SECURITY SERVICES

www.ictprotect.com

Commercial Ships & Cybersecurity Requirements

ict PROTECT
INFORMATION SECURITY SERVICES

IMO IMO's MSC-FAI.1-Circ.3

NIS 2

Classification Soc.

Cyber secure class notation

TMSA3

IACS UR E27

BIMCO

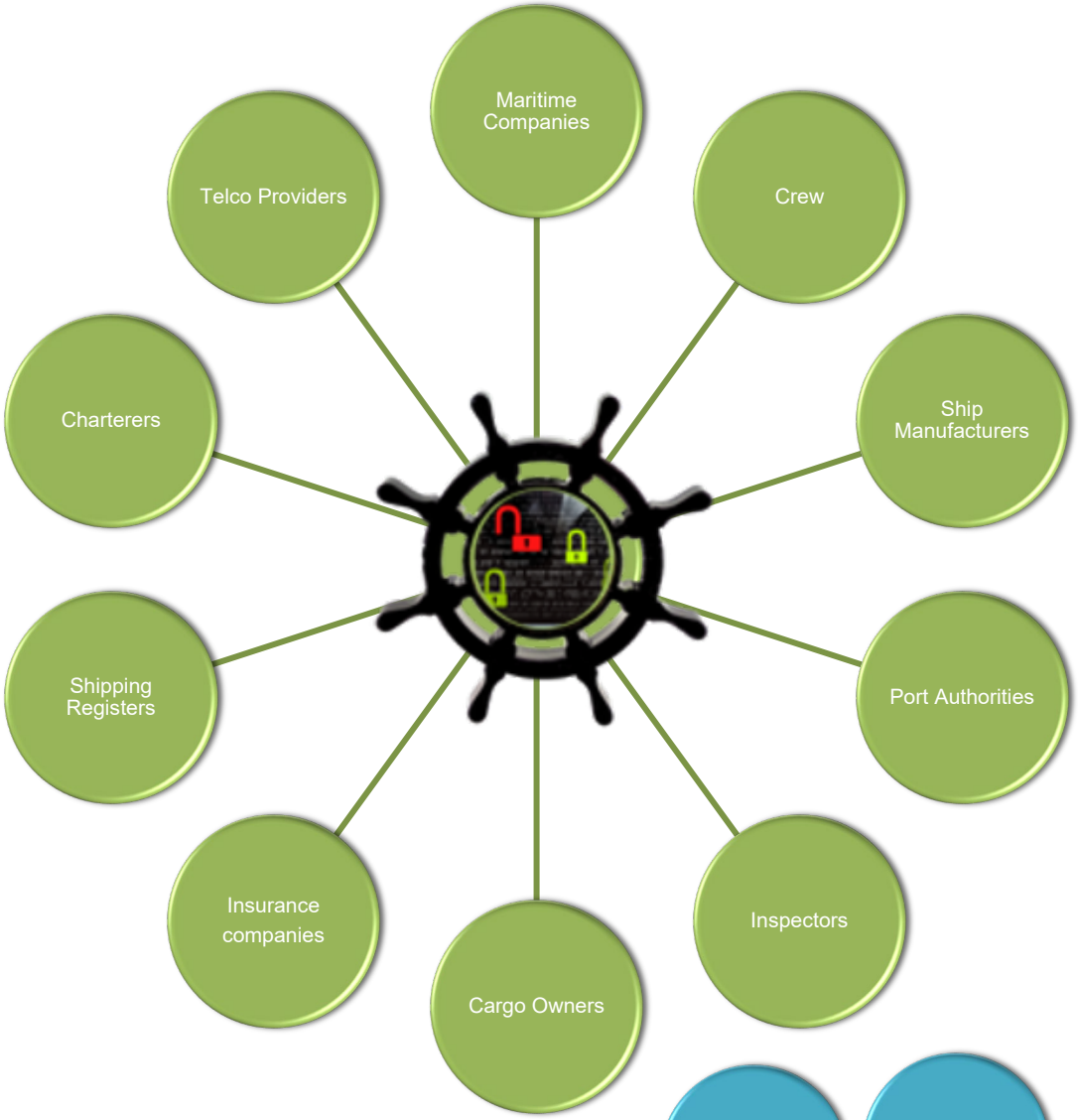
Us Coast Guard, Feb. 2020

IACS, rec.166

ENISA

UK DfT

IAPH



ISO 27001

ISO 22301

ISO 27701

SOC 2

GDPR

CCPA

ISO 27002

NIST CSF

Requirement

Class Notation

Guideline

Standard

Port Guideline

Vessels: Floating Digital Offices

ict PROTECT
INFORMATION SECURITY SERVICES

Navigation Services (AIS, GPS, ECDIS)

Communication Systems

Bridge Officers

Operational Services

Cargo Management

Crew

PMS

Maritime Company Users

Crew network

Inspectors

OT Equipment

Navigation Providers

Cloud Providers

Telco Providers

Makers

Cargo monitoring

Route exchanging to aid in navigation

IIoT

Environmental systems monitoring

Conditions monitoring

Connected Technologies: Advantages and Risks

ict PROTECT
INFORMATION SECURITY SERVICES

Advances in **digital** and **connected technologies** are transforming the global shipping network, **offering opportunities for greener, safer, and more efficient operations.**

