

Autonomous Early-Warning Systems for Maritime Piracy Threat Detection Using AI-Based Sensor Fusion [†]

Sonia Rozbiewska 

Doctoral School, Maritime University of Szczecin, 70-500 Szczecin, Poland; sonia.rozbiewska@gmail.com

[†] Presented at the 3rd International Electronic Conference on Machines and Applications (IECMA 2026), 12–14 May 2026; Available online: <https://sciforum.net/event/IECMA2026>.

Abstract

Maritime piracy remains a significant threat to the safety of commercial shipping and the stability of global supply chains. Contemporary maritime surveillance systems increasingly employ multisensor data fusion to build a coherent operational situation picture. This paper presents a comparative review of commercially available maritime surveillance systems integrating data from radar, AIS, and visual and satellite sensors. Systems were selected based on their representativeness across different application domains (coastal surveillance, VTS, MDA) and the availability of sufficient technical documentation. The review of these solutions enables an assessment of the current level of technological maturity and the identification of limitations of existing architectures in the context of dynamic piracy-related threats. On this basis, the need for developing autonomous early-warning systems utilizing data fusion and artificial intelligence algorithms operating at the ship's operational level has been identified.

Keywords: maritime piracy; maritime security; autonomous systems; smart vessel traffic management; artificial intelligence; sensor fusion; anomaly detection; situational awareness; early-warning systems; ship safety

1. Introduction

Maritime piracy has been a significant threat to the safety of commercial shipping for many years [1]. Disruptions in the functioning of strategic maritime transport routes can lead to increased freight costs, delivery delays and disruptions in global logistics chains, especially in the energy sector [2]. The scale of the potential consequences means that the issue of protecting ships against piracy remains a current subject of interest for both international institutions and the maritime industry [3].

Current methods of counteracting piracy are based mainly on operational procedures, physical security measures and the support of maritime patrols and private security teams [4]. Although these solutions have significantly reduced the number of successful attacks, they are largely reactive in nature and require constant commitment of human and financial resources [4]. The contemporary operational environment, characterized by high ship traffic dynamics and limited visibility of threats at an early stage, indicates the need for more automated and predictive mechanisms to support the decision-making process of crews and maritime traffic control centers [5]. In parallel to the changes in the area of maritime safety, intensive development of technologies for the supervision and management of ship traffic is observed [6]. Vessel Traffic Services (VTS), Maritime Domain Awareness (MDA) and integrated coastal protection systems increasingly use simultaneous



Academic Editor: Antonio J. Marques Cardoso

Published: 26 June 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

acquisition of information from multiple sources, such as maritime radar, Automatic Identification System (AIS), optical and thermal cameras, satellite systems and meteorological sensors [7–10]. A key element of these solutions is the fusion of multi-sensor data, enabling the creation of a coherent picture of the operational situation and the identification of unusual vessel behavior [11].

Beyond building a coherent situational picture, sensor fusion offers a broader set of benefits critical to robust real-world deployments. In particular, it can effectively compensate for sensor failures, measurement noise, and data redundancy, and can maintain system functionality even when individual sensors are temporarily removed or unavailable. These properties make sensor fusion indispensable in modern safety-critical applications, as comprehensively discussed and demonstrated in real-world scenarios.

A wide range of commercial systems employing sensory data integration and correlation for maritime surveillance and coastal protection applications is currently available on the market. These systems constitute an important reference point for the further development of autonomous early-warning mechanisms for security threats, including maritime piracy-related risks.

The aim of this paper is to present and analyze commercially available systems employing data fusion in maritime surveillance and to indicate their potential in the context of developing autonomous early-warning systems for maritime piracy threat detection. The assessment of each system is conducted according to a consistent set of criteria: (1) sensor modalities integrated, (2) data fusion level implemented (per the JDL model), (3) anomaly detection and threat classification capabilities, (4) degree of automation and the role of human operators, and (5) suitability for onboard ship-level deployment. The review of commercial solutions on this basis provides a basis for identifying current technological capabilities and functional gaps that may be addressed by dedicated anomaly analysis and artificial intelligence algorithms operating closer to the ship's operational level.

2. Maritime Common Operational Picture (COP) Modelling in Multi-Sensor Surveillance System

Contemporary maritime surveillance systems increasingly employ multisensor architectures aimed at building a coherent operational situation picture based on information acquired from multiple data sources. The fundamental concept of such solutions is the integration of vessel traffic data, radar observations, and visual information into a unified maritime situation model, referred to in the literature as the Common Operational Picture (COP) [12,13].

The most frequently used data sources in maritime surveillance systems include the Automatic Identification System (AIS), marine radars, optical and thermal imaging cameras (EO/IR), meteorological sensors and, increasingly, satellite data [14,15]. Each of these sources has certain advantages and limitations. AIS provides declarative information about the vessel's position, course and identity, but may be susceptible to errors, delays or intentional transmission blackouts [16,17]. Radar enables the detection of objects regardless of their cooperation with identification systems, but generates noise and false echoes that require filtration [18–21]. EO/IR systems, on the other hand, allow for visual classification of objects, but their effectiveness depends on atmospheric and lighting conditions. Regarding data currency, visual observations are generally considered valid for the duration of a single tracking cycle, typically on the order of seconds to a few tens of seconds depending on the update rate of the imaging system. Data older than one full scan cycle (e.g., exceeding 10–30 s under standard configurations) should be treated as potentially expired and downweighted in the fusion process, particularly in dynamic scenarios involving

fast-moving targets [22,23]. The use of multiple complementary sensors allows for limiting the impact of individual limitations and increasing detection reliability [24–26].

The key element of the discussed systems is the data fusion layer, responsible for integrating heterogeneous information streams into a coherent operational situation model [8,27]. Data from different sensors are characterized by different temporal and spatial resolution, different levels of measurement uncertainty and different information representation [28,29]. The fusion layer therefore acts as a mechanism for synchronizing, correlating and unifying this data in order to create a clear image of detected objects and their behavior [8,11,20]. The literature distinguishes several levels of data fusion, according to the classic JDL (Joint Directors of Laboratories) model. It should be noted that the JDL framework is employed here as an analytical reference model for classifying the reviewed commercial systems, rather than as a model explicitly implemented by the vendors themselves. The mapping of each system's functional architecture to JDL fusion levels represents the author's interpretation based on publicly available technical documentation and literature descriptions. To clarify the concept of data fusion in maritime surveillance systems, Table 1 presents the basic levels of fusion along with typical data sources and sample methods for their implementation.

Table 1. Data fusion levels in maritime surveillance systems and sample implementation methods. Author's own elaboration.

Data Fusion Level	Processing Scope	Typical Data Sources	Example Methods and Algorithms	Application in Maritime Surveillance
Raw data fusion (signal-level fusion)	Integration of unprocessed measurement signals	Radar, sonar, RF signals, EO/IR	Signal summation, adaptive filtering, coherent processing methods	Improved object detection under adverse environmental conditions
Feature-level fusion	Integration of extracted object features	AIS, radar tracks, EO/IR features	Kalman filters, particle filters, Bayesian algorithms	Correlation of radar tracks with AIS, trajectory estimation, object tracking
Object-level fusion	Creation of a unified target track	Radar + AIS + EO/IR	Track-to-track association, data association, gating techniques	Construction of the Common Operational Picture (COP)
Decision-level fusion	Integration of classification and detection algorithm outputs	AI/ML outputs, expert systems	Fuzzy logic, neural networks, ensemble learning	Automated risk assessment and alert generation

