UNIVERCITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Maritime Cybersecurity Practices Scheme (Black Box)

Stergios OIKONOMOU

Master thesis

Georgios STAMOULIS

Lamia

2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «Maritime Cybersecurity Practices Scheme (Black Box)» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία

Υπογραφή

Maritime Cybersecurity Practices Scheme (Black Box)

Stergios OIKONOMOU

Τριμελής Επιτροπή:

Γεώργιος Σταμούλης (επιβλέπων)

Ονοματεπώνυμο, ……

Ονοματεπώνυμο, …….

Επιστημονικός Σύμβουλος:

Ιωάννης Φιλιππόπουλος

Table of Contents

Table of Pictures

List of Tables

Abbreviations

AIS	Automatic Identification System
AMCS	Alarm, Monitoring and Control System
ARPA	Automatic Radar Plotting Aid
BNWAS	Bridge Navigational Watch Alarm System
CCR	Cargo Control Room
CCTV	Closed Circuit Tele Vision
DDoS	Distributed Denial of Service
DoS	Denial of Service
DP	Dynamic Positioning
ECC	Engine Control Console
ECDIS	Electronic Chart Display and Identification System
FW	Firewall
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning Systems
IACS	International Association of Classification Societies
IMO	International Maritime Organization
IS	Information System
ISPFS	International Ship and Port Facility Security Code
IT	Information Technology
LAN	Local Area Network
MODU	Mobile Offshore Drilling Units
MSB	Main Switchboard
MSI	Maritime Safety Information
N/SOC	Network/Security Operation Center
OoW	Officer of the Watch
OT	Operational Technology
PMS	Power Management Systems
RADAR	RAdio Detecting And Ranging
SERS	Ship Emergency Response System
SIEM	Security Information and Event Management

SOLAS	Safety of Life at Sea
SSAS	Shipboard Security Alarm Systems
UMS	Unattended Machinery Space
VDR	Voyage Data Recorders
VINS	Vessel Integrated Navigation System
VLAN	Virtual Local Area Network or Virtual LAN
VoIP	Voice over IP
VRCS	Valve Remote Control System
VTMS	Vessel Traffic Management Service
WAN	Wide Area Network
WIM	Water Ingress Monitoring
WLAN	Wireless Local Area Network

Glossary

Access control is referred as the selective ability to limit or authorize permission to enter or to communicate and/or interact with a system, meaning to use its parameters and functions, its resources and information and its spectrum of components.
Back door means the method to bypass authentication and verification when trying to access a system. In many cases, a back door is deliberately created in hidden parts of the system or it is established via separate software.
Bring your own device (BYOD) is the allowance of staff/personnel to bring their own devices such as smart phones, laptops, tablets onboard and use these to access information and applications that are privileged and defined for business usage.
Cyber-attack means any type of aggressive action that targets both business or personal computer networks, IT and OT systems, and attempts to gain access to offshore and vessels systems and data, aiming to destroy or use them to captive or frame its owners.
Cyber incident is the event, which may result hurtful consequences to an onboard network system, or to its incoming/outcoming information, and which may require an immediate action to diminish these consequences.
Cyber risk management means the procedure that includes the identification, collection, analysis, mitigation means that are involved in a cyber-attack and have to be carried out and taken by the stakeholders.
Cyber system is referred to any blend of facility, equipment, procedure, human resources and communications, consolidated to provide a range of cyber services.
Defence in breadth is a planned set of systematic activities that aim to identify, handle, and minimize exploitable vulnerabilities in IT and OT systems, networks and equipment during their entire life circle of operation. Onboard, this approach will focus in general on network design and integration, on operations and maintenance.
Defence in depth is the technique which uses many layers of independent measures both procedural and technical in order to protect IT and OT systems on board.
Executable software means the software that includes instructions on how to perform specific actions/tasks based on encoded instructions on a computer.
Firewall is a logical or physical barrier that is designed to prevent unauthorised access to IT infrastructure and information.
Firmware is the software embedded in all electronic devices by the manufacturer (not accessible to user manipulation) aiming to provide access and use of the engineered products and systems.
Flaw is the unintended deficiency of functionality in software.
Internet Control Message Protocol (ICMP) means the whole communication rules that are used as notifications of errors in the processing of datagrams, and to all information related to communication.
Intrusion Detection System (IDS) is the software application or device used to run through and observe network systems and their activity for malicious actions and violations, and generates reports to a management station.
Intrusion Prevention System (IPS), also mentioned as Intrusion Detection and Prevention Systems (IDPSs), is the set of network security appliances that tracks network and/or system activities for any malicious activity.
Local Area Network (LAN) is the computer network that intelinks computers within a limited area such as an office building a home, or a ship, by using network media.
Malware is a widely used term to describe malicious software, which aims to infect computer systems and impact on their performance.
Operational technology (OT) is the technology that includes software and network, devices, sensors, that monitor and control onboard systems.

Open Systems Interconnection (OSI) is the model stipulated for computers and imposed by the International Organization for Standardization, for dividing the communication functions into layers.
Patches means the software designed to update software and supporting data in order to improve these or address security vulnerabilities and other bugs in operating systems or applications.
Phishing refers to the process that aims to deceive recipients to share sensitive information with a third party.
Principle of least privilege refers to the restriction of user account advantages only to those with privileges that are essential to functionality.
Producer is the body that manufactures shipboard equipment and its associated software.
Recovery refers to the activities that need to be done after an incident, to restore critical services and operations in both short and medium term and fully restore all capabilities and functions in a longer term.
Removable media is the common term to describe all methods of storing and transferring data between computers. This may include laptops, USB memory sticks, CDs, DVDs and other.
Risk assessment means the process that collects information and evaluates risks, as a guideline to set priorities and develop and implement courses of action.
Risk management is referred as, on one hand, the process of identifying, collecting, analysing, assessing and communicating risk and on the other, of accepting, avoiding, transferring or controlling the risk to an acceptable level, taking into consideration all associated costs and benefits of any actions to be taken.
Sandbox is an isolated environment like a quarantine, in which a program may be run without affecting the underlying computer or operating system and/or other applications. A sandbox is often used when executing and examine untrusted software.
Service provider is a company or individual, who provides and performs software service and maintenance.
Simple Network Management Protocol (SNMP) means the rules that define methods for communicating information in order to monitor and control devices on a network.
Social engineering means the method used to gain access to systems by deceiving a person to reveal confidential and/or personal information.
Software whitelisting is the action to specify the software, which is present and active on an IT or OT system.
Spanning Tree Protocol (STP) is the method of control in a loop topology network, for preventing data from entering never ending loops.
Virtual Local Area Network (VLAN) means a group of layered LANs that are connected and communicate with the same network resources, regardless their geographical location. VLAN use intends to separate networks for administration reasons and in order to increase security level.
Virtual Private Network (VPN) is the network that permits users to send/ receive data across shared or public networks as if their computing devices were directly connected to the private network. That way, they are benefiting from the functionality, security and management policies of this private network.
Virus is referred as a hidden code that can copy itself on a section of the computer software and can maliciously infect and manipulates the operation of a computer program and/or system.
Wi-Fi is the range of all short-range wireless communications that use some type of electromagnetic spectrum to send / receive information.

Abstract

It is generally known and accepted that in a fast connected and technologically dependent world, new areas of vulnerability is born and elevate. This paper explores the unique challenges of maritime cybersecurity to better understand the issues with securing vessels at sea, together with the shore-based infrastructure supporting this industry. More specifically, this paper drives through the possible cyber-attacks on maritime-related systems for navigation, propulsion, and cargo-related functions. The author illustrates the potential severity of the problem by providing a practice scheme of vessel cyber security by using a black box.

Acknowledgements

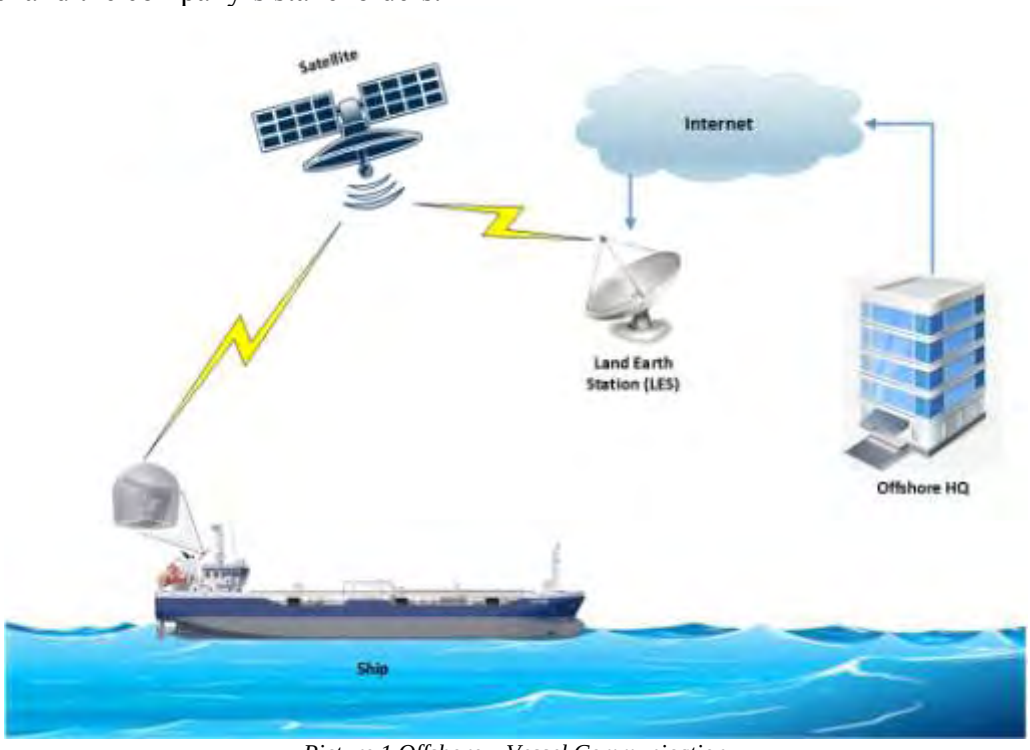
I take this opportunity to tender my special thanks to my thesis advisor Professor Ioannis Filippopoulos of the School of Science, Informatics & Computational Biomedicine at University of Thessaly. I felt blessed to experience such a condescending, friendly and in parallel extremely professional approach by this Professor. My queries and questions were never left without an answer, while I was always shown the right direction whenever he thought I needed it.
I would also like to thank Mr. Konstantinos Grivas an Information Security Officer of Angelicoussis Group who was involved and contributed in the validation survey for this research project. Without the above gentlemen's valuable input and unlimited help, this paper could not have been successfully conducted.
Last but not least, I must express my gratitude to my partner Yota and friends for continuously supporting and encouraging me throughout my study. This achievement would not have been possible without their help and support.

Thank you All.

