DATA DIODE IN MARITIME INDUSTRY

ENHANCING CYBERSECURITY AND ENSURING SECURE TRANSFER FOR MODERN MARINE OPERATIONS

CONNEXITE

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4
INTRODUCTION 5
DIGITAL TRANSFORMATION IN MARITIME INDUSTRY 7
EVOLUTION OF SHIPBOARD SYSTEMS 8
THE RISE OF DATA-DRIVEN MARINE OPERATIONS 8
CHALLENGES OF INCREASED CONNECTIVITY 9
THE NEED FOR SECURE DATA SEGREGATION 10
CYBERSECURITY THREAT LANDSCAPE AT SEA 11
NATURE OF CYBER THREATS IN THE MARITIME DOMAIN 11
REAL-WORLD INCIDENTS AND LESSONS LEARNED 11
VULNERABILITIES UNIQUE TO MARITIME ENVIRONMENTS 12
CONSEQUENCES OF CYBER COMPROMISE 13
GROWING ROLE OF REGULATION AND RISK MANAGEMENT 13
REGULATORY FRAMEWORK AND COMPLIANCE REQUIREMENTS 14
THE INTERNATIONAL MARITIME ORGANIZATION (IMO) FRAMEWORK 14
EUROPEAN UNION NIS2 DIRECTIVE 14
UNITED KINGDOM – MCA CODE OF PRACTICE FOR SHIPS 15
UNITED STATES – US COAST GUARD NVIC 01-20 15
CLASSIFICATION SOCIETIES AND INDUSTRY STANDARDS 16
CERTIFICATION AND COMPLIANCE TRENDS 16
IMPLICATIONS FOR SHIP OWNERS AND OPERATORS 16
WHY ONE-WAY DATA TRANSFER IS CRITICAL 17
SECURITY DILEMMA OF MARITIME CONNECTIVITY 17
DEFINITION AND OPERATION OF DATA DIODE 18
BASIC COMPONENTS AND WORKING PRINCIPLE 19
DATA FLOW CONTROL 19
PRACTICAL MARITIME USE CASES 20
ADVANTAGES OVER CONVENTIONAL SECURITY CONTROLS 21
OPERATIONAL AND BUSINESS BENEFITS 21
STRATEGIC IMPORTANCE FOR THE FUTURE FLEET 21
TECHNICAL ARCHITECTURE OF A MARITIME DATA DIODE SYSTEM 22

SYSTEM OVERVIEW 22
PHYSICAL AND LOGICAL DESIGN 23
TYPICAL NETWORK TOPOLOGY 24
SUPPORTED DATA TYPES AND PROTOCOLS 24
REDUNDANCY AND RELIABILITY 25
INTEGRATION AND MAINTENANCE 25
INTEGRATION WITH MARITIME OPERATIONS 26
OPERATIONAL ACCOUNTABILITY AND PERFORMANCE 27
VALUES OF USING DATA DIODE 29
DATA DIODE TECHNOLOGY IN THE FUTURE 31
EXPECTED INNOVATIONS AND DEVELOPMENTS 31
CONCLUSION 32

EXECUTIVE SUMMARY

The maritime industry is undergoing an unprecedented digital transformation. Once isolated, mechanical systems on ships are now increasingly networked, data-driven, and remotely managed. Navigation, propulsion, maintenance, and cargo systems exchange continuous streams of data with onshore control centers, cloud analytics platforms, and regulatory authorities. This interconnected nature has unlocked new efficiencies—but it has also introduced serious cybersecurity risks.

A modern vessel is effectively a floating data center. Its critical Operational Technology (OT) systems—such as the Engine Control Room, Integrated Bridge System (IBS), and Electronic Chart Display and Information System (ECDIS)—operate alongside corporate Information Technology (IT) systems that manage logistics, communications, and reporting. When these networks are interconnected without sufficient segregation, a single cyber intrusion can compromise navigational safety, disrupt cargo operations, or even endanger human lives.

International regulators have recognized this emerging threat. Frameworks such as the **IMO Resolution MSC.428(98)**, the **EU NIS2 Directive**, the **UK MCA Cyber Security Code of Practice for Ships**, and the **US Coast Guard NVIC 01-20** now require ship owners and operators to embed cyber-risk management within their Safety Management Systems. Compliance increasingly demands technical evidence that critical OT systems are isolated from external connectivity and protected from remote manipulation.

One-way data transfer mechanisms, commonly known as **data diodes**, have become a cornerstone technology in meeting these requirements. A data diode enforces physical unidirectional information flow—allowing ship data (such as performance metrics, engine logs, emissions data, or voyage status) to be transmitted securely to shore-based systems while absolutely preventing any inbound connection that could carry malicious code or control commands back to the vessel. Unlike firewalls or software filters, a hardware-enforced diode cannot be bypassed by configuration error or malware. It creates a physical boundary, impossible to cross.

Deploying data diode solutions within shipboard networks achieves three core objectives:

Cyber Resilience – Ensures that malware, ransomware, and unauthorized remote commands cannot reach the vessel's control systems.

Regulatory Compliance – Provides measurable isolation that satisfies IMO, NIS2, and classification-society cybersecurity standards.

Operational Continuity – Allows continuous flow of critical telemetry to fleet managers and maintenance systems without jeopardizing vessel integrity.

For modern marine operations—where uptime, safety, and data integrity are paramount—the combination of **robust segmentation**, **secure one-way transfer**, and **strong cybersecurity**

architecture is no longer optional but fundamental. The maritime sector's future competitiveness will depend on its ability to move data safely across air-gapped domains, ensuring that digital innovation never compromises navigational or operational security.

INTRODUCTION

The maritime industry stands at the intersection of tradition and transformation. For centuries, ships have been self-contained environments—autonomous in navigation, communication, and operation. Today, however, digitalization has reshaped this reality. Modern vessels are equipped with integrated bridge systems, automated engine controls, IoT-enabled sensors, and satellite-based communications, forming a highly connected ecosystem that continuously exchanges data between ship and shore.

This evolution has brought remarkable benefits: optimized fuel efficiency, predictive maintenance, real-time route adjustments, and improved logistics coordination across global fleets. Data-driven decision-making has become central to the competitiveness and sustainability of maritime operations. Yet, with connectivity comes vulnerability. The same networks that enable operational insight can also become pathways for cyber intrusion, data corruption, or remote system manipulation.

Unlike land-based enterprises, ships operate in geographically isolated and bandwidth-constrained environments, where immediate technical assistance is rarely available. A single compromised system—whether through ransomware, spoofed signals, or unauthorized remote access—can disrupt navigation, risk safety, and cause significant economic and environmental consequences. As a result, **cybersecurity has emerged as a core component of maritime safety**.