At the lowest level, raw data fusion is implemented, which involves directly combining measurement signals before feature extraction. The intermediate level involves object feature fusion, where already processed information such as position, velocity, and object signature is integrated. The highest level is decision information fusion, where the results of classification and detection algorithms are combined to make the final operational decision [30–33]. In maritime applications, feature and object fusion is most commonly used, correlating radar traces with AIS data and EO/IR video imagery to create a seamless target trace [34–36]. This process allows the declared identity of an AIS vessel to be assigned to an object physically detected by radar, and then its class to be confirmed by analyzing the visual image [37]. This makes it possible to reduce the problem of false detections (i.e., erroneous classification of a legitimate vessel as a threat when no actual attack is occurring) and identify vessels that deliberately do not transmit AIS data [37]. An important element of the fusion process is data filtration and estimation of the motion trajectory of detected objects. In practice, probabilistic methods are used, such as the Kalman filter and its variants,

particle filters or Bayesian methods, which enable the prediction of subsequent object positions and compensation of measurement noise typical of marine radars [38,39]. These mechanisms allow for the continuity of target tracking even in the event of a temporary loss of one of the data sources. The next step is to eliminate measurement uncertainty and resolve information conflicts between sensors. This is accomplished by assigning weights to individual data sources based on their reliability in a given operational context, for example, with limited visual visibility or radar interference [24,26,30,40,41]. This approach increases the stability of the created situational awareness and improves the accuracy of further analysis of vessel behavior. The described data fusion mechanisms provide the foundation for subsequent layers of the maritime surveillance system, particularly anomaly detection and threat classification algorithms. Multi-sensor integration enables a shift from simple vessel traffic monitoring to automatic assessment of their behavior and early detection of potentially dangerous situations, including piracy threats. The theoretical algorithms described in this section (Kalman filters, Bayesian association, LSTM-based anomaly detection) are directly relevant to the design of the proposed autonomous early-warning system: they form the computational building blocks whose applicability to the commercial systems reviewed in Section 3 is subsequently assessed, and which are adopted as candidate methods in the system requirements proposed in Section 4. Selected algorithms most frequently used in the individual stages of the data fusion layer in maritime surveillance systems are summarized in Table 2.

Table 2. Typical algorithms used in the data fusion layer of maritime surveillance systems. Author's own elaboration.

Function	Example Algorithms	Purpose
Filtering and trajectory estimation	Kalman Filter (KF), Extended KF, Particle Filter	Reduction in radar measurement noise and prediction of target motion
Radar–AIS correlation	Track association, nearest neighbor, JPDA	Assignment of AIS identity to radar-detected objects
False detection elimination	Bayesian inference, confidence weighting	Mitigation of the impact of unreliable or uncertain sensors
EO/IR data integration	CNN-based object recognition	Confirmation of vessel class
Movement anomaly detection	LSTM, Isolation Forest, HMM	Identification of atypical vessel behavior

Based on the unified situational awareness, an analytical layer is implemented, which increasingly utilizes artificial intelligence and machine learning methods. These algorithms are used to detect vessel movement anomalies, identify unusual navigation patterns, and classify vessels based on visual data [42–46]. In the context of maritime safety, this approach enables automatic indication of potentially dangerous behaviours, such as sudden course changes, stops in open sea, loss of AIS signal or approach of small, fast vessels to commercial vessels [47].

The final layer of the architecture consists of decision-making modules and operator interfaces, which are responsible for presenting analysis results in a clear format and generating alerts when elevated risk levels are detected. Advanced solutions also include recommendations for alternative routes and automatic transmission of information to maritime traffic management centers and security services [48,49]. Based on the analysis of the architecture of maritime surveillance systems, a conceptual model of an autonomous early warning system against maritime piracy threats was proposed, presented in Figure 1.

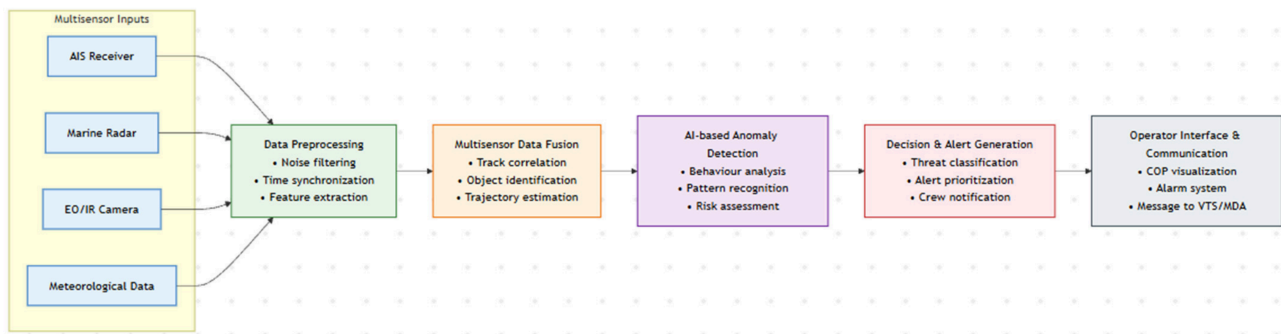


Figure 1. Conceptual architecture of an autonomous early warning system against maritime piracy threats based on multi-sensor data fusion and artificial intelligence algorithms. Author's own elaboration.

The architectural approach described here provides a common foundation for most modern VTS, MDA, and commercial coastal defense systems. At the same time, the development of AI algorithms and the miniaturization of computing devices are gradually enabling the transfer of some analytical functions closer to the operational level of the ship, paving the way for the development of autonomous early warning systems against piracy threats. This trend is supported by recent work demonstrating the feasibility of edge-computing-based multi-source data fusion for autonomous surface vehicles [27], as well as deployed commercial platforms such as Kongsberg's autonomous vessel programs and IMO-recognized e-navigation initiatives, which confirm that real-time onboard processing of fused sensor data is technically achievable within current hardware constraints.

3. Solutions Available on the Market That Combine Data Fusion

Recent years have seen the dynamic development of commercial maritime surveillance systems that utilize multi-sensor data fusion to build a coherent operational picture. These solutions are being implemented in coastal defense systems, maritime traffic management centers, and structures responsible for port and critical infrastructure security. Their common feature is the integration of information from maritime radars, AISs, optical and thermal cameras, and satellite sources, which corresponds to the architecture described in Section 2. A review of available products allows us to determine the current level of technological maturity and indicate directions for further development of early warning systems.

3.1. Airbus Defence and Space—STYRIS® Coastal Surveillance System

STYRIS® (Surveillance, Tracking and Intelligence Radar Integrated System) is an integrated C4ISR maritime surveillance system developed by Airbus Defence and Space, designed to provide continuous surveillance of coastal areas and maritime zones of national responsibility [50]. The system utilizes an open architecture, enabling the integration of heterogeneous sensory data sources and external systems, allowing it to adapt to diverse operational conditions [51].

The data acquisition layer consists of surface surveillance radars operating in the X and S bands, providing detection and automatic tracking of surface objects, including vessels with a small radar cross-section [52]. Complementarily, the system receives data from the Automatic Identification System (AIS), enabling the acquisition of declared vessel identity, position, and motion parameters [52]. Additional sources of information include electro-optical EO/IR sensors, meteorological sensors, and radio signal receivers [52]. The central processing module performs multisensor data fusion, including the correlation of AIS reports with radar detections and visual imagery in order to generate a unified

and continuous object track [52]. As part of the fusion process, declared identities are assigned to physically observed objects; in cases where inconsistencies are detected, alarms are generated indicating potential attempts at identity concealment or the presence of non-cooperative targets [52].

The system enables the execution of analytical functions, including the detection of anomalous behavior, monitoring of restricted areas, and the recording of object movement histories for subsequent event analysis. The operator interface provides the presentation of a unified Maritime Situational Picture, while data exchange mechanisms enable interoperability with other command centers and maritime security systems [53].

Let the state of the object at time k be a vector:

$$\mathbf{x}_k = [x_k, y_k, v_k, \psi_k]^T, \quad (1)$$

where x, y is the position, v is the velocity, ψ is the heading. For a set of measurements from multiple sensors:

$$\mathbf{Z}_k = \{z_k^{(r)}, z_k^{(ais)}, z_k^{(eo/ir)}, \dots\}, \quad (2)$$

the fusion can be expressed as an estimation of the posterior distribution:

$$p(\mathbf{x}_k | \mathbf{Z}_{1:k}) \propto p(\mathbf{Z}_k | \mathbf{x}_k) p(\mathbf{x}_k | \mathbf{Z}_{1:k-1}), \quad (3)$$

where the term $p(\mathbf{Z}_k | \mathbf{x}_k)$ is the product of the reliability of measurements from individual sensors (assuming conditional independence).