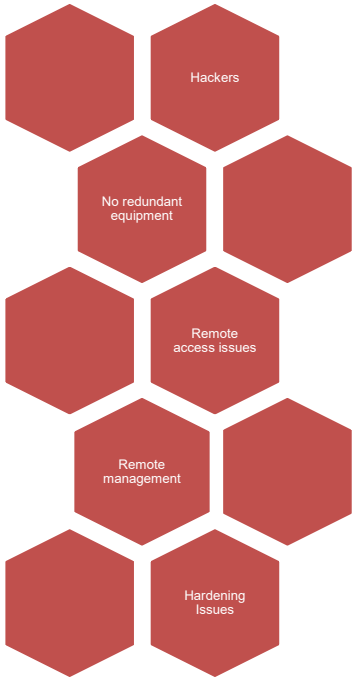
Digital technologies not only enhance sustainability but also **improve safety by automating complex processes, benefiting ports and sea safety**.

Digital technology is considered as a **key enabler for decarbonization plans**

Connected technologies are **crucial for reducing emissions through fleet and route optimization**

OT Systems: operate **semi-autonomously or fully autonomously**, enhancing efficiency and reducing human intervention.

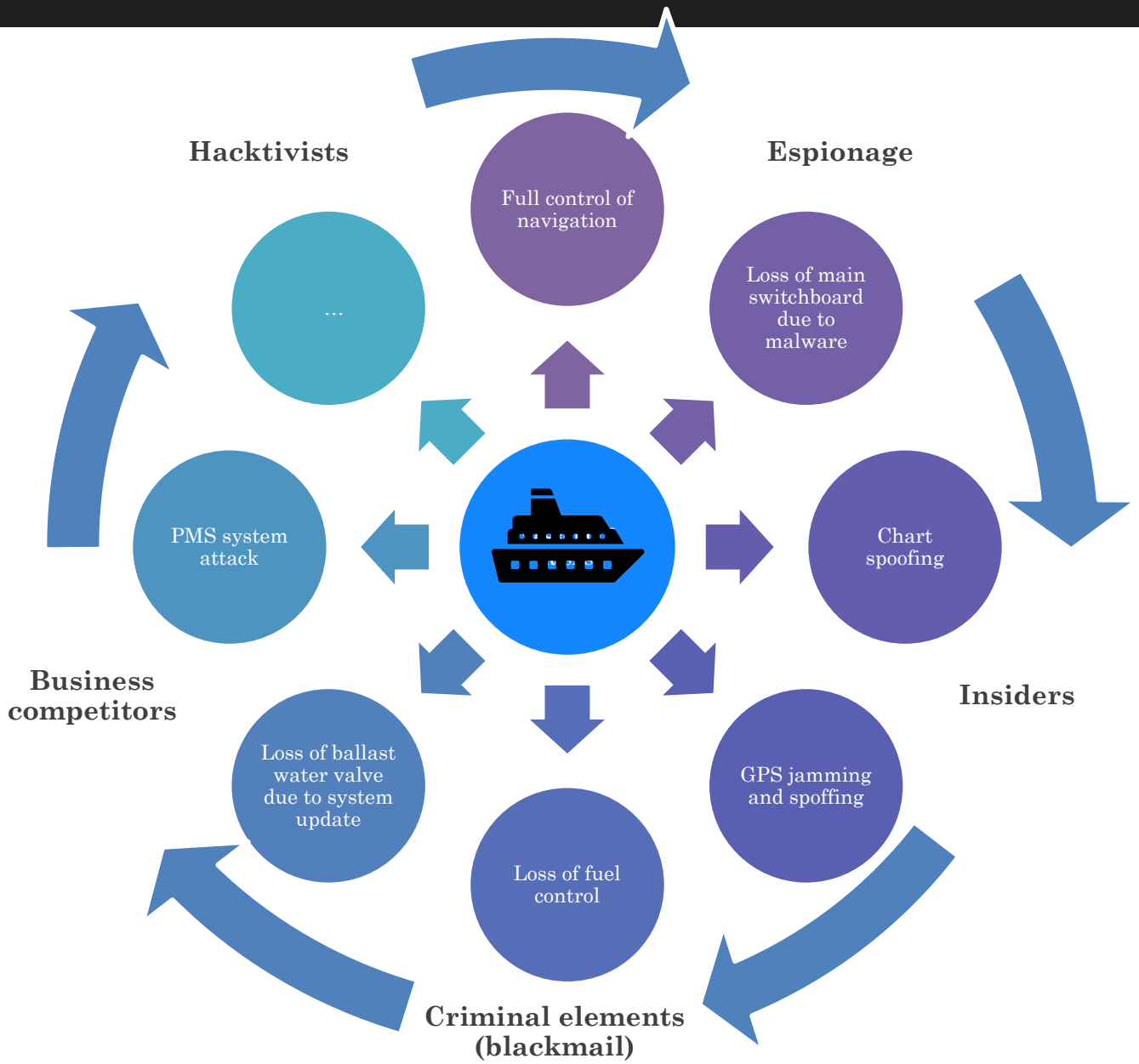
Cybersecurity Issues



The increasing connectivity in the maritime **sector raises concerns about OT cybersecurity, with more connections increasing the likelihood and speed of breaches.**

References: “REVIEW OF MARITIME TRANSPORT”: https://unctad.org/system/files/official-document/rmt2022_en.pdf
DNV: “Maritime Cyber 2023”

