aage hempel
MARINE ELECTRONICS

Digitalisation in the Maritime Industry (2021–2025): Real Impact, Regulatory Drivers, and the Road Ahead — with Implications for Bridge Equipment Service Companies

December, 2025.

Executive summary

Over the past 4–5 years, maritime digitalisation has shifted from isolated "efficiency initiatives" to **regulator- and assurance-driven operational infrastructure**. The most material change is not autonomous shipping or "AI everywhere"; it is the conversion of shipping into a **data-evidenced industry** where compliance, safety management, port interfaces, and environmental performance increasingly depend on **credible digital records**.

Four forces explain the real impact:

1. **Port-call digitalisation** has been structurally mandated via the IMO's Maritime Single Window (MSW) requirement (effective 1 January 2024).
2. **Decarbonisation** has operationalised data through EEXI/CII and associated SEEMP Part III obligations, tied to annual reporting and ratings from 2023 onward.
3. **Cyber risk** has become an ISM/SMS expectation (IMO MSC.428(98)), forcing demonstrable cyber risk management across fleets and supply chains.
4. **Class cyber resilience requirements** (IACS UR E26/E27) are progressively embedding cyber resilience into ship/system assurance for newbuilds (with revised effective implementation timelines cited by class/regulatory updates).

Looking forward, IMO's **2023 GHG Strategy** has set a direction of travel toward net-zero "by or around 2050" with nearer-term checkpoints. A complementary "Net-Zero Framework" package (mandatory fuel-intensity limits plus pricing/reward mechanisms) was approved in April 2025 but has seen formal adoption delayed to 2026, reinforcing near-term uncertainty while maintaining the inevitability of more data-driven compliance.

For **service companies repairing and maintaining bridge equipment**, the implications are direct: service work is now expected to be **traceable, software-aware, cyber-safe, and audit-defensible**. Digitalisation is raising the bar for credibility and liability management as much as it is improving productivity.

---

1. Context: What "digitalisation" now means in maritime

In practice, maritime digitalisation has converged around three pillars:

1. **Digital interfaces** (ship–shore, ship–port, ship–OEM/class/flag).
2. **Digital evidence** (records that can stand up in audits, PSC, incident investigations, and commercial disputes).

3. **Digital control** (cyber risk management, controlled remote access, controlled software/configuration baselines).

This evolution matters because maritime is a high-assurance, multi-party ecosystem. For changes to "stick," they must be compatible with:

- statutory regimes (SOLAS/ISM/MARPOL),
- class rules and survey practice,
- port state enforcement realities, and
- charterer/insurer expectations.

---

2. The real impact over the past 4–5 years

2.1 Port call digitalisation moved from ambition to mandate

The IMO's Facilitation agenda has crystallised in the **Maritime Single Window** requirement: since **1 January 2024**, Member States are required to use a single, centralized digital platform to collect and exchange information for port calls.

Real impact observed

- Reduced tolerance for "agent-only" manual paperwork processes.
- Higher consequences for **data quality** and timeliness (errors become operational disruptions).
- Accelerated integration pressure on owners/operators and their service partners (because port-call data often depends on vessel system status, crew declarations, and equipment readiness).

What did not happen

- A single global user experience. MSW is mandated, but implementation maturity varies by state/port, creating a transitional period of mixed processes.

2.2 Decarbonisation requirements turned operational data into compliance evidence

The last 4–5 years saw environmental regulation move from policy direction to operational mechanics:

- IMO's DCS continues to institutionalise annual fuel and activity data reporting.
- Amendments to MARPOL Annex VI entered into force in late 2022, with **EEXI and CII certification effective from 1 January 2023**, and initial CII-related reporting and ratings following in subsequent cycles.
- This drove widespread adoption of performance monitoring, voyage optimisation, and "compliance-grade" data workflows, because CII/SEEMP Part III expectations link operational actions to documented plans and verification.

Real impact observed

- Digital tools increasingly used not merely to reduce fuel, but to **demonstrate** performance and plan corrective actions.
- Growing importance of data provenance: "where did this number come from, and who validated it?"