A key stage preceding the actual state update is data association, i.e., the assignment of measurements to tracks. For track i and measurement j , gating is typically applied based on the Mahalanobis distance [54]:

$$d_{ij}^2 = (\mathbf{z}_j - \hat{\mathbf{z}}_i)^T \mathbf{S}_i^{-1} (\mathbf{z}_j - \hat{\mathbf{z}}_i), \quad (4)$$

the admission of the (i, j) pair occurs when $d_{ij}^2 \leq \gamma$, where γ denotes the gating threshold. Such a formulation provides a formal justification for the correlation of radar echoes with AIS reports and EO/IR observations within a single track. The value of γ is typically set based on the assumed statistical distribution of measurement errors: under Gaussian assumptions, γ is chosen as a quantile of the chi-squared distribution with degrees of freedom equal to the measurement dimension (e.g., $\gamma \approx 9.21$ for a two-dimensional gate at 99% confidence). In practice, the choice of γ depends on the expected sensor accuracy, the dynamics of the tracked objects, and the density of targets in the scene—a wider gate increases the probability of correct association at the cost of admitting spurious measurements.

The application of STYRIS[®] includes maritime border protection systems, coast guard infrastructure, maritime operations centers, and search-and-rescue coordination facilities. The system represents an example of a mature implementation of multisensor data fusion in the maritime surveillance environment, addressing the requirements of contemporary maritime situational awareness systems. It should be noted that the functional description of STYRIS[®] above is based on publicly available vendor documentation [50,51] and general data fusion literature [52], as independent technical studies or operational evaluation reports for this specific system are not publicly available. The mathematical formulations in Equations (1)–(4) are not claimed to reflect the internal implementation of STYRIS[®] specifically; rather, they represent generic Bayesian multi-sensor fusion models well established in the data fusion literature [54] that are consistent with the class of object-level fusion architectures that systems such as STYRIS[®] are documented to employ. Regarding the assumption of conditional independence among sensor measurements in Equation (3): this

is a standard simplifying assumption in multi-sensor fusion under the Bayesian framework, widely adopted in the literature when sensor noise processes are physically uncorrelated (e.g., radar clutter vs. AIS transmission errors vs. optical degradation). While correlations can exist in practice under shared environmental conditions (e.g., fog affecting both radar and EO/IR simultaneously), the independence assumption remains a tractable and commonly accepted approximation in the absence of detailed joint error models.

3.2. Thales—CoastShield

Thales' CoastShield is an integrated coastal protection system comprising a set of maritime radars, EO/IR cameras, AISs, and a command-and-control platform [55]. Its primary objective is to ensure comprehensive situational awareness in coastal zones, ports, and on approaches to critical infrastructure [55]. Sensor data are integrated within a central management system, where object track correlation and continuous target tracking are performed [55].

Data acquired from surface radars, the AIS, and electro-optical sensors are treated as complementary sources of information on the position and motion of objects. These data undergo a correlation process in which measurements from different sensors are associated with existing object tracks based on the consistency of their spatial and temporal parameters. Subsequently, a unified representation of each object's motion state is generated and continuously updated at successive time steps. The tracking process is implemented within a recursive architecture, comprising a prediction stage, in which the object's position is estimated based on its previous motion state, and an update stage, in which current sensor observations are incorporated. This approach enables compensation for measurement discontinuities and reduction in the impact of noise and errors originating from individual sensors. As a result, the system maintains stable and continuous tracks of vessels even under conditions of temporary AIS signal loss or limited radar visibility. Such integrated tracks constitute the basis for further vessel behavior analysis and the construction of a unified maritime situational picture, which is used by system operators for threat assessment and operational decision-making.

CoastShield's analytical layer uses object classification and anomalous behavior detection algorithms. A motion feature vector is determined for object i [56]:

$$\mathbf{f}_i = [v_i, \dot{\psi}_i, t_{stop}, d_{zone}], \quad (5)$$

including speed, rate of course changes, stop time and distance from protected zones. Detection of abnormal behavior occurs when the following conditions are met:

$$\|\mathbf{f}_i - \bar{\mathbf{f}}_{class}\| > \delta, \quad (6)$$

where $\bar{\mathbf{f}}_{class}$ denotes the reference pattern typical for a given class of vessels, and δ is a predefined decision threshold.

The system enables the identification of situations such as the absence of AIS transmissions, sudden course changes in restricted areas, or the approach of small vessels toward merchant ships. CoastShield represents a typical architecture of a centralized maritime surveillance system, in which multi-sensor data fusion and trajectory analysis form the basis for constructing a shared operational situational picture for maritime security services. The anomaly detection formulation presented in Equations (5) and (6) is a theoretical interpretation by the author, informed by the GeoTrackNet methodology described in [56] and consistent with the functional capabilities attributed to CoastShield in publicly available vendor documentation [55]; it is not claimed to be an exact representation of Thales' internal implementation. Regarding the construction of the reference pattern $\bar{\mathbf{f}}_{class}$: in practice,

such baseline models are typically established through statistical analysis of historical AIS trajectory data for vessels operating in a given area, grouped by vessel type (e.g., tanker, fishing vessel, cargo ship). Methods such as Gaussian mixture models, kernel density estimation, or deep learning-based trajectory encoders (e.g., as in [56]) are used to define normal behavioral envelopes. The threshold δ may then be set empirically using labeled anomaly data or by calibrating the false alarm rate against operational requirements.

3.3. Saab—CoastWatch (Coastal Surveillance/VTS/VTMIS)

CoastWatch, developed by Saab, is a modular maritime surveillance system intended both for coastal area protection and for vessel traffic management in ports and port approach areas [57]. The system is designed using a scalable architecture, enabling the deployment of single observation posts as well as distributed surveillance networks covering extensive stretches of coastline [57]. The primary sensor layer consists of surface surveillance radars operating in the X and S bands, optimized for the detection of targets with low radar cross-sections [57]. These sensors are complemented by AIS receivers and EO/IR electro-optical payloads providing day and night observation capabilities. In addition, the system can integrate meteorological sensors and hydrographic data in order to improve detection performance and the interpretation of the operational situation [57]. Data fusion is performed within a central processing server, where radar measurements, AIS reports, and visual observations are correlated. As a result of this process, a unified motion track is generated for each detected vessel, containing averaged and mutually validated information on position, speed, course, and declared identity. Data association mechanisms enable the automatic assignment of AIS reports to corresponding radar echoes, while inconsistencies trigger alarms indicating the presence of non-cooperative objects or vessels with falsified identification.

The CoastWatch architecture enables real-time object tracking using recursive algorithms for motion state prediction and update, ensuring track continuity even under conditions of intermittent sensor data availability. The system continuously analyzes vessel trajectories, allowing the detection of behaviors deviating from established patterns, such as sudden course changes, prolonged stops in restricted areas, or atypical maneuvers in the vicinity of port infrastructure [57]. The operator interface provides a unified maritime situational picture presented on digital navigational charts, displaying object tracks, surveillance zones, and alarm notifications. Operators are able to manually verify vessel classifications using EO/IR camera imagery and access historical trajectory data. Data exchange mechanisms enable system integration with port VTS systems, traffic management centers, and national Maritime Domain Awareness structures. The description of CoastWatch above is based on publicly available vendor communications and press documentation [57]. Specific internal data fusion algorithms and quantitative performance metrics are not disclosed by Saab in public sources; accordingly, no such claims are made here. The functional description reflects the system's documented capabilities at the architectural level, consistent with the comparative evaluation criteria applied uniformly across all reviewed systems.

3.4. Kongsberg Norcontrol—Foresight (Vessel Traffic/MDA)

Foresight by Kongsberg Norcontrol is an advanced platform for maritime traffic management and situational awareness, deployed in Vessel Traffic Service (VTS) systems as well as within Maritime Domain Awareness (MDA) frameworks [58]. The system integrates AIS data, coastal radar sensors, EO/IR sensors, and meteorological and hydrographic information [58]. These data are consolidated within a central operational database, where object track correlation and trajectory estimation are performed [58]. Foresight provides continuous tracking of vessels, analysis of their behavior, and decision support for operators

of surveillance centers [58]. Through the integration of data from heterogeneous sources, the system enables the detection of situations such as AIS signal loss, vessel stoppage in atypical locations, or deviations from planned routes. The system represents a typical centralized solution in which the data fusion layer constitutes the foundation for subsequent operational analysis of maritime traffic. The description of Foresight is intentionally more concise than those of other systems because the volume of publicly available technical documentation for this platform is more limited. Kongsberg Norcontrol does not provide detailed architectural or algorithmic specifications in public materials [58]. Rather than introduce speculative content, the analysis is restricted to what can be reliably established from available sources, maintaining consistency with the evidence-based approach applied throughout the review.