Stergios OIKONOMOU

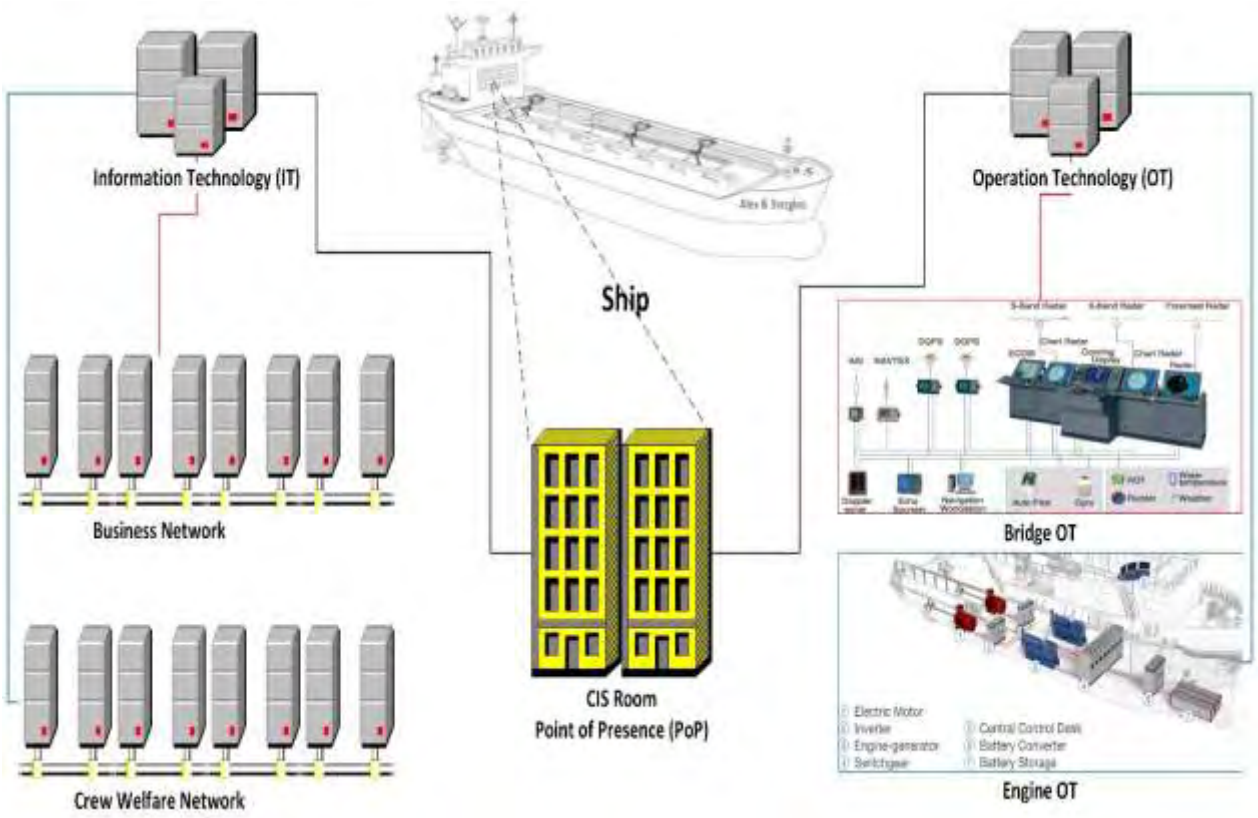
Introduction

Maritime industry has grown to the point where use of Information Technology (IT), Operation Technology (OT) and access of secure Cyberspace is fundamental and critical for offshore HQ interconnection with company's offsite vessels.
Unfortunately, Maritime industry is not among the industries included in the list of the most vulnerable to cyberattacks. But while maritime security may not receive the level of attention given to health care or financial services, it doesn't mean that risks are any less or real.
As a result of that, the International Maritime Organization (IMO) had focused on Marine safety and security and has made these one of its main objectives. Ship owners and stakeholders are obliged to incorporate these guidelines into their safety management systems by 1st January 2021.
With no doubt, cyber threats and cyber-attacks are becoming more frequent and more sophisticated day by day. They range from a simple Denial of Service (DoS) and information gathering attacks up to advanced and complex intrusions that aim to manipulate and compromise information for persistent and in depth attacks. Terrorists seek an asymmetric advantage to attain vessels' sensitive security information.
Therefore, the adoption of the appropriate Cyber Defence measures and capabilities together with the best implementation practices that relate to the elimination of the risk to face and counter the threats from cyberspace, is obligatory. The implementation of a vessel black box will definitely support the procedures and actions needed to materialize cyber security. All steps need to be followed exactly as per the given guidelines, to make sure that no fail will occur or threaten the vessel and the company's stakeholders.



Picture 1 Offshore – Vessel Communication

1. Maritime's Information Systems



Picture 2 Vessel's Information Systems

1.1 Differences between IT and OT Systems

OT systems differ from the traditional IT systems. OT systems (hardware and software) control the physical elements (devices and processes) while the IT systems manage information and cover a spectrum of technologies for information processing, including software, hardware and communication. Historically, OT and IT have been stand-alone systems, still in nowadays the internet has managed to make these operate parallel interfaced with a logical separation.
Disruption of the operation of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage of the marine environment, and impede the ship's operation.
Here follows a list of differences between IT and OT systems in the table as below.

Table 1-1 IT and OT systems differences

Category	IT system	OT system
Performance requirements	■ non-real-time ■ response must be consistent ■ less critical emergency interaction ■ tightly restricted access control can be implemented to the degree necessary for security	■ real-time ■ response is time-critical ■ response to human and any other emergency interaction is critical ■ access to OT should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (reliability) requirements	■ responses such as rebooting are acceptable ■ availability deficiencies may be tolerated, depending on the system's operational requirements	■ responses such as rebooting may not be acceptable because of operational requirements ■ availability requirements may necessitate back-up systems
Risk management requirements	■ manage data ■ data confidentiality and integrity is paramount ■ fault tolerance may be less important. ■ risk impacts may cause delay of: ship's clearance, commencement of loading/ unloading, and commercial and business operations	■ control physical world ■ safety is paramount, followed by protection of the process ■ fault tolerance is essential, even momentary downtime may not be acceptable ■ risk impacts are regulatory non-compliance, as well as harm to the personnel onboard, the environment, equipment and/or cargo
System operation	■ systems are designed for use with commonly known operating systems ■ upgrades are straightforward with the availability of automated deployment tools	■ differing and possibly proprietary operating systems, often without built in security capabilities ■ software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and possible involvement of modified hardware and software
Resource constraints	■ systems are specified with enough resources to support the addition of third-party applications such as security solutions	■ systems are designed to support the intended operational process and may not have enough memory and computing resources to support the addition of security capabilities

1.2 Information Technology System (IT)

1.2.1 Internal Networks (LAN) and Wireless Networks (WLAN)

A Local Area Network (LAN) is either a computer or a data network, which allows nodes to share resources, by interconnecting them in order to exchange data and/or information. These interconnections (data links) operate over wired or fiber-optic cables, or wireless connection like Wi-Fi.

1.2.2 Voice over IP (VoIP)

Picture 3 Voice over IP

The majority of land-based organisations face similar communication challenges to the ones of the vessels. The various segments aim to improve communications, in order to provide employees with a better working environment (such as emergency telephones), and to utilise new methods that will help the business to run more profitably.
Maritime communications may improve via Voice over Internet Protocol (VoIP) telephones which can facilitate communication between offshore headquarters/locations/ports, other maritime areas and a variety of vessels.
Ship owners with a fleet of ships in different geographic locations are in need of the ability and flexibility to communicate between offices in a cost effective way, and traditionally calls over PSTN and Mobile networks can easily lead to huge costs that will burden the owners.
The benefit with VoIP solution is that it's based on open Session Initiation Protocol (SIP) standards that has the ability to transfer the calls free of charge over the internet. Using open standards also means that the solution could be extremely cost effective when it comes to future maintenance and repairs. SIP is the most widely used protocol for controlling multimedia communication sessions such as voice and video calls over IP.
VoIP phones, when deployed in the vessel will allow crew onboard to dial with and receive calls from/to external numbers through SIP (VoIP) from Internet Telephony Service Provider (ITSP). Management also has the option to deploy Pin Codes for designated IP Phones in common areas and subsidize or sell them to crew members to call home and their families.

1.2.3 Application Server

This server is designed to operate and provide host applications to end users such as individuals or organizations, and aims to afford and facilitate high-end services to consumers and business.
An application server consists of a server Operating System (OS) and a server hardware that work together to provide computing-intensive operations and services to the residing application. An application server can execute and provide access when utilizing the installed application's business/functional. The key features of an application server include availability, load balancing, data redundancy and security, management interface (administrator/single user). Additionally, an application server can be connected to organisation systems, networks or intranet and can be remotely controlled/accessed via the internet.
An important reason to use an application server, is because it provides additional layer of security to the organisation. An application server helps to act as an additional barrier to SQL injection cyber-attacks, by sitting in between web pages and databases, as there is no direct link between a web page and a database. This separation carries the need for validation by ensuring that text entered into a form on a website is not being exploited as a malicious SQL call.

1.2.4 End-user Terminals Connected to the Server

The term *end user* usually means an individual with a relatively low level of computer expertise, someone who uses the product after it has been fully developed and marketed. The term is useful because it distinguishes two classes of users, the ones who require a bug-free and finished product (end users), and the others who may use the same product for development purposes. Unless someone is a programmer or software engineer, he/she is certainly an end user.

1.2.5 Standalone Computers for Specific Applications

A desktop or laptop computer that is used on its own, without requiring a connection to a Local Area Network (LAN) or Wide Area Network (WAN) is a Standalone computer.
In offices throughout the 1990s, millions of stand-alone PCs were hooked up to a LAN for file sharing and mainframe access. Today, computers are commonly networked for domestic use, so that family members can share an Internet connection as well as printers, scanners and other peripherals.

1.2.6 Network Switches

A network switch is a device that connects computers, other network devices and computer networks by using a packet switching to forward, receive, process data from/to the destination device.
A network switch is a multiport network bridge that uses hardware addresses to process and forward data. According to OSI model there are two different types of switches, there are layer 2 and layer 3. The layer 3 switches an also process data at the network by additional incorporating routing functionality.

1.2.7 Communication Gateways / Firewalls

A Gateway is a component in computer networking and telecommunications that is part of two or more networks, which may use different protocols and is able to translate one protocol into the other if necessary. A router is an example of a gateway.
Gateways can operate at any network layer, and many times are met as protocol converters. The activities of a gateway are more complex than a switch.
The computers of internet end-users and the application servers which provides for example a webpage are both host nodes. The nodes that connect the networks in between, are gateways. Here follow some examples of gateway nodes:

- the computers that control traffic between company networks
- the computers used by Internet Service Providers (ISPs) to connect users to the internet

A Firewall is a network security system that establishes a barrier between the internal network and external network that cannot be trusted. Additionally, the firewall monitors/controls network traffic (incoming and outgoing), in accordance with preset security rules.
Firewalls are often categorized as either network firewalls or host-based firewalls.

- Network-based firewalls are positioned close to the gateway computers of LANs, WANs and intranets. There are firewall software programmes running on computers or hardware-based firewall.
- Host-based firewalls are positioned on the network node itself and control network traffic in/out of those machines. This firewall can be a daemon or a service as a part of the operating system or an agent application.

1.2.8 External Storage Devices like USB HDD and USB Memory Stick

An external storage device, also referred as auxiliary and/or secondary storage, is a device that contains data that may not be included inside a computer's main storage or memory. An external storage device can be removable or non-removable, temporary or permanent, and accessible over a wire or wireless network.
Types of external storage devices:

- Common portable and fixed external storage devices include Hard Disk Drives (HDDs), a type of magnetic storage, and Solid State Drives (SSDs), which use flash technology with capacities starting in the gigabyte range up to 10 terabytes (TB) and higher.
- Tape is another type of removable magnetic storage. The most widespread tape format is Linear Tape-Open (LTO).
- Optical storage is another type of external storage device, which writes/reads digital content using a laser. Compact Discs (CDs), belong in this category with a capacity of 800 MB; DVDs with a capacity of 4.7 - 9.4 GB; and Blu-ray, with a capacity over 5 GB up to 50 GB.
- Small and removable USB flash drives and cards for smartphones, tablets and cameras etc.

One of the main reasons that security and data integrity are of paramount importance to enterprises and organizations portable, external storage devices should include data encryption and authentication.

1.2.9 Computers for Crew Welfare

Internet enabled vessels is now a common practice in today's world of shipping. New technology has mostly contributed to make shipboard internet affordable for many shipping companies.
Nowadays, internet and social networking sites are part of everyday life, thus the lack of the ability for immediate communication with the outside world may result a malpractice to the vast majority of today's seafarers.
Communication available to crew:

In addition to internet, the following means are among the ones available to ship's staff in order to allow communication with family and friends:

- Personal mobile telephones
- GSM/Mobile phone calling on ship over Satellite.
- Telephones brought on board in port by vendors/salesmen
- Telephones ashore in Seaman Centres / public telephone kiosks
- Telephone booths on the dock
- Satellite voice systems
- Email service

Advantages to crew of having internet on board

- Communication with family and friends made much easier and less expensive via social networking apps
- Can be used to provide e-learning tools and raise computer literacy through usage that leads to a better interaction with automated systems
- Online banking
- Becoming a benefit factor when crew are considering joining a Company as employees
- Maybe a good measure to retain existing employees to keep their morale high
- The ability to keep up-to-date with world events, both on a regional & global scale

Disadvantages of allowing internet access to crew

- Reduced work output
- If wireless access is enabled, crew can access the internet even when on duty
- Increase of fatigue levels (prolonged use of the internet resulting less rest time)
- Conflicts may arise amongst crew, concerning the number of internet enabled computers available
- Photographs uploaded by ship's staff on social media (Twitter / Facebook) may result an unnecessary & potentially negative PR environment for the ship-owner and his prestige.

