Adaptive Multi-Criteria Modeling for Maritime Cyber Risk Management and Resilience Evaluation

Oleksiy Melnyk[1], Oleksandr Shumylo[1], Oleg Onishchenko[1], Serhii Kuznichenko[2], Valentin Ternovsky[1] and Gennady Shcheniavskyi[1]

[1]Odesa National Maritime University, Odesa, Ukraine
[2]Scientific and Research Institute of Providing Legal Framework for the Innovative Development of National Academy of Legal Sciences of Ukraine, Kharkiv, Ukraine

Correspondence to:
Oleksiy Melnyk,
atlantic.chart@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Melnyk O, Shumylo O, Onishchenko O, Kuznichenko S, Ternovsky V and Shcheniavskyi G. Adaptive Multi-Criteria Modeling for Maritime Cyber Risk Management and Resilience Evaluation. Premier Journal of Science 2025;16:100196

DOI: https://doi.org/10.70389/PJS.100196

Peer Review
Received: 22 October 2025
Last revised: 1 December 2025
Accepted: 1 December 2025
Version accepted: 7
Published: 7 January 2026

Ethical approval: This article does not contain any studies with human participants performed by any of the authors.

Consent: This article does not contain any studies with human participants performed by any of the authors.

ABSTRACT

This paper introduces an integrated mathematical model for managing cyber risks in maritime transport systems. The model combines the Analytic Hierarchy Process (AHP), Failure Mode and Effects Analysis (FMEA), Bayesian probability updating, reliability assessment methods, and decision support system (DSS) optimization mechanisms. Its goal is to quantitatively assess and reduce risks from cyberattacks targeting primary autonomous surface vessels and port-based energy infrastructures equipped with energy storage systems and soft open point technologies. Using a multi-criteria evaluation framework, the research performs comprehensive risk quantification, dynamically updates the probabilities of cyber incidents, and examines the technical and operational impacts of cyber interference on system performance. Three operational scenarios are analyzed: normal operation, cyberattack, and adaptive mitigation, to show how risk levels vary and how decision support algorithms can effectively restore system stability. Results indicate that cyber threats may significantly increase overall risk levels, while adaptive optimization within the decision support framework can reduce these risks and improve system resilience. This methodology provides a scientific basis for developing adaptive cyber-resilience strategies for maritime transport and supports the future use of digital twins for vessels and port infrastructures as part of Smart Maritime Infrastructure. The modeling showed that the integration of AHP–FMEA–BN allows reducing the total risk index by 23% for autonomous vessels and by 18% for port power systems compared to the baseline scenario. The scientific novelty of the study lies in the development of an adaptive model that combines multi-criteria assessment, failure analysis, and Bayesian probability updating for dynamic assessment of cyber risks in the maritime sector.

Keywords: AHP–FMEA–bayesian integration, Adaptive maritime cyber risk, Autonomous surface vessel security, Port energy storage resilience, Decision-support optimisation

Introduction

In 2021, the International Maritime Organization (IMO) published the Maritime Cyber Risk Management Guidelines, which define the strategic framework for integrating cybersecurity into the ISM Code. These provisions became the starting point for the formation of mandatory requirements for identifying vulnerabilities and implementing security measures in ship and port information technology systems.

At the same time, recent years have seen a rapid increase in the number and complexity of cyberattacks in the maritime industry. The most common ones include GPS spoofing, manipulation of AIS signals, and ransomware attacks that have led to the shutdown of ports and shipping companies. High-profile incidents at global carriers and European ports confirm that digital disruptions can have cascading effects in international supply chains. Also, despite the existence of international guidelines and the first attempts to formalize approaches to cybersecurity in maritime transport, most existing research remains largely qualitative and does not focus on threat classification, scenario examples, or regulatory requirements, nor do they provide tools for systematic quantitative risk assessment. Therefore, the lack of integrated models makes it challenging to predict the consequences of attacks and select the most effective response measures, given limited resources.

The development of cyber risk management systems in maritime transport is of particular importance in the context of the digitalization of ship and port processes. Papers[1–3] consider approaches to assessing the resilience of security barriers and the formation of risk models based on the analysis of probabilistic networks that allow tracking the dynamics of operational threats in maritime operations. Studies[4–6] are devoted to increasing the operational flexibility of technical systems, including nuclear reactors, LNG terminals, and ship power plants, where adaptive control can reduce the risks of deviations from the normal mode.

Intelligent approaches based on deep neural networks and machine learning methods are developed in,[7–10] which propose models for predicting damage, assessing the consequences of collisions, and determining the degree of degradation of autonomous vessel systems. Paper[11] introduces the concept of quantitative risk analysis (BOQRA), which allows assessing the impact of barriers on the reliability of ship operations. In turn, papers [12–19] consider in detail the human factor-crew reliability assessment, risk analysis in confined spaces, and fuzzy-logic models for high-risk work, which is critical for the integration of technical and organizational safety elements.

