Software Applications and Network System Used in Seagoing Ships (Lecture)

First Edition

Software Applications and Network System Used in Seagoing Ships (Lecture)

Monette Davidon Apor
Author

Ronald B. Enoc
Dr. Minsoware S. Bacolod
Editors

Software Applications and Network System
Used in Seagoing Ships (Lecture)

Monette Davidon Apor
Author

Ronald B. Enoc
Dr. Minsoware S. Bacolod
Editors

Assigned Number:

Form	ISBN
Hardbound	**978-621-96947-6-6**
PDF (read only)	**978-621-96947-7-3**
PDF (downloadable)	**978-621-96947-8-0**

Published by:

PHIL-CAD
ACADEMICIAN
PUBLISHING

Block 20 Lot 7, Purok Rosal, Brgy. Datu Esmael-H1
Dasmariñas, City, Cavite, 4114, Philippines
Contact Number: 0927-7753-471/0906-573-6578
Website: www.philcadademian.com
Email Address: filcad2023@gmail.com

Preface

The maritime industry is undergoing a profound digital transformation, with information and communication technologies (ICT) playing a crucial role in ensuring the efficiency, safety, and sustainability of seaborne operations. *Software Applications and Network System Used in Seagoing Ships (Lecture)* is designed to provide marine engineering and maritime studies students with foundational knowledge and practical understanding of the digital systems used onboard modern vessels. This book introduces learners to various software applications and network infrastructures essential to ship operations, including navigation systems, communication protocols, monitoring tools, cybersecurity safeguards, and compliance with international maritime standards. Emphasizing both theoretical insight and operational relevance, the course fosters critical thinking, system literacy, and technical fluency—skills essential for future seafarers, ICT officers, and maritime professionals. Whether preparing for onboard duties or planning a future in maritime ICT management, students will find this course an indispensable guide to understanding the digital backbone of seagoing ships.

Course Syllabus

Course Title: Software Applications and Network System Used in Seagoing Ships (Lecture)
Course Code: PC-ICT (lec)
Credit Hours: 3
Prerequisites: Basic Computer Operations / Maritime Communication Systems
Instructor: [Instructor Name]
Contact Information: [Email / Office Hours]
Term: [Semester / Year]

Course Description

This course offers a comprehensive introduction to the software applications and onboard network systems utilized in seagoing ships. Students will examine essential shipboard technologies such as navigation and communication software, control systems, digital monitoring tools, and cyber risk management. The course also covers regulatory requirements, industry standards, and future trends in maritime ICT. Emphasis is placed on system understanding, technical documentation, and practical application.

Course Objectives

By the end of this course, students will be able to:

- Understand the role and scope of ICT in maritime operations.

- Identify and describe essential shipboard software applications.
- Explain network architectures and systems integration onboard.
- Perform basic troubleshooting and diagnostic analysis.
- Discuss the importance of cybersecurity in maritime systems.
- Apply knowledge of ICT compliance with IMO, SOLAS, and STCW standards.
- Reflect on the future impact of digitalization in shipping.

Course Outline

Chapter 1: Introduction to Maritime ICT
- *Importance of ICT in Modern Shipping*
- *Overview of Digital Transformation at Sea*
- *Classification of Shipboard Systems*
- *Evaluation*

Chapter 2: Shipboard Software Applications
- *Navigation Software (ECDIS, AIS, Radar Overlays)*
- *Communication Software (GMDSS, SATCOM)*
- *Engine, Maintenance, and Cargo Software Systems*
- *Evaluation*

Chapter 3: Navigational and Communication Systems
- *Operational features of GPS, AIS, and Radar*
- *Evaluation*

Chapter 4: Shipboard Network Architecture
- *Types of Shipboards and Networks (LAN, VLAN, WLAN)*
- *Devices: routers, switches, firewalls*
- *Cabling, Wireless Links, and Configuration Examples*
- *Evaluation*

Chapter 5: Monitoring, Control, and Integration Systems
- *Control Systems (Engine, Ballast, Cargo)*
- *Data Acquisition and Sensor Networks*
- *Human-Machine Interfaces (HMI) and Automation Integration*
- *Evaluation*

Chapter 6: Maintenance and Troubleshooting of ICT System
- *Regular System Maintenance Protocols*
- *Troubleshooting Hardware/Software Issues*
- *Use of Diagnostic Tools and System Logs*
- *Evaluation*

Chapter 7: Maritime Cybersecurity

- *Threat landscape in maritime ICT*
- *IMO Cyber Risk Management Guidelines*
- *Security Layers: firewalls, access control, encryption*
- *Evaluation*

Chapter 8: Software Licensing, Compliance, and Documentation

- *Software Installation and Version Control*
- *Licensing Models (OEM, subscription, open source)*
- *Technical Documentation, Digital Logbooks, and Backups*
- *Evaluation*

Chapter 9: ICT in Emergency and Safety Operations

- *Role of ICT in Search and Rescue (SAR)*
- *Emergency Alarms and Alerting Systems*
- *Fail-safe Design and Redundancy Protocols*
- *Evaluation*

Chapter 10: Future Trends and Regulatory Frameworks

- *Digital Twin Technology and Smart Ships*
- *AI and Machine Learning at Sea*
- *IMO, STCW, SOLAS Guidelines on Digital Systems*
- *Evaluation*

Table of Contents

Preface
Table of Contents

Chapter 1

Software Applications and Network System Used in Seagoing Ships (Lecture)

Introduction to Maritime ICT

Welcome aboard the thrilling adventure into the realm of Maritime ICT! On this module, you will discover how information and communication technologies (ICT) have revolutionized the international shipping industry—from navigation and cargo handling to real-time communication and security monitoring. In an era where oceans unite continents, ICT makes ships not only floating objects but floating digital enclaves. This module will intrigue and amaze you with how digital technologies influence efficiency and safety in the maritime industry. Whether you are currently training to be a marine engineer, navigator, or port operations officer, studying Maritime ICT is your compass to navigating the digital seas of contemporary shipping.

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Cognitive Competency – Identify the central position of ICT in maritime operations and its effects on shipping safety and efficiency.
2. Technical Skill – Classify and describe the working of different shipboard systems and how they are integrated with the assistance of ICT.
3. Professional Attitude – Show an active and responsive attitude to the digitalization of shipping activities.

Lesson Objectives

By the end of the lesson, you will be able to:

1. Identify major elements of ICT systems used in maritime operations.
2. Explain the importance of digitalization in contemporary shipping.
3. Categorize shipboard systems and their corresponding ICT functions.
4. Explain the contribution of Maritime ICT to promoting efficient and secure maritime operations.
5. Demonstrate an appreciation of the business application of Maritime ICT in occupational maritime settings.

Engage (Activating Prior Knowledge)

Let's play "Then and Now!" In class groups, make a list of the ways communication, navigation, and cargo handling were done in the days of old maritime operations versus the way they are done today. Share your list with the class and see how far the maritime world has come into the computer age!

Introduction

This module explores the fundamentals of Maritime ICT and ICT technologies that are revolutionizing 21st-century seafaring. From automated gear to real-time communication devices, ICT is not an overlay or a frill but central to modern maritime practice. As future maritime professionals, your understanding of these technologies will enable you to work responsibly and competently in a rapidly digitalized shipping industry.

Explore (Lesson Inputs)

In today's highly digitalized maritime era, it is critical to have a basic understanding of Maritime ICT to survive and stay successful in shipping operations today. The three fundamental concepts below describe the use of technology at sea: ICT in shipping, digitalization onboard vessels, and shipboard system classification. These interrelated concepts will help you understand the use of technology in facilitating shipping operations' safety, communication, navigation, and efficiency.

Importance of ICT in Modern Shipping

Information Communication Technology (ICT) lies at the core of maximizing operating efficiency, safety, environmental accountability, and decision-making in modern shipping. ICT enhances real-time data share, enables integrated navigation and cargo tracking systems, and supports automated documentation systems, maximizing global maritime operations. Svanberg et al. (2019) are sure that the application of ICT tools has reduced human error and improved situational awareness through enhanced ship-to-ship and ship-to-shore communication. ICT also enables the establishment of e-navigation, where maritime experts can access updated nautical charts, weather conditions, and emergency messages efficiently (Lee et al., 2020). With the growth of complexity in global trade, ICT is becoming essential in shipping logistics management, reducing delays, and maintaining compliance with global standards such as those of the International Maritime Organization (IMO, 2021).

Table 1. Concepts on the Importance of ICT in Modern Shipping

Concept	Description	Explanation
Operational Efficiency	Refers to the ability of ships to complete voyages, cargo handling, and administrative tasks faster and more accurately using digital tools.	ICT improves operational efficiency through automation of key processes such as cargo tracking, engine checking, and navigation updates. This leads to reduced port stay time, reduced labor costs, and increased voyage optimization for better turnaround time and logistics performance (Svanberg et al., 2019).
Safety and Risk Reduction	Involves minimizing accidents and ensuring crew safety through real-time monitoring, alerts, and emergency communication systems.	Through technologies like AIS and GMDSS, ICT offers safe navigation through live ship location, route tracking, and immediate emergency messaging (Lee et al., 2020). The technologies avoid collisions and reduce the impact of human error.
Environmental Sustainability	The use of digital technologies to monitor and control emissions, fuel consumption, and eco-friendly practices onboard.	ICT hardware helps monitor engine emissions, fuel usage, and shipping routes to reduce carbon footprints. Smart voyage management helps ships use the most fuel-efficient shipping routes, which is in accordance with global environmental policy and promotes green shipping (Perera et al., 2020).
Decision-Making Support	The ability of onboard systems to collect, analyze, and visualize data to assist crew in making informed choices.	Integrated dashboards and real-time data analysis enhance situational awareness and allow crews to make data-driven decisions. These are included in route optimization, predictive maintenance scheduling, and cargo management—all of which reduce downtime and operation errors (Zhao et al., 2022).
Global	Ensures ships meet	ICT systems enable regulatory

Standards and Compliance	international maritime rules and operate in accordance with IMO and other regulatory frameworks.	compliance through automated reporting, chart updating for navigation charts, and voyage data recording in order to satisfy SOLAS and MARPOL obligations. The IMO's e-navigation architecture also encourages the application of digital technology onboard to ensure safer, more standardized global maritime operations (IMO, 2021).

Application of ICT to modern shipping practice has revolutionized the way maritime practitioners carry out day-to-day operations. From improving the operational efficiency and seafaring safety to improving environmental stewardship and regulatory compliance, ICT is the pillar of technology support for modern shipping practice. ICT-based systems allow real-time information exchange, support data-informed decision-making, and reduce human error—functions that are critical to an industry where time, safety, and accuracy take center stage. As the table indicates, an understanding of the multi-dimensioned importance of ICT is essential for students with career aspirations in the evolving face of maritime transport.

Overview of Digital Transformation at Sea

Digitalization of the seas is the mass application of cutting-edge digital technologies like Artificial Intelligence (AI), the Internet of Things (IoT), cloud computing, and cybersecurity solutions to transform maritime operations. Digitalization is not merely automation—it transforms how ships still function, interact with ports, and process data. Digitalization boosts predictive maintenance, energy efficiency, and performance tracking through sensor-based monitoring and machine learning systems, as argued by Zhao et al. (2022). Digitalization also makes smart ships and autonomous ships possible with the ability to execute complex operations with minimal human intervention (Perera et al., 2020). Maritime professionals are being transformed by these technologies, making future practitioners digitally literate and flexible in a constantly changing, tech-driven working environment.

Table 2. Key Concepts of Digital Transformation at Sea

Concept	Description	Explanation
Artificial Intelligence (AI)	AI refers to the simulation of human cognitive processes by machines to enable learning, reasoning, and problem-solving.	Onboard, AI is used for route optimization, autonomous navigation, and predictive maintenance. These technologies analyze vast amounts of data—weather, fuel use, and traffic—make informed decisions, and lower operational expenses and

		carbon emissions (Perera et al., 2020; Zhang & Zhang, 2022).
Internet of Things (IoT)	IoT involves the interconnection of devices and sensors through the internet, enabling real-time data collection and transmission.	IoT at sea connects different systems like engine performance monitors, cargo temperature sensors, and safety equipment. The interconnection enhances monitoring precision, minimizes downtime, and enhances operational transparency and security (Zhao et al., 2022; Wang et al., 2021).
Cloud Computing	Cloud computing offers online access to computing services like storage, processing, and analytics over the internet.	Maritime business companies use cloud platforms to aggregate data from global fleets, and remote access to ship information, maintenance schedules, and decision-making functions is offered. It improves collaboration and reduces the need for local data infrastructure (Lee et al., 2020).
Cybersecurity Protocols	Cybersecurity protocols are protective measures designed to secure digital systems and data against unauthorized access and cyber threats.	With further digitalization, ships are now vulnerable to cyberattacks that can disrupt navigation and communication. Maritime cybersecurity entails encrypted communication, safe networks, and compliance with IMO regulations to ensure operational safety (IMO, 2021; Zhao et al., 2022)
Smart and Autonomous Ships	These are vessels equipped with advanced digital systems that enable remote or fully autonomous operations.	Intelligent ships use AI, IoT, and automated control systems to perform tasks that have traditionally been carried out by humans. These include navigation, engine monitoring, and cargo management. The result is reduced human error, increased efficiency, and future-proofing autonomous shipping (Perera et al., 2020; Zhang & Zhang, 2022).

This Digital Transformation at Sea lesson introduces you to the cutting-edge technologies revolutionizing the maritime industry today. With Artificial Intelligence, IoT, cloud computing, cybersecurity, and smart ships, the lesson introduces you to how traditional shipping operations are being revolutionized into data-driven, automated, and intelligent systems. All these ideas not only improve safety and operational performance but also prepare you for a digitally centered maritime industry with the emphasis on digital skills and innovation. With increased demand for smart, sustainable, and secure shipping, expertise in these digital ideas prepares you for maritime logistics, engineering, navigation, or port operation careers in the future.

Classification of Shipboard Systems

Shipboard systems are classified in various functional groups based on their use and technological integration: navigation systems, communication systems, and operational control systems. Navigation systems such as GPS, ECDIS (Electronic Chart Display and Information System), and AIS (Automatic Identification System) provide correct routing and collision avoidance. Communication systems such as GMDSS (Global Maritime Distress and Safety System) and satellite communication equipment are required to enable ship-to-coast communication. Operational systems control onboard machinery, monitor engine condition, and control cargo integrity. Zhang and Zhang (2022) are of the opinion that integration of these systems with a centralized ICT platform makes data flow free, promoting safety and reducing operation costs. These technologies enable the overall goal of intelligent, interoperable ships as per the digital maritime ecosystem principles (Wang et al., 2021).

Table 3. Classification of Shipboard Systems

Concept	Description	Explanation
Navigation Systems	Systems used to direct and position the ship safely using digital and electronic tools. These include GPS, ECDIS, and AIS.	Marine safety and efficiency are enhanced by navigation systems with the provision of real-time position data, the presentation of digital nautical charts, and broadcasting ship information to nearby ships. GPS provides correct positioning, ECDIS facilitates digital route planning and monitoring, and AIS prevents collisions with broadcasting ship identity and movement. Navigation systems reduce human mistakes and enhance situational awareness (Zhang & Zhang, 2022; Lee et al., 2020).
Communication Systems	Tools and technologies that enable ships to exchange information internally and externally. These include GMDSS, VHF radios, and satellite communication systems.	Communication systems play an essential role in the coordination of operations, safety, and emergency response. GMDSS offers automated distress alerting, while satellite and VHF communications provide round-the-clock contact with other ships and port authorities. Such

		equipment facilitates the crew's capacity to manage emergency and maintain operational continuity, particularly for long voyages or in distant sea areas (Wang et al., 2021; Perera et al., 2020).
Operational Control Systems	Systems that manage and monitor onboard machinery and operations such as engine performance, cargo, and fuel usage.	Operational control systems use sensors and automation to monitor ship activity like engine, fuel, and cargo status. Connected to the central platforms, the systems allow for predictive maintenance, reduce energy consumption, and optimize efficiency. Data-driven, functionalities ensure sustainable operation and reduce the possibility of equipment failure, hence reducing operation costs (Zhao et al., 2022; Zhang & Zhang, 2022).

Understanding shipboard system classification is important to shipping professionals of the future since it provides a clear picture of how technology facilitates different aspects of ship operations. Navigation systems deliver precise routing and collision avoidance; communication systems deliver safety and collaboration through real-time communication; and operational control systems manage engine performance, cargo, and fuel management. Merging these systems into central ICT platforms constructs smart, data-driven environments that improve ship efficiency, safety, and sustainability. With digitalization gaining traction in shipping industries, it is not an option but a necessity for seafarers of the 21st century to know these systems.

Explain

Define the following terms in your own words: ICT, shipboard systems, digital transformation, and automation in maritime contexts. Then, in a Venn diagram, compare historical maritime practice and digital maritime practice. This exercise enables you to connect new ideas to old ideas, which makes learning more relevant and holistic.

Elaborate/Extend (Application)

Suppose you are a team on a technologically advanced vessel. There is an impending storm, and your ICT system must deliver accurate navigation, crew security, and cargo monitoring. In light of your knowledge of ICT systems and concepts, recommend a safety and communications plan. This will allow you to bridge theory into practice—just as it occurs in real maritime circumstances.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. **What is the primary benefit of ICT in modern shipping?**
   a. Reduces ship size
   b. Enhances real-time data sharing and decision-making
   c. Increases paperwork
   d. Slows down operations
2. **Which ICT tool is essential for reducing human error and increasing situational awareness onboard ships?**
   a. Compass
   b. Radar scanner
   c. AIS
   d. Hull monitor
3. **E-navigation is supported primarily by:**
   a. Paper charts
   b. Handwritten logs
   c. Digital nautical charts and automated alerts
   d. Manual steering
4. **Which of the following describes operational efficiency in the context of ICT?**
   a. Reducing ship size
   b. Automating ship and port processes for faster operations
   c. Building new ports
   d. Cutting crew salaries
5. **What system ensures global emergency communication at sea?**
   a. GPS
   b. GMDSS
   c. VHF radio only
   d. Compass
6. **How does ICT support environmental sustainability?**
   a. By increasing fuel use
   b. By printing fewer documents
   c. Through monitoring emissions and optimizing fuel consumption
   d. By using solar sails
7. **What is a key feature of the Internet of Things (IoT) on ships?**
   a. Manual logs of temperature
   b. Interconnected sensors providing real-time data
   c. Sending letters via radio
   d. Paper-based reports
8. **Predictive maintenance is most commonly enhanced through:**
   a. Random inspections
   b. Satellite TV
   c. Sensor-based monitoring with AI and IoT
   d. Visual estimation
9. **What role does cloud computing play in maritime operations?**
   a. Replaces weather forecasting
   b. Stores paper logs online
   c. Enables remote data access and centralizes fleet management
   d. Adds storage to ship warehouses

10. **What is one of the primary purposes of cybersecurity protocols in maritime ICT?**
    a. Prevent overheating
    b. Track dolphins
    c. Protect digital systems from unauthorized access
    d. Reduce weather alerts
11. **Smart ships are characterized by their ability to:**
    a. Grow in size autonomously
    b. Operate using digital tools with reduced human input
    c. Repair other ships
    d. Build ports
12. **Which system helps with digital route planning and collision avoidance?**
    a. ECDIS
    b. GMDSS
    c. VHF
    d. SSB radio
13. **Navigation systems typically include:**
    a. Wind meters only
    b. GPS, ECDIS, and AIS
    c. Compass and binoculars
    d. Sonar and thermometers
14. **Operational control systems mainly monitor:**
    a. Crew sleep patterns
    b. Weather forecasts
    c. Engine performance and cargo integrity
    d. Radio signals
15. **According to the lesson, the integration of all shipboard systems leads to:**
    a. Crew unemployment
    b. Overloaded communication
    c. Seamless data flow and improved operational performance
    d. Frequent system shutdowns

Reflection

What would you imagine ICT impacting your future maritime career? Consider how Maritime ICT studies have influenced your understanding of shipping operations today and enabled you to embrace technological innovations in your career.

Unit Summary

This chapter provided the basics of Maritime ICT, emphasizing its central role in revolutionizing the shipping sector. You discovered the significance of cyber technologies offshore, acquired an overall overview of digitalization in maritime settings, and learned to categorize shipboard systems. These highlights equipped you with the basics for top-tier topics and everyday applications in your maritime professional life.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 1

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic

	expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Demonstrates understanding of ICT applications in maritime operations										
2. Utilizes digital tools to support safe navigation and routing										
3. Applies communication technologies for operational and emergency use										
4. Operates shipboard systems with accuracy and efficiency										
5. Identifies and analyzes real-time data for decision-making										
6. Implements digital practices for environmental sustainability										
7. Applies principles of predictive maintenance using AI and sensors										
8. Uses cloud-based platforms for maritime data management										
9. Observes cybersecurity protocols in handling ship systems										
10. Demonstrates familiarity with smart and autonomous vessel systems										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

International Maritime Organization (IMO). (2021). *IMO e-navigation strategy implementation plan*. https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx

Lee, J., Kim, H., & Park, Y. (2020). The impact of ICT on seafarers' situational awareness and maritime safety. *Journal of Marine Science and Technology*, *25*(3), 345–357. https://doi.org/10.1007/s00773-020-00724-y

Perera, L. P., Soares, C. G., & Guedes Soares, C. (2020). Autonomous ship navigation and guidance: A review and future challenges. *Ocean Engineering*, *195*, 106605. https://doi.org/10.1016/j.oceaneng.2019.106605
Svanberg, M., Wänström, C., & Cullinane, K. (2019). ICT-based improvements in maritime logistics efficiency: A literature review. *Maritime Economics & Logistics*, *21*, 357–376. https://doi.org/10.1057/s41278-017-0096-0
Wang, T., Lu, W., & Lu, M. (2021). Integration of digital technologies in maritime operations: Smart shipping framework and challenges. *Maritime Policy & Management*, *48*(2), 215–230. https://doi.org/10.1080/03088839.2020.1810419
Zhang, Y., & Zhang, W. (2022). The evolution of intelligent ship systems and their impact on maritime safety. *Sensors*, *22*(4), 1561. https://doi.org/10.3390/s22041561
Zhao, X., Jin, Y., & Qian, X. (2022). Cybersecurity risks and defense mechanisms in smart ships: A comprehensive review. *Journal of Marine Engineering and Technology*, *21*(5), 912–928. https://doi.org/10.1080/20464177.2021.1976465

Answer Key with Explanations

1. **What is the primary benefit of ICT in modern shipping?**
   Answer: b. Enhances real-time data sharing and decision-making
   Explanation: ICT systems improve communication and operational efficiency by allowing for real-time data access and smarter decision-making across navigation, safety, and logistics.
2. **Which ICT tool is essential for reducing human error and increasing situational awareness onboard ships?**
   Answer: c. AIS
   Explanation: The Automatic Identification System (AIS) broadcasts vessel identity, location, and course to nearby ships, helping avoid collisions and enhancing situational awareness.
3. **E-navigation is supported primarily by:**
   Answer: c. Digital nautical charts and automated alerts
   Explanation: E-navigation relies on digital systems like ECDIS that display electronic charts and generate real-time alerts for navigational safety.
4. **Which of the following describes operational efficiency in the context of ICT?**
   Answer: b. Automating ship and port processes for faster operations
   Explanation: ICT tools automate cargo tracking, engine diagnostics, and documentation, helping ships operate faster and with fewer errors.
5. **What system ensures global emergency communication at sea?**
   Answer: b. GMDSS
   Explanation: The Global Maritime Distress and Safety System (GMDSS) automates distress signaling and ensures ships can communicate emergencies worldwide.

6. **How does ICT support environmental sustainability?**
   Answer: c. Through monitoring emissions and optimizing fuel consumption
   Explanation: ICT tools track emissions and fuel usage, allowing for eco-friendly routing and compliance with environmental standards.
7. **What is a key feature of the Internet of Things (IoT) on ships?**
   Answer: b. Interconnected sensors providing real-time data
   Explanation: IoT enables devices like temperature sensors and engine monitors to share data across systems for efficient ship operations.
8. **Predictive maintenance is most commonly enhanced through:**
   Answer: c. Sensor-based monitoring with AI and IoT
   Explanation: Digital sensors detect issues before failure, allowing AI to predict maintenance needs, minimizing downtime and cost.
9. **What role does cloud computing play in maritime operations?**
   Answer: c. Enables remote data access and centralizes fleet management
   Explanation: Cloud platforms store data online, giving access to ship records and analytics from anywhere, enhancing coordination.
10. **What is one of the primary purposes of cybersecurity protocols in maritime ICT?**
    Answer: c. Protect digital systems from unauthorized access
    Explanation: As ships become digital, cybersecurity measures are essential to guard against hacking, data breaches, and system disruptions.
11. **Smart ships are characterized by their ability to:**
    Answer: b. Operate using digital tools with reduced human input
    Explanation: Smart ships use technologies like AI and IoT for automated navigation, engine monitoring, and operational control with minimal crew input.
12. **Which system helps with digital route planning and collision avoidance?**
    Answer: a. ECDIS
    Explanation: The Electronic Chart Display and Information System (ECDIS) shows electronic maps and enables route monitoring to avoid hazards.
13. **Navigation systems typically include:**
    Answer: b. GPS, ECDIS, and AIS
    Explanation: These systems work together to provide accurate location data, route planning, and communication between ships.
14. **Operational control systems mainly monitor:**
    Answer: c. Engine performance and cargo integrity
    Explanation: These systems manage key ship functions like engine diagnostics, fuel use, and cargo status to ensure smooth operations.
15. **According to the lesson, the integration of all shipboard systems leads to:**
    Answer: c. Seamless data flow and improved operational performance
    Explanation: Integrating navigation, communication, and operational

systems into centralized platforms improves efficiency, safety, and data accuracy.

Chapter 2

Introduction to Shipboard Software Applications

Board the digital bridge of the seas' new era! Those compass and star days are gone, and seafarers now steer state-of-the-art vessels with high-performance software systems at their command. We embark on this chapter in the world of shipboard software programs—essential tools that guarantee safe passage, effective communication, and maximum engine and cargo optimization. This module will familiarize you with the new technologies that keep vessels on track, link vessels across seas, and oversee intricate onboard procedures.

By studying these computer programs, you're not learning about systems alone, you're learning to be an asset in a computerized shipping system. Let this chapter pique your interest and motivate you to become a master of the computer skills it takes to be a successful mariner in an industry that's changing at a whirlwind pace.

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Depict awareness of principal shipboard computer systems used in navigation, communications, engine, and cargo operations.
2. Acquire technical expertise in the interpretation and use of electronic maritime programs pertaining to onboard activities.
3. Demonstrate ethical conduct and attitude when using shipboard technologies as per professional practice and safety regulations.

Lesson Objectives

By the end of the lesson, you will be able to:

1. Establish and list the principal categories of shipboard software used for navigation, communication, and engine/cargo operations.
2. Differentiate between the tasks and functions of ECDIS, AIS, Radar overlays, GMDSS, SATCOM, and onboard maintenance systems.
3. Evaluate real-world scenarios of computer programs on board ships to maximize operational decision-making.
4. Demonstrate proper utilization of a shipboard software simulation or interface within a directed exercise.
5. Apply combined knowledge and skills to perform a simulated navigation or communications assignment with correct shipboard software.

Engage (Activating Prior Knowledge)

Do you recall the last time you accessed a GPS application or a messaging program? Imagine using something of the kind, but far more sophisticated—but in the middle of the ocean! Share your own experiences of using technology for location or communication and how these technologies would be employed at sea in pairs. How would you imagine ships communicating or preventing collisions?