Risks and Attack Vectors



Risk Scenario

ict PROTECT
INFORMATION SECURITY SERVICES

THREAT	DESCRIPTION	VULNERABILITY	DESCRIPTION	Proposed Countermeasure
Control Logic Manipulation	Control system software or configuration settings modified, producing unpredictable results	**Insufficient configuration**	Improperly configured systems may leave unnecessary ports and protocols open. These unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.	Hardening based on best practices (CIS benchmark)
		Critical configurations are not stored or backed up	Procedures should be available for restoring OT/ICS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining OT/ICS configuration settings.	1. Procedures should be available for restoring OT/ICS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. 2. Documented procedures should be developed for maintaining OT/ICS configuration settings.
		Slow / lack of updates	Maintaining ICS/SCADA firmware and software up-to-date is not easy, and it can be very complex for critical infrastructure systems, as an update error could cause severe issues on the whole system. Cyber fragility results from applying a change to the system without having tested it beforehand and having foreseen its effects.	Software updates should be monitored and implemented as needed on time (after proper testing)
		SCADA Software features	SCADA applications and software usually provides basic and modest security features. However, these are not always enabled by default, and could act as additional weaknesses if operators are unaware of the need of enabling these features.	Operators should be aware of the need of enabling features.
		Operating System Vulnerabilities	The whole host of normal IT operating system vulnerabilities are present in SCADA systems. The difference from an IT system is that patching may be performed less rigorously. It is usual for a SCADA system operator to have a running system that is expected to perform without interruptions.	It is usual for a SCADA system operator to have a running system that is expected to perform without interruptions.

Reference: SANS: ICS Layered Threat Modeling, **ENISA**: WP2016 3-1 2 ICS SCADA Dependencies, **NIST**.SP.800-82

Risk Scenario

ict PROTECT
INFORMATION SECURITY SERVICES

THREAT	DESCRIPTION	VULNERABILITY	DESCRIPTION	Proposed Countermeasure
Permit unnecessary data to pass between networks	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, **allowing attacks and malware to spread between networks, making sensitive data susceptible to** monitoring/eavesdropping, and providing individuals with unauthorized access to systems.	**Inadequate firewall and router logs**	Without proper and accurate **logs**, it might be impossible to **determine** what caused a security incident to occur.	The firewall and router logs should be monitored and reviewed at regular time intervals
		Firewalls non existent or improperly configured	A **lack of properly configured firewalls** could permit unnecessary data to pass between networks, such as control and corporate networks, allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/ eavesdropping, and providing individuals with unauthorized access to systems.	Minimization of access paths to the internal network and enhanced concentration of monitoring
		Weak Firewall Rules - Access to specific ports on host not restircted to required IP addresses	Access to specific ports on host **not restricted** to required IP addresses	Using segmentation of security zone within the SCADA network and using distributed firewall within the SCADA Environment can protect the end devices
		Lack of Functional DMZs	The use of several **DMZs** provides the added capability to separate functionalities and access privileges and has proved to be very effective in protecting large architectures composed of networks with different operational mandates.	Firewalls should be used to create DMZs to protect the ICS network. Different DMZs should be created for separate functionalities/access privileges

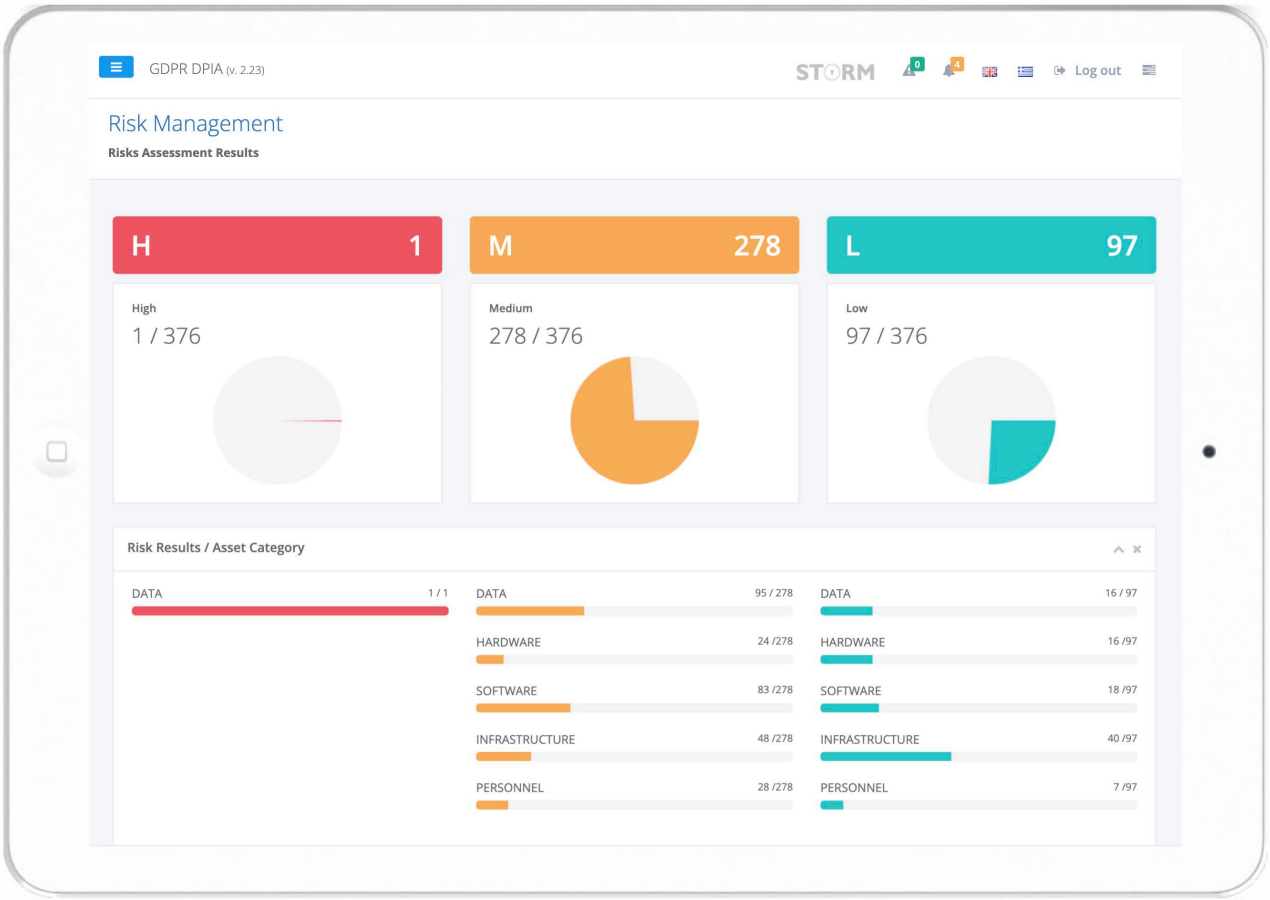
Reference: SANS: ICS Layered Threat Modeling, **ENISA**: WP2016 3-1 2 ICS SCADA Dependencies, **NIST**.SP.800-82

