Universal Library of Engineering Technology Research Article

ISSN: 3064-996X | Volume 2, Issue 3

Open Access | PP: 55-60

DOI: https://doi.org/10.70315/uloap.ulete.2025.0203011

Smart Ship Design: Engineering Considerations for Autonomous Maritime Vessels

Igor Astrakhovych

Houston, TX, USA.

Abstract

In this work an in-depth systemic-analytical review of the engineering solutions underlying the creation of marine autonomous surface ships (MASS) was performed. Under the conditions of a radical transformation of the shipping sector driven by the aspiration to increase operational efficiency, strengthen safety measures and minimize environmental impact, the autonomous control platform emerges as one of the key vectors for industry development. The primary objective of the study — to systematize and critically evaluate the technological barriers and design approaches affecting the performance and reliability of MASS. The methodological foundation is represented by a thorough analysis of contemporary publications in four main areas: sensor suite architecture, dynamic motion control methods, ensuring cyber resilience and implementation of the digital twin concept. As a result, the most complex intersection points between ship subsystems have been identified, primarily between situational awareness modules and cyber threat protection mechanisms. The necessity of moving away from fragmented, component-based design approaches in favor of holistic, end-to-end integration is demonstrated: cyber security must be embedded at the platform architecture level rather than added upon completion of development. In conclusion a conceptual model of the digital twin lifecycle is proposed, providing for continuous adaptation and calibration of its constituents during operation. The presented results can be applied in engineering and design bureaus, among marine robotics specialists, and in the activities of regulators when developing standards and regulations in the field of autonomous shipping.

Keywords: *Autonomous Vessels, Maritime Autonomous Surface Ships (MASS), Intelligent Design, Marine Robotics, Situational Awareness, Cybersecurity, Digital Twin, Autonomous Navigation, Engineering Considerations, Integrated Design.*

INTRODUCTION

The maritime industry is poised for a paradigm shift of a magnitude rivaling the historical move from sail to steam propulsion. Central to this evolution is the advent of Maritime Autonomous Surface Ships (MASS), which stand to redefine marine logistics by delivering unprecedented throughput improvements, finely tuned fuel efficiency, and a leaner human contingent—thereby substantially curtailing the incidence of accidents rooted in human error. The commercial viability of this transformation is already evident: in 2023, the autonomous-vessel sector commanded a market valuation of USD 89.3 billion, with projections estimating growth to USD 217.6 billion by 2033, a compound annual expansion rate of 9.5 percent over the 2024–2033 period [1]. Such momentum is further propelled by imperatives to decarbonize seaborne transport and to reinforce supply-chain robustness amid heightened global uncertainty.

Nevertheless, the realization of fully autonomous shipping hinges on overcoming a suite of intricate engineering challenges. To date, scholarly efforts have tended to isolate individual autonomy facets—be it advanced collision-avoidance algorithms or stand-alone sensor suites—resulting in a piecemeal body of knowledge. What remains lacking is a comprehensive, system-level design methodology that cohesively integrates high-precision navigation, sustained operational reliability, and stringent cyber-resilience into a singular, orchestrated vessel architecture.

This research aims to systematically identify and analyze technological barriers and design strategies that affect the operational performance and reliability of MASS.

The scientific contribution of this work consists in the formulation of a conceptual model for integrated design that unites autonomous navigation subsystems, cybersecurity measures, and digital twin frameworks within the vessel's end-to-end lifecycle.

The hypothesis is that transitioning from disjointed subsystem design to a unified architecture—where

Citation: Igor Astrakhovych, "Smart Ship Design: Engineering Considerations for Autonomous Maritime Vessels", Universal Library of Engineering Technology, 2025; 2(3): 55-60. DOI: https://doi.org/10.70315/uloap.ulete.2025.0203011.

cybersecurity and validation via digital twins are regarded as foundational elements—is a necessary prerequisite for ensuring the safety and reliability of autonomous maritime platforms.

