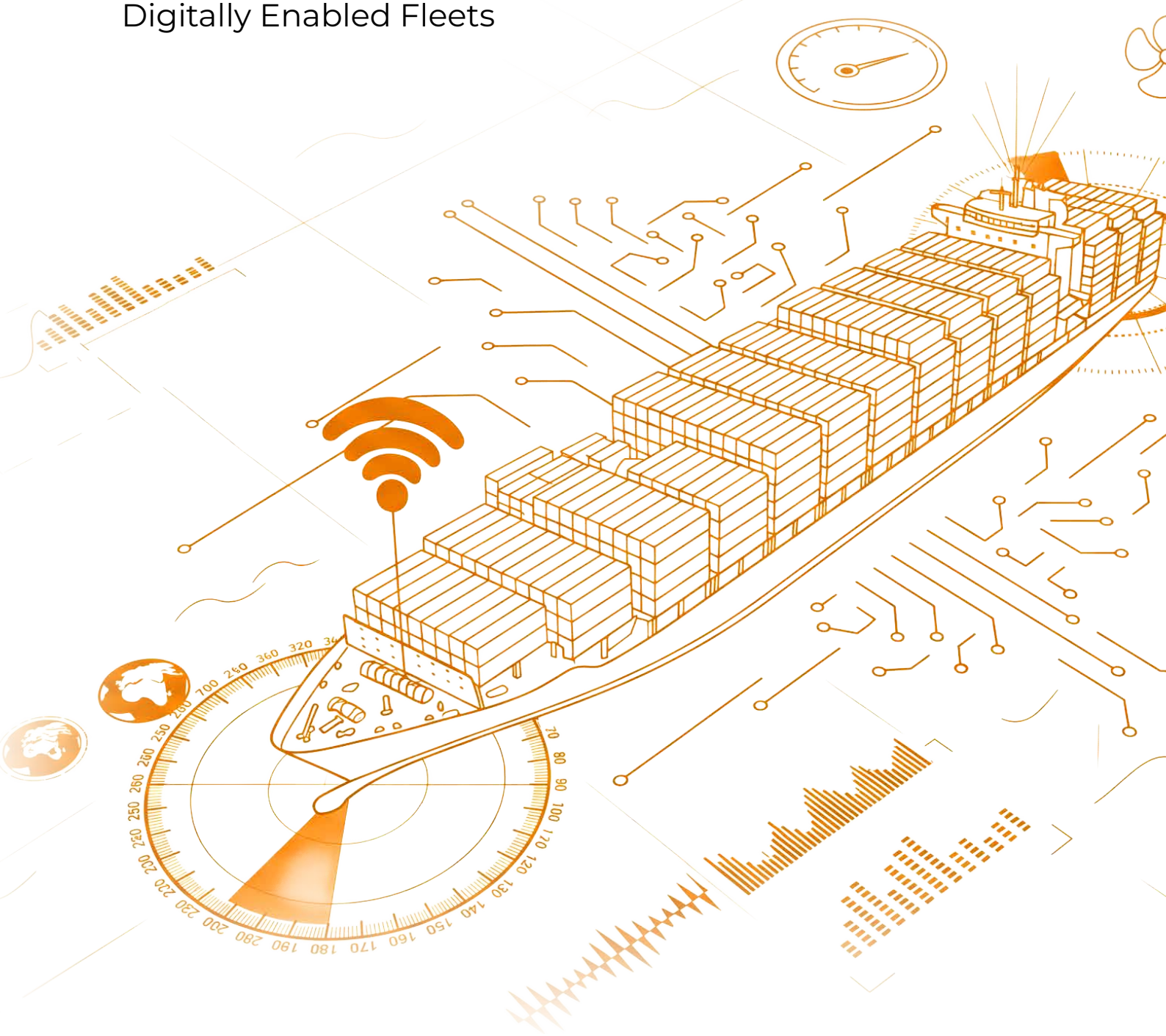
Securing the Connected Ship

A Cyber Risk Management Framework for OT/IT Systems in Digitally Enabled Fleets



Smart Ship HUB

www.smartshiphub.com

Executive Summary

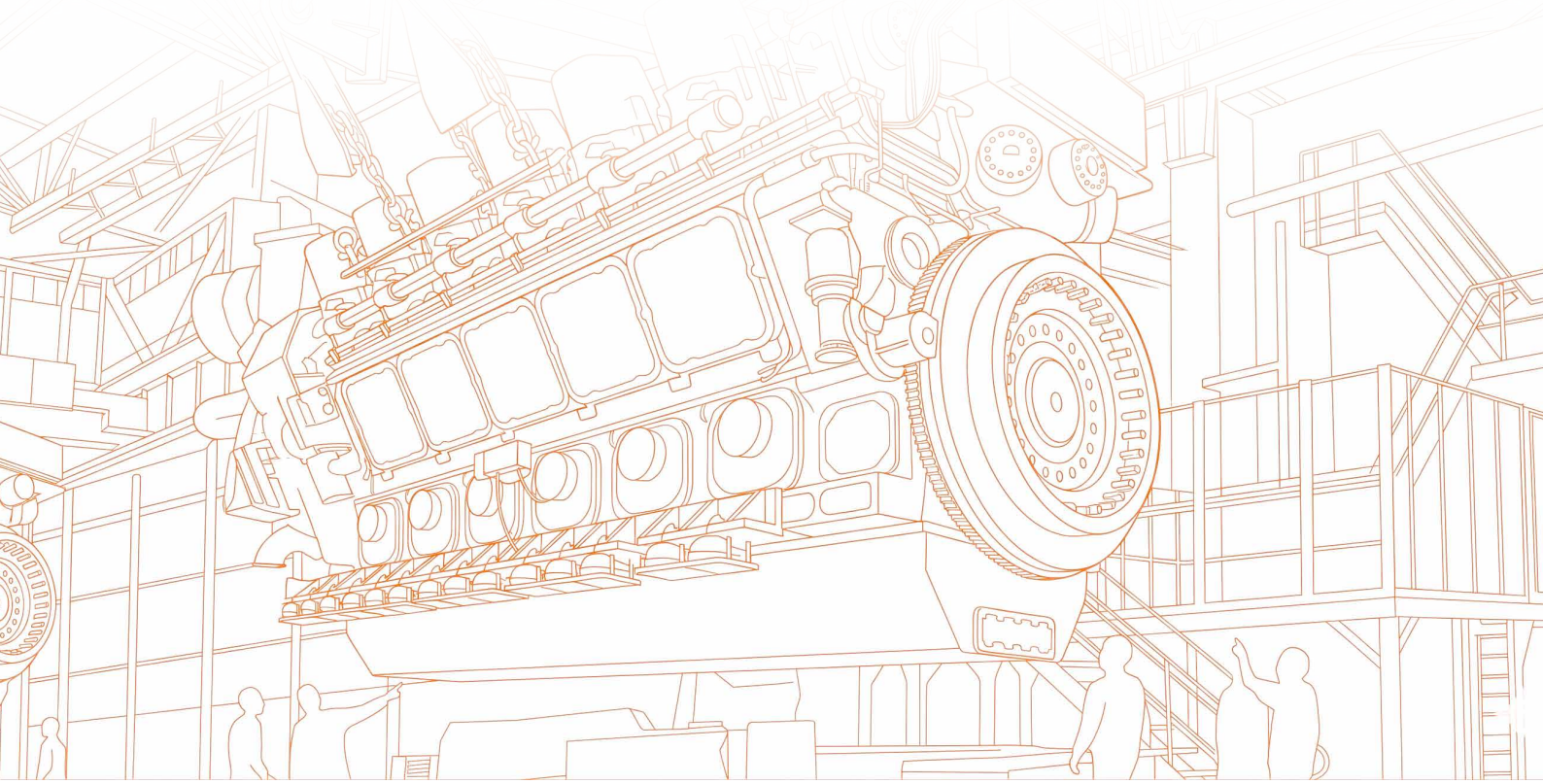
As vessels become increasingly connected, maritime cybersecurity is a core operational priority. This white paper presents a model for managing cyber risks in IT and OT environments faced by digitally-enabled fleets. It discusses the maritime attack surface, explains E26 and E27 requirements in operational terms and outlines a resilience framework to balance secure connectivity with network segmentation. Once governance, consistent monitoring, and safe data practices are in place, daily processes on a vessel or fleet can be enhanced to improve resilience and ensure the safe adoption of advanced digital and remote monitoring capabilities.