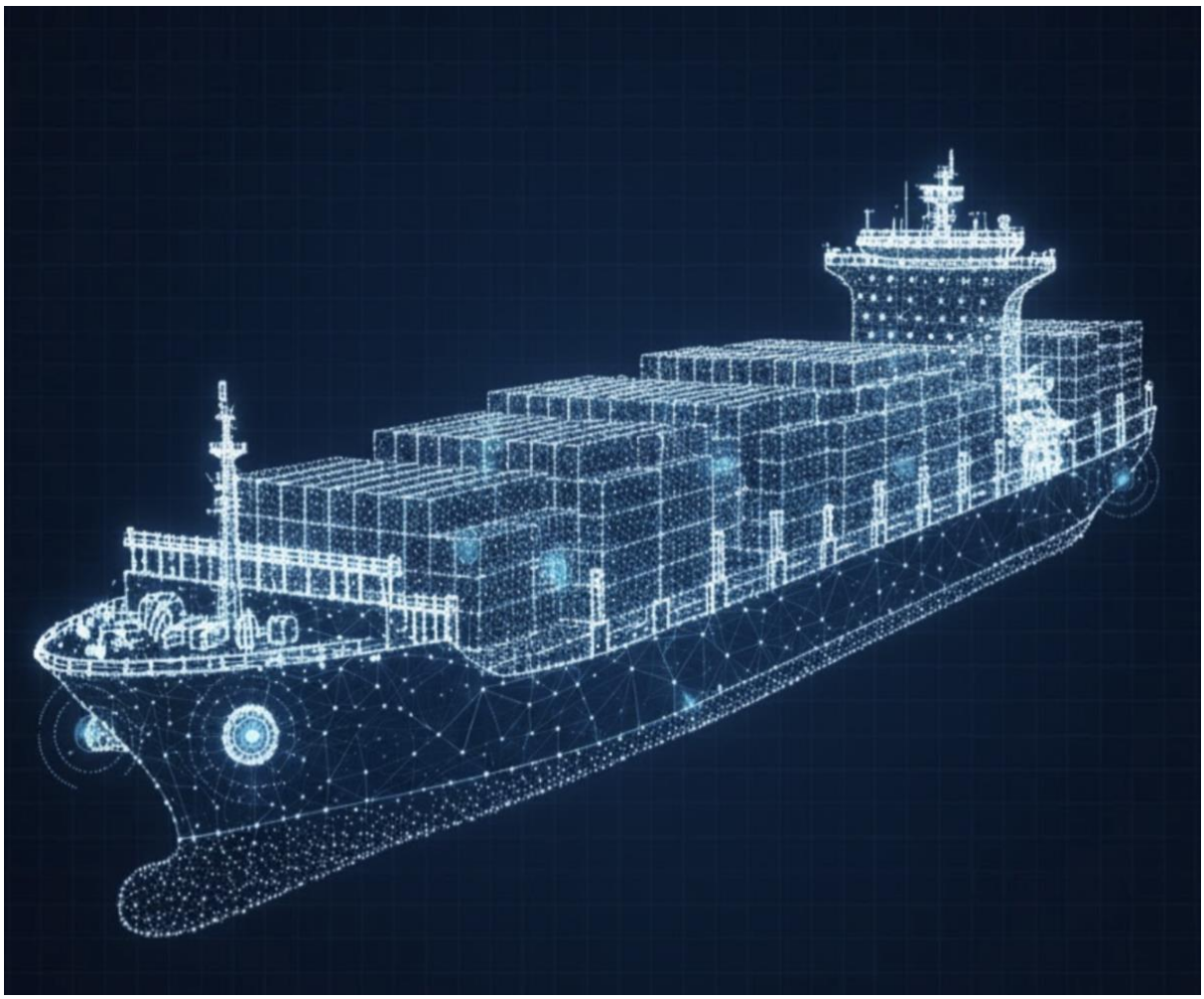
Recognizing this, global regulators—including the International Maritime Organization (IMO), the European Union (via the NIS2 Directive), and national authorities such as the UK Maritime and Coastguard Agency (MCA) and the US Coast Guard—have introduced frameworks mandating robust cyber-risk management across all ship operations. Compliance now extends beyond corporate IT systems to include Operational Technology (OT): the bridge, engine room, and control systems that directly affect a vessel's safety and performance.

Among the most effective approaches to safeguarding these critical domains is the implementation of **secure one-way data transfer solutions**, commonly known as **data diodes**. These devices enforce a physical boundary between trusted and untrusted networks, ensuring that operational data can be transmitted safely to shore without allowing any inbound communication that could compromise onboard systems.

This document examines the evolving cybersecurity landscape in the maritime sector and explores how technologies like data diodes can enable safe digitalization. It outlines regulatory requirements, presents technical architectures for secure one-way data transfer, and highlights operational benefits and certification pathways. Ultimately, it aims to guide ship

owners, operators, and technology providers in achieving a balance between **connectivity and security**, ensuring that the modernization of maritime operations does not come at the cost of resilience and safety at sea. Readers may find duplicate information throughout the document. Since the document is intended to provide insight to a wider audience, similar information may be found in different sections. Readers are free to skip sections not relevant to their role, as this would not break the general flow of the document.

DIGITAL TRANSFORMATION IN MARITIME INDUSTRY



The maritime industry, historically conservative and mechanically oriented, is now undergoing one of the most profound transformations in its history. Driven by automation, connectivity, and data analytics, ships are evolving from isolated operational platforms into fully connected digital ecosystems. This transformation, often referred to as **Maritime 4.0**, parallels the wider Industry 4.0 movement on land—integrating sensors, networks, and analytics to achieve safer, more efficient, and more sustainable operations.

EVOLUTION OF SHIPBOARD SYSTEMS

In the past, critical systems such as navigation, propulsion, and cargo management operated independently, with limited digital control and minimal data sharing. Today, these systems are integrated through **Integrated Bridge Systems (IBS)** and **Integrated Platform Management Systems (IPMS)** that centralize control, logging, and performance data. Common modern components include:

ECDIS (Electronic Chart Display and Information System) for digital navigation

VDR (Voyage Data Recorder) for operational recording and investigation

Engine and power management systems connected via Modbus/TCP or CAN bus

Condition monitoring sensors feeding predictive maintenance algorithms

Satellite communication terminals (VSAT, Inmarsat, Iridium) linking ship and shore

These interconnected subsystems continuously generate and transmit large volume of operational data, covering everything from fuel consumption and hull stress to weather conditions and crew performance metrics.

THE RISE OF DATA-DRIVEN MARINE OPERATIONS

The digitalization of vessels enables new business models and operational efficiencies:

Fleet analytics platforms aggregate telemetry from multiple ships to optimize routing, reduce emissions, and improve utilization.