MATERIALS AND METHODS

In recent years, studies of the autonomous vessel market have demonstrated impressive growth rates and a wide array of implemented solutions. The corporate report by Allied Market Research [1] categorizes the global market according to levels of autonomy, components and vessel types, forecasting significant expansion of the Maritime Autonomous Surface Ships segment by 2033. Gu Y. et al. [2] analyse current logistics solutions, emphasising the benefits of integrating AI algorithms to optimise routing and reduce operational risks, thereby broadening the application of autonomous vessels in cargo transport.

Advanced system-level architectures play a pivotal role in ensuring reliable autonomous control. Koznowski W. et al. [4] propose a multilayered intelligent platform that unites decision-making, forecasting and feedback control modules. Their architecture combines classical trajectory-planning algorithms with neural-network-based risk assessment models, enabling adaptation to unstable maritime conditions and enhancing overall system fault tolerance.

Safety and navigation remain critical aspects of autonomous vessel deployment. Munirathinam N., Krishnamurthi A. [3] focus on optimising large-area surveillance through automatic object recognition based on deep convolutional networks; their approach reduces false alarms and accelerates response to detected targets. Nemoto Y. [9] examines a comprehensive set of measures for navigational safety—from analysing collision scenarios at sea to implementing trajectory-prediction algorithms for other vessels—and underscores the need to standardise risk-assessment procedures and regulate data exchange between autonomous and conventional vessels.

The development of the digital-twin concept has attracted researchers as a means to improve the reliability and efficiency of vessel-system maintenance. Madusanka N. S. et al. [5] review the application of digital twins for monitoring the condition of shipboard machinery, noting a shift from reactive to predictive maintenance. Fera F., Spandonidis C. [6] propose a framework for integrating fault-diagnosis methods into the power systems of autonomous vessels, based on machine-learning techniques and real-time simulations. Xia J. et al. [10] demonstrate the use of a digital twin for partial diagnostics of rotating equipment: their hybrid methodology combines physics-statistical models with deep-learning algorithms to localise defects at early stages.

Cybersecurity for autonomous vessels has become increasingly urgent due to the rise in attacks on critical infrastructure. Tabish N., Chaur-Luh T. [7] conduct a systematic review of vulnerabilities and countermeasures, highlighting the need for embedded anomaly-detection mechanisms and encrypted communication channels. Fathy M., Tarek H. [8] present an integrated framework that unites cyber-protection and navigational safety, in which threat models automatically initiate defensive procedures at both software and hardware levels. Kanwal K. et al. [12], assessing the readiness of modern onboard systems, identify a gap between theoretical developments and practical implementation—many maritime operating systems and protocols are not yet adapted for trusted communications and continuous monitoring.

Finally, Orzechowski S. C., Verheyen W., Sys C. [11] analyse factors influencing the development of a regulatory framework for autonomous inland navigation in Europe. The authors emphasise the requirement for unified technical standards and the establishment of a common legal framework to determine liability in the event of incidents.

Overall, the literature reveals contradictions: market and logistics reports [1, 2] outline optimistic forecasts, whereas practical studies on safety [3, 9] and cybersecurity [7, 8, 12] underscore high levels of uncertainty and potential risks during real-world operation. Divergent assessments exist regarding technological readiness: some authors identify mature methods for automatic detection and diagnostics [6, 10], while others note their limitations due to insufficient validation under real conditions. Insufficiently addressed issues include the interaction of autonomous and conventional vessel systems within a unified navigational ecosystem; methodologies for verifying and validating complex AI models under variable maritime climates; socio-economic and legal aspects of introducing autonomous vessels on regular routes beyond inland navigation; and mechanisms for “human-in-the-loop” intervention and liability in critical AI-failure scenarios. Consequently, further research should focus on interdisciplinary integration of technical, legal and organisational approaches to comprehensively address both the technological and societal challenges of autonomous vessel implementation.