- Increased cross-functional involvement (operations, technical, IT/cyber, compliance, commercial).

What did not happen

- Universal standardisation of data models and interfaces; integration remains a cost and complexity driver.

2.3 Cyber became a safety-management and assurance requirement

A decisive step occurred when IMO's MSC adopted **MSC.428(98)**, encouraging administrations to ensure cyber risks are addressed within existing SMS/ISM frameworks no later than the first annual DOC verification after 1 January 2021.

IMO has continued updating its cyber guidance, including the 2025 revision of the "Guidelines on maritime cyber risk management" (MSC-FAL.1/Circ.3/Rev.3).

Real impact observed

- Cyber risk management is increasingly audited as part of operational safety governance, not treated as a standalone IT exercise.
- Service providers (including bridge-equipment service companies) are drawn into the control perimeter because they introduce laptops, removable media, remote access, and configuration changes.

What did not happen

- A single prescriptive global cyber standard. The regime is still largely "goal-based," meaning operators must demonstrate effective risk management rather than follow one exact checklist.

2.4 Class expectations have started embedding cyber resilience into ship/system requirements

IACS Unified Requirements **E26 (ship)** and **E27 (on-board systems and equipment)** define baseline cyber resilience expectations for newbuilds, with implementation timelines reflected in class regulatory updates and IACS communications.

Real impact observed

- Increased scrutiny of network architecture, access control, update mechanisms, logging, and segregation — especially for systems relevant to safe navigation and ship operations.
- A rising expectation that third-party equipment and service interventions do not degrade cyber posture.

---

3. What the future holds: industry direction and IMO norms

3.1 Environmental regulation: higher ambition, more detailed mechanisms

IMO's **2023 Strategy on Reduction of GHG Emissions from Ships** established enhanced ambition and a structured pathway.

In parallel, the IMO's proposed **Net-Zero Framework** (combining mandatory emissions limits/fuel-intensity requirements and a pricing/reward mechanism) was approved in April 2025 as a step toward legally binding measures, but the extraordinary MEPC session in October 2025 adjourned adoption to 2026.

Implications

- "Regulatory uncertainty" is about *timing and design details*, not about direction: the industry should assume increasing requirements for **measurement, verification, and enforceable incentives/penalties**.
- Digital capability (data capture, validation, reporting, audit trails) becomes a core compliance competency.

3.2 Port and facilitation: MSW as a base layer for wider standardisation

With MSW mandatory, the next phase is likely:

- increased expectations for interoperability and "submit once, reuse many,"
- stronger pressure for structured data rather than PDFs,
- growing integration of port-call systems with operational planning tools.

3.3 Cyber: from "policy in SMS" to demonstrable control maturity

IMO cyber expectations will continue to mature through:

- updated guidance (already refreshed in 2025),
- class adoption and survey practice around cyber resilience (IACS E26/E27),
- and commercial pressure (insurers, charterers, terminals) increasingly asking for evidence rather than statements.

3.4 Navigation digitalisation: incremental, safety- and service-driven

IMO's e-Navigation work (including defined "Maritime Services" for digital information exchange) supports a long-term shift toward standardised ship–shore information services.

The practical result is not a sudden technological jump, but a steady increase in:

- integrated bridge systems reliance,
- digital warnings/traffic services integration,
- and the complexity of software/configuration baselines that must be maintained.

---

aage hempel
MARINE ELECTRONICS

4. Specific implications for a bridge-equipment repair and maintenance service company

4.1 The service company is now part of the compliance chain

Bridge equipment sits at the intersection of:

- SOLAS safety expectations (navigation and communications),
- class survey requirements (fitness, integrity, approved modifications), and
- cyber expectations (safe servicing practices and secure system states).

Digitalisation makes these expectations **more inspectable**. Increasingly, "work performed" must be accompanied by "work evidenced."

4.2 What class/flag/PSC commonly expect to see after service work

A service company should assume that shipowners, class surveyors, and PSCOs will increasingly value:

A) Traceability

- Clear equipment identification (model/serial), technician identity, timestamps, and scope boundaries.

