Contributions Operations Tech

Most maritime AI failures will be data failures, not algorithmic

Splash • March 18, 2026 544 3 minutes read

Anil Kumar Korupoju, a senior surveyor at the Indian Register of Shipping, writes for Splash today, stressing the importance of data integrity.

Artificial intelligence (AI) is increasingly influencing areas of vessel operation that were traditionally governed by human judgement and physical verification. Collision awareness tools, predictive maintenance systems, and structural monitoring platforms now contribute to decisions with clear safety implications. From a classification standpoint, that shift demands closer scrutiny.

Much of the current discussion around AI focuses on model capability: predictive accuracy, anomaly detection, even the promise of autonomy. Far less attention is paid to the integrity of the data feeding these systems. In practical terms, the most serious weaknesses in maritime AI will not stem from flawed algorithms. They will stem from degraded, inconsistent, or poorly governed data.

At sea, data is rarely pristine. Sensors drift over time. Calibrations shift. Automatic Identification System (AIS) signals can be incomplete in congested waters and vulnerable to manipulation in certain regions. Global Positioning System (GPS) quality fluctuates. Time alignment across systems is not always exact. These are not exceptional circumstances; they are routine operating conditions.

An AI system has no inherent awareness that a sensor has moved out of calibration unless controls are designed to detect that change. It will continue to generate outputs that appear coherent and technically sound. The difficulty is that those outputs may gradually diverge from physical reality without triggering an obvious fault condition. Mechanical defects tend to reveal themselves clearly. Data degradation, by contrast, is often subtle and progressive.

As AI moves closer to navigational decision support, that distinction becomes increasingly important. While high-performance GPUs have largely eliminated raw computational power as a bottleneck, fully autonomous manoeuvring in congested or ambiguous traffic is less constrained by computational power and more by complexity: dynamic and unpredictable patterns, rare scenarios and edge cases, conflicting inputs and the need for contextual judgement. Without structured revalidation and clearly defined operating limits, performance can drift outside the tested envelope without immediate visibility.

From a classification perspective, reliance on a single data source is particularly concerning. AIS, for example, is valuable but not infallible. Cross-verification through independent sources has long underpinned safe navigation. AI systems that do not embed that discipline introduce predictable vulnerabilities.

When digital tools influence navigational awareness or structural assessment, data governance becomes a safety matter, not a technical detail. That requires documented data lineage, clearly

defined limits of use (the intended Operating Design Domain, or ODD), traceable version control, and rollback to previously validated configurations. It also requires continuous monitoring to detect performance drift and clear accountability for system updates. These are safeguards against gradual degradation, not responses to visible failure.

For owners, the implications extend beyond technical reliability. If an AI system contributes to a navigational or maintenance decision, accountability does not sit with the algorithm. It sits with the operator. In the event of an incident, questions will focus on data integrity, validation boundaries, and update control. Insurers and financiers are already examining how digital systems are governed, not simply whether they are installed. Claims that AI reduces risk will increasingly require documented oversight and evidence of continuous monitoring. Without that discipline, digital ambition may translate into greater exposure rather than reduced liability.

Cyber integrity should be viewed through the same lens. Once AI outputs inform operational decisions, compromised inputs translate directly into operational risk. Authenticated time synchronisation, controlled access management, network separation, tamper-evident event data, and protected audit logs are not peripheral IT measures; they form part of the assurance framework. Where appropriate, systems should implement cross-sensor reconciliation (e.g., AIS vs. radar/EO) and confidence flags so operators understand when the system is degrading gracefully.

Structural health monitoring provides a useful comparison. Sensor-based fatigue analysis can strengthen inspection planning when properly calibrated and validated against physical findings. However, digital outputs must always be reconciled with engineering assessment and inspection evidence. Data should support professional judgement, not displace it.

Artificial intelligence will continue to expand its role in maritime operations. Classification does not exist to restrain this evolution, but to ensure that when new technologies influence safety, they do so within clearly defined and verifiable boundaries.

If the industry concentrates solely on model capability while overlooking data integrity, it risks introducing vulnerabilities that are far more elusive than traditional defects, because faults in inputs can silently skew outputs. The greater danger lies not in visible system failure but in subtle drift that goes unnoticed until consequences emerge.

From a classification perspective, that is where the focus must now fall.