1.2.10 Applications

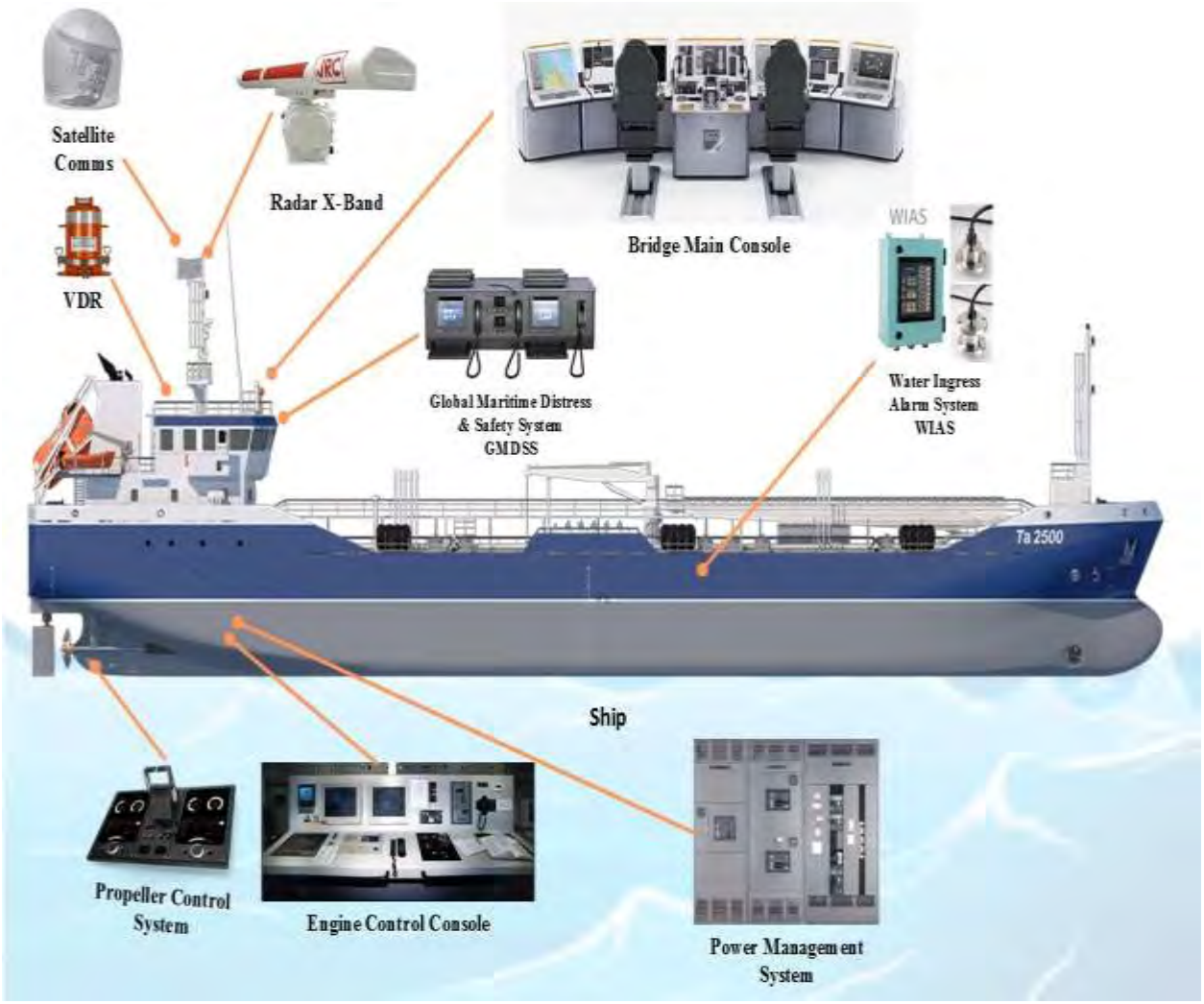
Applications approved by the company and installed on the vessel are:

Table 1-2 Vessel Applications List

Messaging application	Any application used for messaging
ERP application	The vessel's business application
PMS application	For Plan Maintenance
File editing application	i.e. MS OFFICE
File view application	i.e. Acrobat Reader / Foxit Reader
FTP / File download application	If necessary
File compress / un-compress application	i.e 7zip, WinZip etc.
Navigation related applications	ADP / ChartCo / OceanView / e-NP reader / Weather (VVOS, SPOS), Navtor

There might be a few more applications specific for Charterer, Port Authorities, Regulatory Authorities requirements, however they are under Company knowledge and approval.

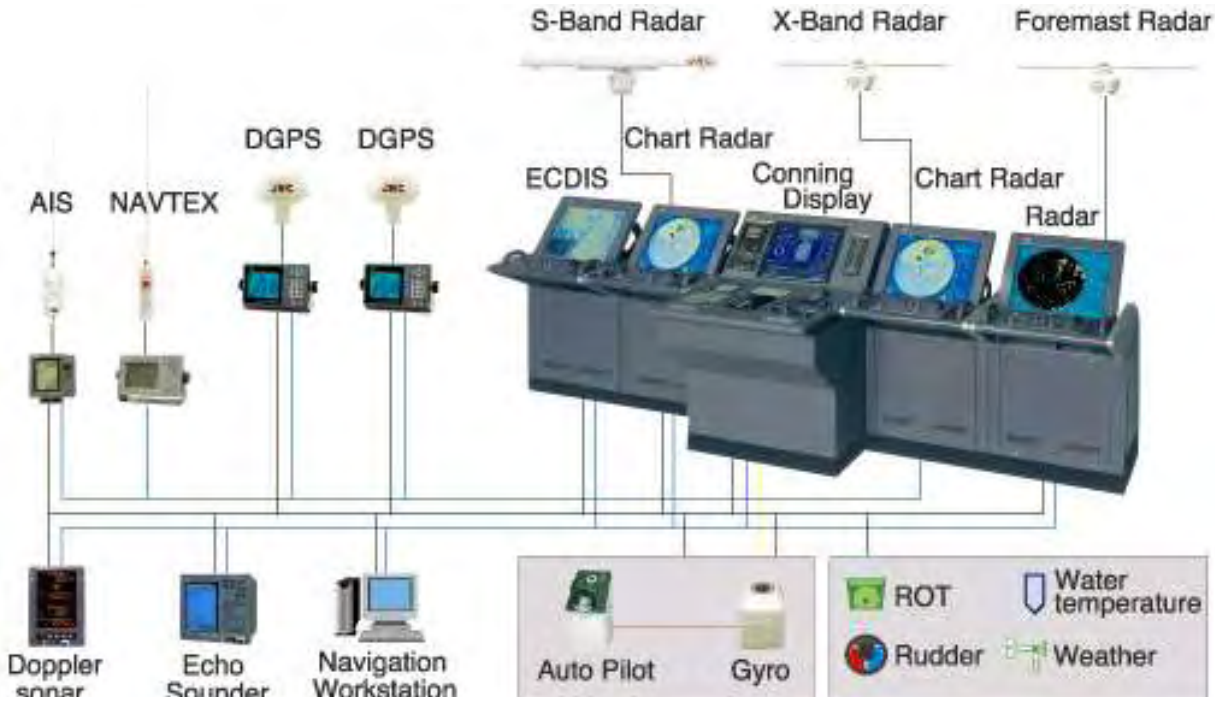
1.3 Operation Technology System (OT)



Picture 4 Vessel's Operation Technology Systems (OT)

1.3.1 Bridge OTs

1.3.1.1 Vessel Integrated Navigation System (VINS)



Picture 5 Vessel Integrated Navigation System (VINS)

According to Bowditch an Integrated Navigation System is "*a combination of equipment and software which uses interconnected controls and displays to present a comprehensive site of navigational information to the mariner.*"
Integrated Navigation Systems (INS) were adopted by IMO in 1998.
The purpose of an INS is to allow manufacturers to provide "added value" to their system(s) by improving interfacing and interconnectivity. This is accomplished via the evaluation of data input from independent sensors. Monitoring integrity is a substantial function of the INS. An INS makes use of a multifunction display by allowing a single visual display unit to simultaneously present information from many systems. INS ensures that workload is kept within the capacity of the Officer-of-the-Watch (OoW) taking human factors into consideration.

1.3.1.2 Global Positioning Systems (GPS)

Picture 6 Global Positioning Systems (GPS)

The Global Positioning System (GPS) is a satellite-based radio-navigation system owned by the United States government and operated by the United States Air Force, which provides users with Positioning, Navigation, and Timing (PNT) services. This system consists of three segments:

- the space
- the control
- the user

Each satellite continually transmits, through radio waves, precise data on its identification, position and time- essentially saying, I am satellite A, my position right now is B and the time now is C. The satellite also transmits some almanac data on all the satellites in the system, plus a signal which lets the GPS receiver on board set (or correct) its time.
On board, the GPS receiver stores the almanac data for continuous use. It also calculates, (based on the A, B and C data above) exactly how far the satellite is from the ship at any given time. In order to calculate Latitude and Longitude and to present a 2D fix on board we need at least three satellites. With a forth satellite we can calculate altitude as well. Should a record of the ship's positions and time is kept, then we can calculation the ship's speed.
GPS information at sea is often replicated on other navigational equipment on the bridge such as radars, electronic navigational systems and communication systems resulting a convenient, easy and seamless navigation.

1.3.1.3 Satellite Communication System

Picture 7 Satellite Communication System

Marine communications are more important than ever, still the solutions that work on land don't work at sea. Fortunately, we live in an era when satellite communications are the answer for everyone from the most casual boater to the most sophisticated cruise ship.
International Maritime Satellite Organization (Inmarsat) founded in 1979 of the as a not-for-profit international organization, set up by the IMO mandate, for the purpose of establishing a satellite communications network for the maritime community.

1.3.1.3.1 Marine Satellite Communications Services

They cover the entire gamut of communications including voice calling, data services for satellite email and Internet Access, and weather and oceanographic data access for navigation.

1.3.1.3.1.1 Marine Satellite Voice Communications

Voice calling (available from Inmarsat and Iridium) keeps recreational vessels in touch with businesses, family and friends back home.

1.3.1.3.1.2 Marine Satellite Phone Email Service

Satellite phone email is one of the most efficient way to communicate on the water. However, satellite data services are either much slower or more expensive than ground-based data service. Satellite phone email service can provide up to 20 times faster service. It also allows companies to send single messages to a virtually unlimited number of recipients with the press of a single button. Additionally, it can be used for other services such as posting GPS locations, retrieving GRIB files, and social media sites.

1.3.1.3.1.3 Marine Satellite Internet Service

Marine satellite Internet access is available at a number of different speeds and prices.
Many companies find that a setup of a simple Iridium satellite phone with its 2.4 kbps uncompressed data feed, will work to browse mobile sites and get weather data.
Iridium OpenPort and Inmarsat FleetBroadband are the latest satellite broadband services available that can provide a connection similar to DSL/Cable service when used with satellite compression software. Still, many satellite users have found themselves in a shock after

receiving bills for service used, that may include downloading megabytes for system updates or Skype sessions when they connected their computers to an open satellite broadband line without firewall. Satellite firewall routers are critical in any satellite broadband installation to ensure maximum speed and block unwanted traffic. An effective router can reduce bandwidth dramatically through compression and blocking unwanted data-hogging sites and services.
In nowadays, satellite internet services are the most sophisticated end that can provide very high speed access, generally at prices that make sense for commercial ship operations.

1.3.1.4 Automatic Identification System (AIS)

Picture 8 Automatic Identification System (AIS)

The Automatic Identification Systems (AIS) is a device that is able to monitor ship traffic in order to contribute to safety of vessels' navigation, it's an autonomous system that transmits navigational information between vessels and land-stations. AIS may operate on two designated marine VHF channels and may transmit/receive distinct messages such as information regarding position, course, speed and identity.
Vessels with AIS transceivers can be tracked by same land stations located in coast lines or by satellite (Satellite-AIS (S-AIS)) when they are out of range of terrestrial networks.
SOLAS forces all vessels engaged in international voyages over 300 gross tonnage (GT) to have an AIS fitted aboard. This also applies to all passenger ships regardless of their size.
The necessity of an AIS.
It's important because it can generate a much better navigation awareness, as it is able to overcome limitations of sight, VHF voice and radar, for congestion avoidance.
How does an AIS work.
The transmission protocol called Self Organizing Time Division Multiple Access (SOTDMA) is the one that allows AIS to be continuously and autonomous operational.
The advantages of an AIS enhance to:

- Safety and efficiency of navigation
- Identification of vessels
- Environment protection
- Reduction of voice radio traffic
- Identification of high risk targets to ensure maritime security
- Provision of additional information during search and rescue missions

1.3.1.5 Electronic Chart Display and Identification System (ECDIS)

Picture 9 Electronic Chart Display and Identification System (ECDIS)

An Electronic Chart Display and Information System (ECDIS) is a computer-based navigation system that complies with IMO regulations and can be used as an alternative to paper navigation charts.
An ECDIS system is a workstation PC which is installed on the bridge of a vessel and usually runs Windows XP. It includes Digital Nautical Charts (DNC) or Electronic Navigational Charts (ENC) and consolidates position information from the GPS. ECDIS interconnection to the shipboard business LAN is made by sensors (serial/NMEA adaptors) that can achieve connection with Radar, Navigational Telex (NAVTEX), Automatic Identification Systems (AIS), Anemometer, and Fathometer, Sailing Directions, Position Fixing, Speed Log and Echo Sounder.

1.3.1.6 Marine Radar Systems

Picture 10 Marine Radar Systems

During the World War II a new system employed that was able to track enemy planes and ships, this is called RADAR (RAdio Detecting And Ranging). In nowadays, many times it's referred as Automatic Radar Plotting Aid (ARPA) which is a result of merged radar and computer technologies that aim to increase area observation.
There are two radar frequencies known as "X" and "S" band.

- "X" band at 10 GHz, provides a higher resolution and a high resolution image
- "S" band, at 3 GHz is less affected by rain and fog

Marine radars are X or S band radars used on ships, in order to detect other ships and land hurdles, for collision avoidance and safe navigation at sea, being a vital component for safety both at sea and near shores. This provides the ability to ship crew to maneuver ships in the worst weather conditions and to navigate "blind", when there is low or no visibility.
Usually, small vessels have an "X" band while big vessels are fitted with both "X" and "S" band radars. Vessels that exceed 300 GT are required to have two marine radars and one of those must be an ARPA.
Shore-based vessel radar systems are used in harbours, to regulate and monitor ship movements in busy waters.

