Certificate in Maritime Data Analytics

Maritime Cybersecurity and Data Privacy

Access Control – Mechanism that limits who can view or use maritime information systems. Related terms: Authentication, Authorization. It enforces policies such as role-based or attribute-based controls. Example: a ship's navigation system only permits crew with valid credentials. Practical use includes restricting remote maintenance access; challenges involve balancing security with operational flexibility in harsh sea environments.

Advanced Encryption Standard (AES) – Symmetric encryption algorithm widely adopted for protecting maritime data at rest and in transit. Related terms: Key Management, Cipher. AES-256 provides strong confidentiality for vessel logs. Example: AIS (Automatic Identification System) data encrypted before cloud storage. Implementation challenges include key distribution across multi-national fleets and ensuring low latency for real-time communications.

Algorithmic Bias – Systematic error introduced by data-driven models that can affect decision-making in maritime analytics. Related terms: Machine Learning, Data Quality. Bias may arise from uneven sampling of vessel types. Practical impact: predictive maintenance alerts favor larger ships. Mitigation requires diverse data sets and continuous validation; challenges include limited access to heterogeneous maritime data.

Anti-Malware – Software designed to detect, prevent, and remove malicious code targeting shipboard networks. Related terms: Virus, Trojan. Deployed on bridge consoles to guard against ransomware. Example: a shore-based monitoring system pushes signature updates to vessels. Challenges involve limited bandwidth for updates and ensuring compatibility with legacy navigation equipment.

Application Programming Interface (API) – Set of rules that allow software components to communicate, often used to share maritime sensor data. Related terms: REST, SOAP. APIs enable third-party analytics platforms to ingest vessel performance metrics. Practical use: integrating weather services with fuel-optimization tools. Security concerns include authentication, rate-limiting, and exposure of sensitive route data.

Artificial Intelligence (AI) – Computational techniques that enable machines to perform tasks requiring human intelligence, increasingly applied in maritime risk assessment. Related terms: Neural Network, Deep Learning. AI can predict piracy hotspots from historical AIS data. Practical applications include autonomous navigation assistance. Challenges involve explainability, data privacy, and regulatory acceptance.

Authentication – Process of verifying the identity of a user, device, or system before granting access. Related terms: Multi-Factor Authentication, Credential. Common methods include passwords, smart cards, and biometric scans on ship bridges. Practical benefit: preventing unauthorized remote diagnostics. Challenges

include ensuring usability for crew under time pressure and protecting credentials from phishing attacks.

Authorization – Determination of what authenticated subjects are permitted to do within a system. Related terms: Access Control List, Role-Based Access. Example: a vessel's engine monitoring system grants read-only access to the captain but full control to the chief engineer. Implementation must reflect crew hierarchies; challenges arise from dynamic crew rotations and cross-company collaborations.

Backup and Recovery – Procedures for copying maritime data and restoring it after loss. Related terms: Disaster Recovery, Redundancy. Regular backups of voyage data recorders (VDR) to an offshore data centre ensure compliance with SOLAS. Practical concerns include encryption of backup media and bandwidth limits on satellite links. Challenges involve guaranteeing integrity of restored data after a cyber incident.

Beaconing – Technique where compromised devices periodically send signals to a command-and-control server. Related terms: Command-and-Control, C2. In a maritime context, infected navigation equipment may beacon to external attackers. Detection relies on network traffic analysis. Mitigation includes strict egress filtering; challenges include distinguishing legitimate telemetry from malicious beaconing on low-bandwidth satellite links.

Binary Exploit – Attack that leverages vulnerabilities in compiled code to execute arbitrary instructions. Related terms: Buffer Overflow, Shellcode. Example: exploiting a flaw in legacy radar software to gain root access. Practical defense includes patch management and code signing. Challenges are heightened by legacy systems that cannot be readily updated aboard vessels.

Blockchain – Distributed ledger technology that provides immutable records, increasingly explored for securing maritime supply-chain transactions. Related terms: Smart Contract, Consensus. Use case: recording cargo handover events to prevent fraud. Practical benefits include traceability; challenges involve scalability, energy consumption, and integration with existing maritime IT ecosystems.

Brute-Force Attack – Method of systematically trying all possible passwords or keys to gain unauthorized access. Related terms: Credential Stuffing, Password Cracking. Attackers may target shipboard Wi-Fi login pages. Mitigation includes account lockout policies and strong password complexity. Challenges include ensuring crew can remember complex passwords while maintaining operational efficiency.