Introduction: The Connected Ship Paradox

Modern marine vessels do not travel between ports as isolated assets. They are nodes in a constantly connected digital ecosystem at sea. A ship's engine performance data is streamed to the shore in real time, navigation updates are communicated via satellite, onboard teams receive remote diagnostic support, and cloud platforms aggregate fleet-wide insights. All these capabilities are changing how vessels are operated, maintained, and optimised.

Viewed from another angle, the same connectivity – that enables efficiency and visibility – also enlarges the cyber-attack surface for shipping. Each sensor, communication link and remote access pathway is a potential new point of exposure. The systems that were once physically apart are now interconnected, blurring the boundary between operational technology (OT) and IT environments.

With these digitalisation-induced changes, fleet operators face a new paradox. They have tools that assist in improving performance and fortifying compliance but also introduce risk that can disrupt voyages, compromise safety, and affect commercial performance. The challenge is to keep connecting ships securely and prevent any of their systems from becoming targets of malicious activities.



Understanding the Maritime Attack Surface

The dense digital ecosystem in which modern vessels operate connects shipboard systems, crews, shore offices, cloud platforms, and third-party service providers. All of these improve operational visibility, efficiency, and facilitate remote support from engineers. The same features make them potential entry points for cyber risks.

In the maritime world, the attack surface goes beyond a ship's hull – it spans the entire supply chain. Therefore, understanding this interlinked environment is the first step to building effective cyber resilience for modern fleets.

Mapping Maritime Cyber Threat Vectors

For connected fleets, cyber risks become physical, operational and commercial. Six prominent threat zones where they originate are:

1. Onboard OT

Operational tech setups, including propulsion control, power management, navigation systems, and cargo automation, are now digitally connected on a vessel. However, many of them have legacy architectures that were not designed for external connectivity. Unpatched software, default credentials, and flat networks can cause lateral movement from a single compromised endpoint to critical machinery systems. Navigation technologies, such as GPS and GNSS, are exposed to signal manipulation risks, such as GPS spoofing and GNSS interference, that can mislead positioning and routing without directly breaching onboard networks.

2. Crew & Welfare Networks

The internet, personal devices and messaging apps used by the crew keep them connected to families and shore teams. The same systems also introduce high-frequency pathways for phishing, ransomware, and malware. If controls are weak, any compromised laptop or USB connection can unintentionally bridge segmented networks.

3. Satellite & Ship-Shore Connectivity

Ship-to-shore connectivity depends on persistent communication channels for performance monitoring and technical support by shore teams. These risks are amplified when onboard networks lack effective segmentation between IT, OT, and welfare systems, allowing a single compromised connection to move laterally across the vessel's digital environment. Without strict access governance and session management, the always-on connections may become long-term footholds for unauthorised access.

4. Cloud & Fleet Platforms

Performance analytics, voyage optimisation tools, and data lakes centralise critical vessel data ashore. Misconfigured cloud storage, weak API security and credential theft can expose operational data or create backdoor access to shipboard systems.

5. Shore Offices & Fleet HQ

Vessels operating as extensions of enterprise IT ecosystems share data with ERP platforms, operations centres and headquarters. So, any breach in the corporate IT environment can also propagate into ship networks via trusted communication channels.

6. Third-Party & Vendor Ecosystem

The control systems running shipboard machinery – such as engine, power management, ballast water management, cargo handling, HVAC – and specialised maritime software often depend on vendor-issued patches, firmware updates, and diagnostic tooling. If these update channels, code repositories, or third-party service environments get compromised, malicious code can be injected into shipboard OT environments as part of otherwise legitimate maintenance workflows.

All these vectors collectively reveal how a connected ship is a multi-part ecosystem that demands strong layers of cyber defence.

IACS E26/E27 in Practice: How Compliance Adherence Becomes a Business Capability

The introduction of IACS Unified Requirements (UR) E26 and E27 brought a turning point for maritime cybersecurity. They made cyber resilience a formal requirement to be embedded in ship design, equipment certification and lifecycle management. However, many fleet owners still view these regulations as a checklist for compliance rather than capabilities to be built.