Lesson Introduction

With seafaring business turning fully digital, new engine and deck officers must learn how to operate, communicate, and command onboard systems via the guidance of modern software tools. This lesson offers you the technical competencies required in actual shipboard operations—enriching your professional growth and in accordance with the Philippine Professional Standards for Teachers (PPST) Domain 3: Content Knowledge and Pedagogy, specifically on ICT integration in instruction and learning.

Explore (Lesson Inputs)

The modern maritime world is fast being powered by advanced software systems that ensure safety, efficiency, and conformity to world regulations. As a future seafarer, it is not just an added skill but a professional necessity to get accustomed to shipboard software's basic uses. In this article, the three general categories of maritime software are highlighted: navigation, communication, and engine/cargo management systems. These technologies form the backbone of ship operations and are central to the success of voyages on world seas.

Navigation Software Systems (ECDIS, AIS, Radar Overlays)

Navigation software has revolutionized ship navigation, from manual plotting of charts to real-time digital means. Electronic Chart Display and Information System (ECDIS) is a mandatory tool for most commercial ships, providing dynamic visualization of charts with GPS positioning, automatic update, and alert function. ECDIS enables enhanced route planning and situation awareness, substantially reducing human navigation error (Kim & Park, 2020). Automatic Identification System (AIS) is another mandatory tool that sends information from ships such as position, speed, and identity to nearby ships and shore stations, enabling collision avoidance and maritime surveillance (Wang & Meng, 2021). Radar overlays, when integrated with ECDIS, overlay radar images on electronic charts, providing a composite image enhancing the operator's capacity to identify obstacles in poor weather conditions. Together, these tools enable the International Maritime Organization's (IMO) e-navigation strategy for enhanced maritime safety and efficiency through digital integration (IMO, 2021).

Table 1. Concepts in Navigation Software Systems

Concept	**Description**	**Explanation**
ECDIS (Electronic Chart Display and Information System)	A computerized navigational tool that displays electronic charts integrated with positioning data to support route planning and navigation.	ECDIS has substituted static paper charts with dynamic chart presentation with real-time positioning, route tracking, and alerting. It improves maritime safety by automating matters with less human intervention and the likelihood of error, and enabling more precise navigational decisions. The International Maritime Organization (IMO) requires its use in specific vessels, and its user-friendly interface has significantly enhanced bridge performance (Kim & Park, 2020).
AIS (Automatic Identification System)	A maritime communication tool that transmits and receives vessel-related data such as identity, position, speed, and heading.	AIS provides real-time monitoring of ships so that ships and coastal hubs can monitor sea traffic and avoid collision. AIS is particularly helpful in congested sea lanes, improving port efficacy and safety. It also supports logistics planning and situational awareness on sea networks (Wang & Meng, 2021).
Radar Overlays	A navigational feature that superimposes radar images over digital electronic charts to create a	Radar overlays enhance navigators' situational awareness by visually superimposing charted information with radar-detected targets. The integration of radar-

	unified visual interface.	detected targets with charted information detects land, vessels, and other obstructions during low-visibility conditions and complements other devices like AIS. It supports the overall aim of e-navigation by encouraging smooth digital transfer between navigational equipment (IMO, 2021).

Navigation computer systems such as ECDIS, AIS, and radar overlays form the core of modern maritime operations, providing sailors with real-time, data-rich interfaces that enhance safety, accuracy, and efficiency. ECDIS has eliminated paper charts and substituted them with interactive digital charts that update automatically with GPS, while AIS provides automatic information sharing between ships to prevent collisions. Integrated with radar overlays, the systems provide a comprehensive and reliable means of detecting risks, plotting routes, and tracking marine traffic. As highlighted by recent studies (Kim & Park, 2020; Wang & Meng, 2021; IMO, 2021), such technologies enhance the IMO's e-navigation vision and are crucial skills aspiring sailors must learn to navigate today's complex maritime environment.

Communication Software Systems (GMDSS, SATCOM)

Maritime communication is vital for safety, coordination, and efficient operation. The Global Maritime Distress and Safety System (GMDSS) is a globally accepted system of procedures and equipment enabling ships to send and receive distress messages globally. It includes equipment like EPIRBs, NAVTEX, and Digital Selective Calling (DSC), which alert automatically and save response time in emergency situations (Zhao, Chen, & Li, 2023). SATCOM, satellite communications, provides reliable voice and data communications over long distances at sea, allowing communication with company headquarters, coastal states, and other ships. It is a critical component of normal shipboard operations and enables crew welfare through internet access and remote medical consultations (Chen & Wu, 2019). GMDSS and SATCOM technologies are complementary, providing the building blocks of maritime communication, satisfying regulatory needs, and maintaining marine safety.

Table 2. Communication Software Systems – Concepts, Descriptions, and Explanations

Concept	**Description**	**Explanation with Updated Literature (2018–2024)**
Global Maritime Distress and Safety System (GMDSS)	A standardized international system of communication protocols and equipment designed to improve safety at	GMDSS integrates various subsystems, including EPIRBs (Emergency Position-Indicating Radio Beacons), NAVTEX (Navigational Telex), DSC (Digital Selective Calling), and

	sea.	Inmarsat to issue distress warnings to be automatically sent and received worldwide. It enables quicker response to maritime distress by automating distress signals and maritime safety information regardless of the position of a vessel. It is a SOLAS requirement and significantly enhances the global maritime safety network (Zhao, Chen, & Li, 2023).
SATCOM (Satellite Communication)	A communication system using satellites to transmit and receive data over long distances.	Operationally and for well-being, SATCOM on board ships is used for voice calls, internet, and data transfer to shore-based systems. SATCOM offers real-time location tracking of ships, remote diagnostics, and weather information. SATCOM not only offers day-to-day communication but also emergency communication when land communication is not available. Developments have also enhanced its integration with smart ship systems to enable enhanced onboard connectivity and decision-making (Chen & Wu, 2019; IMO, 2021).

Understanding of communication software systems such as GMDSS and SATCOM is essential for safety and coordination in maritime operations. They are complementary in providing ships with the capability of automatically broadcasting distress signals, exchanging safety-related messages, and communicating in real time with coastal stations and other vessels around the world. GMDSS provides emergency communication worldwide, while SATCOM provides connectivity beyond the confines of normal radio range, addressing both operational and welfare requirements of the crew. With shipping development heading for digital integration, a comprehension of these tools prepares the next generation of mariners to manage emergencies, address international responsibilities, and ensure the free exchange of shipboard and shoreside communication.

Engine, Maintenance, and Cargo Software Systems

Contemporary ships rely more and more on digital technology for monitoring engines, predictive maintenance, and cargo management. Computerized Maintenance Management Systems (CMMS) are employed for scheduling maintenance, monitoring machinery performance, and signaling potential equipment failure before it occurs. These systems guarantee operational efficiency and reduce unplanned downtime (Liu, Zhang, & Wang, 2020). On the cargo front, Cargo Monitoring Systems (CMS) and load planning software optimize stowage, monitor cargo conditions (e.g., temperature, humidity), and ensure stability and safety compliance. These systems, together, provide real-time monitoring of machinery and cargo, allowing data-driven decision-making in favor of sustainable shipping practices. With ongoing development of smart ships and automation, knowledge of these digital technologies is a key competency for navigating professionals (IMO, 2021).

Table 3. Concepts of Engine, Maintenance, and Cargo Software Systems

Concept	Description	Explanation
Computerized Maintenance Management System (CMMS)	A software system designed to manage and schedule maintenance tasks, track spare parts inventory, and log machinery performance.	CMMS enhances the reliability and efficiency of ship operation through predictive diagnosis and scheduled maintenance. It reduces downtime and the life span of ship equipment by alerting crew members of issues prior to their escalation, resulting in cost-effective and safe operations. (Liu, Zhang, & Wang, 2020).
Engine Monitoring System (EMS)	A system that collects real-time data on engine performance, including temperature, pressure, fuel usage, and RPM.	EMS allows marine engineers to track the performance and condition of propulsion and auxiliary systems in real-time. Through real-time monitoring and analysis, it allows for preventive maintenance and maximum fuel efficiency, an important factor in ensuring environmental compliance. (IMO, 2021).
Cargo Monitoring System (CMS)	A digital system that tracks cargo conditions such as temperature, humidity, and movement during transport.	CMS is important in protecting the integrity of perishable or sensitive products. It ensures regulatory compliance, improves customer confidence, and minimizes loss through spoilage or damage by providing timely notifications and cargo condition records. (Zhao, Chen, & Li, 2023).
Load Planning and Stability Software	A tool used to plan cargo loading and unloading while ensuring vessel stability and safety.	Such a program enables officers to calculate stress, trim, draft, and the vessel's center of gravity, with safe and secure stowage. It prevents structural stress and improves voyage safety by simulating varied

		cargo conditions. (Kim & Park, 2020).
Integrated Automation System (IAS)	A centralized system that connects multiple shipboard operations such as engine control, power distribution, and alarm monitoring.	IAS allows for simpler ship operation with real-time data integration and centralization that is free of human errors. It allows automation within the contemporary smart ships to promote safety, energy efficiency, and operational responsiveness. (Chen & Wu, 2019).

Understanding how engine, maintenance, and cargo software systems interact is essential to making a ship safe, reliable, and operationally efficient. Not only do these computer systems supplant the old manual methods, but they also facilitate better real-time decision-making and international maritime standards compliance. As ships transform into smart ships, data ships, marine professionals must understand how to utilize CMMS, EMS, CMS, load planning software, and integrated automation systems. These technologies allow crew members to minimize risk, maintain operating costs, and maximize overall vessel performance—tasks essential to any future maritime officer.

Explain

Work in threes and develop a Frayer Model to define and describe one of the following terms: ECDIS, AIS, GMDSS, SATCOM, or CMMS (Computerized Maintenance Management System). Fill in the four sections: Definition, Characteristics, Examples, and Non-Examples. Present your completed model to the class. Use Microsoft SmartArt to diagram how these systems are related on a ship.

Elaborate/Extend (Application)

You are a watch officer on a vessel navigating through a busy strait in adverse weather. Using your ECDIS, AIS, Radar overlays, and GMDSS, describe the steps you would take to safely transit and remain in communication with other vessels in the vicinity. Provide a written response or a flowchart to outline your action plan.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. **What does ECDIS primarily replace on board ships?**
   a. Radar antennas
   b. Paper charts
   c. VHF radio
   d. Engine logs
2. **Which system enhances navigational awareness by sharing vessel position** and identity with nearby ships?
   a. SATCOM
   b. Radar overlay

c. AIS
d. GMDSS

3. **What is the main function of radar overlays in navigation?**
a. Identify crew members
b. Monitor machinery performance
c. Superimpose radar data on electronic charts
d. Control fuel injection
4. **Which of the following systems is part of GMDSS?**
a. CMS
b. NAVTEX
c. CMMS
d. AIS
5. **What is the core purpose of the SATCOM system in maritime operations?**
a. To detect underwater obstacles
b. To monitor fuel consumption
c. To transmit and receive communication via satellite
d. To automate deck cargo loading
6. **What kind of alerts does GMDSS provide to enhance maritime safety?**
a. Financial alerts
b. Engine status updates
c. Distress and safety alerts
d. Weather condition logs
7. **What does CMMS stand for?**
a. Cargo Monitoring and Maintenance Software
b. Central Maritime Management System
c. Computerized Maintenance Management System
d. Cargo Maintenance Mechanism System
8. **Which system allows crew to monitor real-time engine temperature and pressure?**
a. SATCOM
b. EMS
c. CMS
d. IAS
9. **The CMS is especially important for transporting which type of cargo?**
a. Machinery
b. Containers
c. Bulk ore
d. Perishable goods
10. **Which software tool ensures proper weight distribution and vessel stability**?
a. CMMS
b. EMS
c. Load Planning and Stability Software
d. SATCOM

11. **Which organization promotes the global use of ECDIS and e-navigation technologies?**
    a. ITU
    b. IMO
    c. SOLAS
    d. MARPOL
12. **Which system integrates power distribution, engine control, and alarms into one interface?**
    a. CMS
    b. IAS
    c. AIS
    d. NAVTEX
13. **What is one benefit of using ECDIS over traditional charts?**
    a. Manual plotting is faster
    b. Offers static route options
    c. Provides real-time GPS positioning and updates
    d. Eliminates need for bridge crew
14. **SATCOM contributes to crew welfare by enabling:**
    a. VHF radio use
    b. Internet access and remote medical consultations
    c. Live radar plotting
    d. Fuel automation
15. **What is the main goal of integrating digital software systems on ships?**
    a. Increase fuel consumption
    b. Replace all crew
    c. Enhance safety, efficiency, and regulatory compliance
    d. Avoid using satellite data

Reflection

How do you see shipboard computer programs affect your professional life as a future mariner? What is the most challenging software system you work with, and how do you plan to become confident in operating it on board at sea?

Unit Summary

We covered in this chapter the basic onboard software applications, including navigation software like ECDIS, AIS, and radar overlays; communication equipment like GMDSS and SATCOM; and engine and cargo management software for safe and efficient ship operation. Mastery of these tools ensures smooth ship operations, safety compliance, and effective coordination of the crew. This knowledge is the technological platform for a prosperous maritime professional career.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 2

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly	Exemplary Competency

Agree)	Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Operates Electronic Chart Display and Information System (ECDIS)										
2. Utilizes Automatic Identification System (AIS) for collision avoidance										
3. Applies radar overlays to enhance situational awareness										
4. Demonstrates use of GMDSS components for emergency communication										
5. Communicates effectively using SATCOM systems										
6. Implements maintenance tasks using CMMS software										
7. Monitors engine performance using EMS										
8. Operates Cargo Monitoring Systems (CMS) to maintain cargo integrity										
9. Uses load planning software to ensure vessel stability and safety										
10. Navigates integrated ship systems through the Integrated Automation System										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Chen, L., & Wu, H. (2019). *Smart ship technology and its impact on maritime communication systems*. **Journal of Marine Science and Engineering, 7**(10), 357. https://doi.org/10.3390/jmse7100357

International Maritime Organization (IMO). (2021). *E-navigation strategy implementation plan (Update)*. Retrieved from https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx

Kim, J., & Park, Y. (2020). *A study on ECDIS-based navigation risk and human error*. **Ocean Engineering, 216**, 107861. https://doi.org/10.1016/j.oceaneng.2020.107861

Liu, Y., Zhang, X., & Wang, L. (2020). *Application of predictive maintenance in the maritime industry using CMMS and big data analytics*. **Journal of Marine Science and Application, 19**(3), 335–347. https://doi.org/10.1007/s11804-020-00143-9

Wang, C., & Meng, Q. (2021). *AIS data application in maritime logistics and safety: An overview*. **Transportation Research Part E: Logistics and Transportation Review, 150**, 102325. https://doi.org/10.1016/j.tre.2021.102325

Zhao, J., Chen, W., & Li, M. (2023). *Enhancing maritime safety through improved GMDSS implementation: A review of technologies and practices*. **Safety Science, 164**, 106069. https://doi.org/10.1016/j.ssci.2023.106069

Answer Key with Explanations

1. **What does ECDIS primarily replace on board ships?**
   Answer: b. Paper charts
   Explanation: ECDIS provides dynamic, GPS-integrated digital charting, replacing the need for manual paper chart plotting (Kim & Park, 2020).
2. **Which system enhances navigational awareness by sharing vessel position and identity with nearby ships?**
   Answer: c. AIS
   Explanation: AIS (Automatic Identification System) broadcasts a ship's position, speed, and other details to enhance visibility and collision avoidance (Wang & Meng, 2021).
3. **What is the main function of radar overlays in navigation?**
   Answer: c. Superimpose radar data on electronic charts
   Explanation: Radar overlays combine live radar images with digital charts to give navigators a clearer, real-time view, especially in low-visibility conditions (IMO, 2021).
4. **Which of the following systems is part of GMDSS?**
   Answer: b. NAVTEX
   Explanation: NAVTEX is a component of GMDSS, providing ships with maritime safety information such as weather warnings and navigational alerts (Zhao, Chen, & Li, 2023).
5. **What is the core purpose of the SATCOM system in maritime operations?**
   Answer: c. To transmit and receive communication via satellite
   Explanation: SATCOM enables global ship-to-shore and ship-to-ship communication using satellites, crucial in remote ocean areas (Chen & Wu, 2019).
6. **What kind of alerts does GMDSS provide to enhance maritime safety?**
   Answer: c. Distress and safety alerts
   Explanation: GMDSS ensures ships can send automated distress messages in emergencies, improving response times and safety (Zhao, Chen, & Li, 2023).

7. **What does CMMS stand for?**
   Answer: c. Computerized Maintenance Management System
   Explanation: CMMS is used to schedule and track ship maintenance and predict failures to reduce downtime (Liu, Zhang, & Wang, 2020).
8. **Which system allows crew to monitor real-time engine temperature and pressure?**
   Answer: b. EMS
   Explanation: The Engine Monitoring System (EMS) provides real-time data on various engine parameters for performance monitoring and predictive maintenance (IMO, 2021).
9. **The CMS is especially important for transporting which type of cargo?**
   Answer: d. Perishable goods
   Explanation: Cargo Monitoring Systems (CMS) monitor temperature, humidity, and other factors crucial for preserving sensitive cargo (Zhao, Chen, & Li, 2023).
10. **Which software tool ensures proper weight distribution and vessel stability?**
    Answer: c. Load Planning and Stability Software
    Explanation: This software calculates draft, trim, and center of gravity to ensure safe stowage and balance during voyages (Kim & Park, 2020).
11. **Which organization promotes the global use of ECDIS and e-navigation technologies?**
    Answer: b. IMO
    Explanation: The International Maritime Organization (IMO) leads the implementation of digital technologies like ECDIS to enhance global maritime safety (IMO, 2021).
12. **Which system integrates power distribution, engine control, and alarms into one interface?**
    Answer: b. IAS
    Explanation: The Integrated Automation System (IAS) connects various shipboard systems for centralized control and monitoring (Chen & Wu, 2019).
13. **What is one benefit of using ECDIS over traditional charts?**
    Answer: c. Provides real-time GPS positioning and updates
    Explanation: ECDIS automates navigation by displaying real-time vessel positions and updating charts automatically (Kim & Park, 2020).
14. **SATCOM contributes to crew welfare by enabling:**
    Answer: b. Internet access and remote medical consultations
    Explanation: SATCOM improves life onboard by allowing internet access, communication with family, and medical assistance (Chen & Wu, 2019).
15. **What is the main goal of integrating digital software systems on ships?**
    Answer: c. Enhance safety, efficiency, and regulatory compliance
    Explanation: Integrated digital systems reduce errors, support data-driven operations, and meet international standards for modern shipping (IMO, 2021).

Chapter 3
Navigational and Communication Systems

Welcome aboard! In this chapter, we set sail on the high-tech age of navigation and communication systems that make marine operations safe, efficient, and networked. Just as a skilled captain needs compass and chart, today's mariners need to become proficient in systems like GPS, AIS, and radar. Far from being mere tools, these systems are lifelines in tempestuous seas, impenetrable fog, or jammed harbors. In this chapter, you will learn how these systems function, how they are compliant with international standards, and why interconnectivity and redundancy are essential to maritime safety. Picture sailing into a storm with no visibility—the choices have to be taken on precise electronic data. This chapter is not going to provide you with technical details alone but with the critical thinking and sense of responsibility demanded of seafarers in the 21st century. Prepare to find out how technology and regulation combined make every trip, however short or long, safe, efficient, and world-coordinated.

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Knowledge: Describe the operational roles and distinctions among GPS, AIS, and radar systems used in marine navigation.
2. Skills: Apply IMO standards to assess adequacy and compliance of onboard comm and navigation equipment.
3. Attitude/Behavior: Demonstrate that you recognize the significance of system connectivity and redundancy in ensuring safety and reliability at sea.

Lesson Objectives

By the end of the lesson, you will be able to:

1. Describe the functions of GPS, AIS, and radar systems in ship operations.
2. Describe the contribution made by the International Maritime Organization (IMO) towards establishing communication systems.
3. Explain how redundancy and interdependent systems enable efficient and safe navigation.
4. Analyze actual maritime situations with an understanding of navigational and communications equipment.
5. (Final Goal): Demonstrate the ability to assess the performance of integrated navigation systems in ensuring ship safety and compliance with IMO regulations.

Engage (Activating Prior Knowledge)

Let's assume you're piloting a ship through thick fog in the middle of the ocean. How would you be aware of where you are and if there are other ships nearby? Discuss this with a fellow student or on our discussion board. What navigation tools have you heard of or seen in use?

Lesson Introduction

It takes more than a keen sense of direction to navigate the seas of the world today—it takes technical expertise in the latest equipment and systems. This lesson explains the operating principles of some of the most important navigation aids, i.e., GPS, AIS, and radar, and regulatory requirements that allow them to function successfully anywhere on the planet. As future maritime industry professionals, you will depend upon these systems to prevent collisions, transmit messages to other ships, and stay aware of your surroundings while following international safety practices.

Explore (Lesson Inputs)

Modern maritime operations depend largely on sophisticated navigational and communications technology that offers situational awareness, safety, and efficient voyage planning and execution. In this, we will outline the three pillars of technology used onboard ships—Global Positioning System (GPS), Automatic Identification System (AIS), and Radar—and worldwide standards and design principles that allow their integration. These are not just technical pillars but also represent the standards and innovations that are developing towards 21st-century maritime navigation.

Operational Features of Global Positioning System (GPS)

The Global Positioning System (GPS) is a space-based navigation system that allows ships to determine their precise location, speed, and time on the entire planet. GPS is crucial in route planning, collision, and emergency situations. Zhang and Lee (2021) say that GPS offers geospatial positioning with the triangulation of signals from a minimum of four satellites with meter accuracy. At sea, GPS facilitates automated navigation and is typically coupled with Electronic Chart Display and Information Systems (ECDIS). Recent studies affirm its reliability and versatility but caution against over-reliance on its vulnerability to signal jamming and spoofing (Chen & Yang, 2022). To mitigate the same, redundancy with other navigation systems is recommended. To Gupta et al. (2020), GPS is now typically coupled with Inertial Navigation Systems (INS) and radar for validation of positional information, with the outcome being enhanced navigational integrity.

Table 1. Key Concepts of Global Positioning System (GPS) in Maritime Navigation

Concept	Description	Explanation
Satellite-Based Navigation	GPS is a global satellite system that transmits signals to receivers on Earth, allowing accurate calculation of position, velocity, and time.	It forms the foundation of navigation at sea, enabling ships to determine their position anywhere on the planet. It enables constant tracking of position, which is very important for voyage planning and safety. It is utilized by marine professionals to traverse long distances of seas and narrow straits with confidence. (Zhang & Lee, 2021)
Triangulation and Accuracy	GPS calculates a vessel's exact position by measuring distances from at least four satellites through triangulation.	This technique offers navigational precision of a few meters, reducing the chances of collision or running aground. High position accuracy is especially important in congested ports or during bad weather, allowing bridge teams to make the best possible navigation decisions. (Gupta et al., 2020)
Integration with ECDIS	GPS is often combined with the Electronic Chart Display and Information System (ECDIS), which visually presents ship positions and maritime data.	With this integration, the location of a vessel is automatically plotted on electronic charts, allowing for real-time tracking and route planning. It simplifies navigation and enhances situational awareness by delivering vital information like depth, traffic, and hazards. (Zhang & Lee, 2021)

Vulnerability and Redundancy	GPS signals can be disrupted by jamming, spoofing, or natural interference, affecting navigation reliability.	For safety purposes, ships have backup systems such as Inertial Navigation Systems (INS) and radar. These systems provide backup positional information sources, which guarantee navigation accuracy in case of failure in GPS and meet international maritime safety standards. (Chen & Yang, 2022)
Role in Maritime Safety	GPS contributes to navigational safety by supporting automated collision avoidance, search and rescue operations, and compliance with reporting regulations.	It allows vessels to transmit accurate location data to the authorities and other vessels within the area, facilitating coordination and prompt response in the event of an emergency. Therefore, GPS is a key component of improving maritime situational awareness and reducing maritime accidents. (Torres & Nguyen, 2018)

Understanding the Global Positioning System (GPS) is essential to maritime professionals since it allows for accurate navigation, effective operation, and increased safety at sea. GPS, as the table suggests, not only forms a satellite-based determination of position but is also part of advanced navigation systems such as ECDIS. Although GPS offers improved accuracy through satellite triangulation, understanding system redundancy due to vulnerability to external factors such as jamming or spoofing is crucial. GPS integration with other systems such as radar and INS offers a reliable navigation system. These dependent systems enhance maritime safety, collision prevention, and compliance with global maritime regulations—abilities and knowledge vital in future maritime officers and navigators.

Automatic Identification System (AIS)

Automatic Identification System (AIS) is an automatic surveillance system for ships that transmits real-time information about ship identity, location, route, and speed through VHF radio waves to vessels in the proximity and the shore-based platforms. AIS improves maritime situational awareness through collision avoidance and traffic management. For Li and Thompson (2019), AIS operates best in busy sea lanes, allowing vessels to detect and recognize each other and make correct navigational choices. The IMO requires AIS fitting on all passenger ships and merchant vessels with more than 300 gross tons in SOLAS Chapter V. Recent studies, however, caution against data jams and spoofing attacks, particularly in high-density areas (Park & Kim, 2023). Integrated navigation systems resolve this through filtering and prioritization of AIS data for decision-making, in line with IMO's e-navigation policy (IMO, 2020). The real-time tracking capability of the system is as much critical in search and rescue missions as in port operations, making AIS an indispensable tool for efficiency and safety operations.

Table 2. Key Concepts of Automatic Identification System (AIS)

Concept	Description	Explanation (with References)
Real-Time Vessel Tracking	AIS transmits data such as vessel identity, location, speed, and course in real-time via VHF radio signals.	Real-time monitoring facilitates real-time tracking of ship movement by ships and coastal states, enhancing situational awareness and safe navigation by minimizing human error in planning and conducting voyages (Li & Thompson, 2019; IMO, 2020).
Collision Avoidance and Traffic Monitoring	AIS supports vessel safety by alerting nearby ships of each other's presence and trajectory, especially in congested sea routes.	AIS facilitates this by providing vessels with navigational data, enabling them to respond quickly to avoid collisions and coordinate their voyages in congested shipping routes, hence reducing the risk of sea accidents (Park & Kim, 2023).
Integration with Navigation Systems	AIS works in combination with other navigational tools like GPS, radar, and ECDIS.	The incorporation of AIS with other systems offers an integrated navigational interface that filters and organizes data, allowing the navigator to better assess their environment with greater efficiency and reducing the cognitive workload of operations (Chen & Yang, 2022).
Regulatory Compliance (IMO/SOLAS)	IMO regulations require AIS equipment on vessels over 300 gross tons and all passenger ships.	Under SOLAS Chapter V, mandatory use of AIS brings global consistency of safety standards, allowing ships and ports to have a common communication system that enhances maritime safety and coordination (IMO, 2020).
Limitations: Spoofing and Data Overload	AIS is vulnerable to cybersecurity threats like spoofing and can produce excessive data in dense maritime environments.	In dense areas, AIS can overburden users with excessive information, and weaknesses like spoofed or even false signals can cause navigation mistakes. These weaknesses emphasize the requirements of combined data verification and redundancy in navigation systems (Park & Kim,

		2023).

Automatic Identification System (AIS) is a principal element of modern maritime navigation and communication, with capabilities for real-time tracking and critical data-sharing functions that enhance maritime domain awareness. When combined with system integration such as GPS and radar, AIS enables safe navigation of congested sea routes. Students in this lesson, however, discover that AIS comes with some limitations concerning data spoofing risks and signal saturation. Such knowledge and understanding of regulatory regulations that govern the application of AIS, such as IMO's SOLAS Chapter V, equip prospective maritime professionals with the knowledge to responsibly and safely utilize such systems and expect and mitigate possible technological weaknesses.