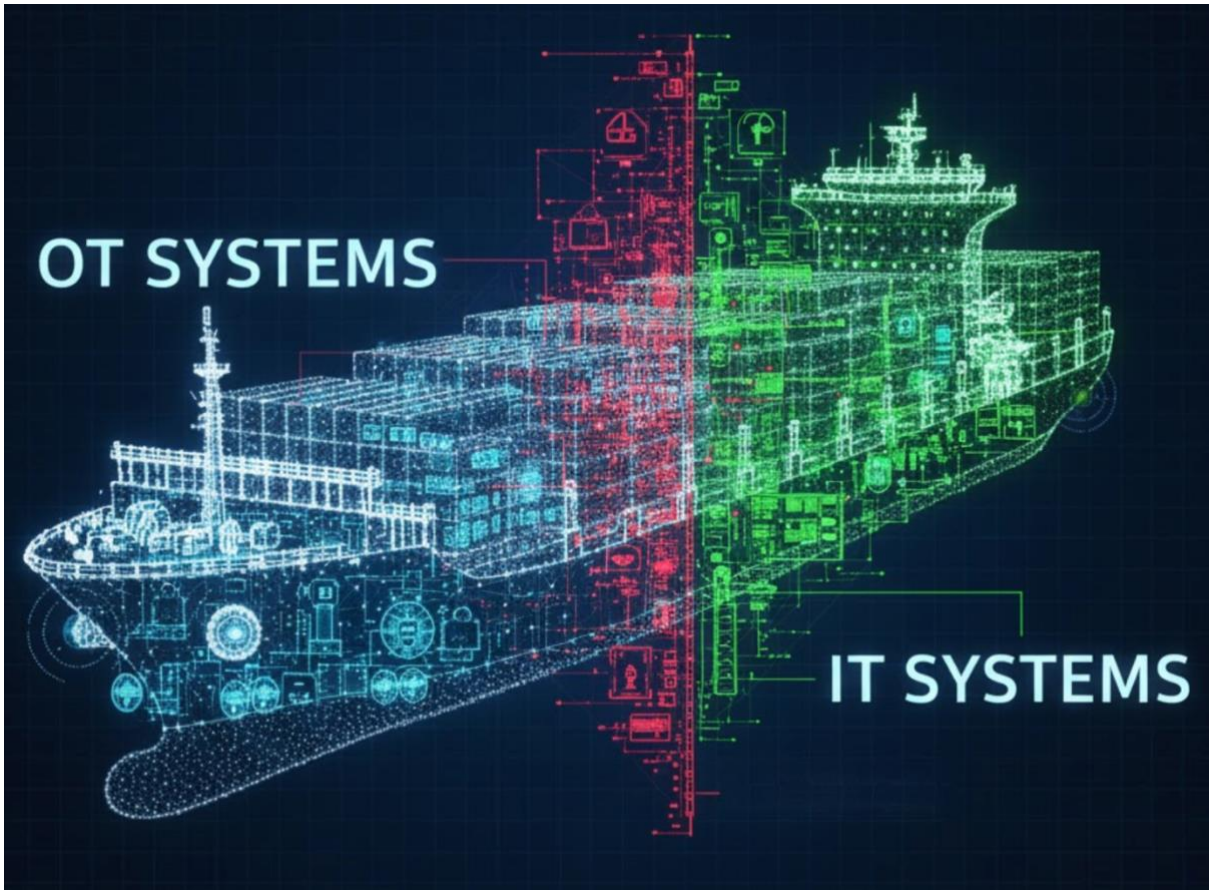
Predictive maintenance reduces downtime by identifying anomalies in engines, pumps, and auxiliary systems before failures occur.

Remote support and diagnostics allow manufacturers and fleet operators to troubleshoot equipment over secure satellite links.

Regulatory and environmental reporting such as emissions monitoring under MARPOL Annex VI depends on accurate, continuous data flow.

Data is no longer a by-product of operations; it is a strategic asset that drives competitiveness and compliance. However, this reliance on data exchange blurs the once-clear boundary between Operational Technology (OT) and Information Technology (IT), creating new cybersecurity challenges.

CHALLENGES OF INCREASED CONNECTIVITY



While digital transformation delivers clear economic and operational gains, it also expands the vessel's **attack surface**. Interconnected networks, remote maintenance links, and cloud-based analytics create potential entry points for cyber threats. Key risks include:

Unauthorized remote access to critical systems through misconfigured communication links

Propagation of malware or ransomware from IT networks to OT domains

Compromised navigation signals, such as AIS spoofing or GPS jamming

Human error in configuration or portable media usage onboard

In many cases, vessels operate in environments with limited IT staff and constrained communication bandwidth, making it difficult to detect and respond to attacks in real time. The

combination of isolation and high operational dependency on digital systems makes maritime networks uniquely vulnerable.

THE NEED FOR SECURE DATA SEGREGATION

To mitigate these risks, cybersecurity in the maritime sector increasingly focuses on **network segmentation**, ensuring that navigational, engineering, and safety-critical systems remain insulated from corporate or external networks. However, operational requirements still demand that data (such as voyage information, equipment logs, or environmental measurements) be transmitted to shore. This creates a fundamental dilemma: how to enable data flow without exposing the ship to inbound threats.

One-way data transfer technologies (data diodes) resolve this dilemma by allowing secure, hardware-enforced transmission of data from ship to shore while guaranteeing absolute isolation from reverse access. As vessels become smarter and more autonomous, the ability to maintain this asymmetrical but reliable data exchange will define the success of digital transformation in maritime operations.

CYBERSECURITY THREAT LANDSCAPE AT SEA

As maritime systems become increasingly digitalized, vessels are no longer isolated entities but complex networks of computers, sensors, and control systems. This expanded connectivity, while operationally transformative, exposes ships to the same types of cyber threats faced by shore-based enterprises, compounded by the challenges of remote operation, long service lifecycles, and limited onboard IT resources. The result is a rapidly growing attack surface across both **Operational Technology (OT)** and **Information Technology (IT)** domains.

NATURE OF CYBER THREATS IN THE MARITIME DOMAIN

Cyber threats in maritime environments span a wide spectrum, from opportunistic ransom attacks to highly targeted, state-sponsored espionage. Typical categories include:

- **Malware and ransomware attacks:** Infection through maintenance laptops, USB drives, or remote support sessions can disable navigation or propulsion systems.
- **Network intrusion and privilege escalation:** Exploiting outdated or unpatched shipboard systems, often running legacy operating systems like Windows 7 Embedded or XP.
- **Data manipulation:** Unauthorized alteration of cargo manifests, voyage plans, or sensor data, leading to operational or regulatory non-compliance.
- **Spoofing and jamming:** Manipulation of **AIS (Automatic Identification System)** or **GPS** signals to obscure vessel position, disrupt routes, or disguise illegal activity.
- **Supply-chain compromises:** Tampering with software or firmware updates delivered during port maintenance or via satellite connections.
- **Insider threats:** Crew members or subcontractors with legitimate access may unintentionally or deliberately compromise system security.

REAL-WORLD INCIDENTS AND LESSONS LEARNED

Several high-profile incidents have demonstrated the tangible risks of maritime cyber compromise:

- **NotPetya (2017):** A global ransomware outbreak that severely disrupted Maersk's logistics operations, leading to an estimated $300 million in losses.

- **Port of San Diego (2018)** and **Port of Houston (2021):** Both suffered ransomware incidents that temporarily halted port operations.
- **AIS spoofing events** in the Black Sea and Persian Gulf regions: hundreds of vessels simultaneously appeared to "teleport" to inland coordinates, indicating deliberate manipulation.
- **E-mail-based frauds** (BEC attacks) targeting chartering and payment systems, causing multimillion-dollar financial losses.

Each of these events underscores a critical reality: cyber incidents at sea can have direct consequences for **safety of life, environmental protection, and global trade continuity**.