1.3.1.7 Global Maritime Distress and Safety System (GMDSS)

Picture 11 Global Maritime Distress and Safety System (GMDSS)

The GMDSS is an automated ship to shore system using satellites and digital selective calling technology. It is an internationally recognized system that distresses the radio communication and safety for ships replacing the previous ship to ship one. The GMDSS is an International Treaty, mandated for ships by IMO SOLAS Convention 1974.
The GMDSS rules stand for:

- Cargo ships of 300 GT and over when traveling in the open sea or on international voyages
- Passenger ships with more than twelve passengers when traveling in the open sea or on international voyages
- Commercial vessels under 300 GT or those above 300 GT traveling only on domestic voyages, fall under the requirements of their State Flag

The GMDSS advantages:

- Provides worldwide ship to shore alerting
- Simplifies radio operations as alerts may be sent by "two simple actions"
- Ensures redundancy of communications (two *separate systems* for alerting)
- Enhances search and rescue operations
- Minimizes unexpected emergencies at sea
- Eliminates reliance on a single person for communications, as it needs at least two operators and two maintenance methods to ensure distress communications capability at all times. This means that every ship is required to carry qualified personnel for these purposes, who are to hold appropriate certificates specified in the ITU Radio Regulations

GMDSS differ in terms of limitations as per the range of services provided.
GMDSS divides the world's oceans into 4 areas, as the various radio systems fitted onboard depend on the area of operation of the ship rather than the size.

- **Sea Area A1** is an area within radiotelephone coverage in a range of 20 – 30 nautical miles of at least one VHF coast station in which continuous DSC alerting is available
- **Sea Area A2** is an area, that excludes Sea Area 1, within the radiotelephone coverage in a range of 100-150 nautical miles of at least one MF coast station in which continuous DSC alerting is available
- **Sea Area A3** is an area, that excludes A1 and A2, within the coverage of an approximately 70 degrees north latitude 70 degrees south, INMARSAT geo-stationary satellite coast station in which continuous alerting is available
- **Sea Area A4** covers the remaining sea areas outside A1, A2 and A3 (the Polar Regions)

Requirements of Ships at Sea:
The system identifies nine (9) specific functions that need to be performed while at sea.

1. Transmission of ship to shore distress alerts by at least two separate and independent means
2. Reception of shore to ship distress alerts
3. Transmission and reception of ship-to-ship distress alerts
4. Transmission and reception of bridge to bridge communications
5. Transmission and reception of Search and Rescue (SAR) coordinating communications
6. Transmission and reception of on-scene communications
7. Transmission and reception of locating signals
8. Transmission and reception of Maritime Safety Information (MSI)
9. Transmission and reception of general radio communications to and from shore based radio systems or networks

1.3.1.8 Voyage Data Recorders (VDRs)

Picture 12 Voyage Data Recorders (VDRs)

Voyage data recorder (VDR) is a system designed to collect data from various sensors on board the vessel as required, in order to comply with the IMO's International Convention SOLAS requirements. It is able to digitize, compress and store data in an externally mounted protective storage unit which is tamper-proof, designed to withstand extreme shock, impact, pressure and heat that could be associated with a marine incident like an explosion, fire, sinking, etc.
The primary use of the VDR is for accident investigation after an incident. The VDR stores the latest data that can be recovered and replayed by the authorities or ship owners for incident investigation of the last 12 hours. Still, it can be used for other purposes in order to record data for preventive maintenance, performance efficiency monitoring, heavy weather damage analysis, accident avoidance and training purposes to improve safety and reduce running costs.
The VDR must at least record the following:

- Date and Time (SVDR)
- Ship’s Position (SVDR)
- Speed and Heading (SVDR)
- Bridge Audio (SVDR)
- Communication Audio (Radio) (SVDR)
- Radar Data (SVDR)
- ECDIS Data (SVDR)
- Watertight and Fire Door Status
- Speed and Acceleration
- Hull Stresses
- Wind Speed and Direction
- Echo Sounder
- Main Alarms
- Rudder Order and Response
- Hull Opening (doors) Status

1.3.1.9 Dynamic Positioning (DP) systems

Picture 13 Dynamic Positioning (DP) systems

Dynamic Positioning (DP) is a computer-based system that automatically maintains a vessel's position and heading by using its own thrusters and propellers. Position reference sensors, together with wind, motion sensors and gyrocompasses, provide information to the computer referring to the vessel's position and the magnitude, direction of any environmental factors that can affect its position. This system contains a mathematical model that includes information pertaining to the location of the thrusters, the wind and current drag of the vessel. This knowledge, allows the computer to calculate the required steering angle and the output of each thruster. This facilitates operations at sea, when anchoring or mooring is not possible due to deep water, congestion on the sea bottom or other problems.
Dynamic Positioning may either be absolute if the position is locked to a fixed point over the bottom, or relative to a moving object like another ship or an underwater vehicle.

1.3.2 Propulsion and Machinery Management and Power Control OTs

1.3.2.1 Engine Control Console (ECC)

Picture 14 Engine Control Console (ECC)

The Engine Control Console (ECC) consists of devices which allow the monitoring and remote control of the engine (main and auxiliary). Many sensors onboard ships continuously feed information on the main engine, auxiliary equipment and generator status to the ECC. This allows full remote start/stop control of the above, making operation simple and easy for the crew. Further to this it's equipped with devices which allow telephone conversation, remote monitoring of alarms, alerting the crew in case of an emergency, and many other functions which are necessary for a safe navigation. The ECC contains its own Alarm, Monitoring and Control System (AMS, AMCS).

1.3.2.2 Main Switchboard (MSB)

Picture 15 Main Switchboard

The Main switchboard is an installation that connects the power generators (auxiliary engines with alternators) and the power consumers (mainly different engine room machineries such as motors, blowers etc.) and is based in the ship's power distribution circuit. Any type of fault in an electrical system supplied from the MSB needs to be isolated, otherwise it will affect all the other systems connected to the same and may cause blackout of the whole ship.
Different safety devices are used on board ship and installed on the MSB and electrical distribution panels that ensure both safe and efficient running of machineries and personnel safety, from electric shock even when one system is at fault.
The main safety devices fitted on main switchboard are the following:

- Circuit breakers: A circuit breaker is an auto shutdown device, which is activated during an abnormality such as overloading or short circuit. Should this occurs, the breaker opens the operating circuit from MSB and therefore protects the same
- Fuses: Fuses are components used for short circuit protection as their material melts and isolates the MSB from the default system when the current passing through the circuit exceeds the safe value
- Over Current Relay: OCR is used mainly for protection from high current on the local panel and the MSB. Relay is normally set equivalent to full load current with time delay
- Dead Front Panel: It is one more safety device (an interlock switch) fitted on the MSB individual panels, which provides protection when someone cannot open the panel until the power of that panel is switched off

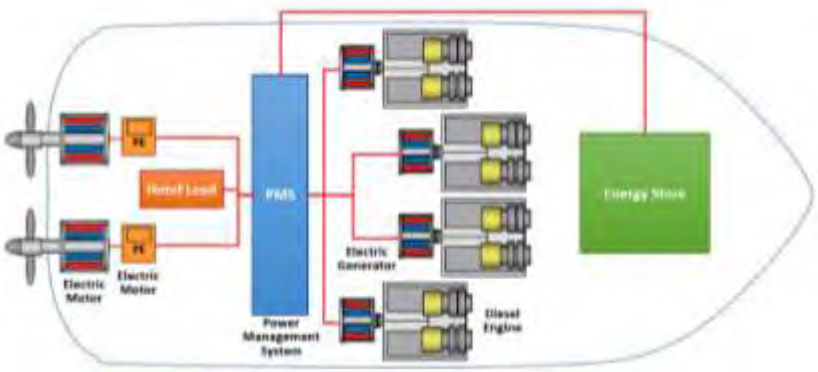
1.3.2.3 *Alarm Monitoring and Control System (AMCS)*

Picture 16 Alarm Monitoring and Control System (AMCS)

The Alarm, Monitoring and Control System (AMCS) is a microprocessor-based system containing all necessary functions for protection and control of the complete ship installation in unattended operations. It offers a wide range of flexible solutions to the vessel needs, therefore it occupies an important position on ships. It provides both audible and visual signals in the event of fault conditions. This ensures all three different operation modes (automatic, semi-automatic or manual remote control) of the whole installation including machinery and cargo.
The functions for protection and control adherence are:

- Power Management Systems (PMS)
- Unattended Machinery Space (UMS)
- Supervision Systems

1.3.2.4 Power Management System (PMS)



Picture 17 Power Management System (PMS)

Power Management System (PMS) is a vital part of the automation and power systems on vessels, and in particular for ships with electric propulsion. The purpose of the PMS is to assure adequate and reliable electrical power supply to the various consumers (communication and navigation equipment, alarm and monitoring system, running of motors for pumps, fans or winches, to high power installation). The PMS controls the power system in order to minimize the fuel consumption, the maintenance cost (by protecting the equipment against malfunctions) and maximize the blackout prevention.

PMS capabilities refer to the below fields:

- Generator Allocation Control (auto-start and auto-stop): The PMS will control the number of generators online based on the current load on the network and operational conditions
- Fast Load Reduction: The power consumption of variable frequency drives is controlled in order to avoid overloading the generators. PMS will force load reduction of some or all of the variable frequency drives until the situation is recovered, when an overload occurs e.g. caused by a shutdown of a generator
- Propulsion Load Limiting Control: Under normal operating conditions the PMS will prohibit an excessive load increase by controlling the maximum individual consumption of e.g. thrusters, drilling units, and compressors
- Blackout Restart: The PMS will perform restart of the power system in case of a total or partial blackout
- Regenerated Power Control: regenerated power is limited to avoid a reverse power situation for the generators. To prevent tripping of generators on reverse power, the amount of re-generated power will be limited by the drilling control system based on the signals from the PMS
- The PMS includes the Redundancy and Criticality Assessment system, an operator support system that monitors the "health" of the electric power system

1.3.2.5 Ship Emergency Response System (SERS)

The Ship Emergency Response System (SERS) is necessary to immediately assess the condition of a ship upon a damage, by establishing the new stability condition in order to evaluate the behavior of the vessel and the necessary actions to be taken for the mitigation of the event.
SERS provides 24/7 rapid access to expert teams of naval specialists. Collaborating closely with the ship / shore staff teams provide independent, proactive technical support and advice.
Provided Services:

- Modeling the geometry of the ship in a dedicated software, by creating a 3D model of the ship compartmentalization storage of all necessary particulars that can be retrieved in case of any casualty
- Evaluation of the ship's damage, immediately upon advice of the proper information and response. Retrieval of pre-defined ship model input of ship's pre-damaged loading condition
- Preparation and performance of emergency exercises which may help clients to deal effectively in case of any emergency situation

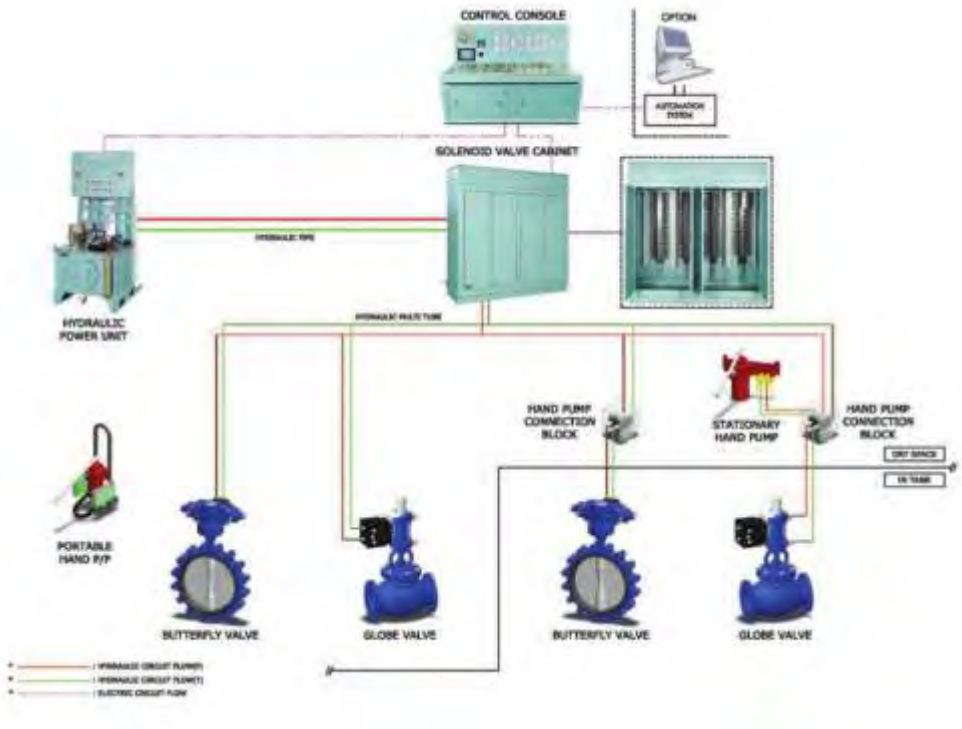
- Can evaluate the operator's emergency options and provide the most viable option re-computation of damage stability and damaged longitudinal strength at new vessel's status

1.3.3 Cargo Management OTs

1.3.3.1 Cargo Control Room (CCR)

The Cargo Control Room (CCR) of a ship is the physical location (may be in its own room, or located on the ship's bridge) where the person in charge monitors and controls the loading and unloading procedure of the ship's cargo. In addition to this, the equipment in the CCR allows the cargo control, monitor / control valve position and cargo tank liquid levels.