3.5. HAVELSAN—VTS/Coastal Surveillance & Marine Traffic Management

HAVELSAN offers a family of VTS and coastal surveillance systems deployed in ports and national maritime traffic management infrastructures [59]. The platform is designed using a distributed architecture, comprising a network of radar sites, EO/IR electro-optical sensors, and AIS receiving stations interconnected with a central data processing center [59]. Radars operating in the X and S bands provide detection and automatic tracking of surface vessels within port and coastal coverage areas, while the AIS supplies declared identification and navigational information. These capabilities are complemented by VHF communication channels and digital communication systems used for operator–vessel interaction.

The data fusion layer performs correlation between declarative information and radar and visual observations. For each object, a motion state vector is maintained [60]:

$$\mathbf{x}_k = [x_k, y_k, v_k, \psi_k]^T, \quad (7)$$

which is updated at successive time steps based on incoming sensor data. The tracking process is implemented recursively following a prediction–update scheme, enabling the maintenance of track continuity even under conditions of intermittent loss of individual data sources. The assignment of AIS reports to their corresponding radar detections is performed through a data association process, in which the spatial and temporal consistency of the measurements is evaluated.

The analysis of vessel motion includes the estimation of kinematic parameters and the assessment of collision risk. For a pair of objects i, j , the time to the closest point of approach (CPA—Closest Point of Approach) is estimated according to the following relationship [61]:

$$t_{CPA} = -\frac{(\mathbf{p}_i - \mathbf{p}_j) \cdot (\mathbf{v}_i - \mathbf{v}_j)}{\|\mathbf{v}_i - \mathbf{v}_j\|^2}, \quad (8)$$

and the corresponding distance, defined as:

$$d_{CPA} = \|(\mathbf{p}_i - \mathbf{p}_j) + t_{CPA}(\mathbf{v}_i - \mathbf{v}_j)\| \quad (9)$$

Based on the values of $t_{CPA,i}$ and d_{CPA} , the system generates collision warnings and supports operators in decision-making related to vessel traffic regulation in port waters. While CPA metrics are primarily associated with collision avoidance, they are directly relevant to piracy detection in the following sense: a rapidly closing vessel on an intercept trajectory toward a commercial ship—particularly a small, high-speed craft whose CPA and t_{CPA} values indicate an imminent approach—exhibits kinematic patterns indistinguishable from a pre-attack maneuver. CPA-based tracking therefore serves a dual

function: conventional collision avoidance for cooperative vessels and proximity-based threat alerting for non-cooperative or suspicious ones.

In the context of maritime security, the system performs anomalous behavior detection by comparing a vessel's current trajectory with movement patterns typical for a given maritime area. Detected behaviors include, among others, sudden course changes, prolonged stops in restricted zones, and discrepancies between declared AIS identity and radar or visual observations. When deviations from established patterns are identified, alarms are generated and forwarded to the VTS operator. As a result, systems developed by HAVELSAN not only fulfill the role of a conventional VTS, but also constitute a component of Maritime Security infrastructure, enabling early detection, tracking, and documentation of incidents related to maritime piracy and other forms of criminal activity at sea. This characterization is based on HAVELSAN's own published product documentation [59], which explicitly positions its coastal surveillance platforms within the maritime security domain. No independent academic validation of HAVELSAN's anti-piracy capabilities is publicly available; the claim should therefore be understood as reflecting the vendor's stated functional scope rather than an operationally verified performance record.

3.6. SRT Marine—GeoVS HUB

GeoVS HUB by SRT Marine Systems, acting as a central integration platform responsible for data consolidation and fusion within maritime surveillance systems, plays a significant role in architectures used for counter-piracy operations [62]. In anti-piracy activities, the ability to detect, track, and classify non-cooperative targets is of critical importance, as such objects often do not transmit AIS signals or deliberately provide false identification data [52]. GeoVS HUB provides mechanisms for the acquisition and validation of data from heterogeneous sensor sources, enabling the detection of discrepancies between declarative information and physical observation [62].

Within the data fusion layer, correlation is performed between AIS reports, radar detections, and visual observations. The absence of an association between an AIS report and its corresponding radar echo constitutes the basis for the automatic classification of an object as potentially non-cooperative. Such objects may subsequently be subjected to enhanced monitoring by higher-level systems, which is particularly important for the identification of small, high-speed craft commonly used in piratical activities. The platform enables the distribution of a unified maritime situational picture to multiple operational centers, patrol units, and command-and-control systems. This facilitates the coordination of maritime security forces and reduces response times to potential piracy-related incidents. In cases where trajectories characteristic of attack preparation are detected—such as prolonged drifting in the vicinity of major shipping lanes or sudden acceleration toward a merchant vessel—the supervisory system may generate alerts and initiate intervention procedures. Distinguishing piracy-related trajectories from legitimate activities such as fishing presents a recognized challenge in the field. Research has shown that a combination of kinematic features (speed profile, course variability, proximity to shipping lanes) and contextual factors (AIS status, vessel size, geographic area, time of day) can be used to differentiate threatening from benign behaviors with practically useful accuracy [42,47]. Nonetheless, false alarms remain a limitation of purely trajectory-based approaches, which reinforces the need for multi-modal evidence (including AIS status and visual classification) and, as noted in Section 5, direct vessel messaging as an additional disambiguation channel.

For a synthetic comparison of commercially available maritime surveillance systems, Table 3 presents their key characteristics in terms of system type, employed sensors, data fusion level, and primary application domains.

Table 3. Comparison of selected commercial maritime surveillance systems using data fusion. Author's own elaboration.

System	System Type	Main Sensors	Data Fusion Level	Primary Application
STYRIS® (Airbus)	Coastal Surveillance/MDA	Radar, AIS, EO/IR, RF, meteo	Object and feature-level fusion	National coastal protection systems, operational centers
CoastShield (Thales)	Coastal Surveillance/Security	Radar, AIS, EO/IR	Object and decision-level fusion	Coastal protection, ports, and critical infrastructure security
CoastWatch (Saab)	Coastal Surveillance/VTS	Radar, AIS, EO/IR, CCTV	Object-level fusion	Maritime traffic surveillance, VTS, MDA
Foresight (Kongsberg)	VTS/MDA	Radar, AIS, EO/IR, meteo	Object-level fusion	Maritime traffic management, situational awareness
HAVELSAN VTS	VTS/Marine Traffic Management	Radar, AIS, EO/IR	Object-level fusion	Port and national VTS systems
GeoVS HUB (SRT Marine)	Data Fusion Platform	Radar, AIS, CCTV	Data- and object-level fusion	Data integration layer in VTS/MDA systems

The conducted comparison confirms that, regardless of the manufacturer, all analyzed systems employ multisensor architectures and perform data fusion at the object level to build a coherent operational situation picture. The integration of marine radar data, AIS, and EO/IR visual sensors constitutes a common foundation of contemporary commercial maritime surveillance solutions. Differences between individual systems mainly concern functional scope and target application domains, ranging from classical VTS systems to comprehensive coastal protection and Maritime Domain Awareness (MDA) platforms. The fusion level classifications in Table 3 were assigned by the author based on a systematic mapping of each system's documented functional capabilities to the JDL model levels defined in Table 1: a system was classified at object level if its documentation confirms unified track generation from multiple sensors; decision level was assigned only when AI-based classification or automated alert generation was explicitly documented. This classification reflects the author's analytical interpretation rather than vendor self-classification. Regarding the absence of quantitative performance indicators in Table 3: detection accuracy rates, false alarm rates, and response times are not disclosed in the publicly available documentation for any of the reviewed systems. The comparison is therefore qualitative in nature, limited to architectural and functional characteristics that could be reliably established from available sources. The conclusion that automatic threat detection at the ship operational level remains limited across all reviewed systems is supported by the consistent observation, across all six platforms, that data processing and decision-making are architecturally located in onshore centers, and that none of the reviewed systems document autonomous onboard anomaly analysis capabilities as a primary function. This structural characteristic—centralized, shore-based processing—is consistently documented across vendor materials [50,51,55,57–59,62] and constitutes the systematic evidence for this conclusion. At the same time, the analysis indicates that most available solutions focus on centralized data processing in onshore centers, while automatic threat detection functions at the ship operational level remain limited. This highlights the need for further development of autonomous early-warning systems performing data fusion and anomaly analysis directly onboard vessels.

4. Proposed System Concept

Based on the analysis of contemporary maritime surveillance system architectures and the review of available commercial solutions, a conceptual model of an autonomous early-warning system for maritime piracy threat detection has been proposed, the architecture of which is presented in Table 4.