RESULTS AND DISCUSSION

The design of intelligent autonomous vessels compels researchers and practitioners to fundamentally rethink traditional shipbuilding methodologies. Rather than undertaking disjointed, phase-by-phase design of the hull, propulsion system, and navigation-sensor suite, a multidisciplinary systems-based approach is required, centered on a unified hardware–software framework that supports the full cycle of autonomous operation. Under the International Maritime Organization (IMO) classification, four autonomy levels for MASS vessels have been defined, providing the foundation for architectural development and specifying the complexity requirements of control systems (Table 1). At each successive autonomy level, requirements grow exponentially for environmental perception capabilities, algorithmic analysis, and decision-making processes, while reliability and operational safety standards become increasingly stringent.

Table 1. Levels of autonomy of Maritime Autonomous Surface Ships (MASS) according to IMO (compiled by the author based on analysis [9, 11, 12]).

Level	Designation	Description
Level 1	Ship with automated processes and decision support	The crew remains on board to operate and manage the vessel's systems and functions. Certain tasks may be automated.
Level 2	Remotely controlled ship with crew on board	The vessel is operated and monitored from a remote location, while crew remain on board and can assume control at any time.
Level 3	Remotely controlled ship without crew on board	The vessel is operated and monitored from a remote location; no crew are embarked.
Level 4	Fully autonomous ship	The vessel's operating system is capable of independently making decisions and determining actions.

A key component of an autonomous vessel at Level 2 and above is the Situational Awareness (SA) subsystem, whose role is to build for the Navigation, Guidance & Control (NGC) module a comprehensive, high-precision, real-time digital representation of the maritime domain. Unlike a human operator, who relies on intuitive perception of the environment, the autonomous system employs a multi-layer fusion architecture that integrates data from heterogeneous sensors.

At the sensor layer, X- and S-band radars detect targets at long and medium ranges, LiDAR scanners generate detailed three-dimensional maps of the immediate vicinity, and electro-optical modules operating in both visible and infrared bands perform object recognition, tracking, and classification. Receivers for the Automatic Identification System (AIS) and the Global Navigation Satellite System (GNSS) exchange navigational and charting information. The data streams produced by these sensors vary in format, update rate, and accuracy.

These heterogeneous streams feed into the computational layer, where advanced techniques—extended and adaptive Kalman filters, Bayesian sensor-fusion methods, and deep neural networks—consolidate disparate reports into continuous tracks, estimate kinematic parameters (heading, speed, acceleration), and intelligently classify objects (e.g., vessel, buoy, shoreline). The output of this processing is the "world model," a dynamic digital representation of the external environment that the NGC subsystem uses to guide and control the vessel. The reliability and accuracy of this world model are directly linked to the safety of the autonomous vessel in complex maritime conditions.