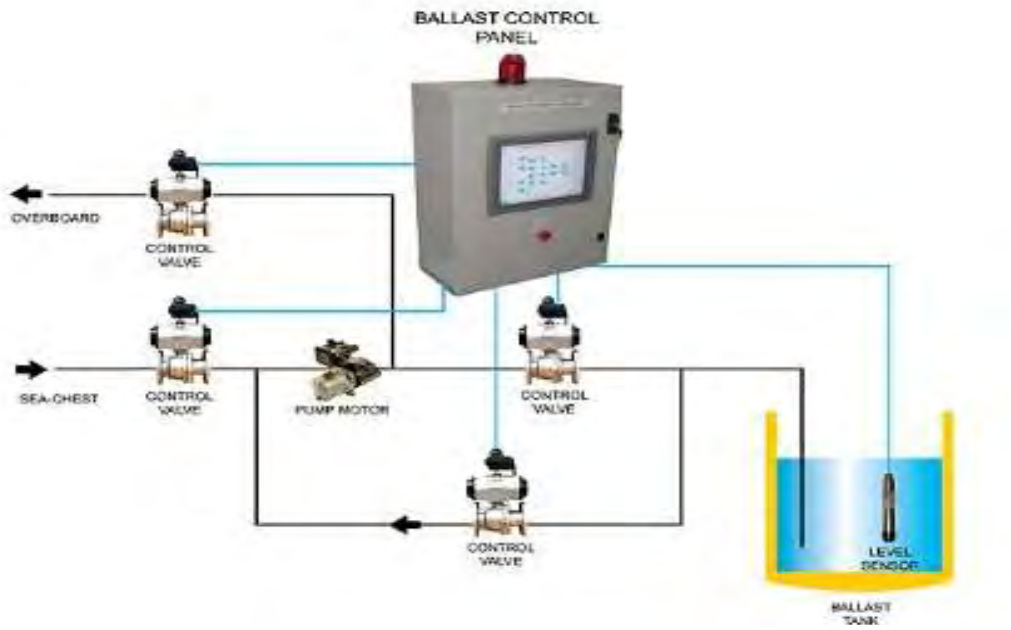
1.3.3.2 Valve Remote Control System (VRCS)



Picture 18 Valve Remote Control System (VRCS)

The Valve Remote Control System (VRCS) is a complete system for valve management and it provides a comprehensive solution for fluid control, together with the gauging system.
The VRCS is used to fill empty tanks, ballast and all service tanks found aboard a ship including cargo. The control console is solid and reliable (with or without control software) and provides a high interface to minimize human errors.
The majority of valves of the VRCS are equipped with electrical or hydraulic actuators that can be remote-controlled from the command console, and are able to provide precise and reliable closing and opening of the valves, regardless of the pressure and temperature. Hydraulic actuators are driven through solenoids and manifolds.

1.3.3.3 Ballast Water Systems



Picture 19 Ballast Water Systems

A ballast water system is a system that allows a ship to pump water in and out of very large tanks to compensate for a change in cargo load, due to shallow draft or weather conditions.
This system is very important for the safe operation of a ship, but it may cause significant threats to the environment and possibly local economies, as it may affect the ecosystem, thus it is one of the biggest problems faced by the shipping industry.
The IMO has regulated this process and set rules regarding Ballast Water Management to ensure that ships comply with the regulations.
The main parameters taken into account for choosing a ballast water treatment system are:

- Environment-friendliness
- Safety of the crew
- Cost effectiveness
- Space availability on board
- Ease of installation and operation

Here follow some types of ballast water treatment technologies available:

- Filtration Systems
- Chemical Disinfection
- Electric pulse/pulse plasma systems
- Heat (thermal treatment)
- Acoustic (cavitation treatment)
- Ultra-violet treatment
- Deoxygenation treatment
- Magnetic Field Treatment

1.3.3.4 Water Ingress Monitoring (WIM)

Picture 20 Water Ingress Monitoring (WIM)

The Water Ingress Monitoring (WIM) is a way of monitoring of water ingress that prevents of the flooding risk in the ship. IMO adopts a concept that monitors not only the presence of water, but also the speed of ingress in the cargo hold spaces. This is achieved via the setting of a two-stage alarm, set at a low level in the hold and another in a short distance above it.
Methods of detection may vary from use of simple float switches, to other for water detection. These alarms should be distinct and separated from other alarms on the bridge, except that a main alarm may be linked to an emergency alarm.

Every system must have:

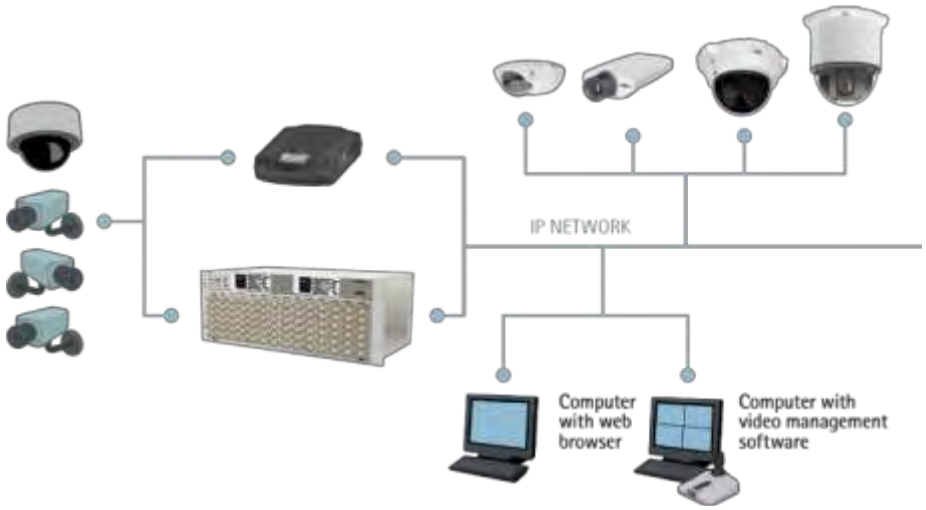
- Indication of power supply status
- Indication of a fault
- Indication of an alarm condition
- Indication of ballast interlock activation
- Audible alarms:
  - Pre-alarm: The visual indicator is accompanied by an audible alarm
  - Main alarm: The visual indicator is accompanied by an audible alarm that is distinct from (and preferably louder than) the other audible alarm
  - Fault alert: The visual indicator is accompanied by an audible alarm, which may be the same as the pre-alarm but must not be mistaken with the main alarm

1.3.3.5 Manifold Pressure Alarm System

Manifolds systems are able to control and reduce pressure from high pressure cylinders to the pressure level which must be used in the vessel pipe line. Manifolds and each connection flange should conform and need to fulfil the strict requirements set by the industry standard (OCIMF). In order to prevent the possible misconnection of the pressure manifold to a shoreside terminal liquid loading line an alarm system must be in place to protect the Cargo transfer. This provision is applicable regardless of the size of the ship.

1.3.4 Access control OTs

1.3.4.1 Surveillance Systems such as CCTV Network



Picture 21 Surveillance Systems such as CCTV Network

The video surveillance system was originally only a CCTV and has been regulated for providing a single channel closed circuit security monitoring service, where there is no security staff available or where collaborative work is required. Obviously, video surveillance systems have contributed to decrease rates of illegal violations and crimes.

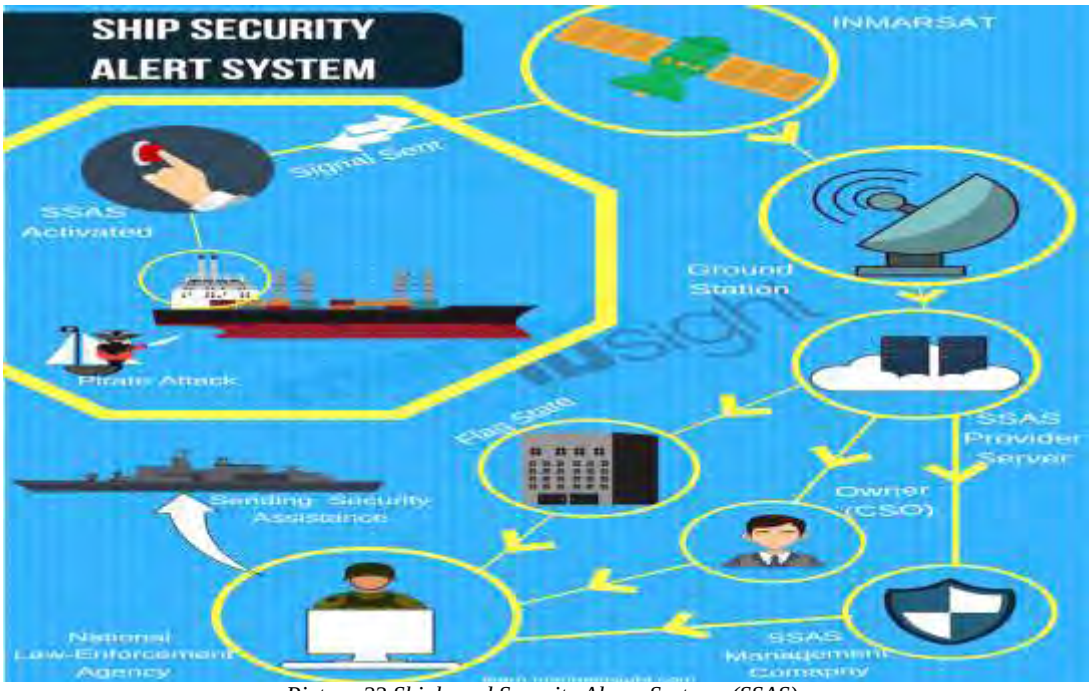
1.3.4.2 Bridge Navigational Watch Alarm System (BNWAS)

Picture 22 Bridge Navigational Watch Alarm System (BNWAS)

The Bridge Navigational Watch & Alarm System (BNWAS) is an alerting monitoring and alarm system that notifies other navigational officers of the ship, when the Officer on Watch (OoW) does not respond or is incapable to perform his/hers watch duties efficiently.
BNWAS monitors bridge activity and detects a possible operator's disability (due to accident, sickness or in the event of a security breach such as piracy and/or hijacking), which may lead to marine accidents. This is achieved through a mix of alarms which alert and warn the deputy OoWs as well as the Master in case of incapacity of the OoW. Unless decided by the Master only, the BNWAS shall remain operational at all times.
The BNWAS primarily has three modes of operation:

- Automatic
- Manual ON
- Manual OFF

1.3.4.3 Shipboard Security Alarm Systems (SSAS)



Picture 23 Shipboard Security Alarm Systems (SSAS)

The Ship Security Alert System (SSAS) is a safety measure for increasing ship's security against of acts of piracy and/or terrorism.

The SSAS is a silent security alarm which does not raise any visual-audio signal on the ship or nearby vessels or security forces. In most cases, the alert is firstly received by the ship's owner or an SSAS management third party, and then forwarded to the ship's flag state. The receivers are obliged to inform the local authorities of the coastal states where the ship is sailing.

How does SSAS work?

- When the maritime security staff comprehends possible danger from pirates or terrorists, a SSAS alert is triggered
- The beacon transmits a specific security alert to the administration and to the owner or the appointed professional SSAS provider and monitoring services, that includes important details about the ship and its location
- The administration, once receiving the signal, will notify the nearest local national authorities, which will dispatch proper military or law-enforcement forces to deal with the terrorist or pirate menace

2. Cyber Security

2.1 Definition

Cyber Security is the complex of a process, activity, ability, capacity, or condition where Information and Communication Technology (ICT) and the information contained therein are protected and secured and/or defended against damage, unauthorized access and use or modification and exploitation, preserving integrity, confidentiality and availability of information in Cyberspace. It contains technologies, policies, processes and practices designed to protect computer networks, programs and data from attacks, damage or alterations, unauthorized access. It surrounds a broad range of threat and vulnerability reduction means, deterrence, direct incident response, resilience, and recovery activities, to cover and strengthen computer network operations, information assurance, law enforcement, politics, diplomacy, military, and intelligence missions.

2.2 Importance of Cyber Security in Maritime

For centuries, vessels are used as merchandise transportation means worldwide. The maritime industry widely depends on computer systems, procedures, human resources and technology. This industry transfers merchandise of trillion of dollars per year in every corner of the globe.
Today, modern vessels are fully computerized, connected to networks with complex works that are associated totally via the cyberspace.
Modern marine vessels are frequently observed and controlled from on shore points thousands of miles away in order to secure effectiveness. This creates a new platform for hackers and pirates who increase their attacks towards the maritime industry.
Hackers could take control of a ship, unleash cyberattacks which shall affect the following operations-services:

- Vessels and safe navigation
- Satellite communication
- Merchandise surveillance systems
- Maritime radar systems
- Automated recognition systems

Therefore, the risk of a cyber-attack is a major threat for the maritime industry, so cybersecurity is of a great importance and an imposed necessity.

2.3 Cyber Threat Landscape

2.3.1 Sources of Threats

2.3.1.1 Organized Crime groups

The current era of cybercrime is no longer dominated by hackers accessing computer systems just for fun or hassle. The development and growth of the digital economy has changed the criminal landscape dramatically. Criminal groups are now shifting from traditional criminal activities to more rewarding and less risky operations such as the cyberspace attacks.