VULNERABILITIES UNIQUE TO MARITIME ENVIRONMENTS

Maritime cyber defense is complicated by several structural and operational constraints:

- **Legacy systems:** Many vessels operate for 20–30 years, using hardware and software long past vendor support.
- **Limited network visibility:** Shipboard networks often lack centralized monitoring or intrusion detection systems.
- **Bandwidth constraints:** Satellite links limit the deployment of heavy security updates or real-time telemetry.
- **Operational isolation:** Response teams and vendors are physically distant, delaying incident containment.
- **Patch management challenges:** Updating navigation or propulsion software may require class approval or dry-dock access.
- **Heterogeneous vendor landscape:** Systems from multiple OEMs may use proprietary or undocumented interfaces.

Together, these factors create environments where traditional IT security models—based on continuous patching, endpoint detection, and centralized response—are often impractical.

CONSEQUENCES OF CYBER COMPROMISE

The impact of a cyber incident aboard a vessel extends far beyond data loss.
Key potential consequences include:

- **Operational disruption:** Loss of propulsion, steering, or navigation data can result in collisions or grounding.
- **Safety risks:** Disabling alarms, sensors, or communication systems endangers crew and cargo.
- **Environmental damage:** Cyber-induced accidents can cause oil spills or hazardous material releases.
- **Financial and reputational losses:** Downtime, regulatory fines, and loss of charter confidence.
- **Supply-chain ripple effects:** Global logistics delays and increased insurance premiums.

GROWING ROLE OF REGULATION AND RISK MANAGEMENT

In response to these escalating risks, regulators and insurers now demand structured cyber-risk management. The **International Maritime Organization (IMO)**, **European Union (NIS2)**, **Maritime and Coastguard Agency (MCA), US Coast Guard**, and national maritime authorities emphasize identifying, protecting, detecting, responding to, and recovering from cyber incidents. Classification societies such as **DNV**, **ABS**, and **Lloyd's Register** have introduced **Cyber Secure** notations that require demonstrable isolation between IT and OT networks.

In this regulatory context, **data diode** solutions are gaining prominence. They provide the physical assurance that even if shore systems are compromised, no command, malware, or signal can traverse back into the vessel's operational core.

In summary, the maritime cybersecurity landscape is defined by a paradox: as ships become smarter and more connected, they also become more vulnerable. Addressing this paradox requires not only awareness and regulation but also architectural solutions that can enforce trust boundaries at the physical layer.

REGULATORY FRAMEWORK AND COMPLIANCE REQUIREMENTS

The global maritime industry is governed by an intricate web of international conventions, regional directives, and national standards. As ships evolve into digitally connected platforms, these frameworks have expanded to address **cybersecurity as an integral element of maritime safety**. Compliance is no longer limited to physical security or pollution prevention; it now encompasses digital resilience, data protection, and the assurance of secure information flow between ship and shore.

THE INTERNATIONAL MARITIME ORGANIZATION (IMO) FRAMEWORK

The **International Maritime Organization (IMO)** is a specialized agency of the United Nations, has established the cornerstone of maritime cybersecurity governance.

IMO Resolution MSC.428(98), adopted in 2017, mandates that cyber risks must be addressed within the **Safety Management Systems (SMS)** required by the **International Safety Management (ISM) Code**.

Ship owners and operators must demonstrate risk identification, protection mechanisms, detection and response procedures, and recovery plans.

The implementation deadline (January 2021) made cybersecurity a mandatory component of vessel audits and certification processes.

The IMO's **Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3)** provide a high-level framework aligned with the **NIST Cybersecurity Framework**, emphasizing the core functions of *Identify, Protect, Detect, Respond,* and *Recover.*

Compliance requires a demonstrable technical separation between critical operational networks (OT) and non-critical systems (IT), a principle where **data diodes** and unidirectional gateways play a direct role.

EUROPEAN UNION NIS2 DIRECTIVE

The **EU Directive on Measures for a High Common Level of Cybersecurity (NIS2)**, adopted in 2023, represents a major regulatory expansion impacting maritime stakeholders across Europe.

It applies to **operators of essential services**, including maritime transport, port facilities, and ship management entities.

Requires **risk management measures**, **incident reporting**, and **supply-chain security assurance** for both IT and OT domains.

Non-compliance can result in fines up to **2% of global annual turnover** or temporary operational suspension.

The NIS2 Directive explicitly calls for *technical and organizational measures* proportionate to the risk, such as network segmentation, secure communications, and system integrity controls.

Data diodes and one-way communication channels are recognized under these principles as effective controls for ensuring secure, tamper-proof data exchange between shipboard OT and onshore IT infrastructures.

UNITED KINGDOM – MCA CODE OF PRACTICE FOR SHIPS

The **UK Maritime and Coastguard Agency (MCA)** published its **Cyber Security Code of Practice for Ships** to establish baseline requirements for British-flagged vessels and UK-based maritime operators.

Emphasizes **defense-in-depth** across IT, OT, and crew training domains.

Defines **five capability tiers**, from basic cyber hygiene to advanced resilience.

Recommends physical and logical segregation between safety-critical and non-critical systems.

References **hardware-enforced one-way gateways** as best practice for preventing inbound cyber threats from external networks.

The MCA framework also integrates with the UK's **NCSC Cyber Assessment Framework (CAF)**, aligning maritime cybersecurity expectations with critical national infrastructure standards.

UNITED STATES – US COAST GUARD NVIC 01-20

The **US Coast Guard's Navigation and Vessel Inspection Circular (NVIC) 01-20** offers guidance for incorporating cyber risk management into Safety Management Systems.

Encourages identification of **critical cyber systems** impacting vessel safety, navigation, or cargo handling.

Requires integration of cyber risk controls into **vessel inspection regimes** and **security assessments** under the **Maritime Transportation Security Act (MTSA)**.

Stresses **segregation of networks** and **limiting remote access** as key risk mitigations.

Recognizes that *mechanisms ensuring unidirectional data flow* provide robust protection against remote intrusion.

CLASSIFICATION SOCIETIES AND INDUSTRY STANDARDS

Major classification societies have complemented regulatory frameworks with their own cybersecurity standards and notations, influencing ship design and retrofitting practices:

DNV – Cyber Secure Class Notation: Covers system architecture, access control, and secure data transfer; explicitly requires one-way communication devices in high-security configurations.

ABS – CyberSafety Program: Provides guidelines for integrating cybersecurity into asset lifecycle management and vessel certification.

Lloyd's Register – Cyber Secure Program: Includes risk-based assessment and verification of shipboard IT/OT segregation.

BIMCO Guidelines on Cyber Security Onboard Ships: An industry reference adopted globally for practical implementation of the IMO's principles.

CERTIFICATION AND COMPLIANCE TRENDS

The convergence of international and national frameworks has created a unified expectation: Ships must **demonstrate secure, traceable, and auditable data flow controls**. Emerging trends include:

Mandatory cybersecurity audits as part of annual ISM and Document of Compliance (DoC) renewals.

Integration of cyber controls into design phase documentation for new builds.

Insurance-linked compliance, where underwriters require evidence of cyber segregation.