Table 4. System requirements of the proposed autonomous early warning system. Author's own elaboration.

Requirement Category	Specification	Justification
Sensor set	AIS, marine radar, EO/IR camera	Ensures complementary data sources enabling detection of both cooperative vessels (AIS) and non-cooperative objects (radar, EO/IR).
Data fusion level	Object-level fusion	Correlation of radar tracks with AIS data and visual information to generate a unified operational situation picture.
Processing mode	Local (onboard), real-time	Eliminates delays resulting from data transmission to onshore surveillance centers.
System response time	<5 s from anomaly detection to alert generation	Ensures rapid crew response to dynamic piracy-related threats.
Detection function	AI/machine learning algorithms	Identification of atypical behaviors such as sudden course changes, AIS signal loss, or approach of small high-speed craft.
Analysis method	Algorithms AI/machine learning	Automatic behavior classification without the need for continuous operator interpretation.
User interface	COP visualization with audible and textual alerts	Provides clear communication of threat information to the ship's crew.
Integration with external systems	VTS/MDA	Enables transmission of threat information to maritime surveillance centers.
Resilience to communication loss	Autonomous system operation	Maintains functionality even in the absence of connectivity with onshore systems.
Operating environment	Maritime conditions (vibration, humidity, salinity)	Ensures reliable operation in shipboard environmental conditions.

The proposed five-layer architecture of the autonomous early-warning system is illustrated in Figure 2. The lowest layer (Layer 1) encompasses the onboard sensor suite, comprising an AIS receiver, marine radar, EO/IR camera, and meteorological sensors, each providing complementary information about the surrounding maritime environment. Raw sensor data are passed to Layer 2, where multi-sensor data fusion is performed at the object level following the JDL framework: signals undergo time synchronisation and noise filtering, followed by track association using Kalman filtering and Mahalanobis-distance gating, and are ultimately consolidated into a unified Common Operational Picture (COP) for each detected vessel, with Bayesian confidence weighting applied to account for varying sensor reliability. The fused tracks are then forwarded to Layer 3, where three parallel AI-based mechanisms operate: an LSTM-based trajectory model detects deviations from expected movement patterns in an unsupervised manner, an Isolation Forest algorithm assigns anomaly scores to vessels exhibiting novel threat signatures not represented in historical data, and a CNN-based visual classifier processes EO/IR imagery to confirm vessel class and identity. The outputs of these three modules are integrated in Layer 4 through decision-level fusion, which produces a consolidated risk assessment. Upon

exceeding a predefined risk threshold, an audible and visual alert is generated for the ship's crew within a target latency of less than five seconds; a context filter additionally incorporates incoming VHF voice communications and digital AIS messages to suppress false alarms triggered by vessels with a legitimate declared reason for anomalous behaviour. Finally, Layer 5 provides optional connectivity to external systems—including VTS/MDA centres, coast guard authorities, and fleet management platforms—enabling transmission of incident data when communication links are available. Critically, Layers 1 through 4 are designed to operate fully autonomously onboard, without dependence on shore-based infrastructure, ensuring that the system maintains functionality even under communication constraints characteristic of open-sea piracy scenarios.

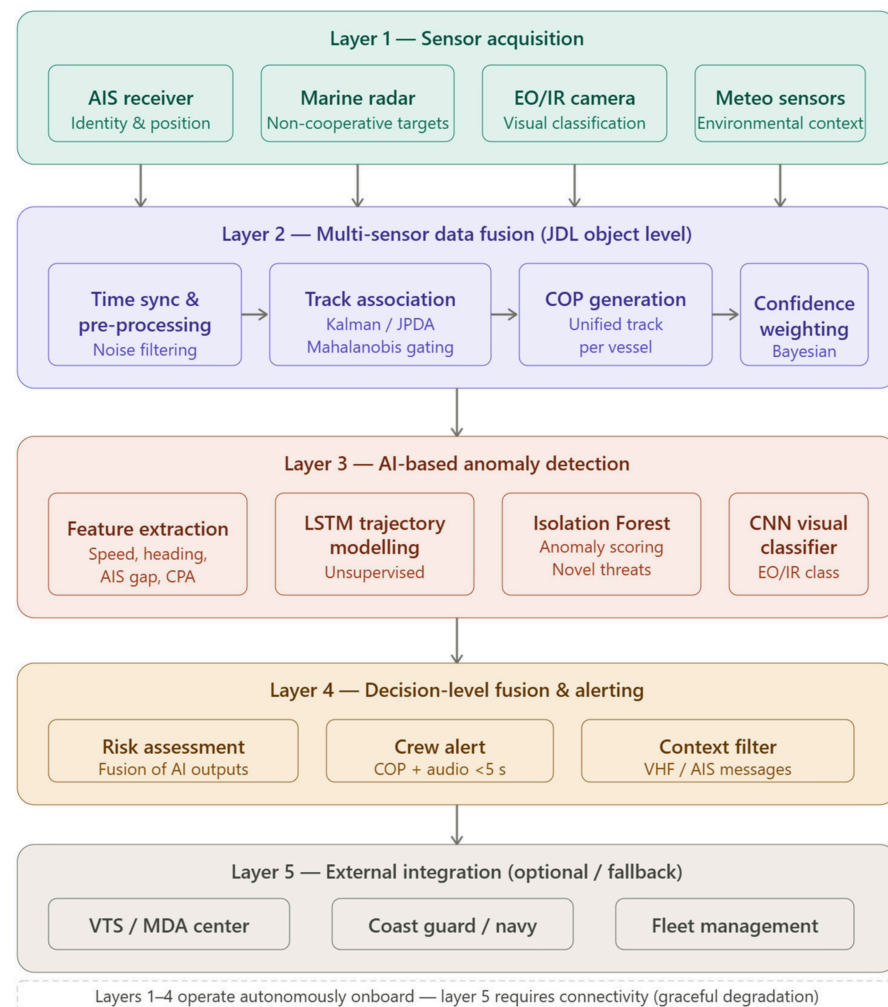


Figure 2. Five-layer architecture of the proposed autonomous early-warning system for maritime piracy threat detection. Author's own elaboration.

The proposed solution assumes shifting selected data fusion and anomaly analysis functions from centralized surveillance centers to the ship operational level, enabling local real-time data processing. The key innovative features that distinguish this concept from existing MDA and VTS architectures are: (1) fully autonomous onboard operation without dependence on shore-based infrastructure, (2) real-time anomaly detection at the ship level with a target response time below 5 s, and (3) integration of AI-based behavioral classification directly within the sensor fusion pipeline rather than as a post-processing layer in an onshore center. The system requirements presented in Table 4 were derived from a synthesis of three sources: the functional gaps identified in the comparative review

of commercial systems (Section 3), established maritime security operational requirements described in the academic literature [42,43,47], and general principles of autonomous shipborne system design informed by IMO e-navigation guidelines. They represent the author's informed conceptual specification rather than the output of a formal expert elicitation or standardization process, and are explicitly proposed as a basis for validation in future work. Regarding AI methodology: the envisioned detection function combines unsupervised anomaly detection methods—specifically Isolation Forest and LSTM-based trajectory modeling—with supervised classification for known piracy behavioral patterns. Unsupervised methods are particularly appropriate for detecting novel threat signatures not represented in training data, while supervised approaches can exploit labeled historical incident data. Publicly available AIS-based datasets (e.g., the MarineTraffic historical AIS dataset, the Danish Maritime Authority open AIS archive) as well as incident databases such as the IMB Piracy Reporting Centre annual reports provide a basis for defining behavioral patterns characteristic of piracy threats, as also discussed in recent literature [42,47]. Regarding computational feasibility: the processing of fused AIS, radar, and EO/IR data at object level in real time is within the capability of current embedded computing platforms. Published work on edge-AI for autonomous surface vehicles [27] demonstrates that object-level fusion and anomaly scoring for maritime targets can be performed at rates consistent with the proposed 5 s response requirement on hardware in the class of NVIDIA Jetson AGX or equivalent platforms. Detailed hardware benchmarking is identified as a priority for the next research phase.