Criminal activities are usually conducted among multi-skilled members via virtual criminal networks over online meetings. Members rarely meet with each other in person, and sometimes do not even have a virtual contact with other "colleagues", thus their networks are structured on a "standalone" basis. This sophisticated chart prevents organized cybercrime groups from being detected and infiltrated by law enforcement.

2.3.1.2 Hacktivists and Hackers

In Internet activism or hacktivism (a portmanteau of *hack* and *activism*), is the subversive use of computers and computer networks to promote a political agenda or a social change. With roots in hacker culture and ethics, its ends are often related to the free speech, human rights, or freedom of information release.
Due to the variety of meanings (some include acts of cyberterrorism while other simply reaffirm the use of technological hacking to effect social change), there is a significant disagreement over the kinds of activities and purposes hacktivism encompasses. Hacktivism does not fit neatly into either white or black hat categories and it is mainly motivated by politics and not profit, as hacktivists are ideological odds feeling justified in their computer attacks against organisations.
The most known group is the *Anonymous*, a collective of clandestine hackers who have taken down and infiltrated computer systems belonging to companies and governments with whom they have political disagreements.
Hacker is the person who intrudes into network systems. A hacker possesses the suitable knowledge and capabilities to control and administer network systems. These persons are usually either computer programmers or network designers but could also be people that even though they do not professionally deal with this information technology field, they have developed such skills and work either in teams (hacking groups) or individually. The hackers' history background begins back in 1960 from the MIT university students. One of the biggest hacking in history, took place in 1969, when two Bell employees composed a few commands in order to increase the computers' speed. This hacking was named UNIX which today is one broadly known operating system.

2.3.1.3 Business Competitors

In many cases we face cyberattacks organised by major business competitors, who try to steal technology, intellectual property and/or source code in order to harm their competitors and cause material damage, delays in the production, negative publicity and loss of money.

2.3.1.4 Disgruntled Insiders

Despite the fact that media mainly focus on external attacks such as malicious email attachments and ransomware, internal threats are one of the most common cybersecurity issues faced by any organisation. Unfortunately, companies spend significantly more time and resources in order to prevent external threats while they oversee the potential damage from insiders. The impact of data breaches that involve dissatisfied employees can be significant, as sometimes they have internal administrative access and privileges to systems and data.
Internal threats are more difficult to be detected and may cause lasting and serious harm. Internal data breaches are mostly motivated by greed. There are cases, when an employee wants to gain a

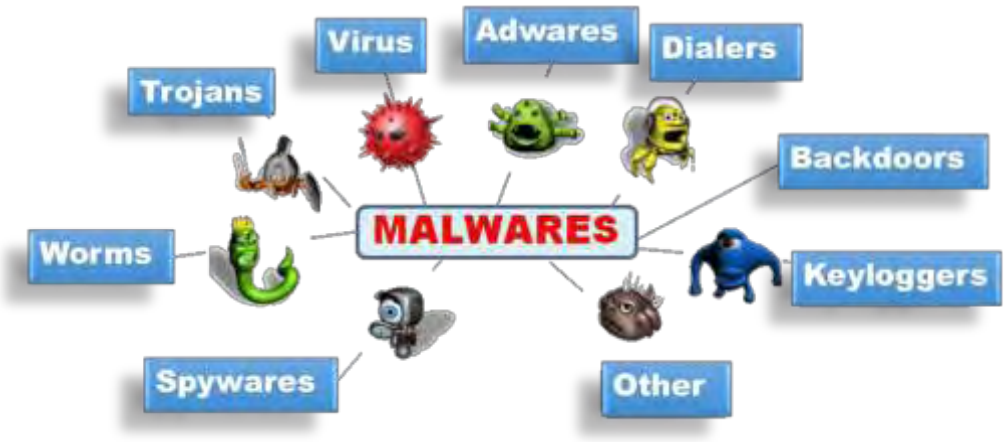
competitive advantage against the business or a new employer. In some other, an employee may collect information and collaborate with another criminal community that aims to identity theft and tax return or bank frauds. Regardless the reason, an angry or financially motivated employee can cause serious damage, especially one with knowledge of information technology and access to sensitive company data.

There are cases where internal breaches often occur when employees leaving their company. It is then that they use their last remaining access to steal business intellectual property or software, copy or delete data, that they could sell or use at their future jobs. Such malicious insiders are the most difficult to catch because they know their way around the company's network and can easily try to hide their footprints. We should not also ignore careless employee who accidently delete or modify or share sensitive and critical information just by not following the established company protocols and procedures.

Obviously, organisations need to monitor and control their employees' access and electronic paths at the time of their departure in order to take any proper measures to restrict any privileged access.

2.3.2 Attack Methods

2.3.2.1 Malware



Picture 24 Type of Malware

Malware is shortened for "malicious software". It refers to some virulent applications that are created with an only intent, that is to damage or disable electronic devices, such as mobile phones, computers or network servers. Its objectives can include breakup of computing or communication operations, theft of sensitive data, private networks access, or hijacking systems forcing them to exploit their resources. The excess use of email and internet over the last decade has led to a significant growth of malware that mainly targets to sensitive personal, financial or business information, for monetary gain. In some other cases objectives include cyberwarfare and espionage, or service disruption targeting specific global companies. The targeted victims can be from governments, enterprises to simple individuals.

Attackers use a variety of methods to plant malware into a computer, and in many cases they often require users to proceed with an action in order for the malware to be installed. A malware

program is successful when it is able to run without being detected, shut down or deleted. Examples of malware are links that ask to be clicked or request to download a file, the opening of an attachment that may look harmless in the first place, but has a malware installer hidden within.

2.3.2.2 Phishing

Picture 25 Phishing

Nowadays, uses are awakening against malware and internet theft, so there is less chance for an alert user to open a random attachment or click on a link or any email that comes his way without checking his sources. Attackers are aware of this, so they attempt to persuade users to install malware or divulge sensitive information by turning to phishing tactics. This means that they pretend to be someone you trust (like your friend, your boss or our bank/tax office) or try to push users to take action on something that they normally wouldn't by relying on human curiosity and emotion.
Pay attention that a phishing email usually carries some urgency and will look legitimate in the first place. The email will have an attachment to open or a link to click. Once this is done, the malicious attachment will be activated and the user will then install malware in his/her computer. Phishers may send a link with a legitimate-looking website that asks users to log in. It is then a well set trap to capture users' credentials.

2.3.2.3 Denial of Service (DoS) or Distributed Denial of Service (DDoS)

Picture 26 Distributed Denial of Service (DDoS)

A Denial-of-Service (DoS) attack is a flood in a website of enormous traffic than the one it was built to bear, that targets to an on purpose overload and an operation failure. It is as if thousands

of site visitors try to access a website that was built for hundreds, obvious with more traffic than it was built to handle, it will collapse.
This, of course, can happen in real life when there is massive news on a tragic global incident that will lead website users to overload traffic by visiting specific websites in order to find out more and inform themselves. Still, many times this kind of traffic overload is malicious, as an attacker floods a website with an overwhelming amount of traffic and shuts it down for all users.
This kind of attack is known as a Distributed Denial-of-Service Attack (DDoS). In some cases, DoS attacks are performed by many computers at the same time making the attack more difficult to overcome, as attackers simultaneously appear from many different IP addresses around the globe, pestering network administrators in their effort to find the source of the attack.

2.3.2.4 Social Engineering

Picture 27 Social Engineering

Social engineering is the state of the art cyberattack to manipulate users to give away their confidential information. Attackers usually seek for ways to trick users in order to obtain passwords or bank account information, access users' computers to secretly install malware that will give them access to passwords and control of the user computer.
Human inclination to trust is a benefit for criminals that use social engineering tactics, as it saves them from trouble to hack a computer. It is much easier for them to fool users to give away their passwords than to try getting them via an attack. Same thing stands for website usage, users need to be sure that sites are safe and legitimate before they can provide any personal information. Security is all about knowing who and what to trust.
It doesn't matter how many locks and deadbolts are on your doors and windows created in a computer if a user trusts someone who says he is someone who is not. User will expose himself in an unknown and dangerous risk.
What Does a Social Engineering Attack look like?

- Email from a friend
- Email from another trusted source
- Using a compelling story or pretext
- Baiting scenarios
- Response to a question you never had

- Creating distrust

3. Ship Network Architecture

3.1 Network System Design

The design of this network system shall enlighten matters such as the compatibility of the various devices in the vessel's network as a whole, meaning data transmission (amount of information, latency, and routes) to the shore company. The design shall also foresee the various potential system states, including initial state, failure state, and normal state, in order to define which communication is to be granted in various failure scenarios.
The network diagrams are available on the vessel and when there is any change in the network design, the network should be retested and updated with the new diagrams.
As a data requirement, it is extremely vital to consider such factors and to prevent ship equipment connected to the network that does not send or receive data from being excessively impacted.

3.2 Network interface for shipboard equipment and systems

3.2.1 Interface

The network system uses the IEEE 802.3 Ethernet standard which is most frequently used for computer networks: Carrier Sense Multiple Access/Collision Detection (CSMA/CD).
The network also uses the standard communication network internet protocol defined by this International Standard.

3.2.2 Connected equipment

The devices connected to the network system should be devices that are able to share information onboard a vessel.
The following are examples of devices eligible for connection to the network:

- Ship's clocks
- Sensor information network converters
- Network-capable multipoint displays
- Engine monitoring systems
- Cargo monitoring systems
- Vessel monitoring camera systems
- Shipboard IP telephone systems

3.3 Equipment Constituting Communication Network System

3.3.1 Switches

A switch is a computer network device with the same functionality as a bridge in OSI reference model layer 2. It may also called a "layer 2 switch".

Some models of switches have intelligent functions for network management such as:

- Rapid Spanning Tree Protocol (RSTP)
- Virtual Local Area Network (VLAN)
- Simple Network Management Protocol (SNMP)

3.3.2 Routers

A router is a communication device that connects different networks. It is responsible for OSI reference model layer 1 to layer 3 connections, and controls the transmission of IP packets between the various networks.
The basic functionality of a router is as follows:

- Filters IP headers
- Has quality of service (QoS) features, including prioritizing line capacity and throttling traffic
- Manages routing information using route-information collection protocols routing information protocol (RIP) and open shortest path first (OSPF)

3.3.3 L3 Switches

L3 switches mainly transfer data in OSI reference model layer 3. Their functionality is nearly equivalent to the one of a router.
They are normally faster than routers because they implement protocol processing in hardware.

3.3.4 Network Cables

The cables used to connect devices shall be selected with speculation for communication speed and distance. Installation of shield cables (shield twisted pair cable, foil twisted pair cable and others) should be selected, depending on the installation environment.
Table 3-1 shows the standard for selecting cables that connect devices, and the specifications for optical-fibre cables and metal cables used by the system. It is necessary to always pay attention to the latest standard.

Table 3-1 Network Cable Standards

Protocol		Standard Protocol	Communication Speed	Cables Used	Range
10BASE-T		IEEE 802.3i	10 Mbps	UTP/Shield Twisted Pair cable: Cat3	100 m
10BASE-F	10BASE-FB	IEEE 802.3j		Multi mode optical fiber	2 000 m
	10BASE-FP				1 000 m
	10BASE-FL				2 000 m
100BASE-T	100BASE-TX	IEEE 802.3u	100 Mbps	UTP: Cat5	100 m
	100BASE-T4			UTP(4): Cat3	100 m
	100BASE-T2	IEEE 802.3y		UTP(2): Cat3	100 m
100BASE-F	100BASE-FX	IEEE 802.3u		Multi mode optical fiber	2 000 m
				Single mode optical fiber	20 km
1000BASE-T	1000BASE-T	IEEE 802.3ab	1000 Mbps	UTP(4): Cat5e	100 m
	1000BASE-TX	TIA-EIA/-854		UTP(4): Cat6	100 m
1000BASE-X	1000BASE-SX	IEEE 802.3z		Multi mode optical fiber	550 m
	1000BASE-LX			Multi mode optical fiber	550 m
				Single mode optical fiber	5 000 m
	1000BASE-CX			Coaxial cable(2)	25 m
10GBASE-T		IEEE 802.3an	10 GMbps	UTP(4):Cat6e	100 m
				UTP(4):Cat6a	100 m
				UTP(4):Cat7	100 m
10GBASE-R	10GBASE-SR	IEEE 802.3ae		Multi mode optical fiber	300 m
	10GBASE-LR			Single mode optical fiber	10 km
	10GBASE-ER			Single mode optical fiber	40 km

3.4 Network administration

3.4.1 Network Administration Requirements and Definitions

Network administration is a mechanism for a continuous monitoring of traffic and nodes, and enables crew to ascertain any anomalies.
The mechanism should be simple to handle that any crew may easily learn how to administer the network without being an expert.

3.4.2 Network Administration Scope

The scope of the network administration addresses only the equipment's network communication.