Studies[20–23] emphasize the importance of environmental and navigational risks in digital ports and transportation networks, in particular in the field of autonomous shipping (MASS) and congestion management. The authors of[24–28] proposed algorithms for system control, route optimization, and mission risk management with limited data. The contribution of works[29–32] is important, where integrated models of

Funding: The authors declare that no funding was received to support the preparation or publication of this manuscript

Conflicts of interest: The authors confirm that there are no known conflicts of interest associated with this publication and no financial support that could have influenced its outcome

Author contribution: Conceptualization, O.M.; methodology, O.M. and S.K.; formal analysis, O.S.; mathematical modeling and algorithm development, O.S.; investigation, O.O. and V.T.; data collection and case study analysis, V.T.; validation, S.K.; criteria development and robustness assessment, S.K.; resources, O.O. and G.S.; integration of results and system-level interpretation, G.S.; writing—original draft preparation, O.S. and V.T.; writing—review and editing, O.M., O.O., and G.S.; visualization, O.S.; supervision, O.M.; project administration, O.M.

Guarantor: Oleksiy Melnyk

Provenance and peer-review: Unsolicited and externally peer-reviewed

Data availability statement: All data generated or analyzed in this study are included in this published article. The study is based on modeling and optimization experiments; no external datasets were generated or analyzed. Supporting input parameters and calculation examples are available from the corresponding author upon reasonable reques

predictive maintenance, adaptive mission control, and safety systems in Arctic conditions were developed.

In the context of vessel technical reliability and operational safety, works[33–35] consider financial, crisis, and organizational risks in management systems, while[36–41] focus on the engineering aspects of marine technologies, such as improving the efficiency of fuel systems, assessing the impact of hull geometry on maneuverability, and using hydrogen and low-sulfur fuels. Studies[42–43] focus on improving expert methods for assessing the risks of ship operations, creating procedures for verifying results, and improving the accuracy of models.

The other publications[44–46] demonstrate the use of neural networks, 3D modeling, and ultraviolet technologies to improve the diagnosis and forecasting of the technical condition of ships and port equipment. They form the transition to modern digital twins and visual decision support systems. Finally, papers[47,48] summarize the methodology for assessing the reliability of complex technical systems and provide a mathematical basis for the transition from binary to multi-state models, which is an important condition for building risk-based ship safety architectures. At the same time, studies[49–50] emphasize the evolutionary nature of maritime transport security - from the formation of historical precedents to the development of modern multicriteria indices for assessing sustainability, assets, and the human factor in shipping systems.

In the context of adaptive multi-criteria modeling for maritime cyber risk management and resilience assessment, the references cited cover a number of relevant aspects. In particular,[51] proposes information-based risk management mechanisms suitable for adaptation in maritime digital infrastructures. In[52,53] investigated algorithmic control of ship dynamic modes, which is important for adaptive real-time risk response, while[54] provides optimization approaches to logistics decisions that are useful in conditions with a high degree of uncertainty,[55] discusses the mathematical foundations of classes of functions that can be used to build adaptive models based on a priori uncertainty in cyber threats, form an interdisciplinary basis for building models capable of multi-criteria analysis and enhancing cyber resilience in the maritime sector.

Works[56–59] and research[60] focus on innovative technologies and technological adaptation as key factors in the development of modern management systems. Source[61] emphasizes the need for dynamic and comprehensive models to improve the energy efficiency of marine vessels in risky conditions. Research[62] reveals cybersecurity challenges in the era of the Internet of Things and justifies the need for integrated approaches to assessing and minimizing cyber threats. In turn,[63] demonstrates the relationship between risk indices and system resilience, which conceptually echoes the principles of resilience of technical and marine complexes. Works[64,65] establish the methodological foundations for taking into account hydrometeorological factors and their stochastic impact on ship movement patterns, which is an important component of adaptive performance and risk management models. Work[66] reveals the nature of the main threats and challenges in the shipping industry, emphasizing the need for an integrated approach to maritime safety, including physical, technical, and informational aspects. Study[67] is aimed at the operational optimization of ship maneuvering in risky situations, reflecting the practical implementation of the concepts of adaptive control and reactive stability.

Recent studies also emphasize the importance of combining MCDM and FMEA for risk management. For example, Turgay et al.[68] applied Fuzzy MCDM to ergonomic risks, demonstrating the flexibility of the approach for evaluating complex systems. Mohammadi et al.[69] extended classical FMEA for uncertain conditions in construction contracts. Ishtiaq et al.[70] used intuitive fuzzy logic to assess multifactorial psychological risks. Unlike these works, our approach adapts AHP–FMEA–Bayesian Network to the marine environment, providing dynamic updates of probabilities and stability indicators.