Radar and System Interconnectivity

Radar (Radio Detection and Ranging) is a radio-wave detection and location technology used in low-visibility conditions such as fog, darkness, or storms. Radar provides feedback on the distance, speed, and direction of close ships or obstructions. As Torres and Nguyen (2018) explain, radar's real-time feedback improves mariners' situational awareness and safe passage through crowded or hazardous waterways. Coupled with GPS and AIS, radar is a component of an integrated navigation picture. Such interconnectivity of systems—the integration of multiple navigation tools to work as one—improves redundancy and fault tolerance. As Chen and Yang (2022) explain, redundancy ensures that if one system (e.g., GPS) fails, others (e.g., radar or AIS) can continue to provide vital information. IMO guidelines make integration of systems possible through standards such as the Performance Standards for Integrated Navigation Systems (INS) that optimize operational efficiency and reduce human error risk (IMO, 2020). Harmonization of navigational data streams not only improves decision-making but also mirrors the maritime industry's transition towards automation and digital resilience.

Table 3. Concepts of Radar and System Interconnectivity

Concept	Description	Explanation
Radar Technology	Radar (Radio Detection and Ranging) uses radio waves to detect and track the position, speed, and direction of nearby objects.	Radar is especially useful under conditions of poor visibility, such as darkness or fog, as it allows mariners to spot nearby ships and hazards beyond the visual range. It is applied in collision avoidance and navigation in dense marine environments. The equipment is viewed as a necessity to enhance real-time situational awareness (Torres & Nguyen, 2018).
System Interconnectivity	Refers to the integration of multiple navigational tools (e.g.,	System integration allows various navigation aids to exchange and present

	GPS, AIS, Radar) into a unified system for improved navigation and decision-making.	harmonized data, providing the operator with a global picture of the surroundings of the ship. The integration minimizes workload and human factors by consolidating data and facilitates decision-making in real-time navigation. It also supports contemporary e-navigation techniques (Zhang & Lee, 2021).
Redundancy in Navigation	The inclusion of backup systems to ensure continuous operation even if one system fails.	Redundancy improves navigation safety through the provision of backup sources of data. In the case of lost signals, leading to a loss of GPS, radar and AIS provide useful information. The layered system minimizes operational risks and provides ongoing situational awareness in changing maritime conditions (Chen & Yang, 2022).
IMO Performance Standards	Guidelines from the International Maritime Organization that set functional and technical requirements for integrated navigational systems and communication.	These standards ensure that interconnected systems offer a minimum safety and performance level. Standards provided by IMO help in harmonizing interfaces and functions to reduce complexity to operators and improve maritime safety globally. They also aid in the effort of developing user-friendly, reliable, and compatible navigational environments (IMO, 2020).
Data Harmonization and Automation	Standardization of data formats and processes across navigational tools to support consistency and automation.	Data harmonization increases system interoperability and reduces cognitive overload of ship operators by ensuring consistency of output data. This is highly important in digital navigation and automated ship systems where efficiency and accuracy take precedence. Harmonized data streams form the foundation of safe and

		scalable maritime automation (Park & Kim, 2023).

The interaction between radar and system connectivity is the basis of today's maritime navigation. Radar provides real-time information under conditions of low visibility, allowing vessels to detect proximate dangers and steer clear of them. In association with GPS and AIS, radar creates an integrated navigation system that enhances situational awareness and reduces the risk of accidents. This connectivity, in line with IMO performance standards, synchronizes data across systems to make it transparent and consistent. Redundancy is crucial by providing a backup in case one of the systems malfunctions, thus guaranteeing operational safety. Such synergies in technology add evidence to the maritime sector's transformation towards automation, making it essential for seafarers to understand not only how each device works individually but also how they interact to enable safe navigation and efficiency.

Explain

In groups or pairs, explain GPS, AIS, and radar in your own words. Discuss their function using a Venn diagram and compare and contrast them. Next, choose one system and explain its definition, characteristics, examples, and non-examples using a Frayer Model. Present your findings on a poster or online presentation.

Elaborate/Extend (Application)

You are part of a ship's bridge crew, and your vessel is approaching a congested port. There is an echo on the radar but no echo on AIS. What would you do? Use your understanding of the principles of the systems to go through the scenario, think about the implications of redundancy, and recommend a course of action consistent with IMO communications guidelines.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. What does GPS primarily use to determine a ship's location?
a. VHF signals
b. Radio towers
c. Satellite triangulation
d. Radar pulses
2. Which navigational tool provides the most precise positional data through satellite communication?
a. AIS
b. Radar
c. ECDIS
d. GPS
3. According to Chen and Yang (2022), which is a major risk associated with overreliance on GPS?
a. Port congestion
b. Software updates
c. Signal jamming and spoofing
d. Limited range

4. What system is commonly integrated with GPS for enhanced digital navigation?
a. LORAN
b. SONAR
c. ECDIS
d. EPIRB
5. What is the primary communication medium for AIS?
a. Satellite link
b. VHF radio
c. Bluetooth
d. Wi-Fi
6. What type of data does AIS transmit in real time?
a. Weather and tides
b. Cargo manifest
c. Vessel identity, speed, and course
d. Engine performance metrics
7. According to IMO regulations under SOLAS Chapter V, AIS is mandatory for:
a. Fishing vessels over 100 tons
b. All pleasure craft
c. Commercial ships over 300 gross tons and all passenger vessels
d. Only naval ships
8. What is one major limitation of AIS in high-density maritime areas?
a. Signal delay
b. Signal jamming
c. Data overload and spoofing
d. GPS interference
9. What does radar primarily detect?
a. Vessel cargo
b. Radio frequencies
c. Objects' speed, bearing, and distance
d. Seafloor topography
10. What role does radar play in poor visibility conditions?
a. Enhances port management
b. Detects smuggling activity
c. Helps identify and avoid nearby hazards
d. Updates vessel schedules
11. What is meant by "system interconnectivity" in navigation?
a. Using walkie-talkies onboard
b. Connecting navigational systems to one interface
c. Operating with a single navigation system
d. Linking crew members via headsets
12. Why is redundancy in navigation important?
a. It shortens voyage duration
b. It increases crew workload
c. It ensures backup systems can take over in case of failure
d. It reduces vessel maintenance costs

13. What is the purpose of IMO performance standards for integrated navigation systems?
a. To improve crew accommodations
b. To regulate international shipping tariffs
c. To ensure safety and interoperability of navigational tools
d. To develop new ship designs
14. Which term describes the consistency of data across multiple navigational systems?
a. System buffering
b. Data harmonization
c. Signal boosting
d. Manual calibration
15. According to Park & Kim (2023), what is a key benefit of data harmonization in maritime navigation?
a. Reduces satellite costs
b. Minimizes the need for AIS
c. Supports automation and reduces cognitive overload
d. Eliminates radar interference

Reflection

How does knowing the integration and reliability of the navigation systems make you a better responsible maritime officer? Consider an example in which technology can prevent or cause an accident. How would you act differently now that you understand this?

Unit Summary

This chapter has looked at the underlying technologies of seafaring navigation—GPS, AIS, and radar—and how they work. It highlighted the value of adhering to IMO standards and strategic benefit of system interconnectivity and redundancy. These technologies are not only essential for safe navigation but are also the building blocks of good decision-making, communication, and leadership at sea. As seafarers, your capability to utilize and assess these systems responsibly will be a great contribution to ensure the safety and success of your future voyages.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 3

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Identifies the functions and limitations of GPS in maritime navigation										
2. Demonstrates understanding of AIS data and its application for collision avoidance										
3. Interprets radar signals for situational awareness in low-visibility conditions										
4. Explains the concept and importance of system interconnectivity										
5. Uses GPS and ECDIS together for accurate route planning										
6. Recognizes AIS regulatory requirements under IMO SOLAS Chapter V										
7. Evaluates the need for redundancy in navigational systems										
8. Applies IMO performance standards when working with integrated navigation systems										
9. Identifies threats such as GPS spoofing and AIS data overload										
10. Demonstrates awareness of data harmonization in automated maritime systems										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Chen, L., & Yang, H. (2022). Enhancing navigational safety through integrated maritime systems: A redundancy-based approach. *Journal of Marine Science and Engineering, 10*(5), 631. https://doi.org/10.3390/jmse10050631

Gupta, R., Lim, C., & Santos, M. (2020). Position accuracy and vulnerability of GPS in maritime navigation: Risk and resilience. *Marine Navigation and Safety of Sea Transportation, 14*(3), 321–328. https://doi.org/10.1201/9781003139037-45

International Maritime Organization. (2020). *E-navigation strategy implementation plan: Guidelines for harmonized display of navigation* *information received via communications equipment*. IMO. https://doi.org/10.1163/9789004421295_037

Li, J., & Thompson, R. (2019). The impact of Automatic Identification Systems (AIS) on collision avoidance in congested waterways. *Ocean Engineering, 186*, 106102. https://doi.org/10.1016/j.oceaneng.2019.106102

Park, D., & Kim, S. (2023). Mitigating AIS data spoofing and overload in high-traffic maritime zones. *Marine Technology Society Journal, 57*(2), 56–68. https://doi.org/10.4031/MTSJ.57.2. 5

Torres, A., & Nguyen, T. (2018). Application of radar technology in maritime navigation and collision prevention. *Journal of Navigation and Marine Safety, 15*(1), 45–53. https://doi.org/10.1017/S0373463317000683

Zhang, Y., & Lee, D. (2021). Integration of GPS and ECDIS in maritime navigation: Benefits and challenges. *Journal of Navigation, 74*(4), 845–861. https://doi.org/10.1017/S037346332000060X

Answer Key with Explanations

1. **What does GPS primarily use to determine a ship's location?**
   Answer: c. Satellite triangulation
   Explanation: GPS determines position by calculating distances from at least four satellites using triangulation.
2. **Which navigational tool provides the most precise positional data through satellite communication?**
   Answer: d. GPS
   Explanation: GPS provides high-precision geolocation using satellite signals, essential for navigation.
3. **According to Chen and Yang (2022), which is a major risk associated with overreliance on GPS?**
   Answer: c. Signal jamming and spoofing
   Explanation: GPS signals are vulnerable to intentional or accidental interference, making redundancy important.
4. **What system is commonly integrated with GPS for enhanced digital navigation?**
   Answer: c. ECDIS
   Explanation: ECDIS uses GPS data to display vessel position on electronic charts in real time.
5. **What is the primary communication medium for AIS?**
   Answer: b. VHF radio
   Explanation: AIS transmits ship data over VHF radio frequencies to other vessels and coastal authorities.
6. **What type of data does AIS transmit in real time?**
   Answer: c. Vessel identity, speed, and course
   Explanation: AIS shares navigational data to enhance safety and situational awareness.
7. **According to IMO regulations under SOLAS Chapter V, AIS is mandatory for:**
   Answer: c. Commercial ships over 300 gross tons and all passenger vessels
   Explanation: SOLAS mandates AIS for large commercial and passenger ships for global maritime safety.
8. **What is one major limitation of AIS in high-density maritime areas?**
   Answer: c. Data overload and spoofing
   Explanation: Too many signals can overwhelm operators, and AIS can be manipulated (spoofed) for deception.
9. **What does radar primarily detect?**
   Answer: c. Objects' speed, bearing, and distance
   Explanation: Radar uses radio waves to determine the position and movement of surrounding objects.
10. **What role does radar play in poor visibility conditions?**
    Answer: c. Helps identify and avoid nearby hazards

Explanation: Radar is essential for detecting vessels and obstacles in fog, night, or storms.

11. **What is meant by "system interconnectivity" in navigation?**
    Answer: b. Connecting navigational systems to one interface
    Explanation: Interconnectivity integrates GPS, AIS, radar, etc., into a unified display for better decision-making.
12. **Why is redundancy in navigation important?**
    Answer: c. It ensures backup systems can take over in case of failure
    Explanation: Redundancy allows ships to maintain navigation using alternate systems if one fails.
13. **What is the purpose of IMO performance standards for integrated navigation systems?**
    Answer: c. To ensure safety and interoperability of navigational tools
    Explanation: These standards promote compatibility and usability of integrated systems for global maritime safety.
14. **Which term describes the consistency of data across multiple navigational systems?**
    Answer: b. Data harmonization
    Explanation: Harmonization ensures that all systems display compatible and consistent data formats.
15. **According to Park & Kim (2023), what is a key benefit of data harmonization in maritime navigation?**
    Answer: c. Supports automation and reduces cognitive overload
    Explanation: Harmonized data allows for clearer, more efficient decision-making and supports digital automation.

Chapter 4

Introduction to Shipboard Network Architecture

Welcome to the information center of modern maritime operations! As ships become high-tech floating data centers, network architecture information is crucial to maintaining effective and secure communication. In this chapter, we cover the lifelines of shipboard connectivity—from wireless systems and local area networks to firewalls and configuration techniques. From receiving real-time navigation data to the bridge to managing the bandwidth needed for crew welfare services, this unit will teach you the fundamentals of how networks function at sea. Get ready to learn how every wire, device, and protocol contributes to the safe navigation of maritime operations!

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Demonstrate awareness of basic networking topologies such as LAN, VLAN, and WLAN within a shipboard environment.
2. Describe the function and configuration of the network devices like routers, switches, and firewalls in maritime environments.
3. Exemplify problem-solving skill in applying the correct cabling and wireless technologies to shipboard communications systems.
4. Be proactive in ensuring safe and efficient digital systems aboard a ship.

Lesson Objectives

By the end of the lesson, you will be able to:

1. Define and identify key network devices like LAN, VLAN, WLAN, routers, switches, and firewalls.
2. Describe the roles of different kinds of cabling and wireless technology in shipboard operations.
3. Provide network setup examples in diagrams and everyday applications.
4. Define shipboard network architecture security issues and best practices.
5. Design a simple but efficient network layout for a shipboard system using the corresponding technologies (Terminal Behavior).

Engage (Activating Prior Knowledge)

Play Ship Systems Match-Up with me! You will be dealt a deck of flashcards consisting of networking devices (e.g., router, LAN, firewall) and shipboard functions (e.g., crew messaging, ECDIS updates, engine room monitoring). Match each network device with its most likely function onboard. How many do you get right?

Lesson Introduction

In the age of global connectivity at sea, high-performance, dependable networks are no longer luxuries—they are necessities. As soon-to-be marine electronics, communications, or navigation systems professionals, your ability to understand and construct shipboard networks will directly affect ship performance, crew safety, as well as operational efficiency. This lesson gives you networking basics and hands-on training for ICT system-related activities aboard, with integration of the Philippine Professional Standards for Teachers (PPST) on the use of ICT in teaching and learning.

Explore (Lesson Inputs)

With the shipping revolution caused by digitization, network architecture is an essential infrastructure component that supports everything from navigation security to crew comfort and ship performance monitoring. With the new ships being nothing short of floating data centers, understanding their network backbone—wired and wireless communication networks, core network hardware, and secure configuration—empowers maritime professionals with the ability to efficiently manage and debug onboard communications systems. The fundamentals of shipboard network architecture are addressed in this chapter: network types, primary network devices, and maritime environment connectivity technologies.

Types of Shipboard Networks: LAN, VLAN, and WLAN

A shipping Local Area Network (LAN) interconnects computers and equipment in sealed environments such as the bridge or engine control room. A Virtual LAN (VLAN) logically segments devices to isolate traffic by function or security, providing flexibility without altering the physical infrastructure. Wireless LANs (WLANs) provide wireless access across the ship, offering mobility and remote access. Zhou et al. (2021) observe that WLANs are significant for crew communications and mobile device utilization on the ship. VLANs improve operational security by isolating sensitive systems from general networks, according to Kim and Kim (2019). The tiered approach provides continuity and reduces cybersecurity risks.

Table 1. Concepts of Types of Shipboard Networks

Concept	Description	Explanation with Literature Review (2018–2024)
LAN (Local Area Network)	A network that connects devices in a limited physical area such as a control room or bridge.	A LAN links onboard devices such as workstations and sensors to facilitate internal communications and data transfer. It is ideal for mission-critical use because of its reliability and speed. LANs facilitate improved shipboard networks to enable localized and long-term communication between principal ship systems (Zhou et al., 2021).
VLAN (Virtual Local Area Network)	A logical segmentation within a LAN that groups devices based on functions or roles, rather than location.	VLANs enhance network efficiency and organization by separating traffic into departments (for example, navigation and crew welfare) without the need for physical networks. Segmentation enhances traffic management and safeguards sensitive systems from abuse, increasing performance and organization (Kim & Kim, 2019).
WLAN (Wireless Local Area Network)	A wireless network that enables devices to connect through Wi-Fi over short distances.	WLANs provide mobile access for ship personnel through smartphones and tablets, with more mobility and less cabling. Their applications have grown with smart devices and remote monitoring systems on board (Zhou et al., 2021).

This lesson familiarizes students with shipboard network design and deployment in actual sea conditions. Understanding LAN, VLAN, and WLAN operations enables students to design, manage, and secure onboard networks. These are of paramount significance to operational efficiency, dependability, and safety in contemporary ships. As digital technology increases in maritime operations, understanding these networks is of vital significance to future professionals.

Network Devices: Routers, Switches, and Firewalls

Three fundamental shipboard network devices support communication: routers, switches, and firewalls. Routers send data packets from one network to another to facilitate communication with outside networks such as satellites or ports. Switches link devices in LANs and manage traffic flow. Firewalls protect trusted systems from untrusted sources by filtering traffic and preventing unauthorized entry. Wu and Lee (2020) point to firewalls as the initial line of defense in maritime cybersecurity, usually with intrusion detection systems. Hassan et al. (2022) mention switches as pivotal in processing sensor and IoT data to provide internal data flow continuity. These devices combined provide the backbone of an effective shipboard network.

Table 2. Network Devices – Concepts, Descriptions, and Explanations

Concept	Description	Explanation
Router	A router is a device that connects different networks and directs data packets between them. In a shipboard network, routers link internal systems to external networks such as satellite or port communication systems.	Routers are essential in data communication between third parties and ships, providing real-time updates on operations, GPS, and navigation. They provide smooth connectivity between onboard and onshore centers that are instrumental in monitoring and navigation. With increased data reliance, routers manage network dependability (Wu & Lee, 2020).
Switch	A switch is a network device that connects devices within a Local Area Network (LAN), such as computers, sensors, and control systems on a ship. It forwards data only to the intended recipient within the network.	Switches handle huge volumes of data for shipboard equipment, enhancing internal communication. They remove bottlenecks and enhance performance on intelligent sensors and IoT-equipped vessels. By selective data transfer, they provide real-time responsiveness and precise monitoring (Hassan, Nguyen, & Turner, 2022).
Firewall	A firewall is a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external sources.	Firewalls are crucial on shipboard networks for defense. They prevent unauthorized access and malicious traffic, safeguarding systems such as engine control and navigation. Usually used in conjunction with intrusion detection systems (IDS), they provide layers of defense against cyber threats, maintaining system integrity and crew safety

		(Wu & Lee, 2020).

This topic puts routers, switches, and firewalls in the context of building a safe shipboard network. Routers provide external communication, switches optimize internal data transfer, and firewalls guard against cyber attacks. Collectively, these devices facilitate continuity in operations and secure maritime operations. Their unique roles offer important information that makes maritime professionals prepare and cope with onboard digital systems as the industry shifts towards smart, secure ships.

Cabling and Wireless Connectivity Technologies

Shipboard networking employs both wireline and wireless technologies to transfer data. Interference-free, high-speed communication through Ethernet cables such as Cat6 and optical fiber cables is necessary for mission-critical applications such as navigation and engine monitoring. Mobility for the crew is provided through handheld devices with wireless connectivity. Wired solutions are the norm for mission-critical systems due to reliability and low latency, according to Jain et al. (2018), while wireless technologies are used to crew welfare and mobile maintenance. Hassan et al. (2022) observe that wireless and cabling solution integration provides a stable, easy-to-use hybrid network, particularly in smart ships and autonomous ships.

Table 3. Concepts of Cabling and Wireless Connectivity Technologies in Shipboard Networks

Concept	**Description**	**Explanation**
Ethernet Cabling (Cat6/Cat7)	Ethernet cabling, including Cat6 and Cat7, is used to connect internal devices within a ship's network infrastructure. These cables support high-speed data transmission and are designed to minimize interference.	Ethernet cables are capable of supporting bandwidth of 10 Gbps and also offer electromagnetic interference shielding, and therefore they are used for navigation control and engine monitor connection, where low latency and reliability are of prime importance (Jain et al., 2018).
Fiber Optic Cabling	Fiber optics transmit data using light, offering higher speeds and longer transmission distances than copper cables. They are immune to electromagnetic interference.	Fiber optic cables are better suited to link systems on big ships to provide secure communication within interference areas such as engine rooms. Their increasing application in smart ships is a testament to the demand for secure connectivity in high-data operations (Hassan et al., 2022).
Wireless Connectivity	Wireless LANs provide network access to mobile	WLAN technologies offer crew tablets and inspection

(WLAN/Access Points)	devices using radio waves and access points strategically placed throughout the ship.	equipment the flexibility of wireless communication. Though not suitable for safety-of-life systems, WLANs increase ease of use and decrease wiring, especially in living areas (Zhou et al., 2021).
Hybrid Network Systems	A hybrid network combines wired and wireless technologies to balance reliability with accessibility. Wired systems handle critical tasks, while wireless links serve non-critical functions.	This approach provides high-performance communication with mission-critical applications while being flexible for less mission-critical applications. By utilizing both the technologies, ships obtain redundancy, increase network robustness, and offer future smart ship capability (Hassan et al., 2022; Jain et al., 2018).
Interference Management	Interference management involves minimizing signal disruptions caused by electronic noise from engines and other onboard equipment.	Ships utilize shielded Ethernet and fiber-optic cable to avoid electromagnetic interference prevalent in metal-rich oceanic zones. Wireless networks manage interference using effective channel allocation and proper access point placement to provide robust signals (Kim & Kim, 2019).

This module emphasizes proper connectivity technology selection for ship networks, such as cabling and wireless. Secure high-speed communications using Ethernet and fiber optic cables are required by critical applications, and wireless interfaces provide convenience and mobility. Hybrid networks created by merging these are a step towards greater performance and flexibility. Proper interference management through shielding and planning provides secure communication in dynamic sea environments, emphasizing the importance of properly designed infrastructure to enable ship safety, automation, and connectivity.

Explain

Use a Frayer Model to list and define networking vocabulary (LAN, VLAN, WLAN, router, switch, firewall). Draw a Venn diagram to compare wired and wireless networks. Summarize in a concise bulleted list for class presentation.

Elaborate/Extend (Application)

You are now part of the new IT support staff of one of the offshore ships. Your task is to design a simple shipboard network with navigation equipment, communication networks, entertainment services, and secure internet access. What hardware will you employ? How will you interconnect them? Describe your design in terms of principles of efficiency, reliability, and security.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. **What type of network connects devices within a limited area on a ship, such as the bridge or control room?**
   a. WAN
   b. WLAN
   c. LAN
   d. PAN
2. **Which network allows logical segmentation of onboard systems without altering the physical layout?**
   a. WLAN
   b. VLAN
   c. SAN
   d. MAN
3. **What type of network provides wireless access using access points?**
   a. VPN
   b. LAN
   c. WLAN
   d. VLAN
4. **What is the main advantage of using VLANs on ships?**
   a. Faster wireless connectivity
   b. Physical layout optimization
   c. Logical traffic segmentation and security
   d. Cheaper cabling
5. **According to Zhou et al. (2021), what role do WLANs play in modern ships?**
   a. Managing firewalls
   b. Providing fixed-line backups
   c. Supporting mobile communications and crew access
   d. Controlling engine power
6. **What is the main role of a router in a shipboard network?**
   a. Filtering email traffic
   b. Connecting internal LAN to external networks
   c. Providing power over Ethernet
   d. Encrypting personal data
7. **What does a switch do in a Local Area Network on board a ship?**
   a. Translates data to binary code
   b. Connects ship to the internet
   c. Forwards data within LAN to intended devices
   d. Blocks unwanted websites

8. **Why are firewalls important in maritime communication networks?**
   a. They manage GPS data
   b. They block electromagnetic interference
   c. They filter and secure network traffic
   d. They serve as wireless hotspots
9. **Which of the following is not typically handled by a switch?**
   a. Managing LAN traffic
   b. Forwarding data to specific devices
   c. Connecting to external satellite networks
   d. Handling data from onboard sensors
10. **What kind of cable is best known for immunity to electromagnetic interference and long-distance transmission?**
   a. Cat5
   b. Coaxial
   c. USB
   d. Fiber optic
11. **Which cabling type is most commonly used for high-speed internal connections like navigation or engine monitoring?**
   a. HDMI
   b. Cat6 Ethernet
   c. Fiber channel
   d. VGA
12. **What is the benefit of using a hybrid shipboard network?**
   a. Lower installation cost
   b. Faster internet browsing
   c. Balance between reliability and flexibility
   d. Guaranteed zero interference
13. **What is a challenge wireless networks must address on board ships?**
   a. Rainwater penetration
   b. Channel interference from onboard systems
   c. Incompatible cables
   d. Signal encryption failure
14. **Which technology supports mobile access to inspection apps and maintenance tools on ships?**
   a. VLAN
   b. Ethernet
   c. WLAN
   d. Firewall
15. **Why are shielded Ethernet cables used in ship environments?**
   a. To enable wireless backup
   b. To save bandwidth
   c. To reduce signal disruption from engine noise
   d. To increase voltage

Reflection

Reflect on the following question: What kind of difference would a well-designed shipboard network make to your future seagoing work or in port operations? Write a short paragraph describing how this information could affect your work as a marine or communication officer.

Unit Summary

Chapter 4 presented the origins of shipboard network architecture in relation to key networking concepts like LAN, VLAN, and WLAN, and fundamental devices like routers, switches, and firewalls. We talked about cabling and wireless connections use in maritime environments and addressed configuration examples applicable to ship environments. Such knowledge equips students to design, manage, and troubleshoot maritime communications networks to ensure safety, operational uptime, and crew comfort in the digitally enabled ship.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 4

Instructions for Use
Pre-Service Teachers

Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators

Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Identifies and differentiates between LAN, VLAN, and WLAN										
2. Explains the purpose and function of routers, switches, and firewalls										
3. Demonstrates understanding of Ethernet and fiber optic cabling technologies										
4. Describes the use and advantages of wireless technologies (WLAN) onboard										
5. Evaluates the benefits of hybrid (wired and wireless) network systems										
6. Analyzes potential sources of interference in shipboard communication systems										
7. Applies basic principles of network segmentation using VLANs										
8. Assesses the role of firewalls in maritime cybersecurity										
9. Compares different cabling options based on speed, distance, and reliability										

10. Illustrates a basic shipboard network layout showing core components										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Hassan, R., Nguyen, T. H., & Turner, D. (2022). *Smart ship networking: Design considerations and integration of maritime IoT systems*. Journal of Marine Science and Engineering, **10**(3), 327. https://doi.org/10.3390/jmse10030327

Jain, R., Dubey, R. K., & Yadav, A. (2018). *Analysis of Ethernet and fiber optic cables in industrial communication networks*. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, **3**(4), 51–56. https://doi.org/10.32628/CSEIT183478

Kim, S., & Kim, H. (2019). *Cybersecurity architecture for shipboard operational networks using VLAN segmentation*. Journal of Marine Engineering and Technology, **18**(1), 40–49. https://doi.org/10.1080/20464177.2019.1570556

Wu, T., & Lee, S. (2020). *Firewall integration and threat management for maritime IT/OT networks*. International Journal of Naval Architecture and Ocean Engineering, **12**(2), 185–192. https://doi.org/10.1016/j.ijnaoe.2020.03.00 1

Zhou, Y., Lin, D., & Chen, H. (2021). *Wireless network deployment and management in smart ships*. Sensors, **21**(9), 3021. https://doi.org/10.3390/s21093021

Answer Key with Explanations

1. **What type of network connects devices within a limited area on a ship, such as the bridge or control room?**
   Answer: c. LAN
   Explanation: A LAN (Local Area Network) connects devices in a limited area like the bridge or control room, supporting internal communication.
2. **Which network allows logical segmentation of onboard systems without altering the physical layout?**
   Answer: b. VLAN
   Explanation: VLAN (Virtual LAN) segments traffic logically based on function or role, enhancing security and efficiency.
3. **What type of network provides wireless access using access points?**
   Answer: c. WLAN
   Explanation: WLAN (Wireless Local Area Network) uses Wi-Fi and access points to provide wireless communication on board.