The following categories of network administration are defined by the ISO OSI:

- perform configuration management
- do not perform billing and confidentiality management
- performance management
- fault management

3.4.3 Network Administration Items

The Administrative items are as follows:

- Node status (included alive signal of network devices)
- Traffic
- Cable disconnections

3.4.4 Requirements for Network Monitoring Devices

The crew should be able to monitor and identify the locations of errors from a network-monitoring device installed on the bridge. The device shall indicate appropriate countermeasures for problems.
Network monitoring devices should have the following functionality:

- Display physical architecture of network
- Alarm
  - When a link is disconnected/connected or the power is turned off/on for a network device or network terminal
  - When there are Packet loops
  - When the traffic exceeds the threshold value
  - When an otherwise defined network-device/terminal anomaly occurs
- Logging
- Traffic display
- Setting configuration
- Fault recovery support
  - Network information
  - Failure remedies
    - Network device stoppage
    - Network device restart
    - Packet loops

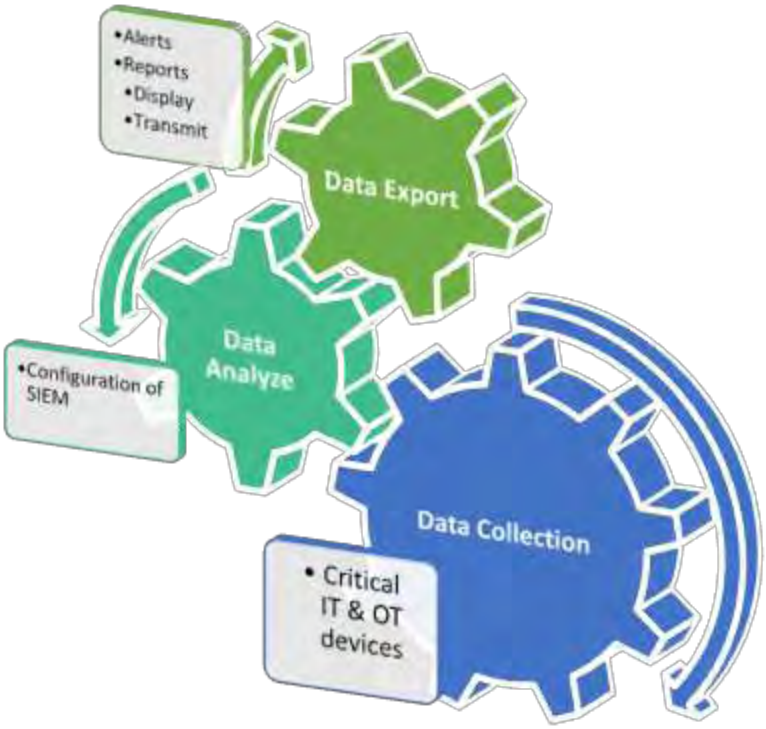
4. Black Box

4.1 Introduction

The main purpose of the black box is to collect and analyze critical data and signals produced by the vessel's network (IT and OT). These are network traffic data log files, firewalls log files, systems logs etc. The black box is able to create alerts, reports and flags when any change that looks suspicious takes place, in order to ensure the following:

- On time alert of cyberattacks
- Safe sailing
- Personnel safety
- Cargo securing

The black box can make an initial analysis on board in cases that are common and easy to detect, and in parallel to transmit in real time data on shore's Security Operation Centre (SOC) for further analysis.
The black box operates as shown/descripted in the diagram as below:



Picture 28 Black box diagram

4.2 Components (Tools)

4.2.1 Maritime Firewall (FW)

The maritime FW performs a traffic and services control, based on the use of protocols and ports in order to filter which packets are allowed and/or rejected by a ship network.
Basic traffic filtering permits or denies the passage of each packet through the firewall by configuring access list implementations that examine packets at the network layer.
The rules used to define network access should be as precise as possible. This is where the principle *of "least privilege"*, should be applied. As many as possible parameters should be specified in the set rules. A 4-layer firewall uses the following parameters as an access rule:

- Source IP address (or range of IP addresses)
  If the service is accessible to everyone, then "*any"* source IP address is the correct and best option. In all other cases, source address should be specified
- Destination IP address (or range of IP addresses)
  This is the IP address of the server that runs the service of which someone wants to allow access. Accessed server (or group of servers) should be always specified
- Destination port (or range of ports)
  This port should match with the service that needs to be accessed. The value of this field should never be "*any*". The service that runs on the server and needs to be accessed is predefined

4.2.2 VLAN Equipment

A "Virtual Local Area Network," or "Virtual LAN" is a custom network that enables groups of devices from multiple networks (both wired and wireless) to be combined into a single logical network. In order to create such a LAN, network equipment like routers and switches must support VLAN configuration. The hardware is typically configured by using a software admin tool that allows the network administrator to customize the virtual network. Assignment of individual ports or groups of ports on a switch to a specific VLAN can be achieved through an administration software. Two (2) VLANs is recommended to be created on vessels. One for Business IT/Ship OT and one for Crew Welfare network.

4.2.3 Voyage Data Recorder (VDR)

Voyage Data Recorder (VDR) means a complete system that includes any item required to interface with the sources of input signals, their processing and encoding together with the final recording, the power supply and the dedicated reserve power source.
The purpose of a VDR is to maintain storage -in a secure and retrievable form- of information concerning the position, movement, physical status, command and control of a ship over the designated time period. Information contained in a VDR should be made available to both the Administration and the ship-owner. This information is for use during any subsequent safety investigation to identify the cause(s) of an incident.
Data items to be recorded

- Date and time
- Ship's position

- Speed
- Heading
- Bridge audio
- Communications audio
- Radar
- ECDIS
- Echo sounder
- Main alarms
- Rudder order and response
- Engine and thruster order and response
- AIS
- Rolling motion
- Configuration data
- Electronic logbook
- Hull openings status
- Watertight and fire door status
- Accelerations and hull stresses
- Wind speed and direction

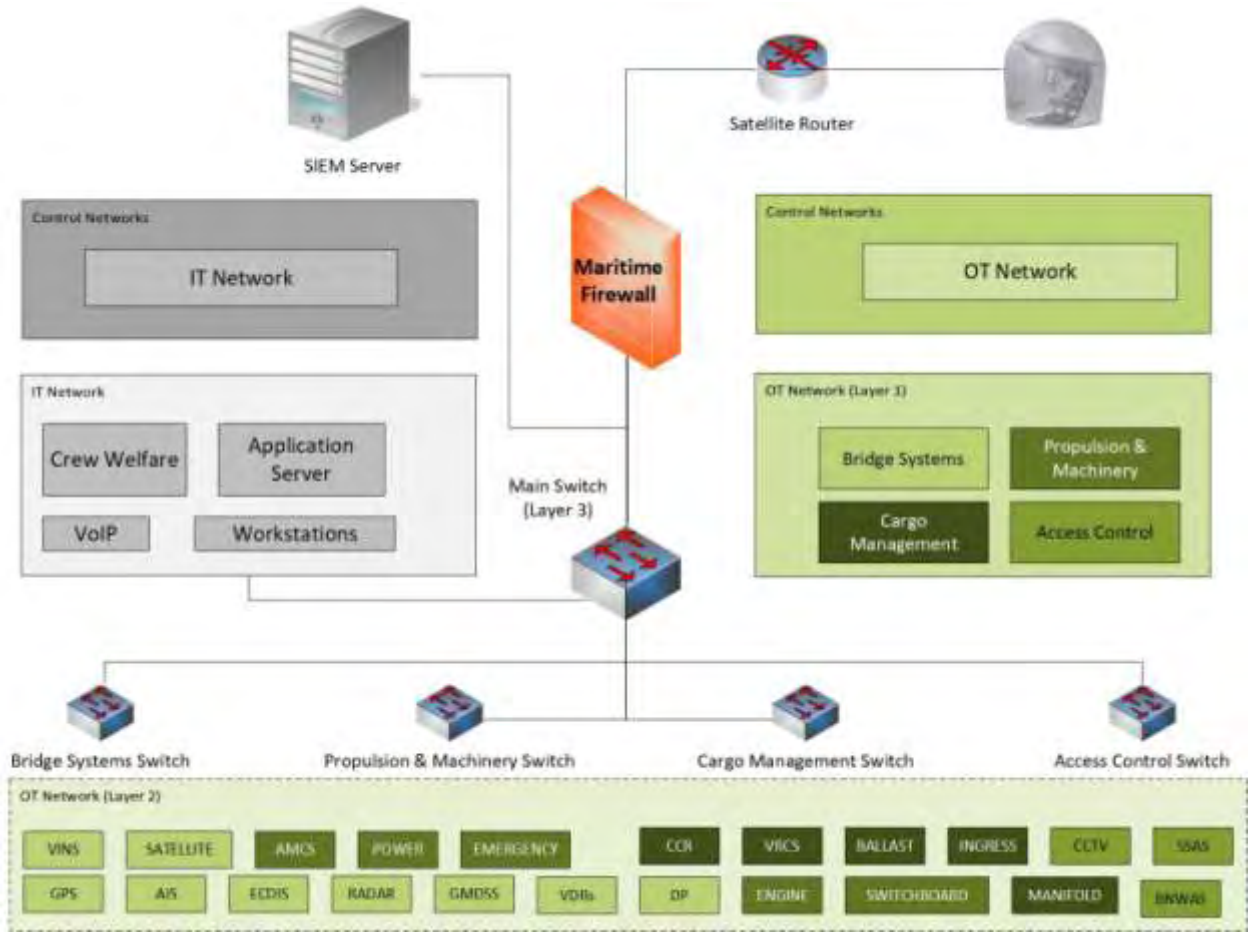
4.2.4 Security Information and Event Management (SIEM)

The Security Information and Event Management (SIEM) system is relatively new to the information technology (IT) environment. The SIEM system is a complex collection of technologies designed to provide vision and clarity on the corporate IT system as a whole, benefitting both security analysts and IT administrators.
The main objective for a security analyst using a SIEM system is to reduce the number of false-positive alerts, in order to avoid being in a "needle-in-the-haystack" situation. On a vessel, IT and computer based OT operations can use the SIEM to identify various types of operational problems such as downed servers and malfunctioning or misconfigured systems, applications, and appliances within a network. The SIEM can be used to identify routine IT/OT system needs, for instance, additional capacity requirements, user training issues, and buggy applications that may need patching, upgrading, or replacing. With a SIEM, many monitoring, alerting, analysis, correlation, and reporting functions are automated.
The SIEM system generally provides the following services:

- Log management
- IT/computer based OT regulatory compliance
- Event correlation
- Endpoint security
- Active response

4.3 Implementation and Operation

4.3.1 Vessel Network Interconnection Diagram



Picture 29 Vessel Network Diagram

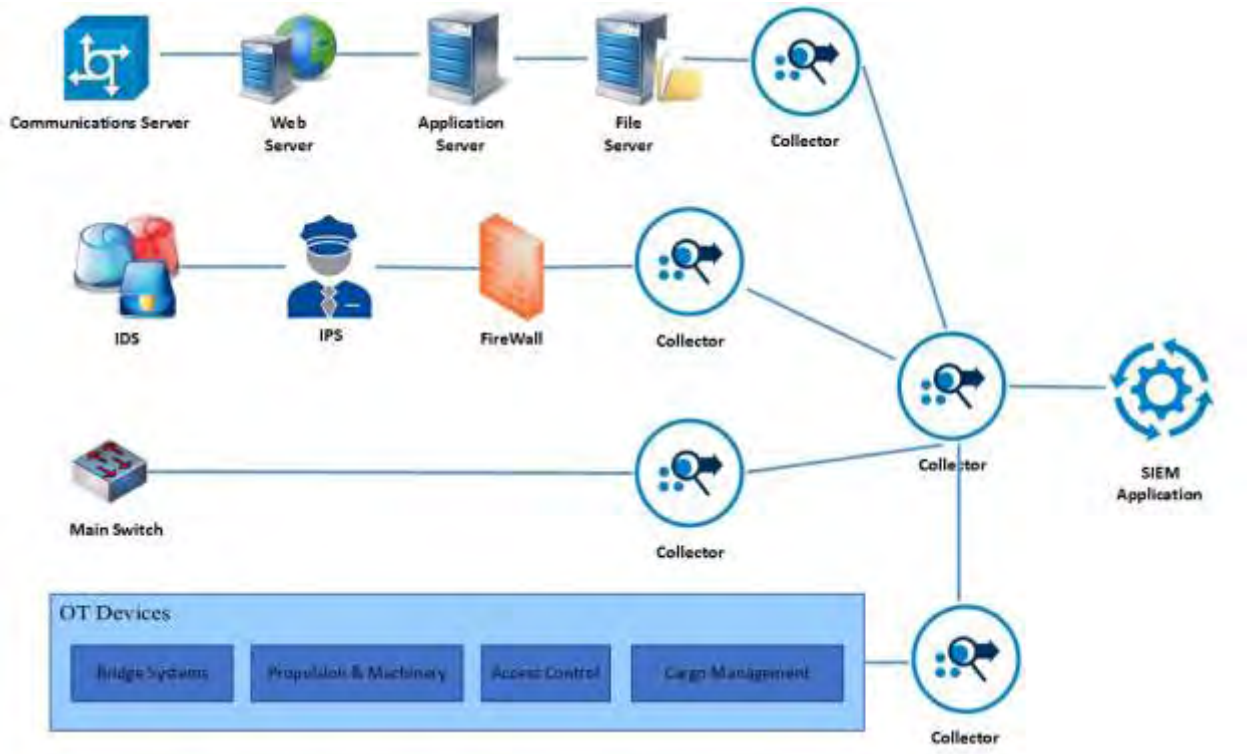
Lately, the demand for ship to shore connectivity that is able to provide remote maintenance and monitoring has grown bigger. Ship networks can be categorized based on their basic functionality such as *'ship administrative network'* or *'ship control network'*. Proper network protection and systems detection, should be provided for inter network communication that is based on network analysis.