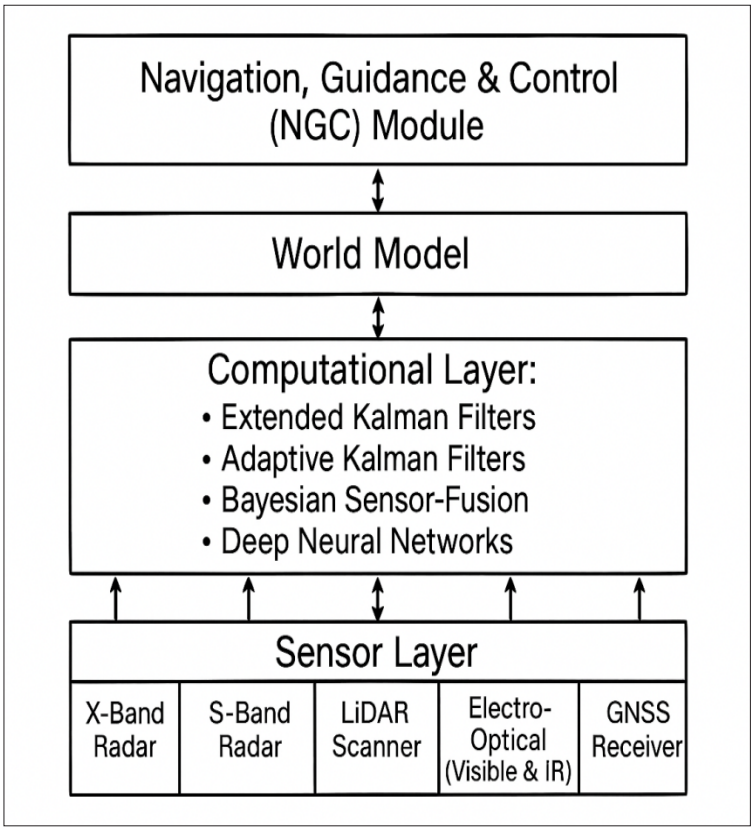

Fig.1. Generalized architecture of the situational awareness system for MASS (developed by the author based on the analysis of [2, 3, 7]).

NGC subsystem constitutes the central computing core of an autonomous vessel, integrating three interrelated functional modules:

1. Navigation ensures continuous determination of the vessel's geographic position, heading, and speed based on GNSS data and inertial sensors.
2. Guidance generates the optimal trajectory from point A to point B, accounting for hydro-meteorological conditions, navigational constraints, and the requirements of the International Regulations for Preventing Collisions at Sea (COLREGs 1972).
3. Control translates the computed trajectories into specific commands for actuators (steering gear, propulsion and steering units), ensuring precise route adherence and execution of collision-avoidance maneuvers.

The primary engineering challenge lies in formalizing the provisions of COLREGs 1972 in algorithmic form: rules such as Rule 2 "Responsibility" and Rule 8 "Action to Avoid Collision" employ terminology that requires "good seamanship" and professional judgment, significantly complicating unambiguous interpretation and implementation in software code [4].

However, even with flawless NGC logic, its effectiveness depends heavily on the level of cybersecurity, necessitating the embedding of protective measures directly into the ship-design process. The architecture of Maritime Autonomous Systems (MASS) is vulnerable at all levels:

- At the sensor level, GNSS signals may be subjected to jamming and spoofing attacks, resulting in distorted positional data.
- The network infrastructure linking sensors, computing nodes, and actuators may be targeted by man-in-the-middle attacks or malware insertion.
- The most serious threat arises from attempts to compromise the NGC subsystem itself, potentially causing loss of control or execution of uncontrolled hazardous maneuvers [7, 8].

To mitigate these risks, the design of contemporary Maritime Autonomous Surface Ships (MASS) is founded on a defense-in-depth approach, which entails:

- strict segmentation and isolation of onboard networks;
- mandatory application of cryptographic protocols at every communication layer;
- deployment and integration of intrusion detection and prevention systems (IDS/IPS);
- design of fault-tolerant modes and redundant algorithms that activate automatically upon detection of anomalies indicative of a potential cyberattack.

Verification and validation of highly complex, tightly integrated systems by traditional means—including physical testing—inevitably lead to excessive costs and prolonged schedules, while remaining unable to cover the full spectrum of possible operational and emergency scenarios. A universal remedy to this challenge is the large-scale adoption of digital twin (DT) technologies. The digital twin of an autonomous vessel is a high-precision, multiphysics representation of the real object, operating in parallel with it throughout all phases of its life cycle [5].

During the conceptual design phase, the DT functions as a virtual testbed for comprehensive trials: within its environment, thousands of combinations of navigational conditions and weather effects can be simulated, and cyberattack scenarios can be exercised to assess control-system resilience—entirely eliminating risk to an actual vessel [6]. This methodology enables early detection and elimination of latent algorithmic defects and the consolidation of test results within a unified digital environment.

Throughout combat and commercial deployment, the digital twin continuously ingests streams of data from onboard sensors and integrated systems, providing operators at the shore-based control center with round-the-clock monitoring of the vessel's real-time status. Furthermore, through analysis of historical and current equipment performance parameters, predictive maintenance is effectuated: potential failures are forecast and maintenance interventions are scheduled before critical breakdowns occur. The overall architecture of the digital twin ecosystem is depicted in Figure 2.