IMPLICATIONS FOR SHIP OWNERS AND OPERATORS

For fleet managers, compliance is not merely regulatory, it is strategic. A compliant vessel:

- Minimizes the risk of operational downtime and cargo delays caused by cyber incidents.
- Qualifies for lower insurance premiums and preferential charter terms.
- Demonstrates due diligence to regulators, customers, and investors.
- Strengthens overall fleet resilience against state and criminal cyber actors.

Hardware-enforced one-way transfer solutions**,** validated through certification and integrated within a vessel's safety management architecture, offer a proven path to achieving these objectives with measurable assurance.

WHY ONE-WAY DATA TRANSFER IS CRITICAL

As maritime operations embrace digitalization, vessels must continuously exchange operational data with shore-based centers for performance monitoring, predictive maintenance, compliance reporting, and logistics optimization. However, every data link between ship and shore represents a potential pathway for cyber intrusion. In a domain where system compromise can directly endanger lives, cargo, and the environment, the direction of data flow becomes a fundamental security control.

One-way data transfer, implemented through hardware-enforced data diodes, provides the most reliable means of ensuring that critical onboard networks remain *physically immune* to external manipulation while still allowing essential information to flow outward.

SECURITY DILEMMA OF MARITIME CONNECTIVITY

Modern ships require connectivity for numerous legitimate purposes:

- Transmission of **engine performance and fuel efficiency data** to shore analytics platforms.
- Uploading of **voyage reports, emission records, and compliance logs** to fleet management systems.
- Communication with OEMs for **remote diagnostics and software updates**.
- Exchange of **logistics and port documentation** via satellite or broadband links.

However, each of these communication channels inherently allows *bidirectional* traffic—creating potential vectors for:

- Malware infiltration through remote maintenance sessions.
- Command injection or system tampering via compromised shore systems.
- Credential theft and lateral movement between IT and OT networks.

Traditional software-based protections, such as firewalls or intrusion detection systems, depend on configuration correctness and ongoing maintenance—both of which are challenging in maritime environments. Misconfigurations, outdated rules, or insider actions can inadvertently reopen critical pathways.

A data diode removes this dependency entirely by using **physical architecture**, not policy, to enforce directionality.

DEFINITION AND OPERATION OF DATA DIODE

A data diode is a pair devices used in the field of information security and its main function is to provide one-way data flow between two different security classified networks. These devices are generally used in environments with high security requirements, especially in industrial control systems (ICS) and critical infrastructures. Main purpose of a data diode is to protect against external threats and to ensure the security of the internal network while allowing transfer of data unidirectionally from one network to another. Data diodes are also designed to prevent data leaks and network breached. Data diodes are hardened software suites combined with special hardware solutions.

BASIC COMPONENTS AND WORKING PRINCIPLE

Basic principle of data diodes is that they are designed to transmit data in only one direction. Some manufacturers refer to these devices as "unidirectional gateways." Data diodes are critical for improving network security by creating segmentation. These devices create a physical barrier between the source and destination network, allowing only certain types of data to pass through. Basic components of data diodes include optical data transmission systems, which enable data to be transmitted between the source and destination networks. These systems convert data signals into optical signals, allowing them to be transmitted securely. Also, data diodes often include data filtering, encryption, and other security protocols. These features ensure that only secure, not-changed and authorized data is allowed through.

DATA FLOW CONTROL

The flow controlled by the data diode forms the basis of network security. These devices ensure that data coming from the source network passes certain security checks before reaching the destination network. Data diodes prevent, possibly unsafe or harmful data flow, having necessary awareness of data types and protocols. For example, a data diode only allows the transfer of data packets of a certain file type such as pdf or jpg, or control protocol like modbus, mqtt, profinet etc. thus protecting the integrity of the network. Data diodes also constantly monitor and analyze network traffic to prevent data leaks and to protect against external attacks. The physical barrier created makes it impossible any incoming data to pass from the external network to protected zones.

Because the receiving interface lacks any physical ability to send data, **no command, packet, or malware** can travel backward into the protected domain. To accommodate modern communication protocols, data diode systems often include:

- **Protocol brokers or replicators** that reconstruct TCP sessions unidirectionally.
- **Caching servers** that receive and forward data to destination systems.
- **Integrity verification modules** ensuring that the transmitted data remains complete and untampered.

This combination enables transparent, real-time data export without violating the unidirectional security boundary.

Use of data diodes is especially important in sensitive environments such as factories, power plants, water treatment systems and similar critical infrastructures and maritime industry is no exception. These devices provide protection against cyber-attacks while also ensuring an

efficient and uninterrupted workflow. The secure transmission of critical information and control commands is fundamental to the proper functioning of these environments.

Data diodes are an essential part of modern cybersecurity strategies and play a key role in increasing the security of industrial control systems (ICS). Using diode technology not only protects against current threats, but also increases resilience to future cyberattacks. Effective use of data diodes creates the foundation for a secure and reliable industrial network infrastructure, which also increases industrial efficiency and security in general. By transferring the data required from the OT network to the IT, to generate reports that help increase business productivity, minimize reporting costs in the OT network, while the necessary visibility to business analysis is provided.

PRACTICAL MARITIME USE CASES

The use of one-way data transfer is increasingly recognized as a **best practice for shipboard network architecture**, with applications including:

- **Voyage and performance data transmission:** Securely sending navigation, fuel, and weather data from the bridge to the fleet operations center.
- **Predictive maintenance:** Forwarding engine and machinery telemetry to OEM support teams while blocking any return access.
- **Regulatory reporting:** Exporting emissions, ballast water, and cargo status data to environmental agencies or charterers.
- **Security event logging:** Sending OT logs and intrusion alerts to a central SOC without permitting inbound scanning or probing.
- **Port and harbor integration:** Providing situational awareness to port authorities without exposing internal control networks.

In each case, the diode ensures that data can *leave* the vessel for analysis but that **no digital pathway exists for commands or code to re-enter**.

ADVANTAGES OVER CONVENTIONAL SECURITY CONTROLS

Control Type	*Limitation*	*Data Diode Advantage*
Firewalls	Software-based, reconfigurable, and susceptible to misrules or exploits	Physical one-way enforcement, immune to software tampering
VPNs	Encrypted but bidirectional—still allows remote entry if compromised	Outbound-only data movement, no inbound channel
Air Gaps	Prevent all communication—including required reporting and monitoring	Controlled, verifiable one-way flow enables safe connectivity

OPERATIONAL AND BUSINESS BENEFITS

Beyond compliance, the adoption of one-way data transfer provides measurable value:

- **Safety and reliability:** Eliminates the risk of remote control over propulsion, navigation, or power systems.
- **Operational continuity:** Enables data sharing without exposing the vessel to external disruption.
- **Simplified compliance:** Meets IMO, NIS2, and class requirements for network segregation.
- **Reputation and trust:** Demonstrates proactive cyber maturity to regulators, insurers, and clients.
- **Lifecycle efficiency:** Reduces dependence on constant patching or remote-access monitoring.

In essence, the data diode allows a vessel to remain *digitally connected but logically untouchable*.