Ship *administrative network* would consist of computers assigned for general administrative tasks and can also include communication with shore locations. Typical examples could be IT systems used for operational and maintenance management, reporting and scheduling, capacity planning, administration tools such as phone, e-mail, or printing services.

Control network on ships may consist of individual and complete systems. It can be logically separated into zones or layers. The key for security countermeasure that is designed to classify devices into security zones is the network segmentation, where identified security practices are utilized to achieve the desired security level. Key systems should be separated and categorized into zones that have common security levels in order to effectively manage security risks and in order to achieve a desired security level for each zone. A demilitarized zone (DMZ) may be used

for high risk control systems, in co-occurrence with a control zone to provide an additional risk reduction opportunities between the low-security level business or administrative network and the high-security level control network.

4.3.2 Data Collection



Picture 30 SIEM Data Collection

Routers, switches, firewalls, servers, OTs equipment that ships have, generate several types of log records. Some of this information may be or not very useful, depending on what it is someone is looking for.

The first part of a SIEM is the source device that feeds information into the SIEM. A source device is the device or application, or some other type of data that you want, to retrieve logs from them which you can then store and process in your SIEM.

SIEM may use several techniques to collect log events from all connected devices. Each of these methods has its advantages. Data collection is the largest challenge for all cases. Potentially log collection can occur from each device in the ship. Every router, every firewall, every server and OTs equipment would route their log files to Collectors, and SIEM applications which in turn would collect all these log files, generate their own log files which would also require collecting etc.

Collectors

Collectors are in-between the actual SIEM application and the hundreds or thousands of agents spread around the network. Collectors are capable of some correlation although they mainly do normalization work, while they can run standalone or combined with SIEM applications, in a single instance.

SIEM applications

A possible (second) target for the aforementioned collection is a SIEM application. It can handle less events per second although it is capable of doing more with these events. It is usually the end-point for all mentioned applications and thus the core of the whole system. The SIEM application is the core of a SIEM environment. It handles things like:

- Risk assessment
- Real-Time Monitoring
- Event correlation
- Vulnerability Scanning
- Data Mining

A SIEM application generates reports and shows overviews. Although it can handle less events than a Logger, it is important to realize that a SIEM application can rely on other devices to do event and flow processing. At the end, this application is set up to recognize any change that is different than the set up scope or business rules.

4.3.3 SIEM Data Processing

Picture 31 SIEM Data Processing

4.3.3.1 Data Collection

Data collection refers to the gather of events from different applications and devices on a network that provide understanding on what is going on. Each device generates an event each time something happens, and collects the events into a single repository known as a log file.

4.3.3.2 Normalization

Normalization permits predicable and consistent storage for all records, for fast searching when fighting the clock in an incident investigation. Furthermore, normalization allows consistent analysis and reporting on every event regardless its data source.
Normalization is actually no longer a requirement on current platforms, but in the early days of SIEM Normalization was a necessity as it was used for database back-end data management.

4.3.3.3 Aggregation

As said SIEM platforms collect data from multiple sources, as these events provide the data needed to analyze the security of our environment. In order to have an end-to-end view, we need to consolidate the collection into one single platform. Aggregation is the process of gathering data and log files from separate sources into a common repository. This collected data is placed into a homogenized data store where analysis, reporting, and forensics take place.
The aggregation process is very important to Log Management and most SIEM platforms as it helps to manage data in a consistent mode. Data ensemble can be achieved by sending data directly into a SIEM/LM platform, or to an intermediate host who can collect this data from the source and periodically feed the SIEM system.

4.3.3.4 Correlation

A SIEM correlation tells the SIEM system which sequences of events may be indicative of anomalies and may imply security weaknesses or cyber-attack. When “x” and “y” or “x” and “y” plus “z” happens, your administrators should be notified.
Here follow some examples of SIEM correlation rules which illustrate this concept.

- Detect new DHCP servers in your network by watching for inside or outside connections which use UDP packets (“x”), have port 67 as the destination (“y”), and the destination IP address isn’t on the registered IP list (“z”)
- Warn administrators if five failed login attempts are tried with different usernames from the same IP to the same machine within fifteen minutes (“x”), if that event is followed by a successful login occurring from that same IP address to any machine inside the network (“y”)

The first example may indicate a cyber attacker who tries to establish a DHCP server to acquire malicious access to your network.
The second example could show a cyber attacker forcing an authentication vector and then successfully acquiring authentication to your network.
SIEM correlation rules may be triggered by human mistakes and simple user errors or technical glitches, still they’re also key indicators of cyber-attacks so security administrators should immediately check them out.

4.3.3.5 Alerting

Type of SIEM alerts:

- user activity reports
- configuration change reports

- access reports
- on-demand operational reports
- Monthly summary reports
- failed login source
- incident tracking reports
- failed login target
- repeat logins from a single IP in one minute
- Multiple intrusion detection system alerts from a single IP address
- repeat attack host
- virus detected
- spyware or virus removed
- Virus detected, but not successfully cleaned or removed

4.3.3.6 Reporting

SIEM should be set up in a proper way in order to create daily/weekly or monthly event reports. These reports are the sum of the collection of all incidents and will be stored in a specific place in order to provide metric and historical reference. The benefit of this library is to improve the configuration of the SIEM.

4.3.4 Display – Transmit

4.3.4.1 Display

The collection of SIEM's alerts should be displayed in designated ship areas like the bridge, the control rooms, etc. in a simple and easy readable format in order to have a network status update to arise awareness.

4.3.4.2 Transmit

The above SIEM data should also be transmitted in real time to the shore SOC in order to be further analyzed and diagnosed to prevent a future cyberattack.

4.4 Network/Security Operation Center (N/SOC)

A Security Operations Center (SOC) is a facility that houses an information security team who is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported. Some additional capabilities of SOCs can include advanced forensic analysis, cryptanalysis, and malware reverse engineering to investigate incidents. The 24/7 monitoring provided by a SOC, gives organizations an advantage to defend themselves against incidents and intrusions, regardless of source, time of day, or attack type. The SOC team is the first line of defence against rapidly evolving threats and needs to work close to enterprises incident response teams to make sure that security issues are addressed and sloved quickly upon discovery.

5. Conclusion

Obviously attackers shall continue to find new methods for network penetration and host compromising. Therefore, defenders need to look for clues of intrusions from as many sources as possible. Collecting and analyzing log data across the enterprise ship network can be a pretty challenging endeavor.

This Thesis presents all information systems available on a vessel (IT & OT), the possible threats against these and the necessity of the cyber-defence in maritime. This paper also examines and displays a vessel's network architecture and the implementation of the black box to detect, monitor and analyze cyber-attacks and to create on time alerts and reports.

Black box solutions can help intrusion detection by collecting all relevant critical data in a central location and provide customizable altering and reporting. In addition to this, black box provides significant value by helping to determine if an incident occurred or not. The challenge for analysts is to create effective alerts in order to catch today's sophisticated and well-funded attackers.

The best parameterization of the Maritime Firewall & SIEM applications will conclude the best possible detection of cyber-attacks to a vessel, so as to ensure early warnings and the implementation of counter measures in order to diminish these threats and attacks.

References

[1] N. AS, "Maritime VoIP Communications for Oil & Gas, Ships and Offshore Facilities," Norphonic AS, Bergen, Norway.

[2] E. E. A. S. (EEAS), "EU Concept on Cyber Defence for EU-led Military Operations and Missions," 2016.

[3] R. M.-C. Bobby Hellard, "ITPRO," 3 Dec 2018. [Online]. Available: http://www.itpro.co.uk/strategy/29643/what-is-an-application-server.

[4] "PC," [Online]. Available: https://www.pcmag.com/encyclopedia/term/51969/stand-alone-pc.

[5] "Wikipedia," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Network_switch.

[6] "Wikipedia," 2018. [Online]. Available: https://simple.wikipedia.org/wiki/Gateway_(computer_networking).

[7] "Webopedia.," [Online]. Available: https://www.webopedia.com/TERM/E/end_user.html.

[8] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Firewall_(computing).

[9] "TechTarge," [Online]. Available: https://searchstorage.techtarget.com/definition/external-storage.

[10] INTERTANKO, "Crew Internet Access on board Ship – a Best Practice Guide," 2011.

[11] L. Alexander and M. J. C. Joseph F. Ryan Capt., "Integrated Navigation System: Not a Sum of Its Parts," University of New Hampshire, 2004.

[12] Manu, "Bright Hub," [Online]. Available: https://www.brighthubengineering.com/seafaring/23017-gps-navigation-and-its-use-on-board-ships/.

[13] "Global Marine Networks (GMN)," [Online]. Available: http://www.globalmarinenet.com/marine-satellite-communications/.

[14] "Wikipedia," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Electronic_Chart_Display_and_Information_System.

[15] "ECDIS," [Online]. Available: http://www.ecdis-info.com/about_ecdis.html.

[16] Y. Dyryavyy, "Preparing for Cyber Battleships – Electronic Chart Display and Information System Security," NCC Group, 2014.

[17] "Rice Electronics," 2008. [Online]. Available: http://www.riceelectronics.com/marine-radar.html.

[18] "Wikipedia," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Marine_radar.

[19] "Policy on Global Maritime Distress and Safety System (GMDSS) For Barbados," 2006.

[20] "Wikipedia," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Voyage_data_recorder.

[21] S. Bhattacharjee, "Marine Insight," Guidelines, 9 Oct 2017. [Online]. Available: https://www.marineinsight.com/guidelines/voyage-data-recorder-on-a-ship-explained/.

[22] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Dynamic_positioning.

[23] "JRCS MFG. CO., LTD," [Online]. Available: https://www.jrcs.co.jp/en/products/detail/engine-control-console/).

[24] Mohit, "Marine Insight," 31 May 2017. [Online]. Available: https://www.marineinsight.com/marine-electrical/what-are-the-main-safety-devices-for-main-switch-board-on-ship/.

[25] J. J. a. F. H. May, "Power Management System for the "Deepwater Horizon" a Dynamically Positioned All Weather Semisubmersible," ,Dynamic Positioning Conference, Huston, US, 2000.

[26] "CBS - Cyprus Bureau of Shipping," 2011. [Online]. Available: http://www.cbs.com.cy/en/html-58-Ship_Emergency_Response_System.html.

[27] "Honeywell," [Online]. Available: https://www.honeywellprocess.com/en-US/explore/products/marine/ship-automation/Pages/valve-remote-control.aspx .

[28] Raunek, "Marine Insight," 7 Oct 2017. [Online]. Available: https://www.marineinsight.com/tech/how-ballast-water-treatment-system-works/.

[29] BIMCO, "Water Ingress Monitoring: Master's guide," BIMCO Marine Committee.

[30] K. Y. M. A. Kyungroul Lee, "Elsevier Ltd.," Elsevier , 2 Jan 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0898122111007218.

[31] S. Bhattacharjee, "Marine Insight," 21 Jun 2017. [Online]. Available: https://www.marineinsight.com/marine-navigation/what-is-bridge-navigational-watch-alarm-system-bnwas/ .

[32] Anish, "Marine Insight," 29 Jun 2018. [Online]. Available: https://www.marineinsight.com/marine-piracy-marine/what-is-ship-security-alert-system-ssas/.

[33] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Hacktivism .

[34] V. Hargrave, "Trend Micro," 17 Jun 2012. [Online]. Available: https://blog.trendmicro.com/whats-the-difference-between-a-hacker-and-a-cybercriminal/.

[35] R. F. W. Samuel Lanier Felker, "Baker Donelson," 27 Jun 2017. [Online]. Available: https://www.bakerdonelson.com/disgruntled-employees-and-other-internal-threats-to-your-cyber-security.

[36] "Global Digital Forensics Inc," [Online]. Available: https://evestigate.com/disgruntled-employees-can-be-insider-cyber-threats-waiting-to-happen-warns-fbi/.

[37] "Rapid7," [Online]. Available: https://www.rapid7.com/fundamentals/types-of-attacks/.

[38] N. DuPaul, "Veracode," [Online]. Available: https://www.veracode.com/security/malware.

[39] "Webroot," [Online]. Available: https://www.webroot.com/ie/en/resources/tips-articles/what-is-social-engineering.

[40] "TechTerms," 23 Nov 2016. [Online]. Available: https://techterms.com/definition/vlan.

[41] M. S. Terje R. Paulsen, "Voyage Data Recorders (VDR)," Gard AS, 2011.

[42] D. R. Miller, S. Harris, A. A. Harper, S. VanDyke and C. Blask, "Security Information and Event Management (SIEM) Implementation," McGraw-Hill Companies, 2011.

[43] "Network Architecture," IACS Rec, 2018.

[44] "AlienVault, Inc.," [Online]. Available: https://www.alienvault.com/blogs.