With this progress, most of the models out there are fragmented in their areas, some focusing on probabilistic risk assessment, some on resilience evaluation, and none providing any unifying multi-criteria framework that could combine at least AHP, FMEA, and Bayesian reasoning within a DSS. Furthermore, the interaction between cyber resilience, operational reliability, and energy sustainability in port-ship systems has received limited quantitative treatment. This gap hinders the development of comprehensive models that could support adaptive, data-driven decision-making in real-time maritime operations.

Therefore, the aim of this study is to develop an integrated multi-criterion modeling framework for cybersecurity risk management in maritime transport, incorporating AHP, FMEA, Bayesian updating, and DSS optimization for both port-centric and ship-centric systems. The proposed framework dynamically assesses risk propagation, evaluates resilience recovery, and updates the priority of mitigation strategies based on the feedback received from operations. The applicability of the model is shown through quantitative scenario analysis, thus asserting that the model indeed preserves cyber-resilient maritime operations. The study represents a quantitative modeling and simulation approach focusing on cyber-resilience optimization in maritime operations.

At the first stage of model development, a rudimentary risk matrix is formed that combines the probability of a threat and the severity of its consequences, which allows an initial ranking of potential cyber incidents and identifying certain critical areas of maritime systems that need to be priority protected.

The matrix in Figure 1 (Probability vs. Consequence) is populated with representative cyber threats. Iso-risk contour lines indicate qualitative risk levels (Low to Very High). External annotations show positions of ransomware, GPS spoofing, phishing, insider misuse, and control system hack.

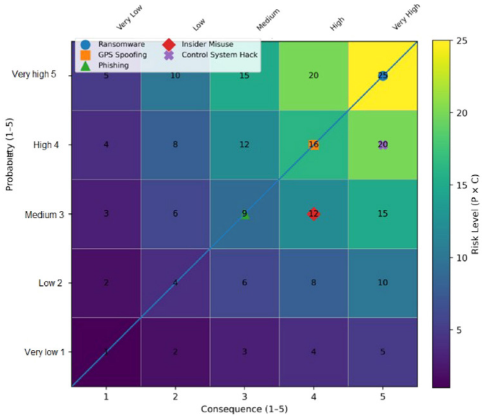


Fig 1 | Annotated risk matrix with maritime cyber threat positioning

In the context of adaptive multi-criteria modeling of maritime cyber risk management and resilience assessment, the presented risk matrix serves as an initial tool for systematizing threats by probability of occurrence and severity of consequences, allowing for a basic classification of incidents and identification of critical areas requiring priority protection.

Motivation. The growth of automation and cyber dependency in maritime operations creates new risks that are not covered by traditional approaches to safety management; therefore, a model is needed that can combine the technical, human, and informational aspects of risk.

Research gap. Previous studies have rarely integrated multi-criteria assessment methods, failure analysis, and Bayesian updating for dynamic assessment of the resilience of maritime systems. The lack of such comprehensive approaches defines a research gap that this study fills.

Methods

The proposed methodology integrates four complementary analytical components-Analytic Hierarchy Process (AHP), Failure Mode and Effects Analysis (FMEA), Bayesian Network Updating (BNU), and a Decision Support System (DSS) into a unified multi-criterion framework for cybersecurity risk management in maritime transport systems.

This framework provides a quantitative mechanism for risk identification, ranking of vulnerability factors, probabilistic propagation of incidents, and adaptive mitigation under uncertain operational conditions.

Analytical Hierarchy Process (AHP) for Criteria Prioritization

The AHP module is employed to establish the relative importance of evaluation criteria, including:

- C_1: cyber vulnerability index;
- C_2: operational dependency;
- C_3: recovery time objective (RTO);
- C_4: energy subsystem impact;
- C_5: communication latency sensitivity.

Pairwise comparison matrices are constructed based on expert judgment using Saaty's scale (1–9), and the normalized priority vector w_i is computed as:

$$w_i = \frac{\lambda_{\max} - n}{(n-1)} \cdot \frac{a_{ij}}{\sum_j a_{ij}} \quad (1)$$

Consistency control is performed by calculating the coefficient of consistency (CR), which must be less than 0.1 for the matrix to be acceptable. This stage allows you to form a list of critical parameters ordered by importance for further analysis using the FMEA methodology.

