

Integrating Maritime Cyber Security within the Framework of the ISM Code & MLC 2006

ABHINAND B — Head of IT Department

Field: Maritime Cyber Security & Information Technology

ABSTRACT

As modern commercial vessel operations undergo rapid digital transformation, traditional operational technology (OT) and information technology (IT) environments have become increasingly interconnected. This paper evaluates the critical intersection of maritime cyber risk management with international maritime regulations—specifically the International Safety Management (ISM) Code and the Maritime Labour Convention (MLC 2006). By analyzing emerging threat vectors across navigation, engine automation, and crew communications, this study details practical strategies for establishing an integrated Safety Management System (SMS) that complies with IMO Resolution MSC.428(98) while preserving seafarer welfare and data privacy rights.

1. INTRODUCTION & OPERATIONAL LANDSCAPE

The contemporary maritime industry relies extensively on integrated digital infrastructure to enhance navigation safety, optimize fuel efficiency, and streamline port logistics. Historically, shipboard Operational Technology (OT)—such as Propulsion Control, Electronic Chart Display and Information Systems (ECDIS), and Automated Radar Plotting Aids (ARPA)—operated in air-gapped isolation from shore networks. However, the rapid expansion of satellite communication (VSAT, Low Earth Orbit networks) has effectively unified onboard OT with shore-side IT systems, dramatically expanding the attack surface of modern commercial vessels.

+400%

Increase in Maritime Cyber Attacks (2020-2024)

MSC.428(98)

IMO Mandate for SMS Cyber Integration

OT / IT

Convergence Vulnerability Vector

MLC 2.4

Crew Communications & Data Protection

2. REGULATORY IMPERATIVES: THE ISM CODE

In response to escalating cyber threats, the International Maritime Organization (IMO) adopted Resolution MSC.428(98), explicitly mandating that cyber risk management be incorporated into existing Safety Management Systems (SMS) governed by the ISM Code. Under the ISM Code, vessel owners and management companies must treat cyber risks with the same rigor as physical safety and environmental hazards. Failure to audit and mitigate identifiable cyber risks renders a vessel unseaworthy under international maritime law, exposing shipowners to severe legal and financial liabilities.

3. SYSTEM VULNERABILITIES & MARITIME THREAT VECTORS

Vessel cyber systems are susceptible to targeting across both IT (business networks, crew welfare Wi-Fi, port documentation systems) and OT (bridge navigation, engine automation, ballast control). Vulnerabilities are exacerbated by legacy software environments, unpatched embedded controllers, and inadequate network segmentation.

System Domain	Primary Subsystems	Vulnerability & Threat Vector	Risk Level
Bridge Navigation	ECDIS, GPS/GNSS, AIS, Radar	GNSS Spoofing/Jamming, unauthorized USB update infection	CRITICAL
Machinery & Engine	Power Management, Engine Control, Ballast	PLC manipulation via compromised maintenance laptops	CRITICAL
Cargo Management	Container tracking, Valve control, Chillers	Ransomware encryption of manifests and sensor telemetry	HIGH
Satcom & Connectivity	VSAT Terminals, Routers, Onboard Wi-Fi	Default credential exploit, unencrypted voice/data traffic	HIGH
Crew Welfare Network	Personal devices, Internet portals	Phishing, malware propagation to administrative IT network	MEDIUM

4. THE MLC 2006 DIMENSION: HUMAN FACTORS & WELFARE

While the ISM Code addresses physical and operational vessel safety, the Maritime Labour Convention (MLC 2006) mandates seafarer welfare, working conditions, and rights. The expansion of shipboard internet connectivity for crew well-being creates a dual challenge: safeguarding seafarer personal data and protecting the vessel against human-centric cyber threats.

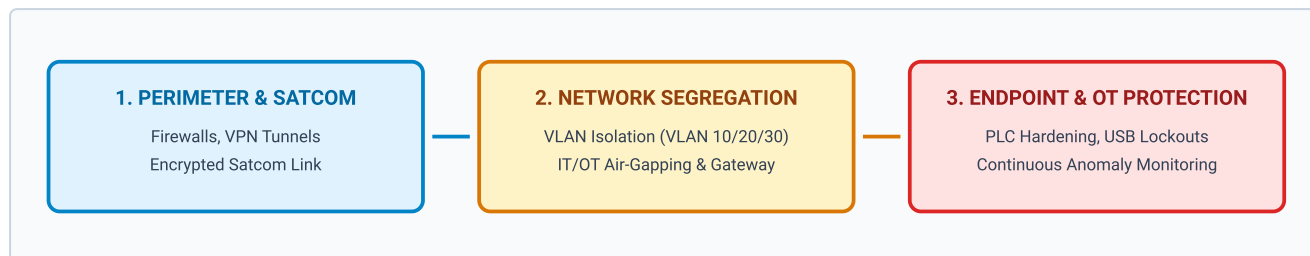
Key MLC & Human-Centric Cyber Security Directives:

- **Seafarer Personal Data Protection:** Protecting crew health records, certification data, and financial remittance details stored on shipboard administrative databases.
- **Secure Crew Communication Access:** Ensuring crew internet portals provided under MLC Regulation 3.1 are strictly segmented from bridge operational networks.
- **Cyber Hygiene & Awareness Training:** Treating crew awareness as a core welfare and safety competency to counter social engineering and phishing attacks.

Human error remains the primary attack vector in maritime cyber incidents. Integrating security awareness into standard crew familiarization trainings ensures that seafarers understand how individual actions—such as connecting unauthorized USB devices or downloading unverified files—directly impact shipboard safety.

5. DEFENSE-IN-DEPTH ARCHITECTURE FOR SHIPS

To establish a resilient operational posture, ship management companies must implement a layered architecture that segregates critical operational tech from non-critical networks, enforces strict access control, and maintains real-time monitoring capability both onboard and at the Fleet Operations Center (FOC).



6. IMPLEMENTATION ROADMAP FOR IT & MARINE OPERATIONS

Achieving compliance with IMO MSC.428(98) and maintaining robust operational continuity requires structured collaboration between shore-side IT departments and sea-going officers:

- **System Inventory & Risk Assessment:** Catalog all onboard microcontrollers, PLCs, servers, and software assets across IT and OT domains.
- **Policy Integration into SMS:** Draft standard operating procedures (SOPs) for incident response, cyber emergency drills, software patching schedules, and third-party technician access control.
- **Crew Training & Verification:** Conduct periodic phish-testing and practical cyber drills alongside traditional fire and abandon-ship drills.
- **Continuous Audit & Recovery Verification:** Verify off-line backup integrity for critical ECDIS navigation databases and propulsion software configurations.

7. CONCLUSION

Maritime cybersecurity is no longer solely an IT concern—it is a foundational pillar of vessel seaworthiness, environmental safety, and crew protection under the ISM Code and MLC 2006. By embedding cyber risk controls into existing safety management systems and enforcing rigorous network isolation, maritime organizations can build operational resilience against dynamic cyber threats.