In essence, E26 and E27 recognise that digital systems now impact safety and vessel availability in the same way as traditional engineering systems do.

E26 — Cyber Resilience of Ships

The requirement focuses on the vessel as a cohesive digital environment. It mandates risk assessment during design, identification of critical systems and protection against unauthorised access or unintended system behaviour. The emphasis is on keeping operations safe even when systems are degraded or compromised. This concept is familiar to marine engineers but is newly applied to cyber risk.

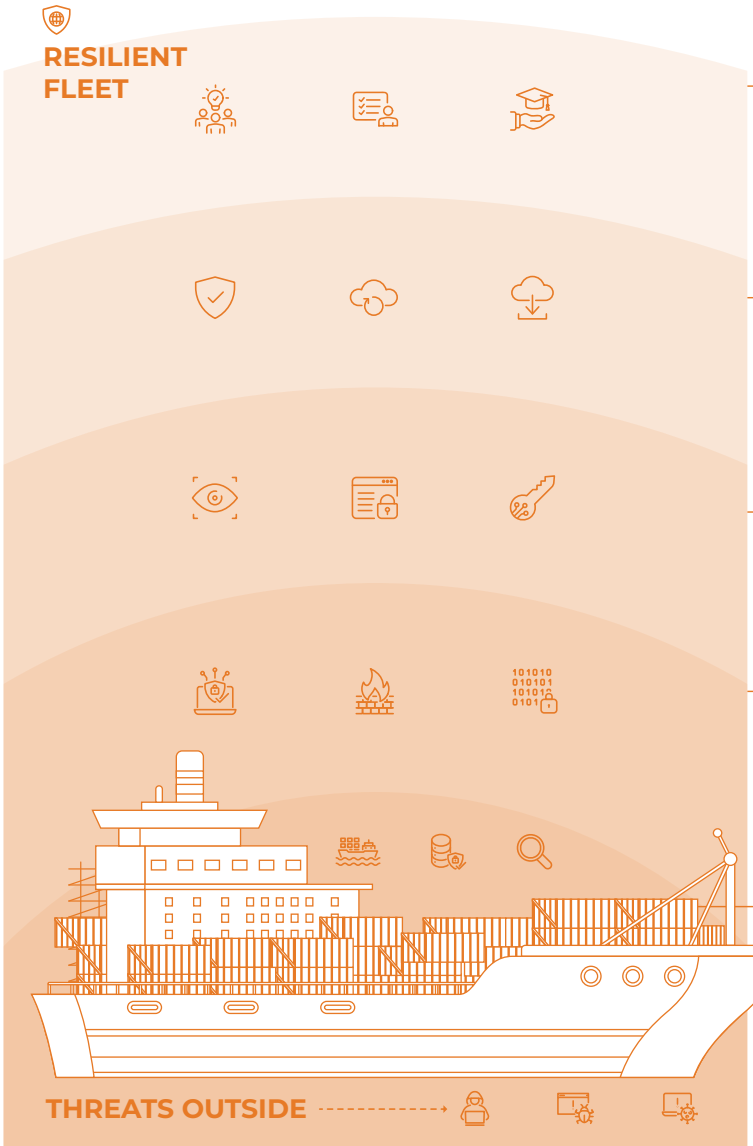
E27 — Cyber Resilience of Onboard Systems and Equipment

E27 moves the spotlight to manufacturers and suppliers. Equipment and machinery must be designed, developed, and maintained to remain safe from cyber threats throughout their lifecycle. Secure software development, controlled updates, vulnerability management, and clear documentation are no longer optional expectations.

The practical challenge for operators is to turn these two requirements into a coherent, working reality by integrating them into daily operational practices. They have to see that the mandates are not treated as one-time certification exercises. There must be consistent visibility into connected systems and clear accountability across ship and shore processes that continue long after delivery.

When E26 and E27 are implemented in this operational, lifecycle-driven way, begin to reveal their strategic value. They provide a structured starting point for embedding cyber resilience into everyday fleet operations, making compliance the foundation for long-term digital confidence.