STRATEGIC IMPORTANCE FOR THE FUTURE FLEET

As ships evolve toward greater autonomy and AI-driven decision support, data flow between vessel and cloud will intensify. Each additional sensor, digital twin, or analytics module increases the number of interfaces exposed to cyber risk. The ability to enforce **trusted, verifiable, and physically isolated communication channels** will therefore become a defining feature of next-generation fleet architectures.

For forward-thinking operators, investing in one-way transfer infrastructure today is not merely a compliance measure—it is a strategic safeguard ensuring that tomorrow's digital fleet remains **safe, resilient, and sovereign.**

TECHNICAL ARCHITECTURE OF A MARITIME DATA DIODE SYSTEM

A maritime data-diode solution provides a secure, hardware-enforced communication channel that ensures information moves in only one direction, from the ship's operational network to external or corporate networks.
Unlike generic network equipment, it is purpose-built to enforce **non-returnable, verifiable data flow**, even under hardware tampering or software compromise. This section outlines its architecture, integration model, and practical deployment scenarios for modern vessels.

SYSTEM OVERVIEW

A complete maritime data-diode setup typically consists of three logical layers:

Source Domain (Protected Critical OT Network)
The onboard operational systems that generate critical data:

- Navigation (ECDIS, radar, GPS, AIS)
- Engine and propulsion control (IPMS, PMS, EMS)
- Cargo handling, ballast, and tank monitoring
- Alarm and safety systems
- Environmental and emission sensors

Data Diode Solution (Security Enforcer)
The hardware module consisting a pair of device that provides **physical one-way connectivity**:

- Transmit-only interface (TX-only) on the OT side
- Receive-only interface (RX-only) on the IT/shore side
- Intermediate software services for data buffering, replication, and integrity checking

Destination Domain (Shore or IT Network)
The systems receiving and processing data for analytics, compliance, and monitoring:

- Fleet Operation Centers (FOC)
- Maintenance and logistics servers
- Cloud or hybrid analytics environments
- Port authority or regulatory systems

The diode acts as a **one way bridge**, allowing selected telemetry to cross the boundary while making reverse communication physically impossible.

PHYSICAL AND LOGICAL DESIGN

At the **physical layer**, the diode enforces unidirectionality using optical isolation. Data diode devices are equipped with special optical module that employ fiber transmitters and photodiodes configured for one-way light propagation. Traffic Is transmitted from a light emitting module to a light absorbing module

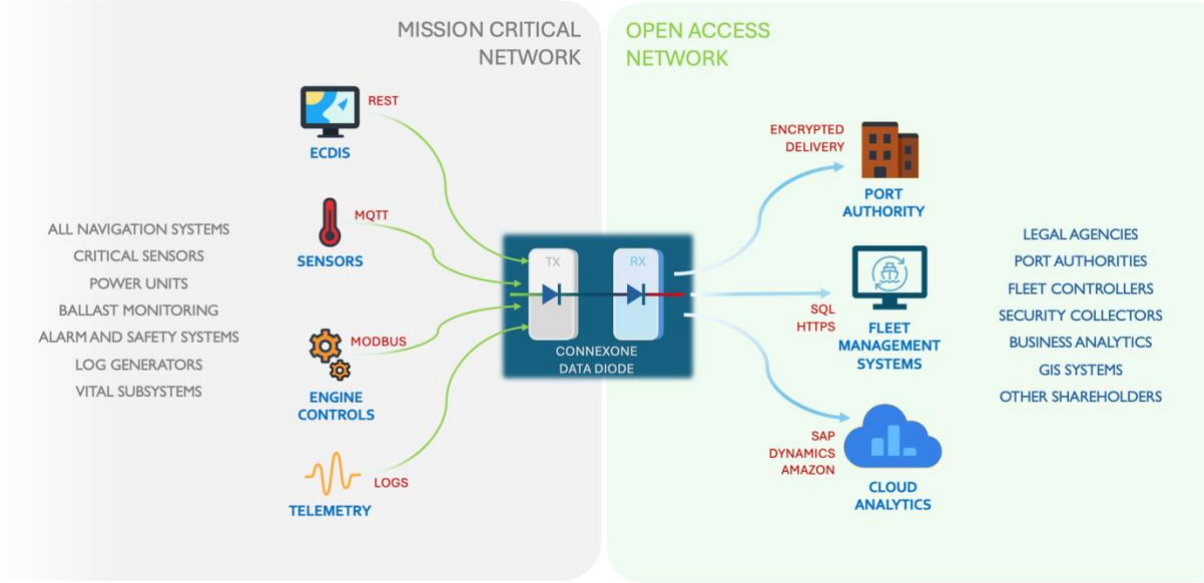
At the **logical layer**, specialized middleware ensures that any network protocols (no matter if it is standard or proprieraty), which normally require acknowledgments, can still function. This is achieved through protocol adaptation components:

- **Protocol Adapters:** Emulates acknowledgment packets internally while ensuring no external reply passes backward.
- **UDP Flows:** Passes stateless datagrams (e.g., NMEA, syslog, SNMP traps) directly through the diode.
- **File Transfer Replicator:** Receive files from a web interface, monitors shared directories or FTP servers on the OT side and transfer data outward.
- **Message Queue Bridge:** Run as an MQTT broker for data generators to subscribe and publish these data to remote site brokers

These software components run in **dual-domain mode**, a receiving device on the OT side and a transmitting device on the IT side, synchronized through the diode's physical one-way channel.

TYPICAL NETWORK TOPOLOGY

As stated above, the topology ensures that **no inbound pathway** exists toward the vessel's operational domain. Even if the IT or cloud network is compromised, malicious packets cannot physically reach the shipboard controllers



SUPPORTED DATA TYPES AND PROTOCOLS

Connexone data diodes are protocol-agnostic and support all protocols that are possibly in use in maritime systems, including but not limited to:

Function	*Example Protocols*	*Description*
Navigation and voyage data	NMEA 0183, NMEA 2000, AIS, ECDIS exports	Securely transmit route, position, and time data
Machinery monitoring	Modbus/TCP, MQTT, PROFINET, OPC-UA,	Share performance metrics and alarms
Log replication	Syslog, JSON, CSV, SNMP	Forward security and operational logs
File and report transfer	FTP, SFTP (replicated), HTTP POST, SMB mirroring	Export reports and sensor snapshots
Compliance and emissions	SQL, REST, XML, CSV to regulatory endpoints	Automated MARPOL Annex VI or MRV submissions

REDUNDANCY AND RELIABILITY

Given the mission-critical nature of maritime operations, data-diode deployments often include:

- **Dual-channel redundancy:** Two independent one-way links (A/B) for failover.
- **Buffered transmission:** Local storage for several hours/days of data if connectivity drops.
- **Health monitoring:** Diode status reporting sent outward to fleet SOCs.
- **Tamper detection:** Embedded sensors or seals that trigger alerts if casing integrity is breached.

This architecture ensures continuous operation even under harsh maritime conditions and intermittent satellite connectivity.