The system integrates data from onboard navigational and observational sensors, in particular the AIS receiver, marine radar, and EO/IR cameras. These data undergo preliminary processing, including time synchronization, measurement noise filtering, and object feature extraction. Subsequently, multisensor data fusion at the object level is performed, involving correlation of radar tracks with AIS data and confirmation of vessel classification based on visual information. Based on the unified operational situation picture, an analytical layer implementing artificial intelligence algorithms is applied to detect anomalies in vessel movement and identify atypical behavioral patterns characteristic of potential piracy threats. In the event of detecting an elevated risk level, the system generates an automatic alert for the ship's crew and enables transmission of information to external maritime traffic surveillance centers.

The defined system requirements provide a foundation for the next stage of designing the detailed technical architecture and selecting appropriate data processing and anomaly analysis algorithms. The requirements in Table 4 are explicitly proposed as an initial conceptual specification derived from the functional gap analysis in this paper; they have not been formally validated through expert consultations or against industry standards. Validation of these requirements—including assessment against IMO e-navigation guidelines, IEC maritime electronics standards, and input from maritime security practitioners—is planned as part of the subsequent research phase. Specifying real-time operational parameters and a local processing mode distinguishes the proposed concept from existing commercial solutions, in which data analysis is primarily performed in onshore centers. Consequently, the presented requirements outline the direction for further research on the implementation of an autonomous early-warning system dedicated to protecting vessels against maritime piracy threats.

The proposed concept complements existing centralized maritime surveillance architectures by offering the potential to reduce response time to dynamic threats, increase resilience to communication constraints, and enhance crew readiness to counter piracy attacks.

Consequently, the proposed model defines a direction for further research on the development of autonomous maritime security systems based on data fusion and artificial intelligence algorithms.

5. Discussion

The conducted review of commercially available maritime surveillance systems confirms that multisensor data fusion has become a fundamental component of contemporary solutions providing situational awareness in maritime domains. Regardless of the manufacturer, the analyzed systems integrate data from marine radars, AIS, and EO/IR visual sensors to build a common operational picture. In many cases, this layer is further supported by artificial intelligence algorithms responsible for object classification and operator assistance. This indicates that the technological foundation for automated threat detection at sea is already present in commercial solutions. At the same time, the analysis demonstrates that the vast majority of available systems are designed primarily for coastal applications and centralized maritime surveillance centers. Platforms such as STYRIS®, CoastShield, CoastWatch, and Foresight focus on delivering a comprehensive situational picture at regional or national scales, supporting security services, coast guards, and port authorities. In this model, data processing and decision-making are performed mainly in onshore centers, while the ship remains a data source and a recipient of warning messages. From the perspective of maritime piracy threats, such an approach presents significant limitations. Pirate attacks are characterized by high dynamics and short response times required for effective counteraction. Relying exclusively on external surveillance centers for threat detection may lead to decision-making delays resulting from data transmission, centralized analysis, and dissemination of warnings to the vessel. In the case of small, high-speed craft attempting boarding, even minute-level delays can substantially reduce the crew's ability to respond effectively. A second notable limitation of commercial systems is their primary focus on building situational awareness, with a relatively lower degree of automation in risk assessment processes. The assessment of automation levels across the reviewed platforms was conducted qualitatively, based on the evaluation criterion defined in the aims paragraph of Section 1 (degree of automation and the role of human operators). For each system, the vendor documentation was examined for explicit statements about automated decision-making, alert generation without operator confirmation, or autonomous threat classification. In all cases, the documentation describes operator-assisted workflows in which alerts are presented to human operators for verification and action, rather than fully automated response pipelines. Although some manufacturers declare the use of AI for object classification, most systems still require active interpretation by human operators. Consequently, the final decision to classify vessel behavior as potentially dangerous remains largely dependent on human judgment. The functional gap identified between current commercial systems and the requirements for piracy-specific early warning is supported by convergent evidence from multiple sources: the consistent architectural pattern of shore-based processing documented across all reviewed systems, the absence of onboard autonomous anomaly detection in any vendor's documented feature set, and findings in the academic literature on maritime security [42,43,47] that identify autonomous onboard threat detection as an open research problem. While no dedicated user needs analysis or stakeholder study was conducted as part of this work, these sources collectively substantiate the identified gap. An additional avenue worth exploring is the integration of direct messages received from the vessel itself—for example via VHF voice communications or digital messaging systems—into the threat analysis process. If a vessel transmits a message explaining an unusual maneuver (e.g., engine trouble or an emergency stop), this contextual information could be used to suppress a potential false alarm, thereby

improving the reliability of automated alert generation and reducing the workload placed on operators.

In light of the presented observations, a functional gap is evident between existing maritime surveillance solutions and the need for early detection of piracy-related threats directly at the ship operational level. In particular, there is a lack of solutions integrating multisensor data fusion layers with anomaly analysis algorithms and automatic alert generation performed locally, in real time, onboard vessels. The identified gap provides a rationale for further research on autonomous early-warning systems in which selected analytical and decision-making functions are shifted from centralized surveillance centers to the ship level. Such an approach enables shortening of the decision-making chain, increasing system resilience to communication disruptions, and improving crew readiness to respond to dynamic threats. The development of compact edge computing platforms and increasingly efficient AI algorithms creates realistic opportunities for implementing such solutions in maritime environments.

Available commercial systems confirm the maturity of data fusion technologies in maritime surveillance; however, they simultaneously highlight the need for further development of specialized, autonomous early-detection mechanisms dedicated to maritime piracy threats.

6. Conclusions and Future Work

This paper presents an analysis of contemporary maritime surveillance systems employing multisensor data fusion and assesses their suitability in the context of early detection of maritime piracy threats. The conducted review indicates that the integration of AIS data, marine radar information and EO/IR visual sensors, supported by artificial intelligence algorithms, has become a standard technological foundation in commercial maritime surveillance and coastal protection systems. Solutions such as STYRIS[®], Coast-Shield, CoastWatch, Foresight, HAVELSAN VTS systems and the GeoVS HUB platform confirm a high level of maturity in building a common operational picture and supporting situational awareness for maritime monitoring services. At the same time, the analysis shows that most available solutions are primarily designed for coastal surveillance and centralized maritime traffic management centers, where data processing and decision-making are performed onshore. Although this model is effective on a regional scale, it reveals limitations in scenarios requiring immediate response at the ship operational level, which are characteristic of dynamic piracy-related threats. Moreover, despite the growing application of AI algorithms, final risk assessment in many systems still largely depends on operator interpretation. These observations confirm the existence of a functional gap between current commercial solutions and the need for autonomous early-warning systems dedicated to maritime piracy threat detection directly onboard vessels. Bridging this gap requires shifting selected data fusion and anomaly analysis functions closer to data sources, enabling reduced response time, increased system resilience to communication constraints, and improved crew readiness to counter emerging threats.

Future research will focus on the development of a detailed and validated system architecture for autonomous onboard piracy early warning, building upon the high-level conceptual requirements outlined in Section 4 of this paper. To clarify the distinction: Section 4 presents a set of functional requirements and a preliminary architectural outline derived from the review; the future conceptual model will constitute a formally specified, algorithmically detailed, and computationally characterized system design, supported by simulation-based validation. It should also be acknowledged that existing onboard situational awareness systems and intelligent shipborne surveillance platforms—such as ECDIS-integrated anomaly detection modules, advanced bridge navigation watch alarm systems

(BNWAS), and research prototypes for autonomous vessel collision avoidance—were not covered by this review, which focused on commercial multi-sensor data fusion platforms. Consideration of these onboard systems in relation to the proposed concept is identified as a direction for future comparative analysis. Particular attention in future work will be given to defining detailed algorithmic specifications, designing real-time data processing architectures, and developing decision-making logic adapted to operational conditions onboard ships. Further research directions include the evaluation of edge computing platforms for maritime environments, analysis of data transmission reliability, and investigation of cybersecurity aspects and algorithm transparency to ensure user trust in automatically generated alerts. It should be noted that the present paper is intentionally scoped as a conceptual and analytical review; experimental validation and quantitative performance evaluation are outside the scope of this work. The absence of an experimental section reflects the current stage of the research, in which a thorough analysis of existing commercial architectures and the identification of functional gaps constitute the necessary foundation for subsequent system design and implementation. Experimental validation, including simulation-based testing and hardware-in-the-loop evaluation, is planned as part of the next phase of the research.