4. **What is the main advantage of using VLANs on ships?**
   Answer: c. Logical traffic segmentation and security
   Explanation: VLANs divide traffic for different ship functions (e.g., navigation vs. welfare) and improve network security.
5. **According to Zhou et al. (2021), what role do WLANs play in modern ships?**
   Answer: c. Supporting mobile communications and crew access
   Explanation: WLANs support mobility, allowing crew to use tablets and smartphones for communication and inspections.
6. **What is the main role of a router in a shipboard network?**
   Answer: b. Connecting internal LAN to external networks
   Explanation: Routers manage data flow between onboard systems and external sources like ports or satellites.
7. **What does a switch do in a Local Area Network on board a ship?**
   Answer: c. Forwards data within LAN to intended devices
   Explanation: Switches connect onboard devices and ensure data is directed only to its destination, reducing congestion.
8. **Why are firewalls important in maritime communication networks?**
   Answer: c. They filter and secure network traffic
   Explanation: Firewalls block unauthorized access and monitor traffic to protect sensitive onboard systems.
9. **Which of the following is *not* typically handled by a switch?**
   Answer: c. Connecting to external satellite networks
   Explanation: Switches operate within LANs. Routers connect LANs to external networks like satellites or ports.
10. **What kind of cable is best known for immunity to electromagnetic interference and long-distance transmission?**
    Answer: d. Fiber optic
    Explanation: Fiber optics use light to transmit data, offering high speed and resistance to interference over long distances.
11. **Which cabling type is most commonly used for high-speed internal connections like navigation or engine monitoring?**
    Answer: b. Cat6 Ethernet
    Explanation: Cat6 Ethernet cables are fast and shielded, making them suitable for mission-critical shipboard systems.
12. **What is the benefit of using a hybrid shipboard network?**
    Answer: c. Balance between reliability and flexibility
    Explanation: Hybrid networks use wired connections for critical systems and wireless for mobility, balancing performance and convenience.
13. **What is a challenge wireless networks must address on board ships?**
    Answer: b. Channel interference from onboard systems
    Explanation: Metal-heavy environments and onboard machinery can cause signal interference, requiring careful WLAN planning.
14. **Which technology supports mobile access to inspection apps and maintenance tools on ships?**
    Answer: c. WLAN
    Explanation: WLAN allows wireless communication with mobile tools like tablets, improving mobility and efficiency on board.

15. **Why are shielded Ethernet cables used in ship environments?**
    Answer: c. To reduce signal disruption from engine noise
    Explanation: Shielded cables protect data from electromagnetic interference generated by ship engines and machinery.

Chapter 5

Introduction to
Monitoring, Control, and Integration Systems

Welcome aboard to one of the most challenging and important facets of shipboard operations—Monitoring, Control, and Integration Systems. Accuracy and automation are the forces behind efficiency, safety, and sustainability at present in the maritime world. This chapter will guide you to the core of how today's maritime vessels are monitored and controlled by advanced technologies. From observing cargo and ballast to managing engine systems and communicating with advanced Human-Machine Interfaces (HMI), this module is designed to empower you with the theoretical and practical pillars of integrated ship operations. Imagine the ship as a living organism—where its sensors are the senses, its control systems are the nervous system, and the crew are the brain and decision-makers. Mastering this chapter means being in closer proximity to the control room, where your decisions and insight will shape the vessel's performance and safety. Ready to take the helm?

Unit Learning Outcomes
By the end of this unit, you will be able to:

1. Demonstrate comprehension of various shipboard control systems like engine, ballast, and cargo control systems.
2. Develop and compare data collection techniques and sensor network setups in naval missions.
3. Exhibit professional demeanor in the proper and effective use of HMI tools and automation systems in simulated shipboard operations.

Lesson Objectives
By the end of the lesson, you will be able to:

1. Determine and define the significant components of engine, ballast, and cargo control systems.
2. Explain how data acquisition systems and sensor networks help monitor ships and their performance.
3. Explain and discuss the role of HMI in control and automation integration.
4. Implement theories of integrated control systems to simulated marine systems.Operate and troubleshoot a basic ship control panel interface as a final performance task.

Engage (Activating Prior Knowledge)

Let us play a little game: "What Controls What?" In groups, list all the ship systems you can recall (engine, ballast, cargo, etc.) and match them with control actions (pumping, heating, steering, etc.). Then ask yourself: How do you envision these actions get initiated or tracked? This will lead us to think about how data and control systems operate in the background.

Lesson Introduction

As future maritime professionals, we need to learn to monitor, control, and integrate shipboard systems. This lesson bridges theory to practice and provides you with the capability to operate ships economically and safely. The Philippine Professional Standards for Teachers (PPST) are aimed at infusing technology in the classroom and future- and lifelong-skills competencies—this lesson is in line with that thrust.

Explore (Lesson Inputs)

New ships rely on advanced systems to ensure safe and efficient navigation across the seas. These are not independent mechanisms but networked systems that are designed to govern, manage, and integrate a number of functions—anything from propulsion to cargo handling. This chapter discusses three of the main aspects of marine control: Shipboard Control Systems, Data Acquisition and Sensor Networks, and Human-Machine Interfaces (HMI) and Automation Integration. The three together form the operational core of smart ships, providing the real-time data and control functionalities that marine engineers and navigators require.

Shipboard Control Systems (Engine, Ballast, Cargo)

Shipboard control systems are designed to manage a ship's main operating processes, including propulsion (engine control), stability (ballast control), and cargo handling. These systems use a combination of automated controllers, mechanical actuators, and software logic to provide optimal performance and safety compliance. Engine control systems regulate fuel injection, power, and temperature, while ballast systems regulate water distribution in tanks for leveling the vessel, and cargo control systems regulate loading, unloading, and internal transfer of liquids or containers. Zhang et al. (2019) report that the integration of digital control logic with real-time feedback mechanisms has significantly improved reliability and responsiveness in these subsystems. In addition, Nguyen and Lee (2021) observe that modern ship control systems typically involve redundancy and fail-safe modes, which are crucial for minimizing risk in challenging maritime environments. These systems are now integrated into ship automation platforms that communicate between different subsystems, with a view to ensuring operation effectiveness and environmental compliance.

Table 1. Concepts of Shipboard Control Systems

Concept	Description	Explanation
Engine Control System	Controls the main propulsion system, including fuel flow, power output, and operating temperatures.	Engine control systems maximize propulsion efficiency using digital automation, tracking real-time engine parameters to maximize operating conditions and fuel injection. They maximize performance using reduced fuel consumption and emissions (Zhang et al., 2019).
Ballast Control System	Manages the intake and distribution of ballast water to maintain vessel stability, trim, and structural integrity.	Automated ballast systems utilize current sensor information to regulate water levels across various tanks to maintain suitable ship balance and compliance with international environmental standards (Nguyen & Lee, 2021; Zhang et al., 2019).
Cargo Control System	Oversees the loading, unloading, and transfer of cargo, particularly in tankers and container vessels.	These systems regulate the transportation of cargo and storage conditions such as pressure, temperature, and volume via programmable logic controllers and feedback sensors, reducing the possibility of operational failure or product loss (Park et al., 2023).
Redundancy and Fail-Safe Features	Incorporates backup systems and emergency protocols	Redundant structures include redundant controllers, power supplies, and communication links

	to maintain safe operation in case of primary system failure.	that ensure continuity and operational safety in the event of failure, thereby facilitating resilient shipboard automation (Nguyen & Lee, 2021).
System Integration	Combines engine, ballast, and cargo controls into a centralized automation system.	Integration allows for centralized monitoring and control and enables faster and more informed decision-making by operators. Integrated platforms offer better interoperability among the subsystems and reduced crew workload (Park et al., 2023; Wu & Yang, 2022).

The shipboard control systems concept is a collection of technologies that govern a ship's most challenging operations—engine propulsion, stability via ballast control, and cargo management. The systems are based on an integration of real-time sensors, automatic controllers, and software integration to provide safe and efficient operation. Through the integration of redundancy and fail-safe modes, they reduce risks of operation in dynamic and often turbulent seafaring environments. Further, contemporary shipping trends are toward system integration, where engine, ballast, and cargo systems are integrated through shared automation platforms. This facilitates operators to manage multiple subsystems using a shared interface, allowing for improved decision-making and situational awareness aboard the ship. Overall, the study of such systems equips students to perform real-world ship operations competently and with technical proficiency.

Data Acquisition and Sensor Networks

Data acquisition (DAQ) systems and sensor networks constitute the foundation of ship automation, enabling real-time monitoring of engine parameters, hull condition, environmental conditions, and cargo status. These systems collect data from a distributed array of sensors feeding into centralized or decentralized data processing units, typically in real-time. Li et al. (2021) outline how development in marine DAQ systems has made possible the development of modular, extensible platforms that can enable predictive maintenance and anomaly detection. Maritime sensor networks are increasingly wireless and interference-free, ensuring data accuracy and ruggedness in voyages. Moreover, the use of Internet of Things (IoT) technologies in shipboard monitoring has made dynamic monitoring of temperature, pressure, fluid levels, and vibrations possible, which are crucial to informed decision-making (Rahman et al., 2022). These smart sensor ecosystems are indispensable to enhanced situational awareness, safety margins, and operational workflow optimization among ship departments.

Table 2. Concepts in Data Acquisition and Sensor Networks

Concept	Description	Explanation
Data Acquisition (DAQ) Systems	DAQ systems are platforms designed to collect and process data from shipboard components like engines, ballast tanks, and cargo systems.	They are a key component of shipping operations through real-time monitoring, anomaly detection, and predictive maintenance. Their modularity allows for simple scalability and integration with automation systems, enhancing operational efficiency and reducing downtime (Li et al., 2021; Zhang et al., 2019).
Sensor Networks	Sensor networks consist of interconnected devices placed throughout the ship to monitor various physical parameters such as temperature, pressure, and vibration.	These networks provide full visibility into the interior and exterior of the vessel. More wireless and fault-tolerant, they enable high-frequency data acquisition that supports system diagnostics and decision-making while running or operating equipment (Rahman et al., 2022).
Real-Time Monitoring	Real-time monitoring is the continuous, immediate tracking of critical shipboard processes without time lag.	This is a principle that guarantees system feedback is obtained in real-time, allowing the crew to react immediately to any failure or deviation. It is essential in safety management, which enhances the ability of the ship to dynamically modify operations in the case of unexpected conditions (Park et al., 2023).
IoT Integration in Marine Systems	IoT integration refers to the use of internet-connected sensors and devices that enable communication between systems and remote data centers.	In the marine environment, IoT facilitates simple data sharing between shipboard equipment and shore control for remote diagnostics, fleet-wide monitoring, and more efficient automation processes (Rahman et al., 2022; Wu & Yang, 2022).
Predictive Maintenance	Predictive maintenance involves using data trends and analytics to anticipate equipment failures before they occur.	By analyzing past and real-time sensor information, vessels can predict when a machine is likely to fail and schedule maintenance beforehand. This reduces the cost of repair, avoids unnecessary replacement, and maximizes the system life (Li et al., 2021).

Understanding of the basic principles of sensor networks and data acquisition allows maritime professionals to understand how vessels "sense" and "respond" to internal and external parameters. With proficiency in such systems, students gain technical skill to keep vessels safe, reduce mechanical failures, and enable efficient running. In combination with IoT and real-time monitoring, such systems now offer advanced capability such as predictive maintenance, which is revolutionizing maritime operations to become smarter, more responsive environments. This training allows future marine engineers and officers to make sense of high-risk situations based on data-driven decision-making.

Human-Machine Interfaces (HMI) and Automation Integration

Human-Machine Interfaces (HMIs) close the interactive cycle between ship operators and automated equipment, facilitating effective monitoring, command input, and system configuration. An HMI may be a physical control panel with lights and buttons or advanced touchscreens and digital dashboards that provide detailed visual feedback of system status. Wu and Yang (2022) state that modern HMI designs emphasize intuitive layout, visual simplicity, and responsive controls, which are critical in minimizing human error and fatigue during extended operations. The integration of automation and HMI systems has enabled the centralization of control of diverse shipboard functions, such as navigation, machinery, and cargo handling. Park et al. (2023) state the trend towards AI-based interfaces that provide real-time suggestions and automate routine processes, further minimizing operator cognitive loads. As maritime operations continue to be advanced, HMIs play a more strategic role in bridging human oversight with machine precision, leading to an improved safer and more efficient shipboard environment.

Table 3. Concepts of Human-Machine Interfaces (HMI) and Automation Integration

Concept	Description	Explanation
Human-Machine Interface (HMI)	HMIs are the interactive tools or systems that enable operators to communicate with shipboard equipment and automated systems. They may include physical buttons, displays, alarms, keyboards, and modern touchscreen dashboards.	HMIs are designed to present real-time data in a simple and intuitive way, enabling operators to see conditions and make critical decisions efficiently. In good design, they reduce cognitive load and operator fatigue, especially with long or high-stress operations. Good HMI design considers clarity, layout, and responsiveness to increase maritime situational awareness and safety (Wu & Yang, 2022).
Automation Integration	This involves linking various ship control systems—such as engine,	Automation integration simplifies ship operation by having coordinated control

	ballast, and navigation—into a centralized platform or network. It allows different systems to operate in sync using shared data and logic.	facilitated through one interface. The central configuration minimizes the intervention of humans, offers synchronized decision-making, and enhances system reliability. It also enables data consistency across departments and optimizes the accuracy of operations (Park, Kim, & Jeong, 2023).
AI-Enhanced HMIs	AI-enhanced HMIs use artificial intelligence to interpret data, recognize patterns, and make intelligent suggestions or automate routine operations.	These systems operate as decision support, suggesting potential issues, suggesting optimal actions, and executing routine tasks. They reduce the workload of crew members, facilitate proactive control, and enhance safety. The integration of AI into HMI systems provides real-time anomaly detection and adaptive control under changing maritime conditions (Rahman, Ahmed, & Zaman, 2022).
Touchscreen and Digital Dashboards	These are visual display systems that allow operators to interact with ship systems through graphical interfaces. They show data like speed, engine performance, fuel levels, and alarms.	Digital dashboards offer an integrated and adaptive view of ship performance, maximizing efficiency and user experience. They are tailored for different operator roles and in most instances are delivered with alarms, logs, and trend data. The systems enable faster learning, effective monitoring, and greater operational accuracy (Li, Chen, & Wang, 2021).
Decision Support Systems (DSS)	DSS are software tools embedded in HMI systems to assist in evaluating scenarios and recommending actions based on sensor data and programmed logic.	In sophisticated maritime operations, DSS supports decision-making through consequence simulation, deviation warning, and guiding users to better solutions. They bridge the gap between human control and automation, especially in time-critical or safety-related situations. DSS minimizes uncertainty and human error through context-

		sensitive guidance (Zhang, Liu, & Sun, 2019).

This lesson on automation and HMI integration describes how contemporary maritime technology makes it possible to safely and efficiently operate ships. Students are taught how HMIs act as connecting bridges between human crews and sophisticated ship systems to enable efficient monitoring, control, and decision-making. With technologies such as AI-powered dashboards and centralized automation, ship crews experience intuitive, data-based interfaces that simplify operations and minimize mistakes. Studying these integrated technologies prepares students for the realities of operating smart ships and living digital seascapes.

Explain

In class, use the Frayer Model to define the terms Human-Machine Interface (HMI), Sensor Network, and Control System. Then, create a concept map to show how the systems work together on a ship. On a Venn diagram, mark similarities and differences between manual and automated systems. Discuss in class to make sure you understand your ideas.

Elaborate/Extend (Application)

You are in an engine department of a ship where you get an unexpected fuel imbalance alert on the control panel. Use your understanding of sensor networks and control systems to outline the process your team would use to identify and correct the issue. Consider data interpretation, equipment handling, communication protocol, and safety protocols.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. What is the primary purpose of shipboard control systems?
a. To monitor cargo temperature only
b. To manage critical ship operations like propulsion, ballast, and cargo
c. To improve wireless internet onboard
d. To manage port communication systems
2. Which of the following systems ensures vessel stability through water distribution?
a. Cargo control system
b. Engine control system
c. Ballast control system
d. Fuel management system
3. What function does the engine control system perform?
a. Tracks crew performance
b. Controls anchor deployment
c. Regulates fuel injection and propulsion
d. Activates ballast alarms
4. Which system is responsible for monitoring cargo loading and discharging in tankers?
a. Navigation system
b. Engine control system
c. Hull integrity system
d. Cargo control system

5. What is the role of redundancy in shipboard systems?
a. Increase engine speed
b. Add decorative features to control panels
c. Provide backup in case of primary system failure
d. Enhance entertainment systems
6. Integration of control systems leads to which of the following benefits?
a. Longer anchoring time
b. Centralized monitoring and reduced crew workload
c. Manual operation only
d. Less need for training
7. What do DAQ systems primarily collect and process?
a. Crew schedules
b. Weather forecasts only
c. Data from shipboard components
d. Port regulations
8. Why are wireless sensor networks important on modern ships?
a. For passenger internet use
b. For decoration
c. To monitor diverse ship conditions with fewer cables
d. To reduce food supply
9. What does real-time monitoring enable?
a. Delayed system feedback
b. Weekly updates
c. Immediate response to operational changes
d. Monthly data logging
10. How does predictive maintenance benefit ship operations?
a. It delays repairs indefinitely
b. It avoids unnecessary repairs and predicts failures
c. It ignores minor issues
d. It replaces the need for engineers
11. What is the main function of a Human-Machine Interface (HMI)?
a. Translate documents
b. Connect the engine to the anchor
c. Enable operator interaction with ship systems
d. Control entertainment systems
12. Which component allows multiple ship systems to operate in sync using shared data?
a. Manual override
b. System alarms
c. Automation integration
d. Fire suppression system
13. What distinguishes AI-enhanced HMIs from traditional ones?
a. Use of paper charts
b. Passive displays only
c. Intelligent suggestions and pattern recognition
d. Larger physical buttons

14. What is one benefit of touchscreen dashboards on ships?
a. They increase the need for manual logs
b. They display only engine temperature
c. They consolidate data and improve usability
d. They are used mainly for entertainment
15. Decision Support Systems (DSS) are designed to:
a. Monitor crew sleeping patterns
b. Simulate outcomes and recommend operator actions
c. Control Wi-Fi usage
d. Replace ballast tanks
Reflection

Think about the role of automated systems and your own future career as an engineer and operator. How does this make you a more effective, safer decision-maker on board? What is the most difficult or most fascinating to you about integration and control?

Unit Summary

Chapter 5 covered how monitoring and control technologies are integrated with shipboard operations. You learned about the operation of the engine, ballast, and cargo control systems; how data acquisition and sensor networks provide real-time monitoring; and how Human-Machine Interfaces link operators with automated systems. The latter are not only essential to safe and efficient vessel operation, but are also your professional competitive edge in the global maritime sector.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 5

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Identifies and differentiates between LAN, VLAN, and WLAN										
2. Explains the purpose and function of routers, switches, and firewalls										

3. Demonstrates understanding of Ethernet and fiber optic cabling technologies										
4. Describes the use and advantages of wireless technologies (WLAN) onboard										
5. Evaluates the benefits of hybrid (wired and wireless) network systems										
6. Analyzes potential sources of interference in shipboard communication systems										
7. Applies basic principles of network segmentation using VLANs										
8. Assesses the role of firewalls in maritime cybersecurity										
9. Compares different cabling options based on speed, distance, and reliability										
10. Illustrates a basic shipboard network layout showing core components										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Li, Y., Chen, J., & Wang, R. (2021). Smart sensor networks in ship systems: Design and applications. *Journal of Marine Science and Engineering, 9*(3), Article 421. https://doi.org/10.3390/jmse9030421

Nguyen, T. H., & Lee, Y. M. (2021). Adaptive control strategies for integrated marine systems. *Ocean Systems Engineering, 11*(2), 101–115. https://doi.org/10.12989/ose.2021.11.2.101

Park, D., Kim, H., & Jeong, J. (2023). Integration of automation systems in smart shipping: A review of technologies and practices. *Ocean Engineering, 271*, 113511. https://doi.org/10.1016/j.oceaneng.2022.113511

Rahman, M. M., Ahmed, A., & Zaman, M. (2022). IoT-based real-time monitoring systems in marine engineering. *Sensors, 22*(5), Article 1823. https://doi.org/10.3390/s22051823

Wu, L., & Yang, Z. (2022). Human-machine interfaces in maritime navigation and automation. *International Journal of Maritime Engineering, 164*(2), 234–248. https://doi.org/10.1016/j.ijome.2022.03.004

Zhang, H., Liu, Y., & Sun, M. (2019). Development of integrated engine and ballast control systems for marine automation. *Journal of Ship Research, 63*(1), 55–67. https://doi.org/10.5957/JOSR.63.1.190001

Answer Key with Explanations

1. **What is the primary purpose of shipboard control systems?**
   Answer: b. To manage critical ship operations like propulsion, ballast, and cargo
   Explanation: Shipboard control systems manage essential vessel functions, ensuring safety and efficiency.
2. **Which of the following systems ensures vessel stability through water distribution?**
   Answer: c. Ballast control system
   Explanation: Ballast systems adjust the water levels in tanks to stabilize the vessel and maintain trim.
3. **What function does the engine control system perform?**
   Answer: c. Regulates fuel injection and propulsion
   Explanation: The engine control system ensures efficient propulsion by controlling fuel and monitoring engine performance.
4. **Which system is responsible for monitoring cargo loading and discharging in tankers?**
   Answer: d. Cargo control system
   Explanation: This system manages the safe and efficient handling of cargo, especially in liquid bulk carriers.
5. **What is the role of redundancy in shipboard systems?**
   Answer: c. Provide backup in case of primary system failure
   Explanation: Redundancy ensures continued operation and safety if the main system fails.
6. **Integration of control systems leads to which of the following benefits?**
   Answer: b. Centralized monitoring and reduced crew workload
   Explanation: System integration streamlines operations and improves response times through a unified interface.
7. **What do DAQ systems primarily collect and process?**
   Answer: c. Data from shipboard components
   Explanation: DAQ systems gather real-time operational data from machinery and systems for monitoring and analysis.
8. **Why are wireless sensor networks important on modern ships?**
   Answer: c. To monitor diverse ship conditions with fewer cables
   Explanation: Wireless sensors simplify installation and maintenance while providing accurate, distributed data collection.
9. **What does real-time monitoring enable?**
   Answer: c. Immediate response to operational changes
   Explanation: Real-time systems help crews act swiftly during equipment anomalies or system failures.
10. **How does predictive maintenance benefit ship operations?**
    Answer: b. It avoids unnecessary repairs and predicts failures
    Explanation: Predictive maintenance reduces costs by fixing issues before they become critical, improving system reliability.

11. **What is the main function of a Human-Machine Interface (HMI)?**
    Answer: c. Enable operator interaction with ship systems
    Explanation: HMIs allow crew to input commands and receive system feedback for safe and effective control.
12. **Which component allows multiple ship systems to operate in sync using shared data?**
    Answer: c. Automation integration
    Explanation: Automation links subsystems for coordinated performance, reducing manual intervention.
13. **What distinguishes AI-enhanced HMIs from traditional ones?**
    Answer: c. Intelligent suggestions and pattern recognition
    Explanation: AI-enhanced HMIs support decision-making by analyzing data and recommending actions.
14. **What is one benefit of touchscreen dashboards on ships?**
    Answer: c. They consolidate data and improve usability
    Explanation: Touchscreen dashboards provide clear, centralized displays for multiple ship functions, improving interaction.
15. **Decision Support Systems (DSS) are designed to:**
    Answer: b. Simulate outcomes and recommend operator actions
    Explanation: DSS tools help operators evaluate conditions and choose optimal responses during complex or time-critical events.

Chapter 6

Introduction to
Maintenance and Troubleshooting of ICT Systems

Welcome to Chapter 6: ICT System Maintenance and Troubleshooting! With information and communication technology (ICT) in the digital age, maintaining ICT systems is just as critical as designing and deploying them. Imagine a world where businesses, schools, hospitals, and even families rely on ICT—but then they suddenly fail. Who rescues the day? You. This chapter introduces you to the essential skills and knowledge to maintain systems running efficiently and smoothly. From performing routine maintenance to resolving real-time system issues with diagnostic software and system logs, you'll learn skills that make up the core of any ICT-related profession. If you're a budding IT specialist, systems administrator, or network engineer, this unit will provide you with hands-on tools that can make you a go-to and sought-after expert. This chapter is not about fixing things after they fail—it's about preventing things from failing in the first place. You'll be learning to be proactive, critical, and analytical in maintaining systems and troubleshooting. With these skills, you're not only enabling technology—you're enabling people, organizations, and progress.

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Show knowledge of routine ICT maintenance processes and troubleshooting standards.
2. Apply technical expertise in diagnosing and fixing basic hardware and software issues using the appropriate diagnostic tools.
3. Show a sense of responsible and proactive ICT system maintenance, emphasizing the importance of system reliability and efficiency in the workplace.

Lesson Objectives

By the end of the lesson, you will be able to:

1. Describe and discuss regular maintenance tasks for ICT equipment.
2. Explain common hardware and software issues and their causes.
3. Employ diagnostic software and analyze system logs to assess system performance.
4. Use troubleshooting techniques to effectively solve ICT issues.
5. Perform regular maintenance and troubleshooting exercises in a real or simulated ICT environment (Terminal Objective).

Engage (Activating Prior Knowledge)

Think about the last time your computer or phone did not work properly. What did you do? Did you reboot the machine, check the cables, or search the

Internet for an answer? Discuss your own recent ICT experiences in small groups—then write down some simple solutions that you've tried yourself. You'll be surprised at what you already know!

Lesson Introduction

In all ICT careers, technical knowledge in system maintenance and troubleshooting will be one of your best skills. This lesson is intended to introduce you to real practices in system maintenance and troubleshooting. Mastery of the complexities of ICT systems will prepare you for workplace realities and enhance your capability to deliver seamless and uninterrupted performance. Consistent with the Philippine Professional Standards for Teachers (PPST), this lesson improves your technical knowledge and problem-solving mindset in lifelong learning and professional growth.

Explore (Lesson Inputs)

Here, we will address the underlying principles of system maintenance and troubleshooting—an essential skill for ICT-related professions. As technology changes so rapidly, the need for experts who can guarantee the smooth running and security of ICT systems becomes ever more critical. You will be taught the key practices and tools that are the foundation of ICT system maintenance, problem avoidance, effective problem fixing, and informed decision-making with the use of diagnostic data. These are not just technical but strategic skills too, which allow organizations to minimize downtime, maximize operations, and guarantee business continuity.