INTEGRATION AND MAINTENANCE

Integration is typically performed during vessel retrofit or new-build phases:

- **Network segregation plan** defines which subsystems belong to the OT, DMZ, and IT zones.
- **Routing and VLAN configuration** ensure diode traffic isolation.
- **Configuration management** is handled locally; no remote administration channel exists on the protected side.
- **Periodic verification tests** use unidirectionality test kits or loopback validation tools to prove compliance during audits.
- **Protocol deployments** define data retrieval and transferring methods during operation

Maintenance involves firmware validation, audit log review, and physical inspection, tasks easily aligned with annual ISM and class survey schedules. Data storage is an important function as most of the data must be achieved during operation due to limited bandwidth and should be transferred once land connectivity is more robust.

The technical architecture of a maritime data diode system merges **hardware isolation**, **protocol intelligence**, and **redundant reliability** into a single protective layer. By allowing critical information to flow securely outward, without any physical means of return, data diodes enable ships to participate fully in the digital maritime ecosystem while preserving the absolute isolation demanded by maritime safety and regulatory compliance.

INTEGRATION WITH MARITIME OPERATIONS

Data diodes deliver the most value when they're embedded in day-to-day ship–shore workflows, not just installed as a "black box." This section maps typical maritime operations to one-way data flows, shows what gets sent, who uses it, and how to run the process reliably under real sea conditions. Below is a table that shows usage of data diode on several operational requirements. Some common controls applied to all items, such as outbound-only health heartbeat, OT-side buffering with threshold alerts, allow-listed topics/paths, integrity hashing at source, quarterly unidirectionality validation (hardware + simulated tests).

Use Case	Objective	Shipboard Sources (OT)	Diode Flow (OT → IT/Shore)	Shore Consumers	Key KPIs
Fleet Performance & Voyage Ops	Give FOC continuous visibility without exposing bridge/engine OT.	ECDIS track/ETA, speed profile, weather route; engine & fuel (SFOC, RPM, load); power–speed deviation; auto noon reports.	OT collector/broker → **Data Diode** → IT collector → FOC dashboard / data lake.	FOC, chartering, route optimization, commercial ops.	Delivery success ≥ **99.5%**; 95th-pct ship→shore delay ≤ **60s**; fuel variance ≤ **3%**.
Predictive & CBM	Enable OEM/tech analysis without any remote access into OT.	IPMS/PMS telemetry (temps, vibration, lube oil), alarms, running hours/counters.	MQTT/OPC-UA on OT → **Diode** → IT message bus / CMMS.	OEM support, Technical Dept., CMMS/ERP.	Mean time-to-insight ≤ **10 min**; shore confirmation ≥ **95%**.
Environmental & Compliance	Automate evidence-grade MRV/DCS/MARPOL reporting with tamper-proof trail.	Fuel flow & emissions sensors, bunkering records, ballast/tank monitors, noon/emissions logs.	OT file drops (CSV/XML) → **Diode** → SFTP/HTTPS to compliance systems.	Compliance team, regulators, insurers.	On-time submissions **100%**; integrity mismatches **0**.
Port/Terminal Harbor Integration	Share situational data outward without allowing inbound probing.	ETA/ATA, berth/cargo status, safety notices; optional aggregated OT security events.	OT/DMZ export → **Diode** → Port Community System / terminal systems.	Port ops, terminal, harbor master, (optional) Port SOC.	Update latency within port SLA; no inbound sessions.
Crew & Passenger IT Segregation	Prevent IT→OT crossover from crew Wi-Fi / passenger services.	Anonymized usage stats, billing counters, capacity metrics (from IT zones only).	IT metrics (not OT) → **Diode** → Billing/capacity tools.	Billing, IT capacity planning.	Zero OT exposure; export coverage ≥ **95%**.
Security Ops (SOC) & Forensics	Centralize security visibility without creating a return path.	Syslog/CEF from OT firewalls/routers/hosts; IDS alerts (OT DMZ); diode health/status.	OT Syslog/CEF → **Diode** → SIEM/SOAR.	SOC/NOC, cyber risk team.	Log completeness ≥ **98%**; dwell time ↓ **30%** vs. baseline.
Software Updates & Change Mgmt	Perform changes safely **without** inbound connectivity.	Pre/post update hashes, version manifests, maintenance window artifacts.	Hash/version attestations → **Diode** → Change records / audit repositories.	Tech Dept., Class/Flag, compliance.	Audit evidence completeness **100%**; rollback success **100%** in drills.

A quick reference table for application data to protocol mapping is also summarized below:

Shipboard Data	*Typical Protocol*	*Diode Adapter*	*Shore Target*
ECDIS voyage/export	File drop (CSV/XML)	File replicator	FOC / Data lake
Engine & CBM telemetry	MQTT / OPC-UA	Msg bridge	CMMS / Analytics
Security logs	Syslog/CEF	Log forwarder	SIEM/SOAR
Emissions/MRV/DCS	CSV/XML	SFTP/HTTPS forwarder	Reg portal / Compliance DB
Alarms & events	SNMP traps / MQTT	Trap → REST mapper	NOC/TSC dashboards

OPERATIONAL ACCOUNTABILITY AND PERFORMANCE

During routine operations, the vessel treats the data diode as part of its voyage discipline rather than an exceptional control. Before departure, the crew verifies the diode heartbeat, buffer headroom, and a signed “readiness token” export to confirm ship-to-shore flow. While underway, telemetry and summaries are pushed on fixed intervals, short cycles (minutes) for live metrics and hourly rollups for efficiency and compliance, without any return channel. If satellite connectivity drops, the OT-side buffer silently absorbs data; only when it approaches saturation does the crew receive a local warning. On arrival, the diode health report and export statistics accompany the port documentation, and each quarter, the ship performs a formal unidirectionality validation combining a hardware loop test with a software simulation to keep audit evidence current.

Clear accountability keeps this simple. The Master and Chief Engineer are responsible for the integrity of OT boundaries and approve what leaves the ship. The ETO/IT Officer runs the diode and OT collectors day-to-day, conducts visual inspections, and maintains configurations on the protected side. On shore, the FOC and SOC monitor collectors, dashboards, and alerts, while the Compliance Officer owns regulatory pipelines and evidence retention. External stakeholders, class, flag, and regulators, consume the exported proof during surveys and audits without ever requiring inbound access to ship systems.

Performance is managed through a small, visible set of KPIs and SLAs that translate directly into business value. Telemetry freshness is tracked via ship-to-shore latency percentiles; export coverage measures what proportion of defined data points successfully arrive each voyage; and integrity is demonstrated through hash-match rates and a standing expectation of zero tamper alerts. Availability is expressed as diode link uptime and the absence of OT buffer overflows, while security posture is evidenced by the rate of OT incidents and the categorical blocking of inbound attempts. These metrics are surfaced on concise dashboards for bridge/engine room and on consolidated views for fleet, compliance, and security teams.

Implementation follows repeatable playbooks. A fast retrofit pattern connects existing OT collectors to the diode and into shore collectors for quick wins on logs, telemetry, and reports

with minimal change to the vessel. A high-assurance pattern adds an OT DMZ with protocol brokers, sanitizers, strict schemas, and allow-lists before traffic reaches the diode, targeting class notations and elevated assurance. Where multiple stakeholders need the same data, a fan-out model sends a single export across the diode to a shore broker that distributes curated feeds to FOC, OEMs, insurers, and port systems—reducing satcom load while keeping control on shore. Across all patterns, the principle remains constant: **outward visibility with physically enforced inward silence**.