Our Proposed Methodology

Conduct Risk Assessment & Risk Treatment

-- Identify IT & OT Assets
-- Identify assets' dependencies
-- Impact Assessment

--Identify Potential Threats
--Evaluate Vulnerabilities
--Propose Mitigation Actions

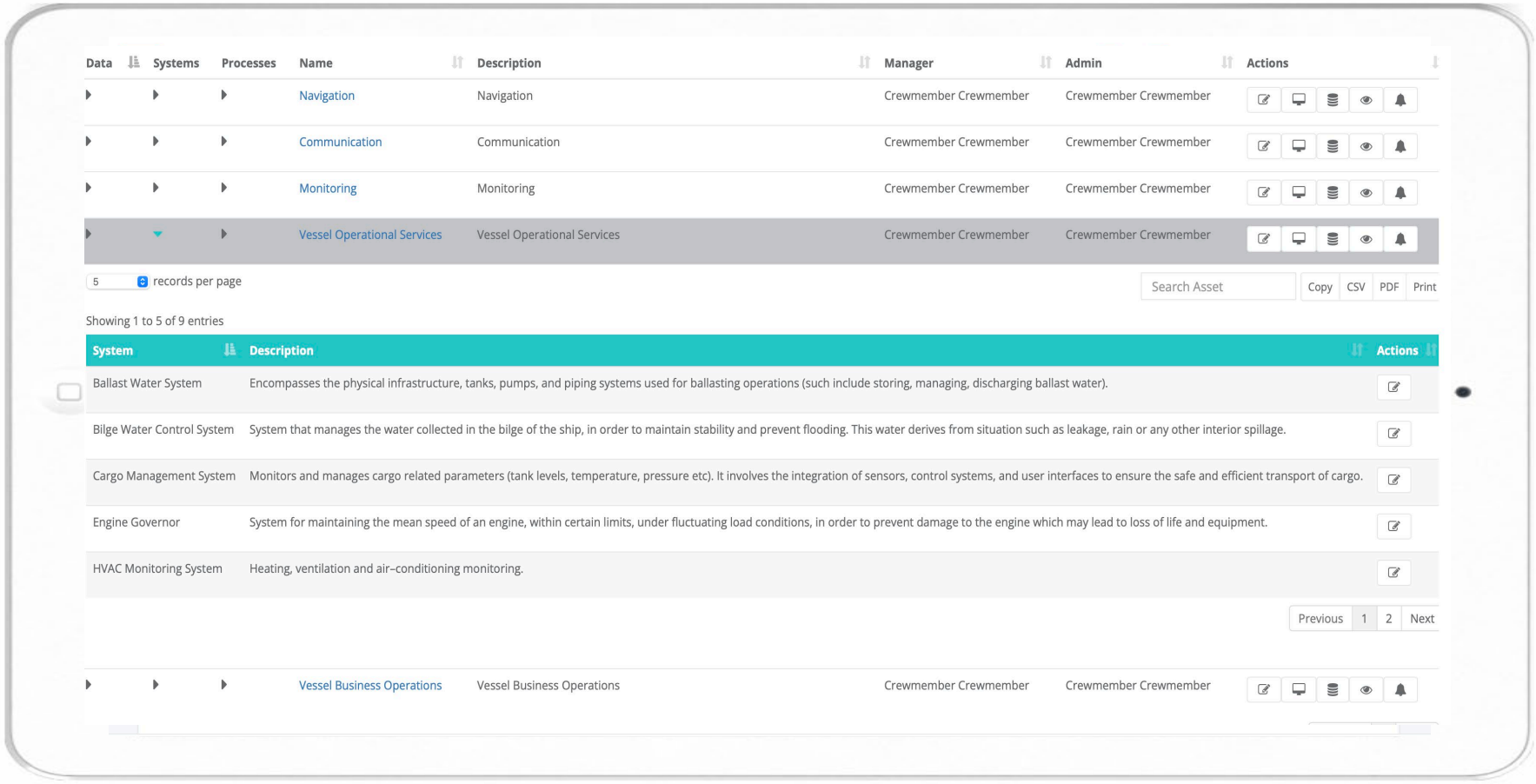


Our Proposed Methodology

Conduct Risk Assessment & Risk Treatment

-- Identify IT & OT Assets
-- Identify assets' dependencies
-- Impact Assessment

--Identify Potential Threats
--Evaluate Vulnerabilities
--Propose Mitigation Actions