Certificate Authority (CA) – Trusted entity that issues digital certificates for establishing secure communications. Related terms: PKI, TLS. In maritime networks, a CA signs certificates for vessel-to-shore VPNs. Practical application: enabling encrypted telemetry from engine sensors. Challenges involve managing certificates across multinational fleets and handling revocation in remote environments.

Cyber Incident Response Plan – Structured approach for detecting, containing, and recovering from cyber events. Related terms: Playbook, Forensics. Includes predefined roles for ship captain, IT officer, and shore-based security team. Practical steps: isolate affected network segment, preserve log evidence, and notify authorities. Challenges include limited on-board expertise and coordination across time zones.

Cyber Risk Assessment – Process of identifying, evaluating, and prioritizing threats to maritime assets. Related terms: Threat Modeling, Vulnerability Scan. Typically involves mapping critical systems such as ECDIS (Electronic Chart Display and Information System). Practical outcome: risk matrix guiding investment in security controls. Challenges stem from rapidly evolving threat landscape and scarce industry-wide threat intelligence.

Data Anonymization – Technique for removing personally identifiable information from maritime datasets. Related terms: Pseudonymization, De-identification. Example: stripping crew names from voyage logs before sharing with analytics partners. Practical benefit: compliance with GDPR while enabling research. Challenges include preserving data utility for performance modeling and preventing re-identification through auxiliary data.

Data Breach – Unauthorized disclosure of sensitive maritime information. Related terms: Leak, Exfiltration. Incidents may involve stolen AIS logs revealing cargo details. Practical response includes notification to regulators and affected parties. Challenges involve quantifying impact, especially when data is aggregated across multiple vessels and jurisdictions.

Data Classification – Process of categorizing maritime information based on sensitivity and required protection level. Related terms: Sensitivity Label, Confidentiality. Typical categories: public, internal, restricted, and classified. Practical use: determining encryption requirements for engine performance data. Challenges include consistent labeling across diverse stakeholders and legacy data repositories.

Data Governance – Framework of policies, standards, and responsibilities governing maritime data lifecycle. Related terms: Data Stewardship, Policy. Encompasses data quality, access, and compliance. Practical implementation includes appointing a data officer for each shipping line. Challenges arise from fragmented ownership of sensor data across ship, crew, and third-party service providers.

Data Integrity – Assurance that maritime information has not been altered in an unauthorized manner. Related terms: Hash, Checksum. Example: using SHA-256 to verify VDR recordings. Practical application: detecting tampering of AIS messages. Challenges include ensuring integrity checks can be performed on low-power devices and over intermittent satellite links.

Data Leakage Prevention (DLP) – Technologies and policies designed to prevent accidental or malicious exposure of sensitive maritime data. Related terms: Content Inspection, Endpoint Protection. DLP can block export of cargo manifests to unauthorized USB drives. Practical benefit: reducing insider threats. Challenges include defining accurate rules for diverse file formats and avoiding disruption of legitimate crew workflows.

Data Privacy Impact Assessment (DPIA) – Systematic process to evaluate privacy risks of maritime data processing activities. Related terms: GDPR, Risk Register. Required when implementing crew health monitoring on board. Practical steps: mapping data flows, identifying legal basis, and proposing mitigation. Challenges involve aligning multinational privacy regulations and obtaining crew consent in multicultural environments.

Decentralized Identifier (DID) – Self-sovereign digital identity that does not rely on a central authority. Related terms: Verifiable Credential, Blockchain. Can be used for vessel identity verification in peer-to-peer cargo exchanges. Practical advantage: reducing reliance on third-party registries. Challenges include standardization across maritime authorities and ensuring interoperability with legacy systems.

Deep Packet Inspection (DPI) – Technique for examining the content of data packets traversing a network. Related terms: Firewall, IDS. DPI can identify unauthorized protocols on a ship's satellite link. Practical use: enforcing compliance with maritime communication policies. Challenges include processing overhead on low-bandwidth connections and privacy concerns when inspecting crew communications.

Denial-of-Service (DoS) Attack – Attempt to make a maritime service unavailable by overwhelming it with traffic. Related terms: Botnet, Flood. Example: flooding a port's vessel-tracking system, causing delays. Mitigation includes traffic shaping and redundancy. Challenges are heightened by the critical nature of navigation services and limited on-board mitigation capabilities.