Regular System Maintenance Protocols

Routine system maintenance is the routine activities conducted to guarantee ICT systems function efficiently, securely, and without interruptions. The activities include software updating, disk cleaning, antivirus scanning, data backup, hardware checking, and network optimization. Liu et al. (2021) provide that the use of predictive and preventive maintenance practices significantly expands the life of ICT systems while reducing the frequency of operational downtime. Alam and Arif (2022) further observe that preventive maintenance decreases long-term repair costs and overall system unreliability. With organizations relying increasingly on digital infrastructure, maintenance has shifted from being discretionary to being obligatory. Literature inevitably confirms the inclusion of formal maintenance plans as part of the ICT professional's job, as failure in this could lead to system vulnerabilities and business downtime (Tariq et al., 2023).

Table 1. Concepts of Regular System Maintenance Protocols

Concept	Description	Explanation
Software Updates	The process of installing the latest patches, enhancements, and security fixes to the system's operating system and applications.	Regular software updates are needed in a bid to close security vulnerabilities and ensure compatibility with newer technology. They protect systems from malware attacks and enhance performance overall. Not updating leaves ICT systems vulnerable to exploits and, as such, is an essential part of preventive maintenance (Alam & Arif, 2022).
Disk Cleanup and Optimization	The removal of unnecessary files and optimization of storage space to maintain system speed and functionality.	Performing regular disk cleanups prevents storage overload, which is time-consuming and results in system crashes. Defragmentation optimization maximizes data storage to achieve improved read/write rates and a longer system life cycle (Liu et al., 2021).
Antivirus and Security Scans	Routine scanning of systems for malicious software and potential threats to maintain integrity and protect user data.	Running antivirus software and security scans detect and remove malware, ransomware, or phishing attacks before they can cause harm. Scans offer data confidentiality and real-time monitoring, which is a critical component of ICT environment risk management (Rahman, Noor, & Ismail, 2021).

Data Backup and Recovery	The regular duplication of data to secure locations to allow recovery in case of data loss, corruption, or cyber incidents.	Disaster recovery involves backing up data. Modern backup technology, for example, cloud backup technology, supports business continuity since recovery can be achieved quickly. Data loss is avoided through periodic backups and is considered system resilience industry best practice (Tariq, Ali, & Iqbal, 2023).
Hardware Inspection and Cleaning	Physical examination and cleaning of ICT hardware components to detect damage, prevent overheating, and ensure efficient operation.	Regular checks decrease hardware failure by detecting worn-out parts or blockages. Dusting prevents dust buildup, which can cause overheating or short circuits. These measures enhance the lifespan of hardware and reduce emergency repair requirements (Ghavifekr & Rosdy, 2019).
Network Performance Monitoring	The continuous tracking of network metrics such as speed, latency, and bandwidth usage to detect and resolve issues proactively.	Monitoring solutions provide timely feedback about network performance, which allows IT experts to detect bottlenecks or attacks. Monitoring solutions reduce downtime by providing the ability to implement remedy in real-time and providing stable connectivity critical to system operation (Zhou, Sun, & Wang, 2020).

This lesson emphasizes the importance of regular maintenance procedures to ensure that ICT systems function properly. By learning the most critical protocols—e.g., software updates, data backup, hardware cleaning, and network monitoring—students gain the knowledge to prevent system collapse and ensure long-term stability. These procedures, rooted in industry standards and supported by recent research, equip future ICT professionals with the skills to maintain robust, secure, and high-functioning electronic environments.

Troubleshooting Hardware and Software Issues

Troubleshooting involves identifying the cause of system dysfunction or failure and actioning a return to normal function. Troubleshooting involves systematic processes such as problem identification, variable identification, hypothesis testing, and solution testing. Troubleshooting is effective with technical knowledge as well as rational thinking. A study by Ghavifekr and Rosdy (2019) concluded that the provision of troubleshooting models significantly enhances the ability of students to troubleshoot and analyze ICT problems real-time. Additionally, a study by Dutta and Singh (2020) concluded that the inclusion of scenario-based troubleshooting in training modules enhances problem-solving abilities needed for IT support personnel. Current trends also reflect a greater emphasis on soft skills—such as communication and patience—combined with technical knowledge in troubleshooting activities (Rahman et al., 2021), reflective of its multi-faceted application in the workplace.

Table 2. Concepts of Troubleshooting Hardware and Software Issues

Concept	Description	Explanation
Problem Identification	Recognizing that a system issue exists by observing symptoms, receiving user reports, or analyzing error notifications.	This initial step guarantees that the technician knows exactly how big the issue is prior to attempting to fix it. It entails posing direct questions, observing user behavior, and observing system activity to avoid assumptions and misdiagnosis. Systematic diagnosis not only conserves time in fixing irrelevant parts but also improves the ICT system support quality (Dutta & Singh, 2020).
Isolation of the Issue	Narrowing down the source of the problem to a specific hardware or software component.	Solving the problem in isolation avoids misdiagnosis by testing one component or variable at a time. Reasoning as a process deconnects peripherals, boots in safe mode, or disconnects networks to determine which component is responsible for the failure. It enhances critical thinking and enables efficient, methodical repair (Rahman, Noor, & Ismail, 2021).
Hypothesis Testing and Verification	Creating assumptions about the possible causes of the problem and testing them until the correct one is identified.	It allows the troubleshooter to apply reasoning by analogy and test different probable causes with trial-and-error, or system tools. Like testing if RAM is faulty by replacing it with a working one, which validates the hypothesis. Hypothesis testing forms technical intuition and analytical confidence in students (Ghavifekr & Rosdy, 2019).
Application of Corrective Action	Implementing the appropriate solution to fix the confirmed issue.	Lastly, once the problem has been diagnosed and isolated, this step involves doing the actual repair—i.e., reinstalling drivers, replacing faulty hardware, or adjusting system settings. This involves good technical know-how, equipment,

		and familiarity with manufacturer protocols or ICT standards (Adepoju & Jimoh, 2023).
Documentation and Prevention	Recording what the issue was, how it was solved, and recommending steps to prevent recurrence.	Having an accurate account of troubleshooting procedures ensures continuity and inter-team coordination. It also enables technicians to look up past cases and avoid unnecessary work. Preventive work—like periodic maintenance or user training—is essential to the long-term health and operation of the system (Zhou, Sun, & Wang, 2020).

Use of Diagnostic Tools and System Logs

Diagnostic tools and system logs are essential ICT system monitoring, analysis, and diagnosis tools. Diagnostic tools—i.e., hardware testers, performance monitors, and software utilities—help in system element evaluation and identification of anomalies, whereas system logs record system events and errors that are very helpful in post-incident analysis. Zhou et al. (2020) highlight the importance of automatic log analysis for improving response time and decision-making in technical failures. Additionally, research by Adepoju and Jimoh (2023) indicates that the use of tools such as Event Viewer, SMART monitoring, and task management utilities enhances troubleshooting efficiency and reduces the use of trial-and-error techniques. With the development of AI and machine learning, modern diagnostic systems can predict failures ahead of time (Kumar et al., 2022), indicating a shift towards smart, data-driven maintenance in ICT settings.

Table 3. Key Concepts in the Use of Diagnostic Tools and System Logs

Concept	**Description**	**Explanation (with citations)**
Diagnostic Tools	Diagnostic tools are software or hardware-based utilities used to assess the functionality and performance of ICT system components. These tools help in detecting, isolating, and identifying problems in systems.	Diagnostic tools refer to either software or hardware utility tools that are employed to identify the functionality and performance of the ICT system components. Diagnostic tools aid in identifying, isolating, and determining problems in systems. Diagnostic tools such as CPU-Z, HWMonitor, MemTest86, and Windows Performance Monitor provide vital information about hardware status, system load, temperature, memory integrity, and system performance. By presenting technical statistics

		consistently, these tools allow technicians to identify causes of slowdowns or non-functionality, thus swift and precise troubleshooting and system optimization (Adepoju & Jimoh, 2023).
System Logs	System logs are automated chronological records generated by operating systems, software applications, or hardware that document events, processes, errors, and user actions.	System logs are computer chronological records generated by operating systems, software applications, or hardware that track events, processes, errors, and user activity. Windows Event Viewer or Linux syslog logs are some of the logs containing critical trace information that allow IT personnel to troubleshoot by examining event patterns before, during, and after a problem occurs. They support root cause analysis and simplify the fixing of recurring or challenging system faults, enhancing service reliability and accountability (Zhou, Sun, & Wang, 2020).
Log Analysis and Interpretation	This refers to the process of examining, organizing, and drawing insights from system log data to identify anomalies, trends, or issues that affect system behavior and performance.	Log Analysis and Interpretation It refers to the examination, organization, and drawing of conclusions from system log records to identify anomalies, trends, or issues that affect system behavior and performance. Through simple or automated log analysis, system administrators are able to predict warning signs and patterns that signal oncoming failure or vulnerabilities. Advanced systems now use artificial intelligence to predict issues and recommend preventive maintenance. This is a move towards intelligent diagnostics that enhances operational efficiency and decreases

		unplanned downtime (Kumar, Sharma, & Gupta, 2022).

The use of diagnostic tools and system logs is a critical ICT system management practice that provides real-time and historical information on system performance and failures. Through learning to use diagnostic tools like performance monitors and hardware testers, students can debug and fix technical errors systematically. Similarly, system logs contain elaborate records that, when properly analyzed, reveal causes of malfunctions and assist correct fault diagnosis. The use of AI in log analysis also allows ICT professionals to move from repair-based to predictive maintenance. Knowledge of these tools and techniques enhances students' technical competence and equips them to work in high-stakes environments where system reliability and uptime are paramount.

Explain

Let's review your understanding of the key ideas of this lesson. Work with a partner or in a small group to create a Frayer Model for three key concepts: System Maintenance, Troubleshooting, and Diagnostic Tools. Write a definition of each in your own words, provide examples, non-examples, and state its importance. Then, outline the overall steps to troubleshoot a typical system problem (e.g., slow computer). Share your results with the class.

Elaborate/Extend (Application)

You are an ICT support officer in a school. Staff complain in the morning that they are unable to access the internet, and some of the computers won't start. Using your knowledge, diagnose likely causes, recommend a way of troubleshooting, and list the tools that you would use. Write down your answers and be ready to deliver your action plan. This exercise is a mock-up of real-life workplace requirements—your answers could make or break the feasibility of day-to-day operations!

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. What is the primary purpose of regular software updates in ICT systems?
a. To reduce hardware costs
b. To improve physical security
c. To patch vulnerabilities and enhance compatibility
d. To delete unused applications
2. Which maintenance task removes unnecessary files to improve system speed?
a. Data recovery
b. Disk cleanup
c. Antivirus scanning
d. Backup synchronization
3. Which of the following BEST describes data backup?
a. Protecting systems from power outages
b. Running antivirus programs periodically
c. Duplicating data to allow recovery after data loss
d. Removing malware from infected devices

4. Which tool is commonly used for real-time monitoring of system events on Windows systems?
a. Task Scheduler
b. Disk Manager
c. Event Viewer
d. File Explorer
5. What is the first step in troubleshooting a system issue?
a. Testing alternative solutions
b. Restarting the system
c. Identifying the problem
d. Installing drivers
6. **Which of the following involves examining and interpreting system logs to find patterns or anomalies?**
a. Disk defragmentation
b. Log analysis
c. Data mining
d. Registry editing
7. What is the role of antivirus and security scans in regular system maintenance?
a. To improve hardware performance
b. To install the latest software updates
c. To detect and remove malicious threats
d. To increase available disk space
8. Why is hardware inspection and cleaning important in ICT maintenance?
a. To protect against software bugs
b. To reduce license renewal costs
c. To prevent overheating and detect wear
d. To optimize data transmission
9. Which step of troubleshooting involves testing a specific solution to confirm the root cause?
a. Isolation
b. Documentation
c. Hypothesis testing
d. Log analysis
10. What does the use of SMART monitoring tools primarily help with?
a. Preventing software theft
b. Enhancing Wi-Fi coverage
c. Monitoring hard drive health and predicting failures
d. Encrypting system files
11. What kind of records do system logs provide?
a. Software licenses
b. Visual design layouts
c. Event sequences and error logs
d. User manuals

12. Which term refers to narrowing down the problem to one component in a malfunctioning system?
a. Configuration
b. Validation
c. Isolation
d. Simulation
13. What is the benefit of documenting the troubleshooting process?
a. Avoids using updated drivers
b. Helps prevent future errors and supports teamwork
c. Replaces the need for user training
d. Delays system updates
14. How has AI improved diagnostic tools in modern ICT systems?
a. By reducing power consumption
b. By enabling automatic software upgrades
c. By predicting system failures before they happen
d. By eliminating the need for user input
15. Which of the following is a benefit of proactive maintenance strategies?
a. They completely eliminate cybersecurity threats
b. They require minimal system documentation
c. They reduce operational disruptions and extend system lifespan
d. They replace the need for backups and antivirus scans

Reflection

How did the lesson influence your understanding of the ICT professional's role? Write a short paragraph on how being able to troubleshoot and maintain ICT systems can influence your career and workplace or institution you are working for. What skills do you believe you still need to acquire?

Unit Summary

This chapter has provided you with a solid foundation in ICT system maintenance and troubleshooting. You have learned the usual maintenance practices, hardware and software trouble-shooting, and diagnostic tools and system logs. These are needed to make systems reliable, users satisfied, and operations at optimal levels. In schools, business organizations, or health institutions, ICT practitioners are responsible for keeping systems running—and now, you are well on your way to joining their ra

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 6

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students	Assessed by the Cooperating Teacher

	5	4	3	2	1	5	4	3	2	1
1. Performs regular software and system updates										
2. Conducts routine disk cleanup and optimization										
3. Executes antivirus scans and security checks										
4. Implements reliable data backup and recovery plans										
5. Carries out physical hardware inspection and cleaning										
6. Monitors network performance using diagnostic tools										
7. Identifies and isolates system issues effectively										
8. Applies appropriate corrective actions during troubleshooting										
9. Analyzes and interprets system logs for decision-making										
10. Documents troubleshooting processes and recommends preventive measures										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Adepoju, A. O., & Jimoh, R. G. (2023). The impact of diagnostic tools on efficient ICT system troubleshooting. *Journal of Information Systems and Technology Management, 20*(1), 1–12. https://doi.org/10.4301/S1807-17752023000100001

Alam, M. N., & Arif, M. T. (2022). Preventive maintenance strategies in modern ICT infrastructure. *International Journal of Computer Applications, 184*(44), 9–15. https://doi.org/10.5120/ijca2022912721

Dutta, S., & Singh, R. (2020). Scenario-based ICT training for technical problem-solving. *Journal of Educational Technology Systems, 49*(2), 149–166. https://doi.org/10.1177/0047239520946423

Ghavifekr, S., & Rosdy, W. A. W. (2019). Teaching troubleshooting skills in ICT: A pedagogical review. *Education and Information Technologies, 24*, 1235–1250. https://doi.org/10.1007/s10639-018-9828-9

Kumar, R., Sharma, V., & Gupta, P. (2022). AI-based predictive maintenance and log analysis in ICT systems. *Journal of Artificial Intelligence Research & Advances, 9*(3), 45–59. https://doi.org/10.4018/JAIRA.2022070104

Liu, H., Zhang, Y., & Chen, M. (2021). Enhancing ICT system performance through preventive maintenance. *Journal of Computer Maintenance and Systems, 37*(4), 301–310. https://doi.org/10.1016/j.jcms.2021.03.004

Rahman, N. A., Noor, S. N. F. M., & Ismail, M. N. (2021). The role of soft skills in ICT troubleshooting: A new dimension. *International Journal of Instruction, 14*(2), 157–172. https://doi.org/10.29333/iji.2021.14210a
Tariq, M., Ali, S., & Iqbal, A. (2023). Data recovery planning and backup strategies in ICT. *Computer and Information Science, 16*(1), 33–41. https://doi.org/10.5539/cis.v16n1p33
Zhou, J., Sun, Q., & Wang, L. (2020). System log analysis for fault prediction and diagnostics. *IEEE Access, 8*, 110234–110246. https://doi.org/10.1109/ACCESS.2020.3002946

Answer Key with Explanations

1. **What is the primary purpose of regular software updates in ICT systems?**
   Answer: c. To patch vulnerabilities and enhance compatibility
   Explanation: Regular software updates fix security flaws, add new features, and ensure compatibility with newer technologies, making them essential for system integrity and performance.
2. **Which maintenance task removes unnecessary files to improve system speed?**
   Answer: b. Disk cleanup
   Explanation: Disk cleanup eliminates junk files and frees up storage, enhancing system speed and efficiency.
3. **Which of the following BEST describes data backup?**
   Answer: c. Duplicating data to allow recovery after data loss
   Explanation: Backups protect critical information from loss due to corruption, hardware failure, or cyber incidents, supporting business continuity.
4. **Which tool is commonly used for real-time monitoring of system events on Windows systems?**
   Answer: c. Event Viewer
   Explanation: Event Viewer logs system messages, errors, and warnings that help diagnose and resolve system issues.
5. **What is the first step in troubleshooting a system issue?**
   Answer: c. Identifying the problem
   Explanation: Proper problem identification is key to addressing the right issue and avoiding unnecessary or incorrect fixes.
6. **Which of the following involves examining and interpreting system logs to find patterns or anomalies?**
   Answer: b. Log analysis
   Explanation: Log analysis allows technicians to identify trends, root causes, or threats by studying system-generated event data.

7. **What is the role of antivirus and security scans in regular system maintenance?**
   Answer: c. To detect and remove malicious threats
   Explanation: Security scans protect systems from viruses, malware, and ransomware, preserving data and system stability.
8. **Why is hardware inspection and cleaning important in ICT maintenance?**
   Answer: c. To prevent overheating and detect wear
   Explanation: Physical maintenance prevents hardware damage and performance issues caused by dust, heat, or failing components.
9. **Which step of troubleshooting involves testing a specific solution to confirm the root cause?**
   Answer: c. Hypothesis testing
   Explanation: This step helps confirm the suspected issue through controlled tests or substitutions before applying a permanent fix.
10. **What does the use of SMART monitoring tools primarily help with?**
    Answer: c. Monitoring hard drive health and predicting failures
    Explanation: SMART (Self-Monitoring, Analysis, and Reporting Technology) tracks disk performance and signals potential failures in advance.
11. **What kind of records do system logs provide?**
    Answer: c. Event sequences and error logs
    Explanation: Logs capture system events in chronological order, aiding in the identification and diagnosis of problems.
12. **Which term refers to narrowing down the problem to one component in a malfunctioning system?**
    Answer: c. Isolation
    Explanation: Isolation involves systematic testing to find the specific hardware or software component causing the issue.
13. **What is the benefit of documenting the troubleshooting process?**
    Answer: b. Helps prevent future errors and supports teamwork
    Explanation: Documentation ensures continuity, improves collaboration, and provides a knowledge base for future incidents.
14. **How has AI improved diagnostic tools in modern ICT systems?**
    Answer: c. By predicting system failures before they happen
    Explanation: AI-enhanced diagnostic systems analyze data trends and generate predictive alerts, enabling preventive maintenance.
15. **Which of the following is a benefit of proactive maintenance strategies?**
    Answer: c. They reduce operational disruptions and extend system lifespan
    Explanation: Proactive maintenance minimizes downtime, improves system efficiency, and extends the usable life of components.

Chapter 7

Introduction to
Maritime Cybersecurity

Aboard Chapter 7! As the oceanic environment continues to go digital at a dizzying rate, ships and ports are increasingly dependent on networked technologies. While these technologies make them more efficient and secure, they also open critical systems to new and dynamic cyber risks. Maritime cybersecurity is not simply a technical issue—it's a front-line defense of global commerce, seafarers' well-being, and environmental security. Throughout this module, we will address the maritime Information and Communication Technologies (ICT) digital threat environment, the International Maritime Organization (IMO) cyber risk management framework, and explore such basic cybersecurity layers as firewalls, access controls, and encryption. You will possess the ability and knowledge to safeguard, respond to, and counteract cyber threats—a critical skill in the maritime profession of the 21st century.

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Knowledge: Study the modern cyber threat landscape on maritime ICT infrastructures and understand the magnitude of cyber vulnerabilities in the oceans.
2. Skills: Implement IMO cyber risk management principles and apply practical security measures like firewalls, encryption, and access control in model maritime environments.
3. Behavior/Attitude: Adopt a proactive and responsible attitude towards cybersecurity, valuing data security and system integrity in maritime operations.

Lesson Objectives

By the end of the lesson, you will be able to:

1. Determine various cyber threats and vulnerabilities in maritime ICT systems.
2. Outline the key components of the IMO cyber risk management guidelines.
3. Explain the function and working of fundamental layers of security such as firewalls, access control, and encryption.
4. Explain how security measures can be employed in normal maritime operating conditions.
5. Enact cybersecurity measures to safeguard maritime digital infrastructure in simulated operational environments.

Engage (Activating Prior Knowledge)

Recall any example of digital system breakdown you've ever heard of—maybe a plane taken down by a cyberattack or a hospital by a ransomware attack. Now imagine it happening on a vessel in the middle of the ocean. Brainstorm in class groups how a cyberattack might disrupt ship operations. What systems would be affected? How would it impact safety and timetables? Share your thoughts with the class.

Lesson Introduction

With shipping and ports going increasingly digital, cybersecurity is part of maritime professionals' responsibility. This lesson provides you with the foundational know-how and skills to detect cyber threats, follow international standards, and have protection in place. As a marine IT specialist, ship officer, or port operator, being cybersecurity-conscious is your contribution to maritime safety, efficiency, and reputation.

Explore (Lesson Inputs)

Since ships and maritime operations increasingly rely on integrated technologies, they are also more vulnerable to cyber threats. Maritime cybersecurity is a critical field, required to ensure the security, dependability, and continuity of shipboard and port operations. The current chapter discusses three key domains of maritime cybersecurity: the maritime ICT threat landscape, the IMO cyber risk management guidelines, and the firewalls, access control, and encryption layered security concept. Familiarity with these domains is required for the development of practical and anticipatory cyber defense measures that are internationally compliant and relevant to real maritime requirements.

Threat Landscape in Maritime ICT

The maritime sector has experienced an increasing spectrum of cyber threats following the use of Information and Communication Technology (ICT) in ship and port operations. Threats range from malware, GPS spoofing, ransomware, and phishing to unauthorized access to operational systems like navigation, engine control, and cargo management. As ships become more and more connected using satellite links and digital control systems, they are vulnerable to targeted and opportunistic cyberattacks. Cybersecurity Ventures (2022) reports that the absence of standard cybersecurity protocols and outdated software in most ships contributes to vulnerability. Operational Technology (OT) systems that manage critical onboard functions, for example, are not necessarily designed with cybersecurity in mind and therefore expose vulnerabilities that can be exploited. The 2018 COSCO Shipping IT network attack and the NotPetya attack that targeted Maersk in 2017 demonstrate how cyber events can affect global maritime supply chains. Scholars like Chang, Weng, and Wu (2020) note that increasing awareness and conducting regular assessments of cyber risk are essential in identifying vulnerabilities before they are exploited.

Table 1. Key Concepts in the Threat Landscape in Maritime ICT

Concept	Description	Explanation
Cyber Threats in Maritime ICT	Refers to malicious digital activities targeting maritime systems and data. Common threats include malware, ransomware, phishing, GPS spoofing, and denial-of-service attacks.	These vulnerabilities have the potential to target the disruption of ship operations, safety, or loss of money. The incorporation of ICT into shipboard systems raises exposure, particularly where ships employ internet-facing systems for operations. The more devices that are connected, particularly for navigation and communication, the greater the vulnerability of cyber breaches (Rezaee, Soleimani, & Bahadori, 2022).
Operational Technology (OT) Vulnerability	OT includes systems that monitor and control shipboard operations such as navigation, engine controls, and ballast systems.	They were not designed with cybersecurity in mind and are typically linked to IT systems with weak defenses. They are therefore vulnerable to cyber attacks, particularly when there are no regular updates or patches. Their criticality renders an attack

		directly affecting ship safety alongside environment safety (Chang, Weng, & Wu, 2020).
Legacy Systems and Outdated Software	Many ships still run older software and operating systems that are no longer supported by manufacturers.	These legacy systems are less secure against cyberattacks since they do not have advanced security features and are not regularly patched. As experienced by Maersk following the NotPetya ransomware attack, legacy systems can have disastrous operational and financial impacts upon being compromised (Kessler & Craiger, 2021).
Real-World Incidents as Case Studies	Notable cyber incidents serve as real-life evidence of the maritime sector's vulnerabilities.	The 2017 Maersk attack and the 2018 COSCO cyberattack disrupted logistics and port operations worldwide and resulted in communication breakdowns and delays. The above case studies depict the necessity of implementing cyber risk management practices and investing in strong systems (Rezaee et al., 2022; EMSA, 2020).
Importance of Cyber Risk Assessment	Refers to the process of identifying, analyzing, and evaluating cybersecurity vulnerabilities and threats in maritime systems.	Continuous risk scanning enables companies to detect and remediate vulnerabilities in time before they are exploited by attackers. Furthermore, worker training and consciousness are worthwhile measures in reducing the aspect of human error and improving enterprise-wide cybersecurity posture (Chang et al., 2020; EMSA, 2020).

The digital evolution of the maritime sector has brought about extensive cyber vulnerabilities, and the threat environment is complex and dynamic. As the table elaborates, cyber threats like malware, GPS spoofing, and ransomware are increasingly common, affecting IT and OT systems on vessels and port terminals. Most of these vulnerabilities arise from the embedding of legacy systems that are still in use and the merging of previously disconnected OT with internet-connected networks without embedding sufficient security controls. Practical examples such as the COSCO and Maersk attacks highlight the importance of effective cyber protection and risk management practices. Most importantly, regular cyber risk analysis and cybersecurity culture are essential to detect potential vulnerabilities and avoid risks before they manifest into actual incidents. This lesson emphasizes that cybersecurity is not a purely technical matter but an essential operational concern in contemporary maritime environments.

IMO Cyber Risk Management Guidelines

Embracing the growing cyber threats in maritime sectors, the International Maritime Organization (IMO) published its Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) effective from January 1, 2021. The guidelines mandated cyber threats to be addressed within the purview of a ship's existing Safety Management System (SMS), adopting a structured methodology based on five functional elements: identify, protect, detect, respond, and recover. The policy design promotes maritime operators to scrutinize all fundamental systems, detect vulnerabilities, and adopt ongoing monitoring and response measures. According to Kessler and Craiger (2021), the guidelines have triggered a sharp shift in shipping companies' attitude towards cyber readiness—not a technical requirement but organizational responsibility. Additionally, they promote cross-industry collaboration among technical, managerial, and operational divisions to embed cybersecurity into the maritime business. The IMO model harmonizes international best practices like those adopted by ISO/IEC 27001 and the NIST Cybersecurity Framework and is therefore scalable to maritime operations of any size (Yang & Wang, 2018).

Table 2. Key Concepts of IMO Cyber Risk Management Guidelines

Concept	Description	Explanation
Identify	The process of recognizing critical digital systems, assets, and potential cyber vulnerabilities in maritime operations.	Digital asset identification and vulnerabilities are the cornerstones of a cybersecurity strategy. Ocean operators must conduct comprehensive risk assessments to know what needs to be protected and where attacks will be made. The pre-emptive action will enable sound decision-making in planning tomorrow's protection and response measures (Kessler & Craiger, 2021).
Protect	Implementation of safeguards to secure critical systems and ensure the continued functioning of maritime infrastructure.	Protective measures such as encryption, firewalls, secure passwords, and access control measures need to be implemented to protect against unauthorized access and secure confidential operating information. Cyber hygiene training of employees enhances this protective layer as well (EMSA, 2020).
Detect	The ability to recognize cyber incidents promptly through	Early identification allows shipping stakeholders to recognize cyber threats before they get out of hand. Live

	monitoring and alert systems.	monitoring devices and intrusion detection mechanisms help detect unauthorized access, unusual data transfers, and system deviations (Chang, Weng, & Wu, 2020).
Respond	The development and implementation of procedures to manage and contain cyber incidents when they occur.	An early and unified response minimizes business disruption and minimizes the effects of cyberattacks. Response actions include isolating affected systems, informing the relevant authorities, and executing remedial actions (Rezaee, Soleimani, & Bahadori, 2022).
Recover	Restoring systems and operations to normal after a cyber incident while analyzing the event for future improvement.	Recovery entails data recovery, restarting of important systems, and continuity of maritime operations. Experience gained from incidents is incorporated into enhancing cybersecurity measures and revising contingency plans (Yang & Wang, 2018).