Data	Systems	Processes	Name	Description	Manager	Admin	Actions
▸	▸	▸	Navigation	Navigation	Crewmember Crewmember	Crewmember Crewmember	
▸	▸	▸	Communication	Communication	Crewmember Crewmember	Crewmember Crewmember	
▸	▸	▸	Monitoring	Monitoring	Crewmember Crewmember	Crewmember Crewmember	
▸	▾	▸	Vessel Operational Services	Vessel Operational Services	Crewmember Crewmember	Crewmember Crewmember	

5 records per page

Search Asset | Copy | CSV | PDF | Print

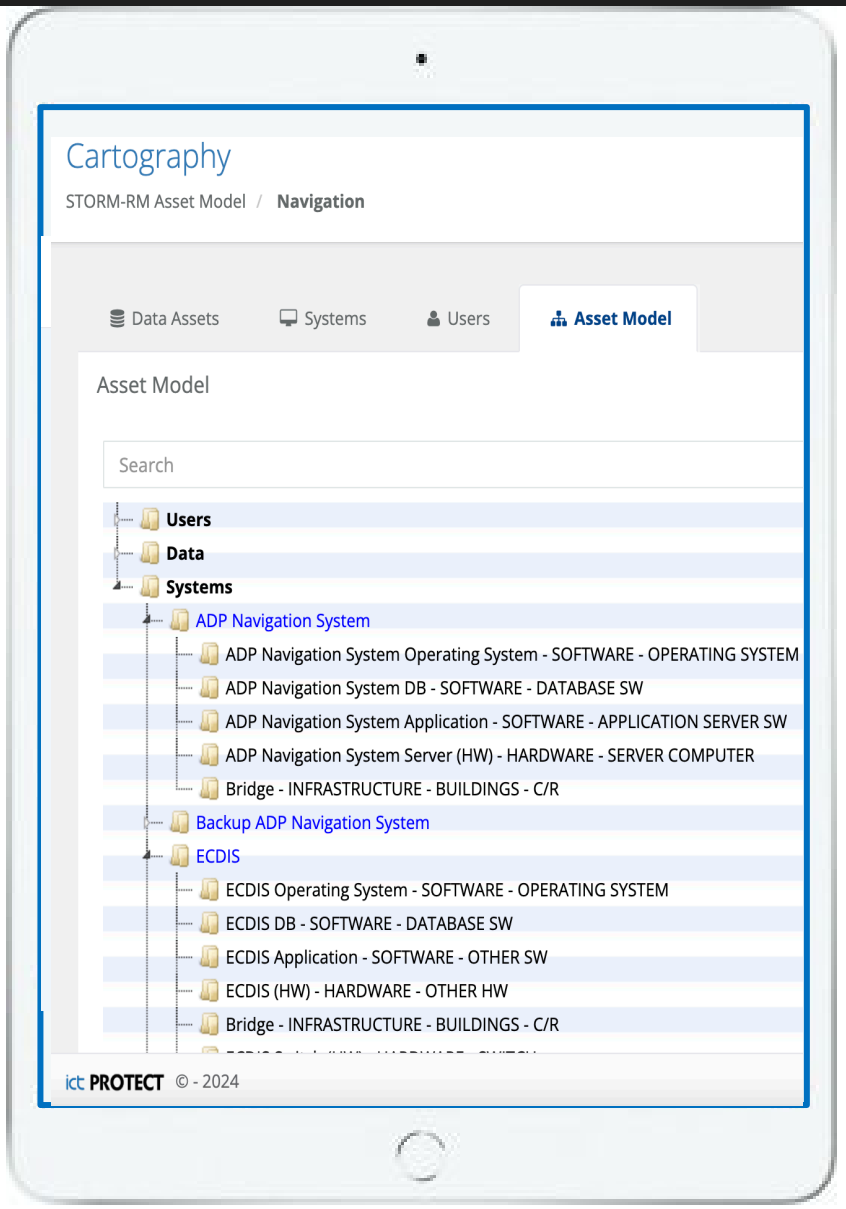
Showing 1 to 5 of 9 entries

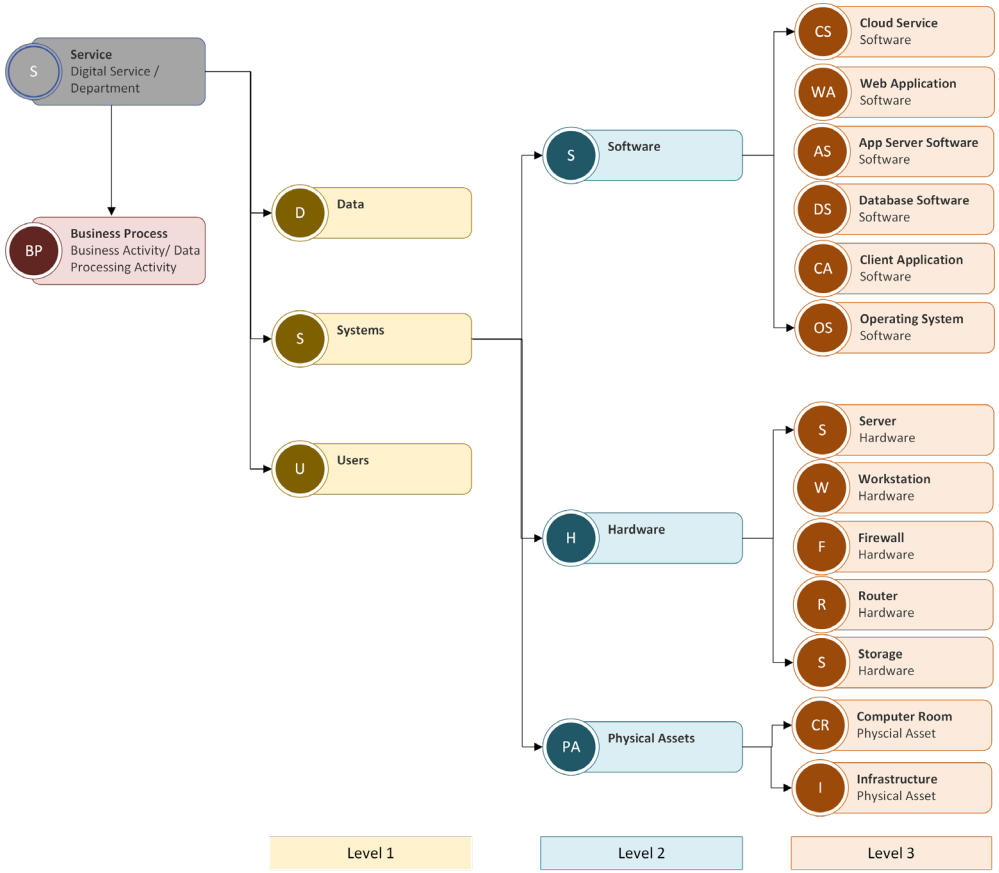
System	Description	Actions
Ballast Water System	Encompasses the physical infrastructure, tanks, pumps, and piping systems used for ballasting operations (such include storing, managing, discharging ballast water).	
Bilge Water Control System	System that manages the water collected in the bilge of the ship, in order to maintain stability and prevent flooding. This water derives from situation such as leakage, rain or any other interior spillage.	
Cargo Management System	Monitors and manages cargo related parameters (tank levels, temperature, pressure etc). It involves the integration of sensors, control systems, and user interfaces to ensure the safe and efficient transport of cargo.	
Engine Governor	System for maintaining the mean speed of an engine, within certain limits, under fluctuating load conditions, in order to prevent damage to the engine which may lead to loss of life and equipment.	
HVAC Monitoring System	Heating, ventilation and air–conditioning monitoring.	