Digital Twin – Virtual replica of a vessel or its components used for simulation and analytics. Related terms: IoT, Simulation. Enables predictive maintenance by mirroring engine sensor data. Practical benefit: testing cybersecurity patches in a safe environment before deployment. Challenges include synchronizing real-time data over constrained satellite links and protecting the twin from cyber-theft.

Domain Name System (DNS) Security Extensions (DNSSEC) – Set of protocols that add authentication to DNS responses. Related terms: Cache Poisoning, Resolver. Secures resolution of maritime service URLs such as port authority portals. Practical implementation reduces risk of spoofed navigation updates. Challenges involve updating shipboard DNS resolvers and ensuring compatibility with legacy satellite terminals.

Endpoint Detection and Response (EDR) – Security solution that monitors and reacts to threats on individual devices. Related terms: Agent, Threat Hunting. Deployed on bridge computers to detect anomalous processes. Practical advantage: rapid containment of ransomware. Challenges include limited processing power on embedded navigation hardware and the need for continuous updates.

Encryption Key Management – Practices for generating, storing, rotating, and revoking cryptographic keys. Related terms: PKI, HSM. Essential for securing AIS data streams. Practical approach: using hardware security modules on shipboard servers. Challenges involve key distribution across vessels operating in remote regions and ensuring compliance with maritime regulatory requirements.

Enterprise Resource Planning (ERP) – Integrated software suite for managing business processes, increasingly connected to maritime data sources. Related terms: Supply Chain, Integration. ERP can ingest fuel consumption data for cost optimization. Practical risk: ERP systems become a target for cyber espionage. Challenges include securing API gateways and maintaining data segregation between commercial and operational domains.

Ethical Hacking – Authorized testing of maritime systems to uncover vulnerabilities. Related terms:

Penetration Test, Red Team. Conducted by third-party auditors on shipboard networks. Practical output: detailed remediation report. Challenges include coordinating testing schedules with vessel operations and avoiding disruption of critical navigation functions.

Federated Identity Management – System that allows a user to use a single set of credentials across multiple maritime platforms. Related terms: SAML, Single Sign-On. Enables crew to access both shipboard monitoring tools and shore-based logistics portals. Practical benefit: reduced password fatigue. Challenges involve establishing trust relationships between disparate maritime organizations and handling revocation when crew change ships.

Firmware – Low-level software that controls hardware components such as radar or AIS transponders. Related terms: Bootloader, Update. Firmware vulnerabilities can be exploited to gain persistent access. Practical mitigation includes signed firmware and secure update mechanisms. Challenges stem from devices with limited storage and the need for OTA updates over satellite links.

Firewall – Network security device that enforces policy rules to allow or block traffic. Related terms: Stateful Inspection, NAT. Shipboard firewalls isolate bridge networks from crew Wi-Fi. Practical configuration includes permitting only NTP and essential maritime protocols. Challenges include maintaining rule sets across a fleet with diverse equipment and ensuring low latency for critical communications.

General Data Protection Regulation (GDPR) – European Union law governing personal data processing, applicable to many maritime operators. Related terms: Data Subject, Consent. Requires privacy notices for crew health monitoring systems. Practical compliance involves appointing a Data Protection Officer and conducting DPIAs. Challenges arise when vessels operate under multiple jurisdictions with conflicting privacy rules.

Geo-Blocking – Technique that restricts access to services based on geographic location. Related terms: IP Filtering, VPN. Ports may block connections from high-risk cyber regions. Practical use: limiting remote access to ship control systems to approved shore locations. Challenges include legitimate crew travel, satellite latency, and dynamic IP allocation on maritime networks.

Honeypot – Decoy system designed to attract and study attackers. Related terms: Deception Technology, Threat Intelligence. Deployed on a ship's network to capture malware targeting navigation software. Practical benefit: gaining insight into attack methods. Challenges include ensuring the honeypot does not interfere with real operations and managing false positives.

Incident Log – Chronological record of events related to a cyber incident. Related terms: Forensics, Audit Trail. Captures timestamps of alerts from intrusion detection systems on a vessel. Practical use: supporting post-incident analysis and regulatory reporting. Challenges involve maintaining tamper-proof logs on devices with limited storage and ensuring synchronization with shore-based incident management platforms.