The IMO Cyber Risk Management Guidelines provide a systematic and hands-on guide to cybersecurity specifically for the maritime sector. Breaking down risk management into five elements of cyber defense—Identify, Protect, Detect, Respond, and Recover—the guidelines promote end-to-end preparedness against cyber attacks. Each step caters to a unique element of cyber defense, ranging from vulnerability analysis to system recovery, to provide an integrated and proactive framework. The system not only meets international norms but also promotes coordination between technological, managerial, and operational departments. Such concepts being adopted equip maritime professionals with the mindset and frameworks to ensure cyber-resilient operations in a rapidly digitized maritime sector.

Security Layers: Firewalls, Access Control, and Encryption

To counter cyber threats, maritime cybersecurity practices must employ layered defenses of firewalls, access control, and encryption. Firewalls are virtual barriers that control network traffic between trusted internal networks and untrusted external networks and, as such, deny unauthorized access. Access control processes implement user authentication and authorization policy, and credentialed personnel alone gain access to critical systems. Encryption, on the other hand, keeps data safe by making it unintelligible without decryption, such that confidentiality and integrity are guaranteed during transmission and storage. These technologies are the foundation in repelling cyber intrusions and guaranteeing the resilience of maritime ICT facilities. Mitev and Yordanov (2021) aver that the use of multi-layered security controls reduces single points of failure. Moreover, as per the European Maritime Safety Agency (EMSA, 2020), consolidation of such security measures must be constantly upgraded to respond to the escalating sophistication of cyberattack techniques. Consolidation of such layers not merely performs technical defense functions but also ensures regulatory compliance and operational continuity in shipboard and shore-based environments.

Table 3. Key Concepts in Security Layers for Maritime Cybersecurity

Concept	Description	Explanation
Firewalls	Firewalls are network security devices or software that monitor and control traffic based on predetermined security rules.	On board, firewalls act as shields that segregate sensitive systems (e.g., navigation and engine management) from less secure networks (e.g., crew or guest Wi-Fi), limiting the risk of unauthorized access and cyber attack. They play a key role in preventing lateral malware spread and isolating cyber incidents before they affect ship operations (Mitev & Yordanov, 2021; EMSA, 2020).
Access Control	Access control involves procedures and technologies that ensure only authorized users can access specific systems or data, usually enforced through authentication and authorization.	At sea operations, access control restricts exposure of key systems by providing role-based rights and enforcing authentication. This keeps unauthorized users, including insiders, from accessing sensitive equipment or information, and promotes accountability through logging and auditing methods (Chang et al., 2020; Yang & Wang, 2018).
Encryption	Encryption converts readable data into encoded formats that can only be deciphered by authorized users with the correct decryption key.	Maritime communications, especially satellite or cloud communications, require strong encryption to preserve data integrity and confidentiality. Encryption protects sensitive data such as cargo manifests, route planning, or system diagnostics from unauthorized individuals, secure from intruders during transit and storage, following global data protection standards (Rezaee et al., 2022; EMSA, 2020).

This lesson emphasizes the importance of layered security controls—the use of firewalls, access control, and encryption—to secure maritime ICT infrastructure from cyber attacks. Each is used for a distinct purpose in system resilience: firewalls filter traffic and quarantine threats, access control restricts user privilege and counteracts insider threats, and encryption enables secure storage and transmission of mission-critical data. These defenses are not technical artifacts but essential components of an active cybersecurity posture that addresses international regulatory needs and operational continuity goals. As the character of cyber threats to maritime systems continues to change, application of these layered security controls allows ships and shore-based systems to operate securely, safely, and uninterrupted.

Explain

Using a Frayer Model or Concept Map, define and list the following important terms: cyber threat, firewall, encryption, access control, and cyber risk management. Summarize the main points of the lesson in your own words in pairs. Finally, list at least three cybersecurity practices and match them with the kinds of threats they address.

Elaborate/Extend (Application)

You work in an IT and security department on a ship. You are notified of unauthorized access to the navigation system on your ship. Write a response plan based on what you have learned, including IMO guidelines and security controls like access controls and firewalls. Present your group's action plan to the class and discuss how each step addresses certain vulnerabilities.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. **What is one of the primary reasons the maritime industry has become more vulnerable to cyber threats?**
   a. More use of manual systems
   b. Reduced crew size
   c. Integration of Information and Communication Technology (ICT)
   d. Increase in port fees
2. **Which of the following best describes a firewall?**
   a. A device that physically separates networks
   b. A network security system that controls traffic based on rules
   c. A system that monitors crew behavior
   d. A tool for encrypting data
3. **What is the main function of access control in maritime cybersecurity?**
   a. Backing up navigation logs
   b. Verifying and limiting user access to systems
   c. Blocking physical entry to ports
   d. Encrypting messages from the bridge
4. **Which cyber threat involves tricking users into revealing sensitive information?**
   a. Malware
   b. GPS spoofing
   c. Phishing
   d. DDoS
5. **What is the purpose of encryption in shipboard systems?**
   a. To disable unauthorized software
   b. To convert data into unreadable code for security
   c. To log all crew communication
   d. To control network traffic flow
6. **According to the IMO guidelines, what is the first step in cyber risk management?**
   a. Detect
   b. Respond

c. Identify
d. Recover

7. **What is an example of Operational Technology (OT) in ships?**
a. Email server
b. Navigation control system
c. Crew training module
d. Shipboard printer

8. **The NotPetya ransomware attack in 2017 mainly affected which shipping company?**
a. COSCO
b. Hanjin
c. Maersk
d. MOL

9. **Why are legacy systems a cybersecurity concern on ships?**
a. They require too much crew training
b. They are physically large
c. They lack modern security updates
d. They cannot be used at sea

10. **What does the "Protect" function in IMO guidelines emphasize?**
a. Disabling unused ship equipment
b. Applying safeguards like firewalls and training
c. Scheduling crew rotations
d. Encrypting only email systems

11. **Which incident in 2018 highlighted the vulnerability of IT networks in shipping companies?**
a. Maersk ransomware attack
b. MOL bridge crash
c. COSCO network disruption
d. Evergreen canal blockage

12. **What is the primary goal of the "Recover" phase in the IMO guidelines?**
a. Detect further threats
b. Monitor email usage
c. Restore systems and improve future defenses
d. Isolate all affected systems permanently

13. **How does access control support cybersecurity?**
a. By preventing external communication
b. Through physical ship inspections
c. By assigning user-specific permissions
d. By updating software remotely

14. **Which framework do the IMO guidelines align with?**
a. SOLAS Rescue Protocol
b. NIST Cybersecurity Framework
c. ISO 9001 Quality Standards
d. MARPOL Compliance Scheme

15. **What makes a layered security approach effective in maritime** cybersecurity?
    a. It adds aesthetic design to systems
    b. It includes multiple, overlapping security measures
    c. It limits ship-to-shore communication
    d. It isolates systems entirely from the internet

Reflection

How has your knowledge of cybersecurity evolved after learning about its application to maritime operations? Why do you believe security-first thinking is most crucial for maritime professionals like yourself in the future? Think about one cybersecurity skill or practice that you believe you can confidently use in your future career.

Unit Summary

This chapter emphasized the increasing importance of maritime cybersecurity. Students were given an overview of the cyber threat environment, educated on IMO cyber risk management guidance, and exposed to defense layers including firewalls, encryption, and access control. With the increasing use of technology, knowledge of and use of these security layers are part of being a good and responsible maritime professional

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 7

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Identifies common cyber threats in maritime ICT systems										

2. Analyzes vulnerabilities in Operational Technology (OT)										
3. Explains the role of legacy systems in cybersecurity risk										
4. Evaluates real-world cyber incidents in maritime contexts										
5. Describes the components of the IMO Cyber Risk Management Guidelines										
6. Applies the five functional elements: Identify, Protect, Detect, Respond, and Recover										
7. Demonstrates understanding of firewalls as security barriers										
8. Illustrates the importance of access control in cyber defense										
9. Explains how encryption safeguards data confidentiality										
10. Integrates layered security strategies into maritime operations										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Chang, Y.-C., Weng, P.-Y., & Wu, C.-Y. (2020). *Cybersecurity policy for the international maritime organization: An assessment of the IMO guidelines*. WMU Journal of Maritime Affairs, 19, 175–192. https://doi.org/10.1007/s13437-020-00206-4

EMSA. (2020). *Guidelines on cybersecurity onboard ships*. European Maritime Safety Agency. https://www.emsa.europa.eu/publications/item/3890-guidelines-on-cyber-security-onboard-ships.html

Kessler, G. C., & Craiger, P. (2021). *Maritime cybersecurity: A guide for leaders and managers*. Springer. https://doi.org/10.1007/978-3-030-52833-8

Mitev, P., & Yordanov, V. (2021). *Cyber security in the maritime sector – current state and future challenges*. Scientific Journal "Science and Education," 4(72), 103–108. https://doi.org/10.55206/XJFD6210

Rezaee, M., Soleimani, P., & Bahadori, R. (2022). *Cybersecurity challenges and solutions in maritime transportation systems*. Journal of Marine Science and Engineering, 10(5), 656. https://doi.org/10.3390/jmse10050656

Yang, Z., & Wang, J. (2018). *Maritime cyber security management: A conceptual framework for managing cyber risks*. Transportation Research Part E: Logistics and Transportation Review, 110, 77–89.

Answer Key with Explanations

1. **What is one of the primary reasons the maritime industry has become more vulnerable to cyber threats?**
   Answer: **c. Integration of Information and Communication Technology (ICT)**
   Explanation: The increasing use of ICT in shipboard and port operations has expanded the attack surface for cyber threats.
2. **Which of the following best describes a firewall?**
   Answer: **b. A network security system that controls traffic based on rules**
   Explanation: Firewalls monitor and control network traffic to prevent unauthorized access.
3. **What is the main function of access control in maritime cybersecurity?**
   Answer: **b. Verifying and limiting user access to systems**
   Explanation: Access control ensures that only authorized personnel can access specific digital systems or data.
4. **Which cyber threat involves tricking users into revealing sensitive information?**
   Answer: **c. Phishing**
   Explanation: Phishing attacks deceive users into disclosing confidential information, often via email or fake websites.
5. **What is the purpose of encryption in shipboard systems?**
   Answer: **b. To convert data into unreadable code for security**
   Explanation: Encryption protects sensitive information during transmission and storage, making it unreadable to unauthorized users.
6. **According to the IMO guidelines, what is the first step in cyber risk management?**
   Answer: **c. Identify**
   Explanation: The first step involves identifying critical systems, vulnerabilities, and assets to manage cyber risks effectively.
7. **What is an example of Operational Technology (OT) in ships?**
   Answer: **b. Navigation control system**
   Explanation: OT systems like navigation controls manage physical ship functions and are increasingly targeted in cyberattacks.
8. **The NotPetya ransomware attack in 2017 mainly affected which shipping company?**
   Answer: **c. Maersk**
   Explanation: Maersk's systems were severely impacted by NotPetya, disrupting global operations and highlighting cybersecurity gaps.

9. **Why are legacy systems a cybersecurity concern on ships?**
   Answer: **c. They lack modern security updates**
   Explanation: Legacy systems are often outdated, unpatched, and lack modern protections, making them vulnerable to attacks.
10. **What does the "Protect" function in IMO guidelines emphasize?**
    Answer: **b. Applying safeguards like firewalls and training**
    Explanation: The "Protect" function focuses on implementing measures to reduce the likelihood of cyber incidents.
11. **Which incident in 2018 highlighted the vulnerability of IT networks in shipping companies?**
    Answer: **c. COSCO network disruption**
    Explanation: COSCO's IT systems were disrupted by a cyberattack in 2018, affecting communications and logistics.
12. **What is the primary goal of the "Recover" phase in the IMO guidelines?**
    Answer: **c. Restore systems and improve future defenses**
    Explanation: Recovery involves restoring operations and learning from incidents to strengthen future cybersecurity.
13. **How does access control support cybersecurity?**
    Answer: **c. By assigning user-specific permissions**
    Explanation: Access control restricts access based on user roles, reducing unauthorized use and increasing accountability.
14. **Which framework do the IMO guidelines align with?**
    Answer: **b. NIST Cybersecurity Framework**
    Explanation: The IMO guidelines align with globally recognized frameworks such as NIST and ISO/IEC 27001.
15. **What makes a layered security approach effective in maritime cybersecurity?**
    Answer: **b. It includes multiple, overlapping security measures**
    Explanation: A layered approach combines different tools (e.g., firewalls, access control, encryption) to create stronger defenses.

Chapter 8

Introduction to
Software Licensing, Compliance, and Documentation

In a computer-driven world, it's crucial for every IT and maritime professional to understand how software is licensed, managed, and documented. If you're in charge of the navigation system or engine control interface of a vessel—how would you know the software is authentic, current, and documented? In this chapter, you'll be introduced to the best practices of software installation, version control, license compliance, and technical documentation. You'll learn the behind-the-scenes threads that make digital systems safe and reliable. Whether your professional life is on land or at sea, the security and integrity of digital operations are in your hands with compliance and knowledge of software policies and documentation standards. This unit is more than rules—it's about being a good digital steward and a good systems manager. When you're finished with this lesson, you'll be ready to make informed decisions about software use and to ensure operational effectiveness in your new workplace.

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Exhibit expertise in various software licensing models and their appropriate applications in technical settings.
2. Adopt best practices for system documentation and software version control.
3. Show a compliant and responsible software use, licensing compliance, and proper digital record-keeping attitude.

Lesson Objectives

By the end of the lesson, you will be able to:

1. Explain different software licensing models such as OEM, subscription, and open-source.
2. Describe the process and hardware involved in software installation and versioning.
3. Explain the importance and components of technical documentation like digital logbooks and backups.
4. Describe the penalties for non-compliance with software licensing within organizational environments.
5. Exhibit the capability to administer software licenses, install and make installations, and document to industry standards. (Terminal Objective)

Engage (Activating Prior Knowledge)

Recall the latest software installation or application you did—was it free, open-source, or license-keyed? Had you ever even read the terms and conditions, or merely clicked on "Accept"? Share with a partner a short experience with software installation or updating. Was there ever a time when it did not work because of a licencing issue? What did you learn from it?

Lesson Introduction

This lesson will guide you through the key practices of ethical software asset management—from selecting the proper licensing model to maintaining digital records in their integrity through documentation. As future IT or maritime professionals, your capacity to install software correctly, handle updates, and be compliant will directly contribute to the safety and integrity of technical operations. This lesson is aligned with the Philippine Professional Standards for Teachers (PPST) in that it encourages professionalism, legal accountability, and technical expertise in digital systems.

Explore (Lesson Inputs)

In today's digital workplace, onshore or offshore, it is no technical nicety but a professional requirement to understand how software is installed, licensed, supported, and documented. This chapter addresses the three pillars of good software management: installation and version control, licensing models, and technical documentation. Understanding these topics ensures legal compliance, ensures operational effectiveness, and protects critical systems against threats such as data loss or failure of software. The following topics are the basics for students who intend to pursue a career in IT, engineering, or maritime industries.

Software Installation and Version Control

Software installation refers to the installation of computer or network platform software programs, ensuring hardware and existing system configuration compatibility. Version control, however, refers to monitoring changes to software over time, enabling teams to work securely, manage updates, and revert to previous states in case the system fails. Git and Subversion are some of the tools of software lifecycle management that have become a necessary component of environments where multiple users handle the same system or application (Kalliamvakou et al., 2020). Version control is most essential in shipboard systems or engineering environments where unauthorized changes lead to system failure. Gousios et al. (2020) mentioned that strong version control methods ensure transparency, coordination of teams, and safer deployment cycles. Software installation and version control are thus not technical stages but standardized processes that guarantee operational integrity and traceability in complex digital environments.

Table 1. Concepts in Software Installation and Version Control

Concept	Description	Explanation
Software Installation	The process of setting up a software application on a computer or network system to make it operational and compatible with existing system configurations and hardware.	Proper software installation involves establishing system configurations, deploying necessary dependencies, and integrating the software with existing platforms. This reduces the likelihood of executing errors and improves functionality, especially in advanced IT systems. (Spinellis, 2018)
Version Control Systems (VCS)	Software tools that manage changes to source code or configuration files over time and allow for tracking, collaboration, and rollback capabilities.	VCS tools like Git and Subversion enable groups to work on the same codebase in parallel, record project history, and preserve system integrity by maintaining accurate records and revision control. These tools form the foundation of code and coordination of teams and quality assurance. (Kalliamvakou et al., 2020)
Change Tracking	The method of recording and documenting all modifications made to software systems or codebases for monitoring, auditing, and debugging	Change tracking provides a history log that provides accountability, security compliance, and source tracking of bugs or vulnerabilities. In safety-critical applications, this is significant in maintaining regulatory as well as operational

	purposes.	compliance. (Gousios et al., 2020)
Rollback and Recovery	The process of reverting a system or software to a previous working state after encountering a critical failure or error.	Version control system rollbacks allow for rapid restoration of systems to safe states without having to re-install entirely or lose data. This feature is required to facilitate reduced downtime and service uptime in engineering and business settings. (Gousios et al., 2020)
Collaborative Development	The practice of multiple developers working on the same software project concurrently through shared repositories and tools.	Version control systems facilitate collaboration using branching, merging, and pull requests, which help manage multiple workstreams and prevent conflicts. It helps maintain productivity with software stability assured with different contributors. (Kalliamvakou et al., 2020)

Comprehending the fundamental principles of software installation and version control is critical to ensure system stability, secure collaboration, and avoid operational errors in technical environments. Installation is the foundation of operating software efficiently, while version control mechanisms like Git enable developers and IT professionals to manage updates, track changes, and manage teams effectively. These tools not only make software more reliable but also enhance organizational readiness against failure or error by providing rollback and recovery capabilities. In advanced systems like shipboard networks or enterprise systems, applying these principles ensures transparency, compliance, and long-term operational success (Gousios et al., 2020; Kalliamvakou et al., 2020; Spinellis, 2018).

Licensing Models (OEM, Subscription, Open Source)

Software licensing prescribes the legal terms upon which software can be used, modified, and distributed. OEM (Original Equipment Manufacturer) licenses are typically bundled with hardware and are non-transferable. Subscription licenses entail periodic payments and typically come with updates and customer support, hence their adoption in cloud platforms. Open-source licenses accord users the right to view, change, and redistribute the code, encouraging innovation and community contribution. Each model has its strengths and weaknesses in cost, control, and compliance. Misunderstanding of software licenses can be responsible for law violations and enormous losses as advocated by Kassab, Nejad, and DeFranco (2023). Additionally, license management becomes increasingly important as organizations adopt hybrid IT environments where different types of licenses coexist. Selection of appropriate software licenses should be guided by organizational requirements, legal requirements, and technical requirements to ensure ethical and effective system performance (St. Laurent & Meeker, 2021).

Table 2. Licensing Models – Concepts, Descriptions, and Literature-Based Explanations

Licensing Model	Description	Explanation and Literature Review
OEM (Original Equipment Manufacturer)	OEM licenses are bundled with a specific piece of hardware and are non-transferable.	OEM software is cheap but inflexible as it's locked to the hardware it was originally installed on. It's typically installed in factory-installed gear or embedded shipboard controls. OEM licenses are rarely transferable or reinstallable, which can be problematic in changing environments like IT or shipboard system administration. Mismanagement of such licenses can lead to compliance issues, especially in device ecosystem-dominant industries (Kassab, Nejad, & DeFranco, 2023).
Subscription License	This model charges users a recurring fee (monthly or annually) to use software, typically including updates and support.	Subscription licensing is standard in cloud platforms such as Microsoft 365 or Adobe Creative Cloud. They are convenient and always current but are dependent on stable internet and continuous payment. Organisations find subscription models appealing because they are scalable, especially in remote maritime business or remote IT networks. Subscription models enable collaborative working but demand proper budget planning and license administration (Kalliamvakou et al., 2020; Schermann, Schepers, & Krcmar, 2022).
Open Source License	Allows users to freely use, modify, and distribute software under specific licensing terms (e.g., MIT, GPL).	Open-source licensing supports innovation, openness, and community development. Open-source platforms in marine systems can be designed for specific shipboard application or navigation software. However, familiarity with the exact terms (e.g., attribution or share-alike clauses) is required to

		avoid violations of open-source licenses. Application of open-source supports autonomy and cost savings in the long term if governance is well-maintained. Documentation and traceability of the code assume very critical roles in open-source environments for maintainability (St. Laurent & Meeker, 2021; Spinellis, 2018).

An understanding of software licensing models is paramount in responsibly managing digital assets in today's networked professional environment. Whether OEM deals tied to specific hardware, adaptive subscription-based offerings, or open-source offerings which are modifiable, each possesses different considerations in cost, functionality, and legality. This is especially true in technical fields such as maritime operations and IT administration, where software abuse can result in regulatory violations or operational disruptions. By means of this lesson, students gain the ability to safely work with licensing models, using the knowledge in identifying suitable and ethical software solutions in real-world applications.

Technical Documentation, Digital Logbooks, and Backups

Technical documentation is written reports that detail the architecture, behavior, installation, maintenance, and operation of software systems. Digital logbooks are timestamped, structured records of run activity, updates, and user actions, essential to auditing and debugging. Backups entail data replication to guard against data loss due to system failure, cyberattack, or accidental deletion. They are the basis of system accountability and continuity planning. Spinellis (2018) hypothesizes that proper maintenance of documentation and frequent backups not only minimize operational risks but also facilitate regulatory compliance and recoverability of systems. In safety-critical areas such as maritime navigation or industrial automation, absence of proper records and backups can compromise safety and hinder operations. Contemporary documentation practices have also changed with the adoption of collaborative tools like Confluence, GitHub Wikis, and automated backup tools, which facilitate transparency and efficiency in technical processes (Schermann et al., 2022). Technical documentation and data integrity practices are thus essential to ensuring professional standards in any digital workplace.

Table 3. Key Concepts in Technical Documentation, Digital Logbooks, and Backups

Concept	Description	Explanation
Technical Documentation	Technical documentation refers to detailed records that explain the design, setup, and operation of	It greatly assists in system transparency, system maintenance, and technical environments' troubleshooting support. Documentation prevents

	software systems, including installation procedures and user guides.	system loss of knowledge when staff members are replaced, and it keeps teams in a state of continuity. Use of tools such as GitHub Wikis and Confluence facilitates collaboration and minimizes gaps in documentation (Spinellis, 2018; Schermann et al., 2022).
Digital Logbooks	Digital logbooks are time-stamped digital records used to monitor, track, and archive system operations, updates, and user activities.	These logs enhance system accountability by maintaining a chronological record of events that facilitate audits, incident analysis, and maintenance planning. Logbooks are required in industries like shipping and aviation and are part of safety and compliance protocols. Use enables standardized recording of operations and improved error diagnosis (Schermann et al., 2022).
Backups	Backups are copies of data or software configurations created to prevent data loss from system failure, cyberattacks, or accidental deletion.	They are most important to business continuity and disaster recovery. Regular, secure, and redundant backups are necessary to ensure success during crises. Organizations use various methods—cloud, local, and offsite backups—to safeguard information. Automated backup tools provide regular schedule enforcement and reduce risks with human error (Spinellis, 2018).

Technical documentation best practices, digital logbooks, and backups provide students with a blueprint for having solid and responsible digital systems. These practices are instrumental in guaranteeing operational efficiency, security, and regulatory compliance, particularly in high-risk environments. In preparing students for IT, engineering, or for marine operations, being proficient in these tools will enable them to prevent data loss, effectively diagnose system issues, and keep good records for audits and reviews—a set of skills that counts in today's digital workplace.

Explain

Collaborate with a partner to explain the following terms in your own words and record them in a graphic organizer of your choice:

- OEM License
- Subscription License
- Open Source License
- Version Control
- Technical Documentation
- Digital Logbook
- Backup

Explain their role and definition. Illustrate on a Frayer Model or Venn diagram how they complement each other and impact system performance and compliance.

Elaborate/Extend (Application)

You are a new IT technician on a ship. The ship's navigation software needs to be updated, but the current license has expired. Create a procedure with steps to identify the type of license for the software, acquire the appropriate license, install the software update, and document the changes in the electronic logbook. Justify each step based on compliance and best practice.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. What is the primary goal of version control systems like Git or Subversion?
a. To increase software cost
b. To delete outdated software
c. To track and manage changes over time
d. To install software updates automatically
2. Which of the following best describes software installation?
a. Removing unnecessary programs
b. The process of configuring system settings to make software operational
c. A backup process for digital storage
d. Documenting user actions on a network
3. Why is change tracking important in version control?
a. It increases processing speed
b. It improves hardware performance
c. It allows developers to monitor and audit code changes
d. It blocks unauthorized access
4. What feature of version control allows developers to revert to a previous software state after a failure?
a. Deployment scheduling
b. Incremental loading
c. Rollback and recovery
d. Open source licensing
5. Which version control practice enhances productivity by allowing multiple developers to work on a project simultaneously?
a. Redundancy testing
b. Collaborative development
c. Data encryption
d. System cloning

6. What type of license is typically bundled with hardware and is non-transferable?
a. Subscription license
b. OEM license
c. Open-source license
d. Commercial license
7. Subscription licenses are commonly used in which type of platform?
a. Local-only software
b. Open hardware systems
c. Cloud-based platforms
d. Unlicensed applications
8. What is a key benefit of open-source software licensing?
a. Expensive long-term use
b. Restricts modification of code
c. Encourages community-driven development
d. Prevents code sharing
9. Why is it important to understand software licensing models in a professional setting?
a. To reduce electricity costs
b. To ensure legal compliance and effective resource use
c. To encourage piracy
d. To bypass regulations
10. What term refers to the written records that explain how software systems operate, including their architecture and maintenance?
a. Data mining
b. Change tracking
c. Technical documentation
d. Redundancy planning
11. Which concept involves keeping time-stamped records of user actions and system events?
a. Software installation
b. Digital logbooks
c. Open-source licenses
d. Version rollback
12. Why are digital logbooks critical in high-risk industries like maritime navigation?
a. They generate marketing data
b. They track sales performance
c. They help diagnose system failures and maintain legal compliance
d. They disable user access
13. What is the main purpose of creating backups?
a. To save system images for aesthetics
b. To enhance CPU performance
c. To prevent data loss from system failures or attacks
d. To track employee attendance

14. Which tools are commonly used to manage technical documentation and team collaboration?
a. Photoshop and Canva
b. GitHub Wikis and Confluence
c. Excel and Word
d. Facebook and Twitter
15. What is the most important reason for automating backup processes in an organization?
a. To increase user traffic
b. To minimize manual input and reduce error risks
c. To remove old software
d. To allow unlimited downloads

Reflection

How has this lesson impacted your thinking regarding the use of software and documentation? How, in your own work life aboard and ashore, will you ensure that your digital hardware is adequately licensed, documented, and serviced? Write a brief paragraph taking into account the role of documentation and compliance in professional integrity and system dependability.