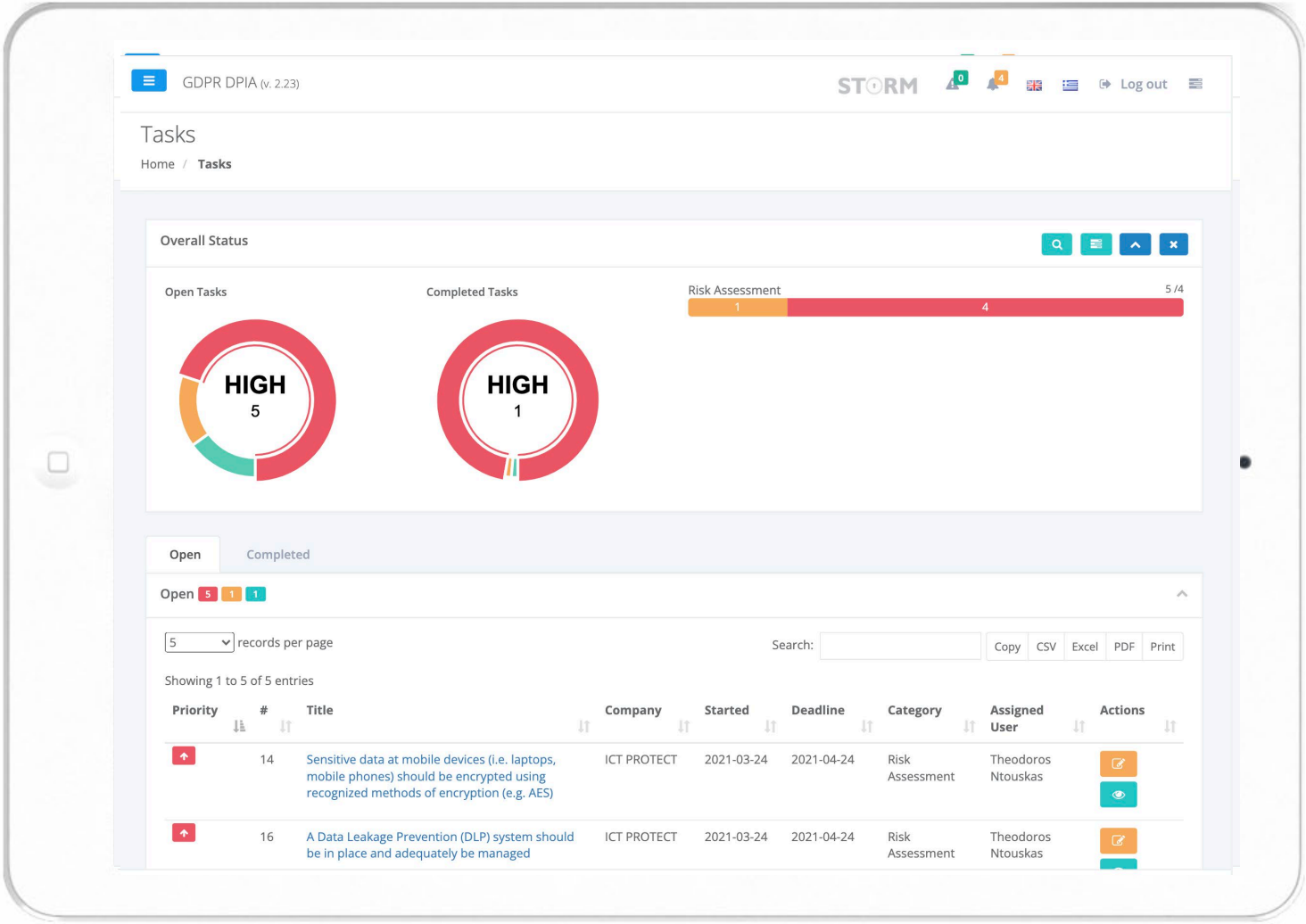
Previous | 1 | 2 | Next

▸	▸	▸	Vessel Business Operations	Vessel Business Operations	Crewmember Crewmember	Crewmember Crewmember	

Vessel IT&OT Asset Model







Issues & «life jacket»

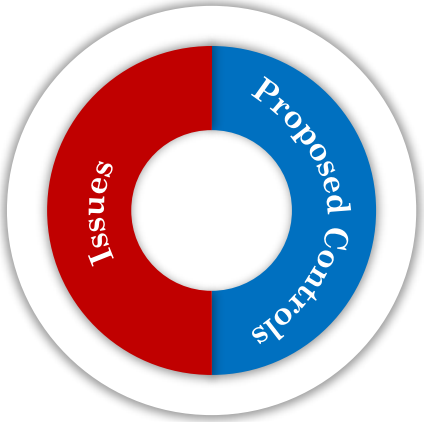
IT & OT Systems are increasingly exposed against cyber risks.

Cyber risks could be exploited either by **satellite networks**

either by the traditional communication channels

significant impact on all maritime entities affecting international economy

Digital supply chain risks
Gartner predicts that by 2025, **45% of organizations worldwide will** have experienced attacks on their software supply chains, a three-fold increase from 2021



IT & OT Risk Assessment
Risk Assessment should depict IT & OT dependencies

Control Remote Access
Remote access capabilities must be adequately controlled

Vulnerability Management & Patch Management Processes should be enforced

Incident Management
Incident response procedure must be in place and adequately followed.

Secure Network Architecture
Network architecture should be designed through the most secure and widely used architecture model for ICS/OT systems, the Purdue Model (ISA 99, IEC 62443).

Architecture Levels – Purdue Model

ict PROTECT
INFORMATION SECURITY SERVICES

Level 5: Enterprise (Enterprise Zone) - Shore Office Network

- Internet
- Satcom

Level 4: Site Business Planning and Logistics (Enterprize Zone) - Vessel Network

- Ship Crew WiFi, Ship Guest WiFi
- Bridge Computers, Captain & Engineer Computers
- Monitoring Systems (Ballast, Cargo, Main engine)
- Ship Stability Program
- VDR

Level 3.5 Industrial DMZ

- Firewall
- Web Proxy (broker service for propulsion, ballast, cargo data)
- WSUS
- ECDIS Update Gateway
- Remote Desktop Gateway

Level 3: Site Manufacturing Operations and Control (Manufacturing Zone) - Bridge-ECR

- VDR (Data Collecting Unit)
- ECDIS
- CCR Computer and equipment
- ECR Computer
- SCADA/Shipboard Integrated Monitoring and Control Systems