The conclusions presented in this paper provide a foundation for further development of autonomous maritime security systems and align with the current transformation trend from centralized surveillance architectures toward distributed, intelligent, and resilient onboard solutions capable of effective early detection of maritime piracy threats.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification System
AI	Artificial Intelligence
BMP	Best Management Practices
CCTV	Closed-Circuit Television
COP	Common Operational Picture
CPA	Closest Point of Approach
C2	Command and Control
EO/IR	Electro-Optical/Infrared
JDL	Joint Directors of Laboratories (Data Fusion Model)
KF	Kalman Filter
MDA	Maritime Domain Awareness
RF	Radio Frequency
VTs	Vessel Traffic Services
VTMIS	Vessel Traffic Management and Information System

References

1. Xu, M.; Ma, X.; Zhao, Y.; Qiao, W. A Systematic Literature Review of Maritime Transportation Safety Management. *J. Mar. Sci. Eng.* **2023**, *11*, 2311. [[CrossRef](#)]

2. Koray, M.; Kaya, E.; Keskin, M.H. Determining Logistical Strategies to Mitigate Supply Chain Disruptions in Maritime Shipping for a Resilient and Sustainable Global Economy. *Sustainability* **2025**, *17*, 5261. [\[CrossRef\]](#)
3. Wambua, M. A Critical Review of the Global Legal Framework on Piracy: 40 Years after UNCLOS. *Marit. Aff. J. Natl. Marit. Found. India* **2022**, *18*, 134–148. [\[CrossRef\]](#)
4. Pandey, S.K. A Comprehensive Classification System of Non-Traditional Maritime Security Threats: A Step towards Enhancing Maritime Security. *Int. J. Sci. Res. Publ.* **2023**, *13*, 227–234. [\[CrossRef\]](#)
5. Tsailas, D.N. Risks and Threats in the 21st Century Maritime Security. *Secur. Sci. J.* **2025**, *6*, 106–144. [\[CrossRef\]](#)
6. Durlík, I.; Miller, T.; Dorobczyński, L.; Kozłowska, P.; Kostecki, T. Revolutionizing Marine Traffic Management: A Comprehensive Review of Machine Learning Applications in Complex Maritime Systems. *Appl. Sci.* **2023**, *13*, 8099. [\[CrossRef\]](#)
7. Ahmed, T.; Creedon, L.; Gharbia, S.S. Low-Cost Sensors for Monitoring Coastal Climate Hazards: A Systematic Review and Meta-Analysis. *Sensors* **2023**, *23*, 1717. [\[CrossRef\]](#) [\[PubMed\]](#)
8. Potamos, G.; Stavrou, E.; Stavrou, S. Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis. *Sensors* **2024**, *24*, 3458. [\[CrossRef\]](#) [\[PubMed\]](#)
9. Ali, B.; Obembe, E. Leveraging Technology for Enhanced Operational Effectiveness in the Nigerian Navy. *J. Sci. Innov. Technol. Res.* **2025**, *9*. [\[CrossRef\]](#)
10. Li, M.; Zhou, J.; Chattopadhyay, S.; Goh, M. Maritime Cybersecurity: A Comprehensive Review. *arXiv* **2024**, arXiv:2409.11417. [\[CrossRef\]](#)
11. Wang, C.; Xu, Y.; Zhang, D. Multi-Modal Perception and Fusion for Maritime Autonomy: A Survey. *Preprints* **2025**. [\[CrossRef\]](#)
12. Zhuang, Y.; Sun, X.; Li, Y.; Huai, J.; Hua, L.; Yang, X.; Cao, X.; Zhang, P.; Cao, Y.; Qi, L.; et al. Multi-Sensor Integrated Navigation/Positioning Systems Using Data Fusion: From Analytics-Based to Learning-Based Approaches. *Inf. Fusion* **2023**, *95*, 62–90. [\[CrossRef\]](#)
13. Hall, D.L.; Llinas, J. An Introduction to Multisensor Data Fusion. *Proc. IEEE* **1997**, *85*, 6–23. [\[CrossRef\]](#)
14. Şengül, B.; Yılmaz, F.; Uğurlu, Ö. Safety–Security Analysis of Maritime Surveillance Systems in Critical Marine Areas. *Sustainability* **2023**, *15*, 16381. [\[CrossRef\]](#)
15. Guerriero, M.; Willett, P.; Coraluppi, S.; Carthel, C. Radar/AIS Data Fusion and SAR Tasking for Maritime Surveillance. In Proceedings of the 2008 11th International Conference on Information Fusion, Cologne, Germany, 30 June–3 July 2008.
16. Melnyk, O.; Kuznichenko, S.; Onishchenko, O. Impact of AIS Manipulation on Shipping Safety and Strategic Countermeasures. *Lex Portus* **2024**, *10*, 31–39. [\[CrossRef\]](#)
17. Ara, N. Vessel Delay Detection and Pattern Mining from AIS Data. Master's Thesis, The University of Texas Rio Grande Valley, Edinburg, TX, USA, 2024.
18. Diao, P.S.; Alves, T.; Poussot, B.; Azarian, S. A Review of Radar Detection Fundamentals. *IEEE Aerosp. Electron. Syst. Mag.* **2024**, *39*, 4–24. [\[CrossRef\]](#)
19. Buyukakkaslar, M.T.; Erturk, M.A.; Aydin, M.A. A Review on Radar-Based Human Detection Techniques. *Sensors* **2024**, *24*, 5709. [\[CrossRef\]](#) [\[PubMed\]](#)
20. Ahammad, T.; Shafi, M.G.R. Enhancing Surveillance Systems with Cost-Effective Ultrasonic Radar for Object Detection and Tracking. *Jagannath Univ. J. Sci.* **2024**, *11*. [\[CrossRef\]](#)
21. Shi, K.; He, S.; Shi, Z.; Chen, A.; Xiong, Z.; Chen, J.; Luo, J. Radar and Camera Fusion for Object Detection and Tracking: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2026**, *28*, 3478–3520. [\[CrossRef\]](#)
22. Wang, S.; Kim, B. Scale-Sensitive Attention for Multi-Scale Maritime Vessel Detection Using EO/IR Cameras. *Appl. Sci.* **2024**, *14*, 11604. [\[CrossRef\]](#)
23. Nagaraju, B.; Rajesh, R. Integrated Electro Optic Infra Red (EO/IR) Simulation for Airborne Maritime Surveillance. In Proceedings of the 2024 IEEE Space, Aerospace and Defence Conference (SPACE 2024), Bangalore, India, 22–23 July 2024; pp. 501–504.
24. Hassani, S.; Dackermann, U. A Systematic Review of Advanced Sensor Technologies for Non-Destructive Testing and Structural Health Monitoring. *Sensors* **2023**, *23*, 2204. [\[CrossRef\]](#) [\[PubMed\]](#)
25. Liu, A.; Huang, Z.; Li, M.; Wan, Y.; Li, W.; Han, T.X.; Liu, C.; Du, R.; Tan, D.K.P.; Lu, J.; et al. A Survey on Fundamental Limits of Integrated Sensing and Communication. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 994–1034. [\[CrossRef\]](#)
26. Yuanyuan, Z.; Bin, Z.; Cheng, S.; Haolu, L.; Jicheng, H.; Kunpeng, T.; Zhong, T. Review of the Field Environmental Sensing Methods Based on Multi-Sensor Information Fusion Technology. *Int. J. Agric. Biol. Eng.* **2024**, *17*, 1–13. [\[CrossRef\]](#)
27. Liu, R.W.; Guo, Y.; Nie, J.; Hu, Q.; Xiong, Z.; Yu, H.; Guizani, M. Intelligent Edge-Enabled Efficient Multi-Source Data Fusion for Autonomous Surface Vehicles in Maritime Internet of Things. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 1574–1587. [\[CrossRef\]](#)
28. Reggiannini, M.; Salerno, E.; Bacciu, C.; D'Errico, A.; Lo Duca, A.; Marchetti, A.; Martinelli, M.; Mercurio, C.; Mistretta, A.; Righi, M.; et al. Remote Sensing for Maritime Traffic Understanding. *Remote Sens.* **2024**, *16*, 557. [\[CrossRef\]](#)
29. Baek, W.-K.; Kim, E.; Jeon, H.-K.; Lee, K.-J.; Kim, S.-W.; Lee, Y.-K.; Ryu, J.-H. Monitoring Maritime Ship Characteristics Using Satellite Remote Sensing Data from Different Sensors. *Ocean Sci. J.* **2024**, *59*, 8. [\[CrossRef\]](#)