Industrial Control System (ICS) – Systems that monitor and control shipboard machinery. Related terms: SCADA, PLC. Includes engine monitoring, ballast control, and cargo handling automation. Practical security concerns focus on preventing unauthorized manipulation of critical functions. Challenges are heightened by legacy protocols lacking authentication and the need for real-time response.

Internet of Things (IoT) – Network of interconnected sensors and devices on vessels. Related terms: Edge Computing, MQTT. IoT devices collect temperature, hull stress, and fuel flow data. Practical benefit: granular analytics for performance optimization. Security challenges include weak default credentials, limited patching capabilities, and exposure of devices to public satellite networks.

Key Exchange – Process by which cryptographic keys are securely shared between parties. Related terms: Diffie-Hellman, TLS Handshake. Used to establish encrypted channels between a ship's bridge system and shore-based analytics servers. Practical considerations include selecting algorithms resistant to quantum attacks. Challenges involve computational overhead on low-power shipboard hardware.

Legal Hold – Directive to preserve electronically stored information for potential litigation. Related terms: E-Discovery, Preservation. When a cyber incident occurs, maritime companies must retain logs from navigation systems. Practical steps: disabling auto-deletion policies and documenting preservation actions. Challenges include coordinating holds across multiple jurisdictions and ensuring data integrity during long-term storage.

Legacy System – Older hardware or software that remains in operation despite newer alternatives. Related terms: Obsolescence, Compatibility. Many vessels still run legacy radar consoles lacking modern security patches. Practical risk: unpatched vulnerabilities become entry points for attackers. Challenges include cost of replacement, certification requirements, and crew training on new equipment.

Machine Learning (ML) – Subset of AI that enables systems to learn patterns from maritime data. Related terms: Supervised Learning, Feature Engineering. ML models predict fuel consumption based on AIS trajectories. Practical benefit: optimizing voyage planning. Challenges involve data privacy when using crew movement data and ensuring model robustness against adversarial manipulation.

Malware – Software designed to disrupt, damage, or gain unauthorized access to computer systems. Related terms: Trojan, Ransomware. Maritime examples include ransomware encrypting VDR recordings. Practical defense: regular backups and endpoint protection. Challenges include limited bandwidth for updates and the need to maintain mission-critical availability of navigation software.

Man-in-the-Middle (MITM) Attack – Interception and possible alteration of communications between two parties. Related terms: SSL Stripping, Eavesdropping. An attacker could modify AIS messages en route to a port authority. Practical mitigation: mutual TLS authentication and certificate pinning. Challenges stem from satellite link latency and the difficulty of implementing end-to-end encryption on legacy devices.

Multi-Factor Authentication (MFA) – Security method requiring two or more verification factors. Related

terms: OTP, Token. MFA is used for remote access to shipboard control systems. Practical example: password plus hardware token. Benefits include reduced credential theft risk. Challenges involve ensuring token availability on vessels with limited connectivity and training crew on secure usage.

Network Segmentation – Division of a network into isolated zones to limit lateral movement. Related terms: VLAN, DMZ. Segments separate bridge navigation systems from crew entertainment Wi-Fi. Practical outcome: containing breaches to non-critical zones. Challenges include managing inter-segment routing for legitimate data flows and maintaining performance on bandwidth-constrained maritime networks.

Operational Technology (OT) – Hardware and software that directly monitors or controls physical devices. Related terms: ICS, SCADA. In maritime contexts, OT includes engine control units and ballast water treatment systems. Security focus is on preventing manipulation that could endanger vessel safety. Challenges involve integrating OT security with existing IT policies and dealing with proprietary protocols lacking built-in security.

Outbound Data Filtering – Process of inspecting and controlling data leaving a maritime network. Related terms: DLP, Egress Filtering. Prevents accidental transmission of confidential cargo manifests. Practical implementation includes rule sets that block large file uploads to untrusted destinations. Challenges include balancing operational needs for legitimate data exchange with strict privacy requirements.

Penetration Testing – Simulated cyber-attack performed to evaluate security posture. Related terms: Red Team, Vulnerability Scan. Conducted on shipboard networks to discover insecure configurations. Practical deliverable: prioritized remediation list. Challenges include scheduling tests around critical voyages and ensuring that testing tools do not interfere with navigation equipment.

