Deloitte.

Together makes progress

Resilient OT environments for the future of autonomous maritime shipping

Introduction

Autonomous maritime shipping is likely to reshape global logistics and supply chains. By increasing the overall efficiency and reducing operational costs, safe vessel operation depends on secure digital systems, reliable connectivity, and effective support from shore. Operational Technology (OT), once isolated and stable, starts interacting with onboard Information Technology (IT) networks, satellites, and remote operations centers. At the same time, recent industry cases demonstrate how cyber incidents can disrupt entire fleets, ports, and supply chains including heavy monetary consequences. Therefore, the resilience of maritime OT requires special attention due to its specific technical requirements. Maritime OT must not only be protected, but also remain available, reliable, and recoverable under deteriorated conditions. As autonomy and remote operation increases, resilient OT environments become a core prerequisite for safe, controllable, and continuous vessel operations.

Background

Autonomous Shipping

In recent years, autonomous shipping has progressed from experimental deployments to early commercial adoption. Various initiatives already demonstrate the feasibility of supervised autonomous navigation and remote vessel operation, promising improved safety by reducing human error, the main cause for maritime accidents. At the same time, increased digitalization and connectivity introduces new risk vectors, such as integrated navigation systems, remote-control capabilities, as well as satellite-based communication drastically expands the attack surface. To summarize, the same connectivity that enables autonomy also becomes the primary pathway for its disruption, making "resilience by design" mandatory.

What is OT?

One of the most prominent definitions of OT refers to the hardware and software that monitors and controls physical processes. In contrast, IT primarily manages data and information flows while OT is designed around availability, continuity,and predictable control of real-world operations. It frequently involves systems that are characterized by prolonged lifecycles, including limited update availability as well as legacy components. In the maritime context, OT includes propulsion, steering, navigation, cargo handling, ballast, auxiliary machinery, and other safety-critical onboard functions. These systems no longer operate in isolation, but as tightly connected parts of a single operational environment. Disruptions can affect vessel movement, stability, machinery performance, and safety.

Therefore, they differ from many land-based OT settings, as ships are mobile, self-contained, and maintenance-constrained, with limited intervention options at sea. As digital integration and shore-based support increases, resilient maritime OT becomes essential for safe, continuous, and controllable vessel operations. The distinction is vital as making security-only efforts also fall short. The lack of immediate human intervention at sea requires safe operation during partial outages, delayed support options, and well-defined fallback procedures for critical functions.

Technical Foundations

Technical Basics/Terminology

To gain transparency, it requires looking into the complex and interconnected IT and OT vessel's network. It is often referred to as the Ship Area Network (SAN) and includes various Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition systems (SCADA), sensors, and actuators operating propulsion, steering, and auxiliary systems. Communication relies on protocols such as Transmission Control Protocol (TCP), Controller Area Network (CAN) bus, and National Marine Electronics Association (NMEA), which frequently lack authentication or encryption. Modern navigation stacks combine Global Positioning System (GPS), radar and Automatic Identification System (AIS) systems, creating complex sensor-fusion environments. As autonomy increases, these systems support automated decision-making and remote operation, requiring highly reliable, validated data flows and secure, segmented network architectures.

The following core domain's structure this complex environment as most relevant ones from a resilience and attack-surface perspective:

01 Ship Area Network

The Ship Area Network is the digital backbone of a modern ship, connecting onboard IT and OT systems, from navigation sensors to engine controls. Its segmentation and reliability determine how effectively data flows across the vessel and is therefore critical for autonomy, remote monitoring, and secure operations. A resilient SAN minimizes lateral movement risks and prevents single-points of failures.

02 Engine & Control Systems

Engine, propulsion, and machinery control systems rely on PLCs, sensors, and actuators to ensure stable vessel performance. These systems are highly availability focused and often built on legacy architectures, making them sensitive to disruptions. In autonomous operations, continuous monitoring, anomaly detection, and fail-safe control paths become indispensable.

03 Bridge & Positioning

Bridge systems integrate GPS, radar, AIS, Electronic Chart Display and Information System (ECDIS, and sensor fusion algorithms to maintain situational awareness. Autonomous navigation depends on the integrity and cross validation of these data sources, making spoofing or jamming a critical operational threat. Robust validation and fallback modes ensure safe navigation even under degraded conditions.

04 Ballast Water Management & Sewage Treatment

Ballast and sewage treatment systems are essential for vessel stability, environmental compliance, and safe operations. They often consist of isolated, vendor-specific OT components that were not originally designed for remote connectivity or cybersecurity. As ships become more digitally integrated, these systems must be monitored to prevent unintended manipulation or operational downtime.