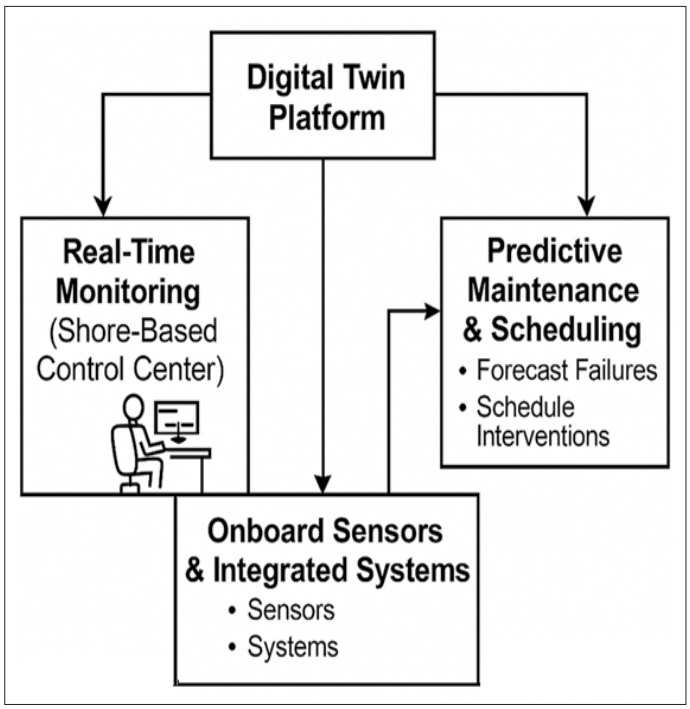

Fig. 2. Conceptual ecosystem of a digital twin in the MASS life cycle (compiled by the author based on the analysis of [5, 6, 10]).

The economic viability and pace of integration of Maritime Autonomous Surface Ships (MASS) are directly linked to the maturity of key technologies—from the reliability of

artificial intelligence systems and sensors to the flexibility of software architectures and the capabilities for cyber-physical integration. However, the transition to fully autonomous Level 4 vessels remains constrained by capital expenditures (CAPEX), which increase substantially during research and development, design, construction and certification of these platforms. Additional barriers include incomplete international and national regulatory frameworks, as well as the absence of standardized insurance mechanisms and liability regimes for incidents. Consequently, over the next five to ten years the most realistic scenario for scaling autonomy will involve the phased deployment of Level 2 and Level 3 vessels operated from remote shore control centres. This strategy will not only build essential operational experience but also create an evidence base to guide the harmonization of technological, legal and insurance systems, thereby strengthening confidence in fully autonomous navigation platforms.

The design of intelligent vessels demands an integrated, systems-level approach that unites traditional shipbuilding engineering methods, robotic solutions, modern information and communication technologies, and cybersecurity protocols. Analysis indicates that segregated development across these disciplines induces bottlenecks in the overall process: insufficient sensor reliability may distort navigation data, while unresolved software vulnerabilities can negate the advantages of even the most advanced hardware. As an effective response to these challenges, an end-to-end methodology is proposed, grounded in the principle of security by design and incorporating multi-level validation of design solutions through a digital twin. Under this framework, the intelligent vessel is treated not as a collection of discrete subsystems but as a unified cyber-physical ecosystem, where requirements for reliability, fault tolerance and security are defined at the conceptual design stage and assured throughout the vessel's entire lifecycle.

CONCLUSION

The study has outlined a comprehensive methodology for the analysis and synthesis of engineering solutions for both contemporary and future autonomous vessels. It was determined that the transition from traditional component-level design to the development of Maritime Autonomous Surface Ships (MASS) requires the establishment of a unified, integrative architecture in which the situational-awareness, navigation, control, and cybersecurity subsystems are regarded not in isolation but as an interconnected ensemble.

The safety of an autonomous vessel is directly dependent on the completeness and reliability of the information provided by the situational-awareness subsystem. Ensuring this reliability demands not only the deployment of high-resolution and multispectral sensors but also the development of noise- and fault-tolerant multisensor data-fusion algorithms capable of processing complex and dynamic maritime scenarios.