Phishing – Social engineering technique that tricks users into revealing credentials. Related terms: Social Engineering, Spear Phishing. Crew may receive emails appearing to be from port authorities requesting login details. Practical countermeasure: security awareness training and email filtering. Challenges include multilingual crews and the high turnover rate of seafarers, which reduces training effectiveness.

Port-Based Network Monitoring – Surveillance of vessel communications while docked. Related terms: IDS, SIEM. Ports can monitor AIS streams for anomalous patterns indicative of data exfiltration. Practical benefit: early detection of compromised ships. Challenges involve privacy considerations, data sharing agreements, and the sheer volume of traffic to analyze in real time.

Privacy by Design – Approach that embeds data protection into system development from the outset. Related terms: DPIA, Data Minimization. Vessel telemetry platforms designed to collect only necessary data for performance analytics. Practical outcome: reduced regulatory exposure. Challenges include aligning privacy goals with operational requirements for comprehensive monitoring.

Public Key Infrastructure (PKI) – Framework for creating, managing, and revoking digital certificates. Related terms: CA, TLS. PKI enables secure VPN connections between ship and shore. Practical steps: issuing

certificates to each vessel's gateway. Challenges involve large-scale certificate lifecycle management across fleets and ensuring revocation lists are promptly propagated to remote locations.

Quantum-Resistant Cryptography – Cryptographic algorithms designed to withstand attacks from quantum computers. Related terms: Post-Quantum, NIST. Emerging standards may replace RSA for securing maritime communications. Practical benefit: future-proofing vessel data links. Challenges include limited computational resources on shipboard hardware and the need for interoperability with existing infrastructure.

Ransomware – Malware that encrypts data and demands payment for decryption. Related terms: Crypto-locker, Extortion. Notable incidents have targeted VDRs, rendering accident investigations impossible. Practical mitigation includes immutable backups and network segmentation. Challenges involve ensuring backups are not also encrypted and dealing with jurisdictional issues when attackers operate from offshore locations.

Redundant Navigation System – Duplicate set of navigation equipment providing failover capability. Related terms: Backup, Fault Tolerance. Redundancy reduces impact of cyber attacks that compromise primary ECDIS. Practical implementation may involve dual-redundant inertial navigation units. Challenges include increased cost, space constraints on vessels, and ensuring both systems receive consistent updates.

Remote Access VPN – Secure tunnel allowing shore-based personnel to connect to shipboard networks. Related terms: IPSec, TLS. Enables engineers to troubleshoot engine monitoring software from on-shore offices. Practical security measures include MFA and strict IP whitelisting. Challenges include managing latency over satellite links and ensuring that VPN credentials are not reused across multiple vessels.

Risk Register – Documented list of identified risks, their impact, likelihood, and mitigation strategies. Related terms: Risk Assessment, Treatment Plan. A maritime operator's register may include threats such as AIS spoofing and supply-chain data leakage. Practical use: prioritizing security investments. Challenges involve keeping the register up to date as new technologies like autonomous cargo drones are introduced.

Secure Shell (SSH) – Cryptographic network protocol for secure remote command execution. Related terms: Port Forwarding, Key-Based Auth. Used by shore engineers to access shipboard Linux servers. Practical advantage: encrypted management channel. Challenges include ensuring key rotation and preventing credential reuse across multiple vessels.

Security Information and Event Management (SIEM) – Platform that aggregates and analyzes security logs. Related terms: Log Correlation, Alerting. SIEM can correlate firewall logs with IDS alerts on a ship's network. Practical benefit: real-time detection of coordinated attacks. Challenges include bandwidth constraints for transmitting logs to shore and the need for tuned correlation rules to reduce false positives.

Security Operations Center (SOC) – Centralized team responsible for monitoring and responding to security events. Related terms: Incident Response, Threat Hunting. A maritime SOC may monitor fleet-wide

telemetry and network traffic. Practical tasks: triaging alerts from vessel firewalls. Challenges include staffing with maritime-specific expertise and handling incidents across multiple time zones and regulatory regimes.

Shipboard Network Architecture – Design of communication pathways among vessel systems. Related terms: Topology, Segmentation. Typically includes separate VLANs for bridge, engine room, and crew areas. Practical considerations: ensuring low latency for navigation while isolating non-critical traffic. Challenges involve retrofitting older ships and maintaining security across heterogeneous equipment vendors.