Level 2: Area Supervisory Control (Cell / Area Zone) - Bridge-ECR

- Switches
- Firewall
- HMI Propulsion
- HMI Power Management

Level 1: Basic Control (Cell / Area Zone) - Bridge-ECR

- GPS, PLC, HMI
- CAN bus
- Echosounder

Level 0: Process (Cell / Area Zone) - Bridge-ECR

- Sensors
- Actuators

References

- IMO - MSC-FAL.1/Circ.3 – Guidelines on Maritime Cyber Risk Management, July 2017,
  - https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
- IMO - RESOLUTION MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, June 2017,
  - https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf
- United States Coast Guard, February 2020, Guidelines for addressing cyber risks at Maritime Transportation Security Act (MTSA) regulated facilities,
  - https://dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime%20Cyber%20Assessment%20%20Annex%20Guide%20(MCAAG)_released%2023JAN2023.pdf?ver=NE11YUspj_kNa3xRoMd0TQ%3d%3d
  - https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023
  - https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Commercial-Vessel-Compliance/CVCmms/
- IACS (International Association of Classification Societies (IACS)) UK, Rec 166 - Recommendation on Cyber Resilience - New Corr.1 July 2020 Clean,
  - https://www.iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1/ https://iacs.org.uk/download/10965
- OCIMF - TMSA3 - Tanker Management Self-Assessment, April 2017,
  - https://www.shipnet.no/key-elements-of-tmsa-3/
- BIMCO - The Guidelines on Cyber Security Onboard Ships v4,
  - https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
- BIMCO - Cyber Security Workbook for On Board Ship Use, 2nd Edition, 2021,
  - https://www.bimco.org/about-us-and-our-members/publications/cyber-security-workbook
- BIMCO- The Guidelines on Cyber Security Onboard Ships
  - https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
- IMO – ISM Code, 2018 Edition,
  - https://www.dohle-yachts.com/wp-content/uploads/2021/05/ISM-Code-2018.pdf
- ENISA – EU, Port Cybersecurity – Good practices for cybersecurity in the maritime sector, November 2019,
  - https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
  - https://www.enisa.europa.eu/publications/ics-scada-dependencies
- United Kingdom Department of Transport - Cyber Security for Ports and Port Systems, January 2020,
  - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf
- IAPH – International Association of Ports and Harbors, Port Community Cyber Security,
  - https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf
  - https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf
- ISA/IEC 62443 series of standards in order to address the need to design cybersecurity robustness and resilience into industrial automation control systems
  - https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

Our services

ict PROTECT
INFORMATION SECURITY SERVICES

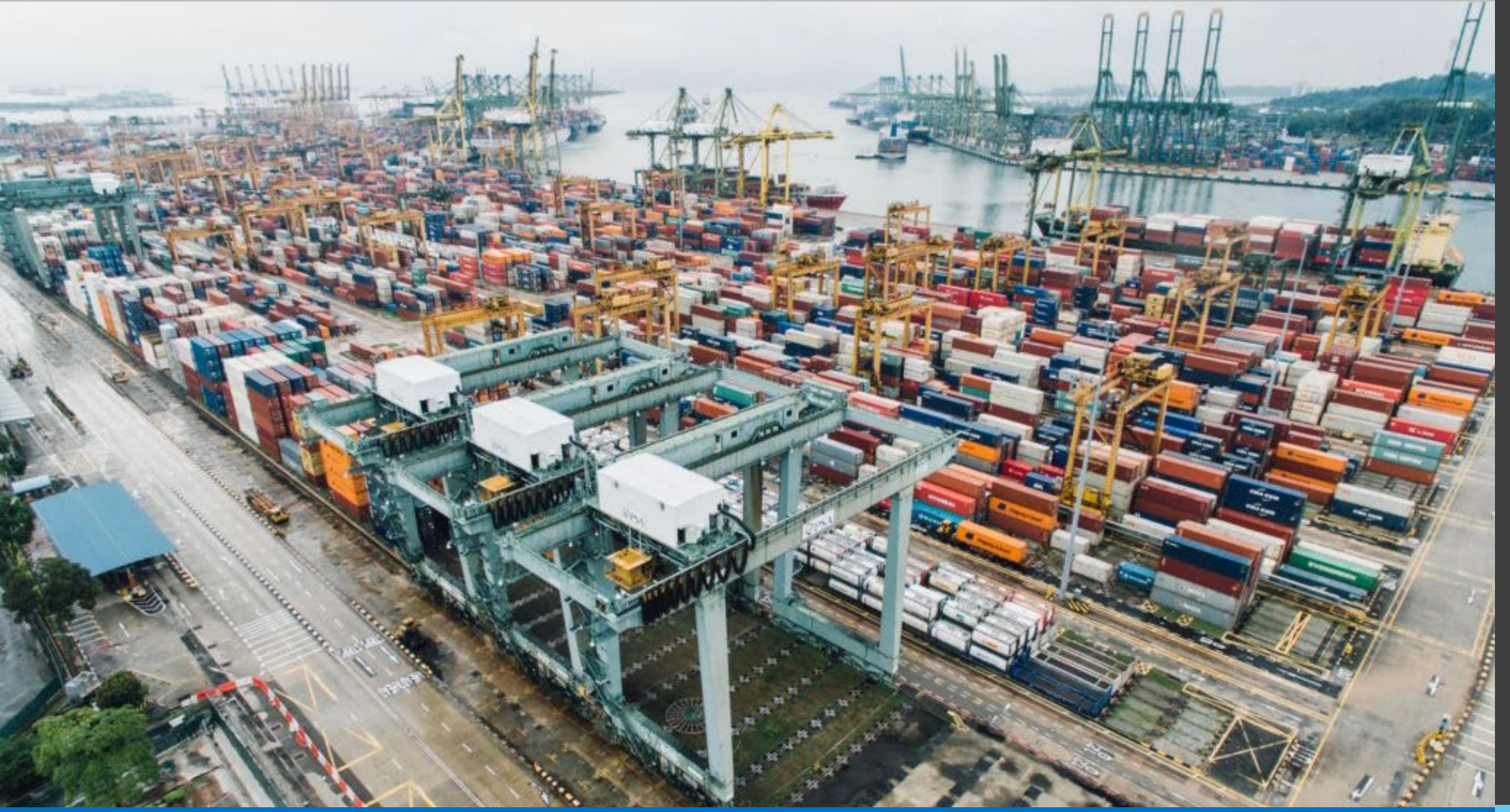
Assurance Services

Compliance Services

Security Management Services

Training Services

STORM
RISK MANAGEMENT
SaaS



Let’s do business

info@ictprotect.com

ict PROTECT
INFORMATION SECURITY SERVICES