An autonomous maritime platform must be treated as a high-value cyber-physical system, demanding a defense-in-depth architecture that spans its entire life cycle. From the earliest conceptual phase through to decommissioning, security controls should be embedded at every layer—encompassing cryptographic protections for navigation-aiding signals to thwart spoofing attempts, as well as hardened firmware, secure boot processes, and intrusion-resistant software architectures to guard the control and propulsion subsystems against both remote and direct assaults on hardware and code.

State-of-the-art digital-twin frameworks furnish a rigorous environment for system verification, validation, and real-time health monitoring aboard such vessels. By mirroring physical assets in a virtual domain, these models substantially curtail the financial and operational risks inherent in live sea trials, while enabling condition-based and predictive maintenance programmes that drive down unplanned downtime and emergency interventions.

Moving forward, scholarship must concentrate on formulating concrete, reproducible methodologies and converging on industry-wide standards to operationalize this holistic security paradigm. Equally vital is the evolution of human-systems interface protocols—defining how shore-based operators interact with autonomous platforms—to ensure that remote oversight remains intuitive, reliable, and resilient under adverse conditions.

REFERENCES

1. Autonomous Ships Market Size, Share, Competitive Landscape and Trend Analysis Report, by Level of Autonomy, by Component, by Ship Type, by Propulsion: Global Opportunity Analysis and Industry Forecast, 2023 – 2033 https://www.alliedmarketresearch.com/autonomous-ships-market (access date: 05/10/2025).
2. Gu Y. et al. Autonomous vessels: state of the art and potential opportunities in logistics //International Transactions in Operational Research. – 2021. – Vol. 28 (4). – pp. 1706-1739. https://doi.org/10.1111/itor.12785
3. Munirathinam N., Krishnamurthi A. Maritime Security Optimization for Large Scale Surveillance through Automated Object Detection //Proceedings of 6th International Conference. – 2024. – Vol. 19. – pp. 217-228.
4. Koznowski W. et al. Research on synthesis of multi-layer intelligent system for optimal and safe control of marine autonomous object //Electronics. – 2023. – Vol. 12 (15). https://doi.org/10.3390/electronics12153299.
5. Madusanka N. S. et al. Digital twin in the maritime domain: A review and emerging trends //Journal of Marine Science and Engineering. – 2023. – Vol. 11 (5). https://doi.org/10.3390/jmse11051021.

6. Fera F., Spandonidis C. A Fault Diagnosis Approach Utilizing Artificial Intelligence for Maritime Power Systems within an Integrated Digital Twin Framework //Applied Sciences. – 2024. – Vol. 14 (18). https://doi.org/10.3390/app14188107.

7. Tabish N., Chaur-Luh T. Maritime autonomous surface ships: A review of cybersecurity challenges, countermeasures, and future perspectives //IEEE Access. – 2024. – Vol. 12. – pp. 17114-17136. https://doi.org/10.1109/ACCESS.2024.3357082.

8. Fathy M., Tarek H. A Cybersecurity-Integrated Framework for Ensuring Operational Safety in Autonomous Maritime Navigation Systems //Journal of Robotic Process Automation, AI Integration, and Workflow Optimization. – 2025. – Vol. 10 (4). – pp. 1-25.

9. Nemoto Y. Navigation safety of Maritime Autonomous Surface Ships //Australian Journal of Maritime & Ocean Affairs. – 2024. – pp. 1-15.

10. Xia J. et al. A digital twin-driven approach for partial domain fault diagnosis of rotating machinery // Engineering Applications of Artificial Intelligence. – 2024. – Vol. 131. https://doi.org/10.1016/j.engappai.2024.107848.

11. Orzechowski S. C., Verheyen W., Sys C. A systematic literature review of factors influencing the regulation of autonomous inland shipping in Europe //European Transport Research Review. – 2024. – Vol. 16 (1). – pp. 54.

12. Kanwal K. et al. Maritime cybersecurity: are onboard systems ready? //Maritime Policy & Management. – 2024. – Vol. 51 (3). – pp. 484-502. https://doi.org/10.1080/03088839.2022.2124464.