The Layered Maritime Cyber Resilience Model



GOVERNANCE & CULTURE

Policies, training, vendor management, lifecycle security

INCIDENT RESPONSE & RECOVERY

Preparedness, response execution, and recovery capability

CONTINUOUS MONITORING

Detect, analyze, and respond early

SECURE ARCHITECTURE & SEGMENTATION

Isolate, control access, minimize lateral movement

ASSET VISIBILITY

Know your assets, connections, and criticality

For connected fleets, cyber resilience is built by multiple technologies and controls that combine visibility, architecture, monitoring, response and governance. Each layer is added to mitigate risk and limit the impact of possible incidents. Deployed together, they make cybersecurity a continuous operational discipline that underpins safe and reliable fleet connectivity.

Resolving the Connectivity vs Segmentation Dilemma

In the maritime industry, cybersecurity has long been maintained using a simple principle: keep ship systems isolated. Enterprises saw air-gapped networks as the safest way to protect critical operations. The approach worked because vessels had operated for years largely as self-contained environments. But the methods for cyber defence become more complex as fleets rely more on real-time performance data, remote diagnostics, and continual optimisation.

High-frequency data flows are regular in modern marine operations. Shore teams have to track machinery health, improve fuel efficiency, analyse voyage performance, and support crews in real time. Classification reporting, emissions compliance, predictive maintenance, and charter transparency also need AI systems and continuous data exchange between ship and shore. Strict isolation is not practical in this environment.

Increasing connectivity extends the attack surface, but limiting it restricts the capabilities that balance efficiency, safety and decarbonisation performance. The solution, therefore, lies in secure connectivity as a design principle between and within vessels.

For a resilient architecture, simple isolation has to be replaced by controlled interaction. Strong access and identity management must ensure that only authorised users and systems communicate with vessel networks. Network segmentation should be sufficient to stop lateral movement of threats if a breach occurs. Continuous monitoring is required to keep anomalies visible before they turn into incidents.

Implementing these capabilities depends on reliable data pipelines, and they must also operate within tightly governed security frameworks. With connectivity and segmentation designed together, fleets unlock operational insight without increasing cyber exposure. In doing so, they achieve both performance and protection simultaneously.

Building a Fleet Governance Framework to Improve Maritime Cyber Resilience

Designing secure connectivity is the beginning. The next challenge for mariners is to turn architectural principles into routine operational practice.

Cyber resilience must be embedded in governance, procurement, training, and incident response. A repeatable framework must allow cyber risk to be managed as systematically as a vessel's physical safety and compliance. The pillars of this framework include:

1. A living asset inventory and risk baseline

Operators and AI systems need to constantly track connected assets across ship and shore — from bridge systems and engine controls to crew welfare networks and cloud platforms. Regular risk assessments should identify critical systems, data flows, and potential exposure points as fleets evolve.

2. Zero-trust remote access as standard

Remote diagnostics and vendor access must be controlled by strict identity verification, least-privilege permissions, and time-bound sessions. Default trust models cannot be accepted any more in connected environments.

3. Continuous monitoring across vessel networks

Threat detection should not be based on periodic checks. Always-on monitoring is essential. Behavioural analytics and anomaly detection can reveal suspicious activity before it disrupts operations.

4. Crew awareness and cyber culture

Seafarers are a vital line of defence. Practical training, clear reporting processes, and realistic drills help them build stronger cyber awareness in their daily routines on board.

5. Incident response plans

Fleets must also prepare for containment and recovery before incidents occur. Defined escalation paths and tested response playbooks reduce downtime and uncertainty.

6. Vendor and supply-chain governance

Service partners and equipment providers require consistent access controls, security standards, and accountability. Third-party risk must be treated as fleet risk.

The core idea of such a model is to make cyber resilience a managed, measurable capability that leadership teams can track, audit, and strengthen as digital fleets expand.

Cybersecurity as a Permanent Fleet Management Priority

As the pace of digital transformation increases, cyber resilience is set to become a defining characteristic of high-performing fleets. For vessels that depend on connected systems, real-time analytics, and remote collaboration, secure data pipelines are essential to innovate with confidence. Digitalisation will deliver its full value when connectivity is trusted, governed, and continuously protected.

For future-ready operators, cyber risk is not a technical concern. They are treating it as part of everyday fleet management. Security considerations are being built into operational planning, procurement decisions, and performance monitoring. For vessels that are designed to manage both connectivity and protection, cybersecurity is a permanent operational discipline in the maritime industry.