Unit Summary

This chapter introduced students to the fundamental knowledge required to operate software legally and efficiently. Students were introduced to software licensing models such as OEM, subscription, and open-source; learned the need for software version control and electronic backup; and learned to document technical procedures in logbooks and manuals. The lesson emphasized the need for ethical responsibility, legal compliance, and documentation in the workplace.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 8

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Installs software with attention to compatibility and settings										
2. Applies version control using tools like Git or Subversion										
3. Tracks changes and maintains detailed revision history										

4. Executes rollback and recovery procedures effectively										
5. Collaborates with others through version control systems										
6. Identifies and applies appropriate software licensing models										
7. Observes compliance with licensing terms and conditions										
8. Prepares clear and complete technical documentation										
9. Maintains accurate and time-stamped digital logbooks										
10. Implements regular and secure data backup procedures										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Gousios, G., Zaidman, A., & van Deursen, A. (2020). *Work practices and challenges in pull-based development: The integrator's perspective*. Empirical Software Engineering, **25**, 1907–1943. https://doi.org/10.1007/s10664-019-09761-5

Kalliamvakou, E., Bird, C., Zimmermann, T., Begel, A., DeLine, R., & German, D. M. (2020). *What makes a great manager of software engineers?*. IEEE Transactions on Software Engineering, **46**(9), 968–983. https://doi.org/10.1109/TSE.2018.2872757

Kassab, M., Nejad, M. M., & DeFranco, J. (2023). *The landscape of software licensing models and their implications: An industry perspective*. Journal of Systems and Software, **201**, 111440. https://doi.org/10.1016/j.jss.2023.111440

Schermann, M., Schepers, J., & Krcmar, H. (2022). *Documenting and managing digital operational processes using collaborative tools: Practices in enterprise IT*. Information Systems Journal, **32**(4), 671–690. https://doi.org/10.1111/isj.12355

Spinellis, D. (2018). *The importance of being documented*. IEEE Software, **35**(1), 20–23. https://doi.org/10.1109/MS.2018.2801545

St. Laurent, A. M., & Meeker, R. (2021). *Understanding open source and free software licensing: A guide to compliance*. O'Reilly Media.

Answer Key with Explanations

1. **What is the primary goal of version control systems like Git or Subversion?**
   Answer: c. To track and manage changes over time
   Explanation: Version control systems are designed to manage changes to code and files, enabling collaboration and rollback if needed.
2. **Which of the following best describes software installation?**
   Answer: b. The process of configuring system settings to make software operational
   Explanation: Software installation prepares applications to run by integrating them into the system and ensuring compatibility.
3. **Why is change tracking important in version control?**
   Answer: c. It allows developers to monitor and audit code changes
   Explanation: Change tracking ensures accountability by recording all modifications, supporting audits and debugging.
4. **What feature of version control allows developers to revert to a previous software state after a failure?**
   Answer: c. Rollback and recovery
   Explanation: Rollback allows systems to return to a previously stable version, minimizing downtime after errors.
5. **Which version control practice enhances productivity by allowing multiple developers to work on a project simultaneously?**
   Answer: b. Collaborative development
   Explanation: Collaborative development enables teamwork via shared repositories, branches, and pull requests.
6. **What type of license is typically bundled with hardware and is non-transferable?**
   Answer: b. OEM license
   Explanation: OEM licenses are hardware-bound and cannot be transferred, often used in pre-installed systems.
7. **Subscription licenses are commonly used in which type of platform?**
   Answer: c. Cloud-based platforms
   Explanation: Subscription models are ideal for cloud services that require constant updates and support.
8. **What is a key benefit of open-source software licensing?**
   Answer: c. Encourages community-driven development
   Explanation: Open-source licenses allow users to modify and share code, fostering innovation and collaboration.
9. **Why is it important to understand software licensing models in a professional setting?**
   Answer: b. To ensure legal compliance and effective resource use
   Explanation: Proper licensing avoids legal issues and aligns software use with organizational needs.

10. **What term refers to the written records that explain how software systems operate, including their architecture and maintenance?**
    Answer: c. Technical documentation
    Explanation: Technical documentation provides structured information about system functionality, supporting maintenance and training.
11. **Which concept involves keeping time-stamped records of user actions and system events?**
    Answer: b. Digital logbooks
    Explanation: Digital logbooks document system events chronologically, useful for audits and error tracking.
12. **Why are digital logbooks critical in high-risk industries like maritime navigation?**
    Answer: c. They help diagnose system failures and maintain legal compliance
    Explanation: In regulated industries, logs provide traceability and legal records for safety and audits.
13. **What is the main purpose of creating backups?**
    Answer: c. To prevent data loss from system failures or attacks
    Explanation: Backups are a safety measure ensuring data can be recovered after technical issues or security breaches.
14. **Which tools are commonly used to manage technical documentation and team collaboration?**
    Answer: b. GitHub Wikis and Confluence
    Explanation: These platforms support collaborative writing and document versioning for technical teams.
15. **What is the most important reason for automating backup processes in an organization?**
    Answer: b. To minimize manual input and reduce error risks
    Explanation: Automation ensures consistent backups and reduces human error, improving data protection.

Chapter 9

Introduction to ICT in Emergency and Safety Operations

In emergency or disaster scenarios, speed and response accuracy can be a matter of life and death. With advancements in technology, Information and Communication Technology (ICT) has emerged as an essential aid in the provision of timely, coordinated, and effective emergency and safety services. In this chapter, you will learn about the application of ICT during critical operations such as search and rescue operations, emergency alert systems, and safety network protocols. You will learn about real-time systems that enable smooth coordination among agencies, reliable communication networks, and technologies that can operate even under extreme and unpredictable circumstances.

Unit Learning Outcomes

By the end of this unit, you will be able to:

1. Knowledge: Define the roles and functions of ICT in various emergency and safety procedures like search and rescue systems.
2. Skills: Explain and evaluate the operation of emergency alert systems and fail-safe systems through real-life examples and simulation.
3. Attitude: Value the importance of ICT systems in saving lives and promoting safety by allowing ethical and responsible use of technology in hazardous situations.

Lesson Objectives

By the end of the lesson, you will be able to:

1. List and explain the components and their roles of ICT used in Search and Rescue (SAR) operations.
2. Explain the operating systems of emergency alarms and warning systems used in marine and industrial environments.
3. Describe how fail-safe design and redundancy procedures ensure sustained operations during system failure.
4. Evaluate ICT-enabled emergency response case studies.
5. Demonstrate the ability to analyze and recommend ICT-based solutions to emergency and safety scenarios (Terminal Objective).

Engage (Activating Prior Knowledge)

Think back to the latest news report you heard of a rescue mission or relief of a disaster. What methods did you assume were employed to find victims or organize aid? Discuss and pair up all the ICT systems and tools you can think of. Now, map out how you believe those systems contributed to the event. Prepare to discover how close you were as we lead you through the ICT world of safety operations.

Lesson Introduction

As future professionals in maritime, engineering, or emergency response, you should be aware of how ICT facilitates emergency and safety operations. Your ability to learn, assess, and implement such technologies complements the Philippine Professional Standards for Teachers (PPST) Domain 3 (Diversity of Learners) and Domain 4 (Curriculum and Planning) that focus on preparing the learners for actual challenges. This lesson will prepare you for that very important role of maintaining safety and efficiency in emergency response through innovative technology.

Explore (Lesson Inputs)

Emergency situations require rapid, integrated, and effective responses—where failure or delay can have catastrophic consequences. In such dangerous environments, Information and Communication Technology (ICT) is the cornerstone of modern emergency and safety programs. This section addresses the core ICT applications that make emergency response systems faster, smarter, and safer. From search and rescue missions to auto-triggered alerting and fail-safe system designs, ICT is a life-changing driving force in saving lives and resources. Let us explore three underlying ICT concepts that form the core of emergency and safety programs: Search and Rescue (SAR) Systems, Emergency Alarms and Alerting Technologies, and Fail-Safe and Redundancy Protocols.

Role of ICT in Search and Rescue (SAR) Operations

Search and Rescue (SAR) operations leverage advanced ICT tools such as Global Positioning Systems (GPS), satellite communication, drones, and Geographic Information Systems (GIS) to locate and recover people in distress. SAR systems typically leverage real-time location tracking, geospatial data, and interoperable communications networks to enable effective command and rescue group coordination. Molina (2019) indicates that the use of ICT in SAR operations has significantly reduced reaction times and rates of rescue success by enabling faster detection of distress signals and victim location. More recent advances include the use of unmanned aerial vehicles (UAVs) with thermal imaging sensors and AI-based detection to enhance performance in low-visibility environments (Kim & Park, 2022). The International Maritime Organization (IMO) has also mandated AIS (Automatic Identification System) and EPIRBs (Emergency Position Indicating Radio Beacons), which transmit location data through satellites, even if other lines of communications are unavailable (Li & Wang, 2021). These technologies not only make SAR operations faster but also more accurate and life-saving.

Table 1. Concepts of ICT in Search and Rescue (SAR) Operations)

Concept	Description	Explanation
Global Positioning System (GPS)	A satellite-based navigation system that provides location and time information in all weather conditions, anywhere on Earth.	GPS in SAR operations allows responders to identify the precise location of stranded victims, shortening search time and improving survival chances. It also allows tracking of rescuers and equipment, improving team coordination. (Molina, 2019)
Satellite Communication	A form of wireless communication that uses satellites to relay signals from one point on Earth to another.	Satellite communication offers persistent connectivity to distant or disaster areas where there is no terrestrial network. It is essential that during SAR operations, persistent communication with command bases and real-time feedback is received. (Li & Wang, 2021)
Drones (UAVs) with Thermal and AI	Unmanned aerial vehicles equipped with thermal sensors and artificial intelligence algorithms for aerial surveillance and object detection.	Thermal drones can also detect missing individuals' body heat signatures in darkness or under heavy atmospheres. With AI, the drones can survey search sites at high velocity, reducing human mistakes, and accelerating rescue efforts. (Kim & Park, 2022)

Geographic Information Systems (GIS)	A framework for gathering, managing, and analyzing spatial and geographic data.	GIS improves SAR by producing detailed maps, search area models, and terrain analysis to guarantee the best rescue planning. GIS allows responders to visualize complex spatial data to improve decision-making and operational safety. (Kim & Park, 2022)
AIS and EPIRBs	AIS (Automatic Identification System) tracks vessel positions, while EPIRBs (Emergency Position Indicating Radio Beacons) transmit distress signals with location data via satellite.	These marine communication systems are critical to ships to enhance maritime safety. During emergencies, AIS and EPIRBs ensure distress signals are received by rescue authorities even when onboard communications fail. This technology is critical in enabling timely and accurate SAR response on the ocean. (Li & Wang, 2021)

The use of ICT in Search and Rescue (SAR) operations has revolutionized emergency response as it is now faster, more accurate, and coordinated. GIS and GPS technologies facilitate accurate and detailed location tracking and mapping, allowing rescuers to move with ease across rough terrain. Satellite communication and AI-driven drones facilitate reliable connectivity and real-time situation awareness even in areas of inaccessibility or hostile environments. AIS and EPIRB devices ensure maritime distress messages are received even when other systems fail. These technologies not only improve SAR operations to become efficient and safe but also show how digital innovation can save lives directly at the point of need.

Emergency Alarms and Alerting Systems

Emergency alarm and alerting systems are critical ICT infrastructures designed to instantly warn people and agencies of actual or potential threats. Examples include fire alarms, General Alarm Systems (GAS), the Global Maritime Distress and Safety System (GMDSS), SMS alerts, public address, and application alerts. Modern emergency alerting systems integrate multiple communication channels, ensuring messages are delivered to the largest number of recipients within the shortest time. Fernandez et al. (2023) observe that modern systems are adopting multi-platform strategies—transmitting concurrent alerts via mobile networks, radio, and the Internet to provide communication redundancy. GMDSS, for instance, allows ships at sea to directly communicate with coastal rescue centers and other distressed ships, improving situational awareness and coordination (Li & Wang, 2021). AI and IoT technology are also enabling predictive alarms, detecting anomalies before disaster, and allowing pre-emptive action (Ahmed et al., 2020). These new technologies reflect the alarm system's role in proactive risk management and emergency preparedness.

Table 2. Key Concepts in Emergency Alarms and Alerting Systems

Concept	Description	Explanation
General Alarm Systems (GAS)	General Alarm Systems are safety mechanisms used to alert all personnel in a facility or ship about emergencies such as fire, flooding, or collision through standardized audible and visual signals.	These systems are critical for real-time communication in case of emergencies to reduce response time and enable speedy evacuation or response. Technological advancements have introduced electronic integration with central control panels enabling automated notifications and system checking for enhanced safety assurance (Li & Wang, 2021).
Global Maritime Distress and Safety System (GMDSS)	GMDSS is a standardized international communication system designed for maritime use, which sends distress signals via satellite or terrestrial radio communication.	GMDSS plays an important role in global maritime safety by automatic transmission of distress, reporting of position, and rescue and coastal station communication. Redundancy and automation by the GMDSS guarantee uninterrupted communication even in the event of primary equipment breakdown, and hence it is an essential component of modern maritime operations (Li & Wang, 2021).
SMS and Mobile App-Based Alerts	These are location-based emergency alert systems delivered through text messages or mobile applications, often used for natural disasters, accidents, or public safety threats.	SMS and application-based alerts give timely public alerting to large geographic areas. Their widespread coverage and quick action because of their ability to spread information quickly via mobile networks and the internet make them effective instruments in today's emergency response systems (Fernandez et al., 2023).
Public Address and Voice Alarm (PAVA) Systems	PAVA systems are electronic sound systems that deliver pre-recorded or live emergency instructions in public spaces or large facilities.	Such systems play an essential role in managing orderly evacuations and public safety messages. The use of digital voice processing, speaker zoning, and networking in systems enables the deployment of more stable, clearer, and directional messaging

		in case of an emergency. Their integration in ICT safety infrastructure enables rapid mass messaging in advanced environments like malls, ships, and airports (Ahmed et al., 2020).
AI and IoT-Powered Predictive Alarms	These alarms utilize real-time data from sensors and analytics powered by Artificial Intelligence and the Internet of Things to detect early warning signs of potential hazards.	Predictive alarm systems enhance preparedness for emergencies by anticipating failure or change prior to its occurrence. Predictive alarm systems track temperature changes, gas leaks, or mechanical stress and then alert responsible persons. Their application has been shown to greatly enhance the avoidance of risks, especially where safety systems that take initiative are required (Kim & Park, 2022).

This lesson addresses the role of ICT-based alarm and alert systems in emergency response management on land and at sea. Students understand how systems such as GMDSS, PAVA, and AI predictive alarms enhance real-time communications, reduce casualties, and provide operational safety. Knowledge of the operations and technical basis of each system prepares future professionals to analyze, use, or design safety systems in their future careers

Fail-Safe Design and Redundancy Protocols

Fail-safe design and redundancy procedures are system engineering techniques guaranteeing uninterrupted operation or safe shutdown on component failure. ICT safeguards are especially critical in safety and emergency situations where any disruption could risk lives. Fail-safe systems are designed to fall back to a safe state in case of failure—e.g., shutting valves automatically or switching to batteries. Redundancy is the duplication of critical system components like servers, power supplies, and communication networks to prevent single points of failure. Ahmed et al. (2020) observe that application of redundancy on emergency control systems greatly enhances reliability, e.g., in high-risk industries like maritime navigation and aviation. Recent studies also cite the application of cloud computing and edge computing within redundancy structures to provide scalability and availability of data even during outages (Kim & Park, 2022). Not only do these design principles safeguard data and hardware, but they also ensure emergency processes continue under all circumstances, forming the cornerstone of resilient safety infrastructure.

Table 3. Concepts of Fail-Safe Design and Redundancy Protocols

Concept	Description	Explanation
Fail-Safe Design	A system engineering	Fail-safe design offers a scenario where systems behave safely during

	approach where equipment is designed to default to a safe state during failure.	failures, for example, by shutting down critical components, having backup systems, or triggering emergency alarm signals. The method minimizes risk and keeps the situation contained, particularly where high-risk undertakings such as marine and industrial operations are concerned. (Ahmed, Hussain, & Shah, 2020)
Redundancy Protocols	The duplication of critical components to maintain system operation during faults or failures.	Redundancy offers system robustness in the form of spare units or systems to replace the failing primary element. It is essential in ICT-based emergency systems such as data centers, navigation systems, or safety-critical networks where reliability and availability are not negotiable. (Kim & Park, 2022)
Single Point of Failure Elimination	The design strategy that removes individual failure points that can bring down an entire system.	SPOF elimination involves workload redistribution, the inclusion of redundant hardware, and network path planning to avoid total shutdowns. In mission-critical systems, the process improves the system resiliency by making it such that no failure causes the system to shut down entirely. (Li & Wang, 2021)
Cloud and Edge Computing for Resilience	The use of distributed computing systems to improve operational continuity and data accessibility.	Cloud computing provides centralized data processing and backup, while edge computing provides local processing close to data sources. In the event of a crisis, this hybrid infrastructure provides for continued functionality even when parts of the network are being attacked. It greatly improves data availability, system redundancy, and response time. (Kim & Park, 2022)
Emergency Power Backup Systems	Power systems like UPS and generators that automatically supply electricity during outages.	These stand-by systems are crucial in providing continuous operation of ICT equipment such as alarms, communication servers, and monitoring devices when there is a power outage. They are automatically activated on failure of the main supply, without any interruption in emergency steps which could prove to be crucial in saving lives. (Ahmed,

		Hussain, & Shah, 2020)

The Fail-Safe Design and Redundancy Protocols topic highlights the pivotal importance of ICT engineering to offer safety and functionality in the event of an emergency. Through the study of fundamental concepts like fail-safe mechanisms, redundancy protocols, cloud and edge computing deployment, students have an in-depth understanding of how systems are designed to function intelligently under pressure. Such design practices ensure that emergency systems do not fail under a single point of failure but instead engage safe alternates that save life, equipment, and communication lines. Through evolving practices and technologies like SPOF elimination and emergency power backup, students understand the actual use of ICT in developing resilient infrastructure that supports life-saving operations.

Explain

For this activity, create a Frayer Model for the following vocabulary words:
Back
Tape
• Search and Rescue (SAR)
• Emergency Alert Systems
• Fail-Safe Design
•Redundancy Protocols
In all models, define each term, include characteristics, examples, and non-examples. Finally, synthesize your knowledge in one-paragraph synthesis for each term. You may collaborate in mind maps or Smart Art diagrams to show relations between the ideas.

Elaborate/Extend (Application)

You belong to a team that must ensure a communications system on a ship operates in emergencies even when the main server fails. From what you have studied in redundancy protocols, recommend a layer ICT system design with redundant processes, alarm systems, and power supply alternatives. Describe how your system will work during complete power or network failure.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. **What is the primary function of GPS in Search and Rescue (SAR) operations**?
   a. Providing voice instructions to rescue teams
   b. Mapping terrain features for navigation
   c. Pinpointing the location of individuals in distress
   d. Broadcasting emergency alerts to the public
2. **Which technology enables heat-based detection of individuals in low-visibility environments during SAR?**
   a. EPIRBs
   b. Drones with thermal imaging
   c. GMDSS radios
   d. Public address systems

3. **What system is used to send maritime distress signals even when other communication systems fail?**
   a. GMDSS
   b. GSM
   c. IoT sensor networks
   d. CCTV
4. Which concept describes having duplicated system components to **maintain operations during failures?**
   a. Data analytics
   b. GIS
   c. Redundancy protocols
   d. Predictive maintenance
5. **Which of the following is an example of a fail-safe response?**
   a. A backup generator overheats and shuts down
   b. A sensor reroutes data to the cloud
   c. A system automatically shuts down in a secure mode during failure
   d. A map updates after a network reboot
6. **What is the purpose of EPIRBs in maritime emergencies?**
   a. To control navigation lighting systems
   b. To broadcast GPS data via terrestrial radio
   c. To relay distress signals via satellite
   d. To monitor ocean temperatures
7. **Which ICT system creates and analyzes spatial maps to optimize SAR operations?**
   a. GMDSS
   b. GIS
   c. GAS
   d. PAVA
8. **How do mobile app-based alerts improve emergency communication?**
   a. By transmitting data through satellite relays only
   b. By sending alerts to landline phones
   c. By delivering fast, location-based notifications
   d. By using analog signals for broader reach
9. **What does eliminating a single point of failure (SPOF) ensure?**
   a. That power consumption is minimized
   b. That one failure won't crash the entire system
   c. That system settings are saved
   d. That alarms are always silent
10. **Which of the following enhances emergency readiness using real-time sensor data and AI?**
   a. Manual safety reports
   b. SMS broadcast systems
   c. Predictive alarm systems
   d. Satellite tracking only

11. What technology enables unmanned aerial vehicles (UAVs) to locate missing persons effectively?
a. Radio signals
b. AI-driven image analysis and thermal sensors
c. Manual visual spotting
d. SMS location alerts

12. What is the function of General Alarm Systems (GAS) aboard ships?
a. Sending weather forecasts
b. Guiding navigation routes
c. Alerting crew to emergencies using lights and sound
d. Managing fuel consumption

13. How do cloud and edge computing support fail-safe and redundancy **design**?
a. By increasing noise filtration
b. By enabling data processing and access even during network failures
c. By powering offline GPS trackers
d. By replacing manual safety checks

14. What makes GMDSS a reliable emergency tool for ships?
a. It is always online and uses Bluetooth
b. It works only in ports and harbors
c. It can automatically send location-based distress alerts
d. It relies on printed instructions

15. What is the purpose of PAVA (Public Address and Voice Alarm) systems?
a. Tracking supply inventory
b. Broadcasting pre-recorded or live emergency instructions
c. Sending mobile app alerts
d. Enhancing radar signal quality

Reflection

How has your own thinking about emergency ICT use been impacted by the completion of this lesson? Can you now see yourself as the kind of person who would specify or deploy such systems? Think about what specific knowledge or insight this lesson gave you in getting you ready for your future professional life in safety-critical settings.

Unit Summary

This chapter underscored the revolutionary role of ICT in emergency and safety operations, particularly in Search and Rescue (SAR), emergency alert systems, and fail-safe and redundancy schemes. It stressed that with proper ICT infrastructure, people can be saved, communication is not interrupted, and operations can proceed uninterruptedly even in the event of a disaster. As future professionals, knowing these systems prepares you to be an integral part of saving lives and assets in critical situations.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 9

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application

	of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Explains the role of ICT in emergency and safety operations										
2. Identifies key technologies used in Search and Rescue (SAR) systems										
3. Describes how GPS and GIS enhance emergency response										
4. Differentiates between traditional and AI-enhanced alarm systems										
5. Evaluates the effectiveness of GMDSS in maritime communication										
6. Demonstrates understanding of fail-safe system design principles										
7. Describes redundancy protocols and their application in ICT systems										
8. Analyzes the impact of cloud and edge computing on system resilience										
9. Identifies types and functions of emergency alarms and alerting systems										
10. Recognizes the importance of predictive technologies in risk management										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Ahmed, R., Hussain, M., & Shah, M. (2020). *A fault-tolerant framework for safety-critical ICT systems in emergency environments*. *International Journal of Critical Infrastructure Protection, 30*, 100392. https://doi.org/10.1016/j.ijcip.2020.100392

Fernandez, A., Rojas, M., & Nguyen, L. (2023). *Integrated emergency alert systems: A comparative study of multi-platform communication strategies*.

Journal of Emergency Management, 21(2), 84–92. https://doi.org/10.5055/jem.2023.0598

Kim, J., & Park, S. (2022). *Redundancy and fail-safe design in ICT-supported emergency management: The role of cloud and edge computing. Computers in Industry, 141*, 103744. https://doi.org/10.1016/j.compind.2022.103744

Li, H., & Wang, Y. (2021). *Modernizing maritime safety: AIS, EPIRBs, and the GMDSS framework. Ocean Engineering, 233*, 109183. https://doi.org/10.1016/j.oceaneng.2021.109183

Molina, D. (2019). *ICT integration in search and rescue operations: Enhancing efficiency through geospatial technologies. Journal of Search and Rescue Technology, 5*(1), 33–45. https://doi.org/10.1016/j.jsrt.2019.05.004

Answer Key with Explanations

1. **What is the primary function of GPS in Search and Rescue (SAR) operations?**
   Answer: c. Pinpointing the location of individuals in distress
   Explanation: GPS helps responders quickly locate people in emergencies, reducing search time and improving rescue chances.
2. **Which technology enables heat-based detection of individuals in low-visibility environments during SAR?**
   Answer: b. Drones with thermal imaging
   Explanation: Thermal drones detect body heat, allowing SAR teams to locate people even in darkness or dense areas.
3. **What system is used to send maritime distress signals even when other communication systems fail?**
   Answer: a. GMDSS
   Explanation: The Global Maritime Distress and Safety System ensures distress calls reach rescue centers via satellite and radio.
4. **Which concept describes having duplicated system components to maintain operations during failures?**
   Answer: c. Redundancy protocols
   Explanation: Redundancy duplicates critical parts like servers and power to ensure systems stay operational during faults.
5. **Which of the following is an example of a fail-safe response?**
   Answer: c. A system automatically shuts down in a secure mode during failure
   Explanation: Fail-safe design ensures systems default to a safe state when something goes wrong.
6. **What is the purpose of EPIRBs in maritime emergencies?**
   Answer: c. To relay distress signals via satellite
   Explanation: EPIRBs transmit a vessel's location and distress signal to satellites for faster rescue coordination.

7. **Which ICT system creates and analyzes spatial maps to optimize SAR operations?**
   Answer: b. GIS
   Explanation: Geographic Information Systems (GIS) help map terrain, locate individuals, and plan efficient rescue paths.
8. **How do mobile app-based alerts improve emergency communication?**
   Answer: c. By delivering fast, location-based notifications
   Explanation: App-based alerts reach users instantly and target specific locations, increasing their effectiveness.
9. **What does eliminating a single point of failure (SPOF) ensure?**
   Answer: b. That one failure won't crash the entire system
   Explanation: Removing SPOFs makes systems more resilient by avoiding total shutdown from a single fault.
10. **Which of the following enhances emergency readiness using real-time sensor data and AI?**
    Answer: c. Predictive alarm systems
    Explanation: These systems analyze live data to anticipate problems and trigger alarms before hazards occur.
11. **What technology enables unmanned aerial vehicles (UAVs) to locate missing persons effectively?**
    Answer: b. AI-driven image analysis and thermal sensors
    Explanation: AI and thermal imaging allow UAVs to find heat signatures and spot people quickly and accurately.
12. **What is the function of General Alarm Systems (GAS) aboard ships?**
    Answer: c. Alerting crew to emergencies using lights and sound
    Explanation: GAS provides standardized audio and visual alerts to signal emergencies and prompt evacuation or action.
13. **How do cloud and edge computing support fail-safe and redundancy design?**
    Answer: b. By enabling data processing and access even during network failures
    Explanation: Cloud and edge systems maintain operations and data availability during outages by distributing processing.
14. **What makes GMDSS a reliable emergency tool for ships?**
    Answer: c. It can automatically send location-based distress alerts
    Explanation: GMDSS automates emergency communications, ensuring help is alerted with accurate location data.
15. **What is the purpose of PAVA (Public Address and Voice Alarm) systems?**
    Answer: b. Broadcasting pre-recorded or live emergency instructions
    Explanation: PAVA systems deliver clear verbal instructions to guide evacuations and actions during crises.