05 Cargo Area & Tank

Cargo handling and tank monitoring systems control loading, discharge, pressure, temperature, and safety mechanisms across cargo compartments. Their correct functioning is crucial both economically and for safety, especially in tanker or gas carrier environments. Integrated monitoring and secure automation help prevent hazardous situations and support predictive maintenance.

System Interaction in Autonomous Shipping

Proposed autonomous vessel concepts rely on tightly integrated system architectures, in which sensor data supports navigation logic and automated control of propulsion, steering, and dynamic positioning. Depending on regulatory approval and technical maturity, Shore Control Centers are expected to monitor vessel status and potentially support remote operations. AI-driven algorithms rely on continuous data integrity, making manipulation or spoofing a major operational risk. OT and IT boundaries blur as performance monitoring, predictive maintenance, and remote diagnostics require continuous connectivity. Without robust segmentation, monitoring, and fallback modes, a single compromised subsystem, navigation, communication, or engine control, can cascade into full vessel loss of control.

Challenges & Solutions

Data Provisioning and Land Ship Connectivity

Future maritime vessels rely on high quality, continuous data exchange between the ship and shore. However, maritime connectivity has a limited bandwidth and availability. Furthermore, they pose an ideal entry point for attackers, as it restricts real time monitoring, patching, and anomaly detection. For instance, leveraging certain latest technologies can even present a political threat by itself to rely on a single vendor and therefore being dependent on it. Increased connectivity also introduces the risk of poorly secured remote access channels, that already have been exploited in previous maritime cyber incidents. Therefore, secure communication, encryption, authentication, jamming resilience, and robust network architectures are essential for safe and reliable autonomous operations.

Heterogeneity of Systems

Ships contain a diverse ecosystem of vendor-specific OT components with varying standards, documentation quality, and patch cycles. Many systems are outdated and were retrofitted into digital networks without cybersecurity considerations. This leads to inconsistent architecture, limited asset visibility, and complex integration challenges. As autonomy scales, such heterogeneity complicates security monitoring, incident response, and lifecycle management. Therefore, a unified governance framework and standardized OT risk assessment practices are critical to overcome these barriers.

Spoofing & Jamming

Navigation systems are ideal targets for external attackers, as fundamental decisions are made based on the estimated position. Jamming disrupts position detection, while spoofing injects manipulated coordinates into navigation systems. For instance, AIS transmissions lack authentication, allowing false “person overboard” signals or phantom vessels. As autonomous vessels rely on sensor fusion of positioning sensors, cameras, radar and lidars, attackers gain opportunities to influence automated decision making. Multi-layer cross validation across independent sensors is necessary to detect and reject manipulated data before it affects maneuvering.

Maintenance Workforce vs. Autonomy

State-of-the-art maritime operations use onboard engineers who troubleshoot mechanical and digital systems most of the time. However, a reduced crew presence on board also comes with fewer opportunities to manually intervene when systems malfunction or IT/OT infrastructure is compromised. Therefore, autonomous vessels will likely shift the responsibility for maintaining the on-board systems towards shore teams (e.g. analog to road-assistance mechanisms) and automated diagnostics, requiring remote maintenance capabilities, robust fail-safe modes, verified firmware updates, and well designed fallback procedures.

Conclusion

To address cybersecurity risks in OT-heavy maritime environments, including autonomous vessel operations, a range of technical and organizational measures is commonly discussed. These measures include OT security operations, secure remote access, governance and readiness activities, threat detection, asset visibility, incident response, and business continuity. These measures are often structured end-to-end across ship-based and shore-based systems and aligned with established standards and regulatory frameworks, including IEC 62443 and NIS2.

Too summarize, resilient OT maritime environments can be achieved when (1) most critical processes remain stable locally and under harsh conditions, (2) degraded and compromised network segments are segregated through segmentation, (3) multi-sensor validation ensures that navigation decisions are reliable, and (4) recovery operations are realistic and feasible even with no or just limited human intervention capabilities for maintenance.

Organizations seeking support in analyzing, designing, or assessing such measures may consider engaging external service providers with maritime and OT security experience. Deloitte provides maritime cybersecurity services covering fleet-wide OT assessments, port infrastructure security, and large-scale cyber transformation programs. Deloitte's services include an end-to-end approach including risk-based maturity assessments aligned with the relevant standards and regulatory requirements, as well as advisory activities in vessel and shore environments.

Contact

Fabian Mihailowitsch

Partner I Cyber
Technology & Transformation
Tel: +49 89 290366 998
fmihailowitsch@deloitte.de

Benjamin Janzer

Partner I Cyber
Technology & Transformation
Tel: +49 89 290367 665
bjanzer@deloitte.de

Designed by CoRe Creative Services. RITM2489953