Smart Contract – Self-executing code stored on a blockchain that enforces agreement terms. Related terms: Blockchain, DLT. Used for automating payments when cargo is off-loaded. Practical benefit: reducing paperwork and fraud. Challenges include legal recognition of contracts, ensuring code correctness, and integrating with existing maritime customs systems.

Software-Defined Networking (SDN) – Approach that centralizes network control via software. Related terms: Controller, OpenFlow. SDN can dynamically re-route traffic on a vessel to isolate compromised segments. Practical advantage: rapid policy changes without physical re-cabling. Challenges involve reliable controller connectivity over satellite links and ensuring compatibility with legacy maritime equipment.

Supply-Chain Security – Protection of hardware and software components from tampering during acquisition. Related terms: Trusted Supplier, Vendor Risk. Includes verifying firmware signatures of navigation radios. Practical steps: maintaining approved vendor lists and conducting periodic audits. Challenges stem from global sourcing, counterfeit components, and limited visibility into offshore manufacturing processes.

Threat Intelligence Feed – Stream of data about emerging cyber threats. Related terms: IOC, STIX. Maritime operators subscribe to feeds that include indicators of compromised maritime IP ranges. Practical use: updating intrusion detection signatures. Challenges include filtering noise, correlating with vessel-specific assets, and ensuring timely distribution to ships at sea.

Threat Modeling – Structured analysis of potential attackers, assets, and vulnerabilities. Related terms: Attack Tree, STRIDE. Maritime threat model may consider nation-state actors targeting cargo manifests. Practical outcome: identifying high-impact attack vectors. Challenges involve keeping models current with evolving tactics and integrating domain-specific maritime knowledge.

Transport Layer Security (TLS) – Protocol that encrypts data between applications. Related terms: Handshake, Cipher Suite. TLS secures web portals used for vessel performance dashboards. Practical requirement: using TLS 1.3 to mitigate known vulnerabilities. Challenges include certificate management on vessels with intermittent connectivity and ensuring legacy equipment supports modern cipher suites.

Two-Way Radio Encryption – Securing voice communications between ship and shore. Related terms: Secure Voice, FM-DX. Encrypted VHF radios prevent eavesdropping on distress calls. Practical implementation uses AES-256 algorithms. Challenges involve key distribution to all crew members and ensuring encryption does

not degrade signal quality under adverse weather conditions.

Vulnerability Scan – Automated process that identifies security weaknesses. Related terms: Pen Test, CVE. Scans can be scheduled on shipboard routers to detect outdated firmware. Practical benefit: proactive remediation before attackers exploit flaws. Challenges include limited processing capability on embedded devices and the risk of false positives disrupting navigation services.

Vessel Data Recorder (VDR) – Device that records navigation and operational data for accident investigation. Related terms: CCTV, Black Box. VDR data must be protected against tampering. Practical security controls include encryption at rest and tamper-evident seals. Challenges involve balancing data retention periods with privacy regulations and ensuring reliable backup when vessels are out of range of shore facilities.

Vessel Traffic Service (VTS) – Shore-based system that monitors and manages ship movements. Related terms: AIS, Radar. VTS relies on accurate AIS data, which can be spoofed. Practical security measures include cross-checking AIS with radar signatures. Challenges include integrating cyber-risk assessments into traditional safety-of-navigation procedures.

Virtual Private Cloud (VPC) – Isolated segment of a public cloud used for maritime analytics. Related terms: VPC Peering, Subnet. Enables secure storage of fleet telemetry while keeping traffic separate from other cloud tenants. Practical benefit: granular network controls for maritime workloads. Challenges involve ensuring compliance with data sovereignty laws when data crosses international waters.

Vulnerability Disclosure Program – Formal process for receiving and responding to security reports. Related terms: Bug Bounty, Responsible Disclosure. Shipping companies may invite researchers to report flaws in their navigation software. Practical steps: establishing a clear reporting channel and defined remediation timelines. Challenges include coordinating responses across multiple vendors and managing public reputation risk.

Zero-Trust Architecture – Security model that assumes no implicit trust, even inside the network. Related terms: Microsegmentation, Identity-Centric. In maritime settings, each device, from engine sensor to bridge console, must authenticate before communicating. Practical implementation includes continuous verification and least-privilege policies. Challenges involve retrofitting existing ship systems and maintaining performance for latency-sensitive navigation data.