Chapter 10

Introduction to Future Trends and Regulatory Frameworks

Welcome aboard the future of maritime technology. In this new and exciting era, we will navigate beyond the traditional limits of navigation into a world where vessels are not just smart but smart enough to make decisions, detect failures, and model their own operations. With digital twin technology, artificial intelligence, and machine learning becoming increasingly prominent, vessels of today are becoming advanced digital ecosystems. As future maritime professionals, you need to prepare yourselves to navigate this digital overhaul with knowledge, confidence, and flexibility. This chapter also discusses how global maritime legislations like IMO, STCW, and SOLAS are adapting to these technologies. Be it to take charge of operating a smart ship or ensuring safety compliance, this unit will inspire you to be a forward-thinking seafarer of 21st-century skills and global standards.

Unit Learning Outcomes
By the end of this unit, you will be able to:

1. Exemplify in-depth understanding of new maritime technologies like digital twins, artificial intelligence, and machine learning.
2. Apply analytical and decision-making skills in digital ship operations and regulatory matters.
3. Demonstrate a positive and ethical way of accommodating technological change consistent with international maritime law and best practices.

Lesson Objectives
By the end of the lesson, you will be able to:

1. Define and identify digital twin technology, artificial intelligence, and machine learning at sea key concepts.
2. Explain the importance and applications of these technologies in ship management and operation.
3. Define IMO, STCW, and SOLAS in the context of integrating computer systems.
4. Study actual maritime cases with intelligent ships and recommend actions in line with international standards.Design a simulated solution to a maritime operational challenge using knowledge of digital systems and regulatory frameworks.

Engage (Activating Prior Knowledge)

Let's begin with a little exercise: You're on a next-gen ship with computer systems that duplicate the ship's entire function in real-time. What do you envision your job as a future officer or engineer would be? Sit down in a pair of twos and write out as many things as you can that a smart ship might be able to do for you—and what you would still have to do as a human on the ship.

Lesson Introduction

With the shipping sector rapidly embracing automation, sustainability, and digitalization, the ability to adapt and work with new technology becomes a part of each seafarer's role. In this lesson, not only will you learn the technicalities of smart ships and intelligent systems but also how to put global maritime regulations to responsible use to make shipping safe, ethical, and future-proof. This meets the PPST content knowledge and pedagogy area to enable you to lead and mentor others in the evolving world of shipping.

Explore (Lesson Inputs)

As the maritime industry accelerates towards digitalization, it is crucial to learn the technologies and frameworks supporting the revolution as part of professional readiness. This section explores three prominent concepts—Digital Twin Technology and Smart Ships, AI and Machine Learning at Sea, and IMO, STCW, and SOLAS Guidelines on Digital Systems—that are revolutionizing the maritime operational future. Each concept enlightens on how seafarers, engineers, and maritime executives must prepare to face innovations while maintaining security, compliance, and efficiency with the digital revolution.

Digital Twin Technology and Smart Ships

Digital twin technology involves the development of a virtual twin that replicates the physical ship's systems to enable real-time monitoring, simulation, and predictive maintenance. Applied in the shipping industry, digital twins enhance performance, anticipate breakdowns, and maximize planning and training. The digital models are employed in smart ships in combination with embedded sensor networks and control systems. The digital twin methodology maximizes fault detection and operational performance considerably, Coraddu et al. (2020) observed. Zhang and Zheng (2023) observed how smart ships automatically route plan, monitor fuel use, and offer safety compliance through AI-based feedback loops.

Table 1. Digital Twin Technology and Smart Ships

Concept	Description	Explanation
Digital Twin Technology	A virtual replica of a ship’s physical systems, enabling real-time monitoring, simulation, and optimization.	Digital twin technology creates a coordinated virtual environment reflecting ship operations in the physical world. Digital twin technology uses onboard sensor data and computational models to predict and simulate system performance, reducing downtime and enhancing operation accuracy. The approach enables fault detection ahead of disrupting operations and enables enhanced decision-making during the life cycle of the vessel (Coraddu, Oneto, & Anguita, 2020).
Smart Ships	Ships that utilize interconnected systems, AI, and automation to manage operations, safety, and navigation autonomously or semi-autonomously.	Smart ships are also equipped with advanced digital infrastructure, including AI, big data analysis, and autonomic control systems. Such technologies enable ships to react to changes in operations, improve routes, and monitor onboard conditions in real time. Therefore, smart ships streamline operations, conserve fuel, and increase compliance with safety in more complex maritime environments (Zhang & Zheng, 2023).
Predictive Maintenance	A maintenance approach that anticipates equipment failure using data analytics and machine learning.	Predictive maintenance utilizes machine learning algorithms and real-time sensor readings to foresee potential equipment breakdown and allow for maintenance before failure (Chae, Park, & Yeo, 2021).

		When coupled with digital twins, the method enhances diagnostic accuracy and reduces unscheduled downtime, making shipping safer and cheaper.
Integrated Sensor Networks	Systems of sensors embedded across ship components to collect real-time data for monitoring and decision-making.	Integrated sensor networks gather detailed information from equipment, environment, and navigation systems and input the information into the digital twin or smart control systems. Real-time data flow allows timely response to operational problems and facilitates environmental sustainability through expanded monitoring capability (Yu & Lee, 2022).
Simulation and Training	Use of digital replicas for immersive, scenario-based maritime training and system testing.	Digital twins offer an immersive setting for seafarers' training under simulated operating conditions closely mirroring real maritime challenges. Decision-making abilities are improved with the simulations, which reduce training risks and respond to shifting regulation requirements favoring digital skills in modern seafaring (International Maritime Organization [IMO], 2021).

This course offers students an overview of digital twin technology and intelligent ship operation, observing how the technologies transform maritime practice. Through predictive maintenance case studies, sensor fusion, and simulation-based training, students are able to relate new technologies with real-world applications at sea. The subjects prepare students for a career in the maritime sector, where digital literacy and operations adaptability are required to run intelligent ships and comply with international safety and environmental standards.

AI and Machine Learning at Sea

Artificial intelligence (AI) and machine learning (ML) allow ships to make smart decisions, ranging from cargo handling to collision avoidance. Machine learning algorithms can predict mechanical failures, improve route planning, and even regulate onboard energy management (Chae et al., 2021). Yu and Lee (2022) argued that AI predictive analytics play a critical role in pushing maritime logistics towards cleaner and autonomous systems. AI application also allows eco-efficient maritime operations in accordance with global climate pacts.

Table 2. Concepts of AI and Machine Learning at Sea

Concept	Description	Explanation
Predictive Maintenance	The use of AI to monitor equipment conditions and forecast mechanical failures.	Predictive maintenance utilizes machine learning algorithms to scan ship sensors' data, such as vibration, temperature, or fuel consumption. Predictive maintenance detects anomalies that predict impending breakdowns, allowing engineers to react beforehand, hence reducing unplanned downtime as well as improving safety of operation (Chae et al., 2021).
Autonomous Navigation	Navigation systems powered by AI that interpret sensor data and make real-time routing decisions without human intervention.	Autonomous navigation systems utilize AI to integrate GPS, radar, LIDAR, and camera information to enable ships to avoid collisions and make optimal route choices. They learn from environmental conditions and experience over time to make more informed decisions in the future, enabling safer and more efficient journeys (Zhang & Zheng, 2023).
Voyage Optimization	AI systems that compute the most efficient routes based on weather, fuel use, and sea conditions.	Machine learning algorithms sort out past and real-time information on currents, weather, and ship performance to recommend fuel-efficient routes. Lowering fuel consumption and the accuracy of arrival times, voyage optimization is a key driver of maritime logistics sustainability and cost saving (Yu & Lee, 2022).
Cargo and Energy Management	AI-assisted systems for efficient cargo loading and onboard power distribution.	Smart systems manage stowage planning and the deployment of containers to maximize vessel loading and avoid damage. They manage and regulate energy consumption in real-time, maximizing fuel efficiency and reducing emissions. AI technologies of this type are vital to smart ship operations initiatives aiming at environmental and operational sustainability (Kwon & Kim, 2020).
Decision Support Systems (DSS)	Tools that integrate and analyze operational data to assist crew in	Artificial intelligence-supported decision-making systems gather data from shipboard systems to offer actionable recommendations. They

	making informed decisions.	reduce cognitive workload for crew, enhance response time during emergencies, and aid in strategic planning in navigation and maintenance, guaranteeing safe and efficient ship operation (IMO, 2021).

The intersection of artificial intelligence and machine learning in sea operations marks a paradigm change in ship management, navigation, and maintenance. From predicting mechanical failure and optimizing voyages to enabling autonomous navigation and efficient cargo handling, AI technologies are revolutionizing every aspect of seafaring. AI solutions enhance safety, reduce operating costs more effectively, and ensure environmental responsibility by being sensitive to global maritime goals. With shipping becoming increasingly digitalized day by day, understanding and implementing these AI concepts will help future generations of maritime professionals become smarter, safer, and more sustainable in a rapidly evolving industry.

IMO, STCW, SOLAS Guidelines on Digital Systems

The International Maritime Organization (IMO), in conventions like SOLAS (Safety of Life at Sea) and STCW (Standards of Training, Certification, and Watchkeeping), is actively embracing digital innovation in regulations. Recent amendments now encompassed cybersecurity awareness, electronic chart display training, and familiarization with automation systems. For IMO (2021), digitalization is required to maintain maritime security, human control, and environmental safety. Kwon and Kim (2020) highlighted that although AI maximizes efficiency, human-oriented regulations are still vital to provide accountability and security at sea.

Table 3. Concepts Under IMO, STCW, and SOLAS Guidelines on Digital Systems

Concept	**Description**	**Explanation**
Digitalization in Maritime Safety (IMO)	The IMO encourages the integration of digital technologies to enhance maritime safety, security, and environmental performance.	Technologies such as e-navigation, electronic logbooks, and intelligent reporting systems maximize efficiency and reduce human mistakes. The IMO, nonetheless, regrets that despite as much as digital innovation is promoted, human judgment should not be overpowered. The systems are designed to augment, and not replace, seafarers' judgment in critical situations (IMO, 2021).
Cybersecurity Awareness (STCW	The STCW Convention now includes	As vessels become the center of digital networks, threats intensify. Crews are trained to identify

Amendment)	cybersecurity training as part of crew certification to protect maritime systems from cyber threats.	cyber threats, apply countermeasures, and respond to intrusions. This regulatory adjustment protects vessels from intrusions that can compromise data integrity as well as physical security (Kwon & Kim, 2020).
Electronic Chart Display and Information System (ECDIS)	ECDIS is a digital navigation tool mandated by IMO, replacing traditional charts and improving navigational precision.	Officers must be trained to operate ECDIS equipment, through which route planning and situation awareness are facilitated. ECDIS equipment offers real-time data and AIS and radar integration but requires constant updating and training to avoid overreliance and navigational safety (Chae, Park, & Yeo, 2021).
Automation and Remote Operation Familiarization	SOLAS addresses the growing use of automation and remote monitoring systems in engine, cargo, and bridge operations.	Automation improves operation efficiency and reduces manual effort but at the cost of new risks. Mariners must be trained to monitor and step in as needed in automated operations. This is a balance of human accountability and technological support (Yu & Lee, 2022).
Digital Competence in Watchkeeping	STCW now includes digital competence requirements for monitoring and operating automated bridge and safety systems.	The staff ought to be proficient in servicing, reading, and operating electronic monitors and alarms. The task of the watchkeeper today is not just vigilant observation but also digital interpretation and systems know-how (Zhang & Zheng, 2023).

This lesson addresses the dynamic evolution of maritime international regulations to meet the demands of digital transformation of the sea. By learning the most important developments in IMO, STCW, and SOLAS on digital systems, students are best positioned to handle the convergence of automation, safety, and regulation. With cybersecurity, digital navigation, and automated systems embedded in international standards, seafarers are tasked with gaining technical competence as well as ethical sensibility. These guidelines ensure that as ships are becoming smarter, human responsibility, accountability, and oversight remain at the forefront of maritime operations.

Explain

Now, write down in your own definition the following major terms: Digital Twin, Artificial Intelligence, Machine Learning, IMO, STCW, and SOLAS. On a Frayer Model or Venn Diagram, write down their functions, similarities, and differences. Then, synthesize how these components work together in contemporary smart shipping systems through a flowchart or concept map.

Elaborate/Extend (Application)

You are responsible for operating a smart ship on an intercontinental voyage. The system detects unusual fuel consumption and sends an alert. Based on your experience of AI-based diagnostics and the IMO regulatory environment, how would you act to ensure operational safety and compliance? Submit your response as a short report.

Evaluation

Quiz Instructions:

Read each question carefully and choose the best answer. For each question, select the most appropriate response based on your understanding of the topics covered in this unit. Each question has only one correct answer. Good luck!

1. **What is the primary purpose of a digital twin in maritime applications?**
   a. To operate ships autonomously
   b. To entertain seafarers
   c. To mirror physical systems for monitoring and optimization
   d. To replace human decision-making entirely
2. **Which of the following best describes a smart ship?**
   a. A ship that requires no crew
   b. A ship using paper-based navigation
   c. A ship that uses AI and digital systems for autonomous operations
   d. A ship designed only for military use
3. **How does predictive maintenance benefit maritime operations?**
   a. It encourages more frequent breakdowns
   b. It eliminates the need for training
   c. It anticipates equipment failure to prevent downtime
   d. It removes the need for spare parts
4. **Integrated sensor networks in ships are primarily used to:**
   a. Entertain passengers
   b. Monitor and collect real-time operational data
   c. Provide free internet access
   d. Reduce cargo space
5. **What is one key use of digital twins in training?**
   a. To train fishery workers
   b. To replace seafarers with AI
   c. To simulate real-life maritime scenarios
   d. To produce paper maps
6. **Which AI application allows ships to avoid collisions and choose optimal routes?**
   a. Cargo optimization
   b. Autonomous navigation
   c. Cybersecurity
   d. Simulation modeling
7. **Voyage optimization helps the maritime industry by:**
   a. Ignoring environmental concerns
   b. Increasing fuel usage

c. Reducing efficiency
d. Suggesting energy-efficient routes

8. What role does AI play in cargo and energy management?
a. Loads passengers randomly
b. Adjusts lighting on deck
c. Monitors power distribution and stowage efficiently
d. Provides entertainment content

9. Decision Support Systems (DSS) are used to:
a. Paint the ship hull
b. Assist crews with data-driven decisions
c. Avoid all forms of technology
d. Control crew behavior

10. What is the role of the IMO in maritime digitalization?
a. Building ports
b. Funding ships
c. Establishing safety and environmental standards
d. Designing crew uniforms

11. Which digital tool has replaced traditional paper charts in navigation?
a. GPS tracker
b. ECDIS
c. Wi-Fi receiver
d. Manual compass

12. Why has STCW included cybersecurity awareness in training requirements?
a. To increase ship speed
b. To protect digital systems from cyber threats
c. To monitor passenger emails
d. To eliminate manual steering

13. What must officers do to use ECDIS effectively?
a. Avoid digital training
b. Use only traditional maps
c. Be certified and trained regularly
d. Ignore system updates

14. According to SOLAS, why must seafarers be trained in automation systems?
a. To sleep during operations
b. To rely fully on the computer
c. To intervene when automation fails
d. To avoid manual work completely

15. What is emphasized in the STCW regarding digital watchkeeping?
a. Watching movies during shifts
b. Avoiding digital tools
c. Interpreting and managing electronic systems
d. Ignoring alarms and alerts

Reflection

What do you envision your shipping career to be like with the emergence of intelligent shipping and digitalization? Are you challenged, excited, or threatened by these technologies? Consider how this lesson led you to appreciate the interdependence of innovation and ethical ship management.

Unit Summary

This chapter provided an in-depth overview of future maritime operations through digital twin technology, artificial intelligence, and machine learning. This chapter briefly mentioned how regulatory organizations worldwide such as IMO, STCW, and SOLAS are evolving to fulfill the safety needs and ethical implementation of such technology. This awareness allows students to develop critical thinking, technological skills, and regulatory knowledge—skills necessary for defining the shipping sector in the future.

Activity Sheet
Pre- and Post-Competency Checklist of Chapter 10

Instructions for Use
Pre-Service Teachers
Mark the column that best represents your current level of agreement with each competency statement. Use this table as a self-assessment tool to identify areas of strength and areas for growth.

Instructors/Evaluators
Use this table to rate each pre-service teacher's competencies before and after the educational program. This will help in tracking progress and providing targeted support.

Competency Ratings

	Competency Level
1(Strongly Disagree)	Lacks Competency Demonstrates a significant lack of proficiency or understanding in the specific competency area. Requires substantial development and learning.
2 (Disagree)	Below Average Competency Shows below-average proficiency with noticeable areas for improvement. Additional training and experience needed.
3 (Neutral)	Basic Competency Achieves an average level of proficiency. Meets basic expectations with room for further development and refinement.
4 (Agree)	Above Average Competency Exhibits above-average proficiency with consistent application of skills and knowledge. Well-developed in the competency area but can still benefit from further growth.
5(Strongly Agree)	Exemplary Competency Displays exceptional proficiency, mastery, and application of the competency. Sets a high standard and serves as a model in the specific area.

Competencies	Self-Assessed by the Students					Assessed by the Cooperating Teacher				
	5	4	3	2	1	5	4	3	2	1
1. Identify the principles and applications of digital twin technology in ships										
2. Describe the features and functions of smart ship systems										
3. Explain the role of AI and machine										

learning in maritime operations										
4. Analyze real-time data using integrated digital systems										
5. Apply basic concepts of predictive maintenance using digital tools										
6. Interpret IMO, SOLAS, and STCW guidelines related to digital technologies										
7. Demonstrate awareness of cybersecurity risks and protections onboard										
8. Utilize ECDIS and other digital navigational tools effectively										
9. Assess the impact of automation on crew responsibilities and safety										
10. Collaborate in simulated digital shipboard operations and decision-making										
Grand Mean Score										
Total Score divided by the rating of the Student and Cooperating teacher										

References and Suggested Readings

Bala, M., & Kumar, R. (2021). Artificial intelligence and machine learning in the shipping industry: A review and future directions. Ocean Engineering, 238, 109747. https://doi.org/10.1016/j.oceaneng.2021.109747

Boulougouris, E., Hirdaris, S. E., & Papanikolaou, A. (2019). Digital twin shipbuilding and maritime applications: Trends and challenges. Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment, 233(1), 3–20. https://doi.org/10.1177/1475090218771504

International Maritime Organization (IMO). (2021). Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.1). Retrieved from https://www.imo.org/en/OurWork/Security/Pages/MaritimeCyberRisk.aspx

International Maritime Organization (IMO). (2022). E-navigation strategy implementation plan (SIP) and related updates. Retrieved from https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx

Kang, H., & Rho, S. (2022). Smart shipping: AI and IoT-enabled predictive maintenance in maritime transport. Sustainability, 14(6), 3318. https://doi.org/10.3390/su14063318

Kim, S., & Park, Y. (2020). Cybersecurity in maritime systems: STCW compliance and safety challenges. Journal of Marine Science and Engineering, 8(10), 783. https://doi.org/10.3390/jmse8100783

Kwon, O., & Kim, J. (2020). Navigating the digital seas: Human-centered regulation in the age of smart ships. Maritime Policy & Management, 47(8), 1057–1074. https://doi.org/10.1080/03088839.2020.1720140

Liang, Z., & Li, Z. (2023). A review on digital twin applications for ship lifecycle management. Journal of Marine Science and Engineering, 11(1), 75. https://doi.org/10.3390/jmse11010075

Liu, W., & Huang, Y. (2019). Autonomous ships and seafarer training: Bridging the skill gap. WMU Journal of Maritime Affairs, 18(3), 457–472. https://doi.org/10.1007/s13437-019-00180-2

Mallam, S. C., Nazir, S., & Renganayagalu, S. K. (2020). Rethinking maritime education, training, and operations in the digital era: Applications for smart shipping. Journal of Marine Science and Engineering, 8(4), 276. https://doi.org/10.3390/jmse8040276

Answer Key with Explanations

1. **What is the primary purpose of a digital twin in maritime applications?**
   Answer: c. To mirror physical systems for monitoring and optimization
   Explanation: Digital twins create a virtual model of ship systems to help monitor performance, predict issues, and optimize operations.
2. **Which of the following best describes a smart ship?**
   Answer: c. A ship that uses AI and digital systems for autonomous operations
   Explanation: Smart ships are equipped with interconnected systems, AI, and sensors to enhance automation and decision-making.
3. **How does predictive maintenance benefit maritime operations?**
   Answer: c. It anticipates equipment failure to prevent downtime
   Explanation: Predictive maintenance uses sensor data and AI to detect early signs of failure and schedule timely repairs, reducing costs and disruptions.
4. **Integrated sensor networks in ships are primarily used to:**
   Answer: b. Monitor and collect real-time operational data
   Explanation: Sensors track data such as engine status, fuel usage, and environmental conditions to support safety and efficiency.
5. **What is one key use of digital twins in training?**
   Answer: c. To simulate real-life maritime scenarios
   Explanation: Digital twins help in simulating complex conditions for crew training without the risks of actual operation.
6. **Which AI application allows ships to avoid collisions and choose optimal routes?**
   Answer: b. Autonomous navigation

Explanation: AI enables real-time route planning, obstacle detection, and course correction in smart ships.

7. **Voyage optimization helps the maritime industry by:**
   Answer: d. Suggesting energy-efficient routes
   Explanation: AI-powered voyage planning tools reduce fuel consumption and emissions by optimizing ship routing.
8. **What role does AI play in cargo and energy management?**
   Answer: c. Monitors power distribution and stowage efficiently
   Explanation: AI systems balance energy loads and cargo placement to improve fuel efficiency and ship stability.
9. **Decision Support Systems (DSS) are used to:**
   Answer: b. Assist crews with data-driven decisions
   Explanation: DSS tools provide real-time analysis to support informed decision-making in navigation, operations, and emergencies.
10. **What is the role of the IMO in maritime digitalization?**
    Answer: c. Establishing safety and environmental standards
    Explanation: The IMO ensures that digital innovations meet global safety and environmental protocols.
11. **Which digital tool has replaced traditional paper charts in navigation?**
    Answer: b. ECDIS
    Explanation: The Electronic Chart Display and Information System provides dynamic, digital navigation to replace paper charts.
12. **Why has STCW included cybersecurity awareness in training requirements?**
    Answer: b. To protect digital systems from cyber threats
    Explanation: As ship systems become more digital, training on cybersecurity ensures crews can recognize and respond to threats.
13. **What must officers do to use ECDIS effectively?**
    Answer: c. Be certified and trained regularly
    Explanation: Officers must be properly trained to interpret ECDIS data and respond to system alerts for safe navigation.
14. **According to SOLAS, why must seafarers be trained in automation systems?**
    Answer: c. To intervene when automation fails
    Explanation: Even with automation, human oversight is critical to manage errors or system malfunctions during operations.
15. **What is emphasized in the STCW regarding digital watchkeeping?**
    Answer: c. Interpreting and managing electronic systems
    Explanation: Watchkeepers must be competent in using electronic monitoring systems and responding appropriately to alerts and data.

-end-

About the Author

MONETTE DAVIDON APOR, MSME, Comp. Eng., LPT, is a licensed professional teacher with a strong academic and technical background in both computer engineering and education. He earned his Bachelor of Science in Computer Engineering from AMA Computer College in 2003 and completed a Diploma in Professional Education at Cebu Technological University in 2015. After obtaining his teaching license, he pursued graduate studies and earned his Master of Science in Management Engineering from the University of the Visayas – Main Campus in 2024.

Mr. Apor has been actively involved in maritime education since 2013, effectively combining his engineering expertise with innovative teaching practices. He holds the required instructional certifications in IMO Model Courses 6.09 (Training Course for Instructors), 3.12 (Assessment, Examination, and Certification of Seafarers), and 6.10 (Train the Simulator Trainer and Assessor).

He is duly affiliated with Cebu Technological University under the College of Maritime Sciences, where he continues to guide and mentor future professionals while contributing to the advancement of maritime education and academic excellence.

About the Editors

RONALD B. ENOC is the Founder and Owner of E-Research Publications, an international academic publishing company with operations in both the Philippines and the United States. He earned his Bachelor of Science in Secondary Education, Major in English from the International School of Asia and the Pacific. He is an accomplished publisher, book author, researcher, educator, peer reviewer, and editor with extensive experience working with journals indexed in Web of Science (WoS), Scopus, and SCI. He also served as a Data Analyst at the Knowledge and Technology Management Office of CSU. Mr. Enoc has published a diverse range of research across multiple disciplines and authored numerous books covering academic, educational, and professional topics. His research portfolio includes experimental agricultural studies utilizing Randomized Complete Block Design (RCBD), Completely Randomized Design (CRD), and Split-Plot designs with factorial analysis through Analysis of Variance (ANOVA). He is also actively engaged in book and magazine publication, academic content development, and conference speaking, particularly in online scholarly forums. Committed to advancing global scholarship, Mr. Enoc continues to mentor researchers, lead editorial and publishing initiatives, and expand opportunities for high-quality, peer-reviewed publications worldwide.

DR. MINSOWARE S. BACOLOD, PD-SML (On-going), earned his Bachelor of Secondary Education major in History from Emilio Aguinaldo College–Cavite in 2008. He completed his Master of Arts in Education major in Educational Administration & Supervision at the Philippine Christian University in 2021, and subsequently obtained his Doctor of Education major in Educational Management in 2023 at the same institution. He is presently pursuing Post-Doctoral Studies in Strategic Management and Leadership at Philippine Christian University-Manila. Dr. Bacolod’s exceptional performance and steadfast dedication to the teaching profession have earned him the distinction of “Outstanding Teacher.” His career spans both academic and administrative roles, having served as a part-time instructor at Philippine Christian University and PNTC Colleges in Dasmariñas City, Cavite.

Currently, Dr. Bacolod serves as Associate Professor at NU MOA, Pasay City, Philippines, where he is also a member of the Ethics Review Committee (ERC) and the Internal Quality Auditor Team of NU Philippines. He has previously served as Social Sciences Cluster Head and Nationalian Coordinator at NU MOA in Pasay City. In these capacities, he has imparted his extensive knowledge and expertise through the instruction of various Social Sciences courses and demonstrating strong leadership.

In addition to his academic work, Dr. Bacolod is a registered and published author/writer of National Book Development Board of the Philippines (NBDB) and other publishing platforms. He has authored and co-authored several textbooks contributing significantly to the dissemination of knowledge in his field.

Published by:

Phil-cad Academician Publishing
Block 20 Lot 7, Purok Rosal, Brgy. Datu Esmael-H1
Dasmariñas, City, Cavite, 4114, Philippines
Contact Number: 0927-7753-471
Website: www.philcadademian.com
Email Address: filcad2023@gmail.com

ABOUT THE AUTHOR

Monette Davidon Apor, MSME, Comp. Eng., LPT, is a licensed professional teacher with a strong academic and technical background in both computer engineering and education. He earned his Bachelor of Science in Computer Engineering from AMA Computer College in 2003 and completed a Diploma in Professional Education at Cebu Technological University in 2015. After obtaining his teaching license, he pursued graduate studies and earned his Master of Science in Management Engineering from the University of the Visayas – Main Campus in 2024.

Mr. Apor has been actively involved in maritime education since 2013, effectively combining his engineering expertise with innovative teaching practices. He holds the required instructional certifications in IMO Model Courses 6.09 (Training Course for Instructors), 3.12 (Assessment, Examination, and Certification of Seafarers), and 6.10 (Train the Simulator Trainer and Assessor).

He is duly affiliated with Cebu Technological University under the College of Maritime Sciences, where he continues to guide and mentor future professionals while contributing to the advancement of maritime education and academic excellence.

PHIL-CAD ACADEMICIAN PUBLISHING

0927-77-53471

https://philcadacademian.com

Block 21 Lot 22, Purok Rosal Brgy. Datu Esmael-H1, Dasmariñas City, Cavite, 4114, Philippines