By binding each maritime workflow to a **one-way, audited data lane**, operators gain real-time insight without introducing remote-control risk. The diode becomes a routine part of voyage ops, maintenance, compliance, and security—quietly guaranteeing that the ship stays **connected outward, unreachable inward**.

VALUES OF USING DATA DIODE

Modern fleets add value from data diodes across four dimensions: **safety**, **continuity**, **compliance**, and **cost**. Hardware-enforced one-way transfer preserves operational visibility while removing the catastrophic tail-risk of inbound compromise.

Safety & Cyber Resilience

- Physically prevents command/control into OT (navigation, propulsion, power).
- Stops ransomware and remote-access misuse from reaching ship control planes.

Operational Continuity

- Keeps performance/maintenance data flowing even under heightened cyber posture (no need to “pull the plug” on connectivity during incidents).
- Buffered exports ride out satcom outages; automatic resume prevents data loss.
- Crisis posture without blackout, keeps exporting data to shore SOC/FOC during an incident while keeping OT unreachable.
- Vendor management of OEMs analyze rich datasets without remote access exceptions that erode assurance.

Compliance & Assurance

- Demonstrable network segregation for IMO/ISM, NIS2, MCA, USCG, and class notations.
- Evidence-grade reporting (hashes, WORM storage) streamlines audits, PSC, and vetting.

Commercial Trust

- Signals cyber maturity to charterers, ports, and insurers; supports better charter terms and premiums.

Any preventive measure comes with a cost. It needs to be assessed what this cost recovers and how long it takes for the return on investment. Data diodes provide excellent figures when it comes to cost and ROI. Initial costs include data diode appliances and licenses, together with a one-time installation service cost. All required integration with shore collectors and brokers is covered in initial service. As long as data diode solutions remains under a valid service contract all software updates and new protocol integrations would be provided without any additional cost. SIEM integrations, log parsing, offline data archival, all comes within the software package, so there will not be any hidden cost as operation continues.

Data diode implementations have impacts on insurer and charterer agreements:

- **Underwriting:** Documented one-way segregation + SIEM export often qualifies for cyber endorsements and excess reductions.

- **Charter parties:** Demonstrable cyber posture can be negotiated into performance clauses (fewer cyber-caused delays, improved transparency).
- **Financing:** For green/efficiency-linked financing, continuous, tamper-proof telemetry supports verified emissions and performance disclosures.

DATA DIODE TECHNOLOGY IN THE FUTURE

EXPECTED INNOVATIONS AND DEVELOPMENTS

Data diode technology quickly finds its place in the field of cybersecurity and will continue to develop and lead to significant innovations in the future. The evolution of this technology would include advancements in both hardware and software. Among the expected developments, increased data transfer speeds and wider bandwidths will be prominent. This will allow data diodes to process larger data volumes more quickly and will be especially critical for big data analytics and real-time data processing requirements.

The integration of AI and machine learning is another major development expected in data diode technology. This will help data diodes detect and prevent cyber threats more effectively and will also be used to optimize data flow and improve network performance.

Quantum processing capabilities introduces new options for encryption solving, risking current implementations future usage, as data is no longer sent without any secure delivery option. Combining data diodes with one-time-pad or post-quantum encryption would extend expected lifetime of the products.

In addition, future data diode technologies can be designed to be more modular and flexible, meaning modern devices that can easily adapt to different network structures and changing operational requirements, and offer customizable solutions. Also, advances in wireless communication technologies can expand the use of data diodes and offer new types of connectivity options.

Maritime digital twin ecosystems is getting to be the standard, where safe data flow to simulation and training platforms from actual fleets would be implemented as part of usual operations, where data diode plays a significant role.

CONCLUSION

Maritime operations have entered a new era where data is mission-critical to safety, efficiency, compliance, and competitiveness. Ships are now highly connected platforms, continuously exchanging telemetry with shore for voyage optimization, condition-based maintenance, emissions reporting, and security monitoring. This transformation creates undeniable value, but it also expands the attack surface and elevates operational risk in environments where a single compromise can endanger life, cargo, vessels, and the marine environment.

Throughout this document, we've shown that the core challenge is not whether ships should be connected, but **how** they can be connected safely. Traditional controls such as firewalls, VPNs, and access policies, are necessary but insufficient in isolation. They are software-defined, reconfigurable, and vulnerable to misconfiguration or exploitation. In contrast, **hardware-enforced one-way transfer (data diodes)** delivers a non-negotiable security boundary that preserves outward visibility while making inbound digital access physically impossible. This quality is precisely what regulators, classification societies, insurers, and responsible operators increasingly expect.

The case for data diodes is therefore both technical and strategic. Technically, they provide verifiable unidirectionality, protocol adaptation for real-world workflows, buffering for satellite outages, and evidence-grade integrity with hashing and immutable storage. Strategically, they reduce tail-risk from catastrophic cyber events, improve audit readiness under IMO/ISM, NIS2, MCA, and USCG regimes, unlock measurable operational gains (fuel, uptime, maintenance), and reinforce trust with charterers, ports, and underwriters. Our practical mappings, spanning fleet performance, CBM, compliance, port integration, SOC visibility, and change management, demonstrate that one-way data lanes fit seamlessly into day-to-day maritime workflows.

Equally important, this approach **scales**. Whether you retrofit a single vessel or roll out fleet-wide, the pattern remains constant: define the export scope, buffer and hash at source, enforce one-way transmission via a data diode, and fan-out on shore to analytics, CMMS, SIEM, and compliance systems. With clear roles (Master/Chief Engineer accountable for OT integrity; ETO operating the diode; FOC/SOC/Compliance consuming exports) and a lean KPI set (latency, coverage, integrity, availability, and incident rates), operators can manage performance and prove assurance without adding crew burden.

Looking forward, the value of assured one-way connectivity only increases. As fleets adopt AI-assisted routing, digital twins, and greater automation, the volume and sensitivity of ship-to-shore data will grow. Post-quantum and high-assurance cryptographic controls will mature, but they will complement, not replace, the need for **physical** trust boundaries. Data diodes, combined with strict OT/IT segregation, signed updates delivered in port, and rigorous evidence packs, provide a resilient foundation for the autonomous and data-intensive fleet of the next decade.

For operators, the path is clear and actionable:

- **Design for asymmetry:** Treat outward visibility and inward silence as a first principle of shipboard architecture.
- **Codify workflows:** Bind each operational process (voyage, maintenance, compliance, security) to a dedicated one-way lane with KPIs and evidence capture.
- **Prove it, repeatedly:** Validate unidirectionality quarterly; hash, store immutably, and surface metrics in simple dashboards for crew and shore.
- **Scale with governance:** Use a shore-side broker to serve multiple stakeholders without duplicating satcom traffic or expanding the attack surface.

In short, the maritime sector does not have to choose between connectivity and safety. With hardware-enforced one-way transfer at the center of a layered security posture, fleets can remain **connected, compliant, and resilient**, realizing the benefits of digitalization without conceding control of their most critical systems. This is the blueprint for modern marine operations: **secure data out, nothing back in.**