B) Software/configuration management

- Firmware/software versions recorded, parameter baselines protected, integration points verified (sensor sources, network links, alarm logic).

C) Functional verification

- Evidence of post-service testing aligned to equipment criticality.

D) Cyber hygiene

- Controlled remote access, controlled removable media, and controlled service tools.

These items align closely with IMO's SMS-driven cyber expectations and the direction of class cyber resilience requirements.

4.3 The "Digital Proof Package" (recommended standard output per attendance)

To align with evolving SOLAS/IMO/class expectations, a service company should standardise a minimum evidence bundle:

1. **Digitally generated service report** (unique ID, timestamps, technician ID)
2. **Equipment identity register** (model/serial/locations) and any changes recorded
3. **Software/firmware versions** (before/after where changed)
4. **Test and verification record** (including interfaces relevant to safe operation)
5. **Defect and limitation statement** (what remains outstanding; operational impact)

6. **Cyber servicing checklist** (remote access used; media used; accounts touched; source of updates; logging)

This "proof package" is not bureaucracy; it is risk management. It reduces:

- post-incident disputes about workmanship,
- audit friction with class/flag,
- and cyber exposure arising from uncontrolled tools and access.

4.4 Strategic opportunities for service companies

Digitalisation creates competitive differentiation for service providers that can offer:

- **Pre-attendance diagnostics** (log review, fault isolation, spare staging) to increase first-time-fix rates
- **Fleet-wide configuration and version governance** (especially for ECDIS/radar/INS/VDR ecosystems)
- **Cyber-safe servicing** as a formal product (documented controls, auditable practices)
- **Compliance-support services** (evidence packs tailored for audits/PSC readiness)

---

5. Recommendations: how maritime stakeholders should respond

For shipowners/operators

- Build a "compliance-grade" data spine that serves emissions reporting, operational decisions, and auditability.
- Treat cyber controls as an ISM reality, including vendor access governance.
- Require service partners to provide standardised digital evidence outputs.

For bridge-equipment service companies

- Implement a group-wide, standardised **digital service record** and evidence pack.
- Formalise **software/configuration control** as a technical discipline (not an informal technician practice).
- Adopt and document **cyber-safe servicing procedures** consistent with IMO cyber guidance and class expectations.
- Integrate with customer workflows (CMMS/ERP where applicable) so service evidence is immediately usable for compliance and assurance.

For regulators, class, and industry bodies (observed direction of travel)

- Continue driving interoperability (MSW and related data exchange standards).
- Reduce ambiguity by translating high-level cyber expectations into clearer evidence norms, while preserving goal-based flexibility.

Conclusion

In the last 4–5 years, maritime digitalisation has produced real impact primarily by making shipping **more measurable, more auditable, and more integrated** — especially in port interfaces, emissions performance, and cyber risk governance. This is accelerating, not slowing.

For bridge-equipment repair and maintenance companies, the future is defined by a single principle: **service credibility must be demonstrable**. The service provider that can deliver secure, software-aware maintenance with consistent digital evidence will become the preferred technical advisor — well aligned with where IMO norms, class assurance, and commercial expectations are heading.

Contact Information

Aage Hempel Group
24/7 Hotline: +34 664 736 909
Email: sales@aagehempel.com / service@aagehempel.com
Web: www.aagehempel.com

As a bonified and trusted international service company, Aage Hempel Group supports shipowners and ship management companies by translating regulatory and digital complexity into practical, audit-ready outcomes. Through globally consistent bridge-equipment service, software- and configuration-aware maintenance, and cyber-safe servicing practices, Aage Hempel Group delivers traceable digital-service-standard records (DS^2) that stand up to class, flag, and PSC scrutiny. With strong OEM relationships, certified technicians across multiple jurisdictions, and the ability to provide pre-diagnostics, first-time-fix execution, and compliance-grade evidence, the Group acts not only as a service provider but as a technical advisor, helping owners protect safety, maintain compliance, and operate with confidence in an increasingly data-driven maritime environment