30. Schmitt, M.; Zhu, X.X. Data Fusion and Remote Sensing: An Ever-Growing Relationship. *IEEE Geosci. Remote Sens. Mag.* **2016**, *4*, 6–23. [[CrossRef](#)]
31. Hussain, M.; O'Nils, M.; Lundgren, J.; Mousavirad, S.J. A Comprehensive Review on Deep Learning-Based Data Fusion. *IEEE Access* **2024**, *12*, 180093–180124. [[CrossRef](#)]
32. Brena, R.F.; Aguilera, A.A.; Trejo, L.A.; Molino-Minero-Re, E.; Mayora, O. Choosing the Best Sensor Fusion Method: A Machine-Learning Approach. *Sensors* **2020**, *20*, 2350. [[CrossRef](#)] [[PubMed](#)]
33. Avornu, C.; Akama, S.D.; Avornu, E.K.; Aveyom, V. Data Fusion for Predictive Maintenance of Industrial Assets Using Digital Twin. In Proceedings of the 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Jakarta, Indonesia, 6–7 October 2022; pp. 115–121.
34. Chen, S.; Gao, M.; Shi, P.; Zeng, X.; Zhang, A. Target Ship Recognition and Tracking with Data Fusion Based on Bi-YOLO and OC-SORT Algorithms for Enhancing Ship Navigation Assistance. *J. Mar. Sci. Eng.* **2025**, *13*, 366. [[CrossRef](#)]
35. Heymann, F.; Banys, P.; Saez, C. Radar Image Processing and AIS Target Fusion. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2015**, *9*, 443–448. [[CrossRef](#)]
36. Zhang, F.; Xia, Z.; Jin, S.; Liu, X.; Zhao, Z.; Zhang, C.; Fu, H.; Xing, K.; Liu, Z.; Xue, C.; et al. Ship Target Feature Detection of Airborne Scanning Radar Based on Trajectory Prediction Integration. *Remote Sens.* **2025**, *17*, 3858. [[CrossRef](#)]
37. Tetreault, B.J. Use of the Automatic Identification System (AIS) for Maritime Domain Awareness (MDA). In Proceedings of the OCEANS 2005 MTS/IEEE, Washington, DC, USA, 18–23 September 2005; pp. 1590–1594.
38. Fowdur, J.S.; Baum, M.; Heymann, F.; Banys, P. An Overview of the PAKF-JPDA Approach for Elliptical Multiple Extended Target Tracking Using High-Resolution Marine Radar Data. *Remote Sens.* **2023**, *15*, 2503. [[CrossRef](#)]
39. Vo, X.H.; Nguyen, T.K.; Nguyen, P.B.; Duong, V.M. Advanced Method for Improving Marine Target Tracking Based on Multiple-Plot Processing of Radar Images. *Electronics* **2024**, *13*, 2548. [[CrossRef](#)]
40. Ziółkowska, N.; Szlapczyńska, J. From Mathematical to AI-Based Methods: A Review of Marine PNT Data Fusion and Uncertainty Handling. *Comput. Sci. Rev.* **2026**, *60*, 100864. [[CrossRef](#)]
41. Hoehner, F.; Langenohl, V.; El Moctar, O.; Schellin, T.E. Scenario-Based Sensor Selection for Autonomous Maritime Systems: A Multi-Criteria Analysis of Sensor Configurations for Situational Awareness. *J. Mar. Sci. Eng.* **2025**, *13*, 2008. [[CrossRef](#)]
42. Thakur, A.S.; Alex, T.L.; Nighojkar, A. Artificial Intelligence in Maritime Anomaly Detection: A Decadal Bibliometric Analysis (2014–2024). *J. Inst. Eng. India Ser. C* **2025**, *106*, 665–689. [[CrossRef](#)]
43. Durluk, I.; Miller, T.; KostECKa, E.; Tuński, T. Artificial Intelligence in Maritime Transportation: A Comprehensive Review of Safety and Risk Management Applications. *Appl. Sci.* **2024**, *14*, 8420. [[CrossRef](#)]
44. Qi, Y.; Yang, J.; Bai, A.; Liu, J. A Method for Real-Time Detection of Vessel Abnormal Behavior Based on CNN-LSTM. *Expert Syst. Appl.* **2025**, *288*, 128303. [[CrossRef](#)]
45. Farahnakian, F.; Heikkonen, J.; Nevalainen, P. Abnormal Behaviour Detection by Using Machine Learning-Based Approaches in the Marine Environment: A Literature Survey. In Proceedings of the 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 20–22 July 2022; pp. 1–11.
46. Vaarandi, R.; Tsiopoulos, L.; Visky, G.; Ur Rehman, M.; Bahşi, H. A Systematic Literature Review of Cyber Security Monitoring in Maritime. *IEEE Access* **2025**, *13*, 85307–85329. [[CrossRef](#)]
47. He, Z.; Wang, C. Evolving Regularity and Geographical Patterns of Global Piracy Incidents Distribution. *Secur. J.* **2025**, *38*, 11. [[CrossRef](#)]
48. Soldi, G.; Gaglione, D.; Forti, N.; Millefiori, L.M.; Braca, P.; Carniel, S.; Simone, A.D.; Iodice, A.; Riccio, D.; Daffina, F.C.; et al. Space-Based Global Maritime Surveillance. Part II: Artificial Intelligence and Data Fusion Techniques. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 30–42. [[CrossRef](#)]
49. Priyadharshini, S.D.; Vadivazhagan, K. Enhanced Vessel Detection in Maritime Surveillance Using Multi-Modal Data Integration and Deep Learning. In Proceedings of the 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 3–5 October 2024; pp. 1090–1099.
50. STYRIS® for Coastal Surveillance. Airbus Defence Solutions. 2025. Available online: <https://www.defence-solutions.airbus.com/en/solutions/sea/styris-coastal-surveillance-system> (accessed on 12 May 2026).
51. STYRIS® for Ports Management and Vessel Traffic Services. Airbus Defence Solutions. 2025. Available online: https://www.defence-solutions.airbus.com/sites/g/files/jlcba231/files/2025-03/styris_vts_brochure.pdf (accessed on 12 May 2026).
52. Hall, D.; Llinas, J. *Multisensor Data Fusion*; CRC Press: Boca Raton, FL, USA, 2001.
53. Li, Z.; Feng, L.; Yang, A. Fusion Based on Visible Light Positioning and Inertial Navigation Using Extended Kalman Filters. *Sensors* **2017**, *17*, 1093. [[CrossRef](#)] [[PubMed](#)]
54. Bar-Shalom, Y.; Li, X.R.; Kirubarajan, T. *Estimation with Applications to Tracking and Navigation: Theory, Algorithms and Software*, 1st ed.; Wiley: Hoboken, NJ, USA, 2002.
55. Thales Group. Available online: <https://www.thalesmaritime.com/> (accessed on 12 May 2026).

56. Nguyen, D.; Vadaine, R.; Hajduch, G.; Garelo, R.; Fablet, R. *GeoTrackNet*—A Maritime Anomaly Detector Using Probabilistic Neural Network Representation of AIS Tracks and *A Contrario* Detection. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 5655–5667. [CrossRef]
57. Saab Press Centre Saab Signs Coastal Surveillance System Contract With Croatia. Available online: <https://www.saab.com/newsroom/press-releases/2016/saab-signs-coastal-surveillance-system-contract-with-croatia> (accessed on 12 May 2026).
58. Kongsberg Norcontrol Foresight—Maritime Surveillance. Available online: <https://www.kongsbergmaritime.com/products/naval-systems/> (accessed on 12 May 2026).
59. HAVELSAN Coastal Surveillance and Marine Traffic Management. Available online: <https://www.havelsan.com/en/beyond-today/coastal-surveillance-and-marine-traffic-management> (accessed on 12 May 2026).
60. Huang, W.; Feng, H.; Xu, H.; Liu, X.; He, J.; Gan, L.; Wang, X.; Wang, S. Surface Vessels Detection and Tracking Method and Datasets with Multi-Source Data Fusion in Real-World Complex Scenarios. *Sensors* **2025**, *25*, 2179. [CrossRef] [PubMed]
61. Sun, W.; Zheng, K.; Feng, Z.; Jiang, Y. A New Collision Risk Assessment Algorithm Based on Ship's Finite-Time Reachable Set. *J. Mar. Sci. Eng.* **2025**, *13*, 2174. [CrossRef]
62. SRT Marine Systems. Available online: <https://srt-marine.com/> (accessed on 12 May 2026).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.