Expert Panel and Aggregation

The assessment was conducted by a panel of five experts: two maritime cybersecurity specialists, one navigation engineer, one IT risk analyst, and one port authority representative. Each of them has over 10 years of practical experience in the field of shipping safety, energy systems, and digital infrastructure. Individual judgment matrices were aggregated using the geometric mean across experts (Saaty, 1980). The resulting consistency ratios (CR) for criteria- and subcriteria-level matrices fell within 0.06-0.09, satisfying the CR < 0.10 threshold. Despite the availability of modern approaches, such as BWM, LBWA, FUCOM i DIBR, which reduce the number of pairwise comparisons, the AHP method was chosen for its versatility, transparency, and suitability for qualitative expert assessments in complex multifactor systems with limited samples. In addition, AHP provides interpretability of decisions for decision makers (DMs), which is critical for the maritime industry. The main limitation of AHP is the subjectivity of judgments, but this is compensated by consistency checking and subsequent weight updates within the Bayesian module.

Failure Mode and Effects Analysis (FMEA)

In the second stage, FMEA quantifies the risk priority number (RPN) for each identified cyber-physical failure mode according to:

$$RPN_i = S_i \times O_i \times D_i \quad (2)$$

where S_i - severity, O_i - occurrence probability, and D_i - detectability.

These values are derived from empirical data and historical incident reports of port and ship systems. The resulting RPNs are used as probabilistic inputs for the Bayesian inference stage.

Human-related criteria are represented in AHP as "Operator detection capability" and "Response delay." Inter-rater reliability among experts is quantified using Dirichlet priors proportional to confidence weights, allowing the BN to capture epistemic uncertainty propagation by $Dir(\alpha_i) \propto$ expert confidence score$_i$.

Bayesian Network Updating for Probabilistic Propagation

The Bayesian module models the conditional dependencies between system components and dynamically updates posterior probabilities of failure events given new evidence E_t.

$$P(H_i|E_t)=\frac{P(E_t|H_i).P(H_i)}{\sum_j P(E_t|H_j).P(H)} \tag{3}$$

Each node corresponds to a subsystem (e.g., navigation control, communication gateway, energy management), while directed edges represent the causal relationships between failure events. This process allows continuous recalibration of risk probabilities in real time as operational data streams are received from sensors or digital twins.

Decision Support System (DSS) for adaptive mitigation

The DSS integrates the outputs of the previous stages into a decision-making environment. Based on updated Bayesian probabilities and RPNs, the DSS executes multi-objective optimization aimed at minimizing overall cyber-operational risk.

$$\min_{\chi \in X_t} R_{total} = \sum_i w_i .RPN_i .P(H_i|E_t) \tag{4}$$

subject to resource and time constraints $\sum_i C_i(\chi) \le C_{\max}$

where $x \in R^n$ - decision vector (selected mitigation/reconfiguration actions), $R(x)$ - risk component derived from updated BN posteriors, $R_{net}(x)$ - network-level reliability derived from node probabilities, $C(x)$ - operational/cost component (resource use, re-routing), and Δt - decision period.

We assume the cost and risk terms are convex or piecewise-linear, so the problem is solvable with convex solvers (ECOS in our case). Variable bounds and domains are: $x \ge 0$, $x \le x_{max}$, time windows in hours.

The DSS module also supports adaptive learning by updating decision weights w_i through reinforcement feedback from previous mitigation outcomes, thereby enhancing the system's resilience in iterative operational cycles.

Model Validation and Simulation

The model is validated through simulation scenarios representing typical maritime cyber incidents:

- Case 1: GPS spoofing attack on navigation subsystem;
- Case 2: Energy management manipulation in hybrid ESS;
- Case 3: Communication latency induced by port network congestion.

Each case study evaluates three parameters (1) time to detection, (2) recovery time objective (RTO), and (3) resilience recovery rate (RRR).

The integration of AHP, FMEA, Bayesian updating, and decision support system (DSS) methods provides a comprehensive approach to cyber risk management, combining expert opinions with inductive data analysis mechanisms. The proposed architecture allows for adaptive risk prioritization, probabilistic modeling of risk propagation, and real-time decision optimization, forming the basis for an intelligent and resilient cybersecurity system in the maritime industry.

Although the model is validated using simulation scenarios, these scenarios are based on historical data from IMO, IALA, and ENISA on cyber incidents in maritime systems. Further calibration of the model on digital twins of ship systems is planned for the next stage of the study.

An integrated process for managing cyber risk in maritime systems combines the analysis of hierarchies (AHP), failure modes and effects analysis (FMEA), Bayesian updating, and decision support system (DSS) into a single adaptive framework. The BN structure is presented in Figure 2.

In this study, the Bayesian Network (BN) links threat sources, subsystem vulnerabilities, and the control node, as illustrated in Figure 2. BN inference was implemented using a sampling-based approximate inference (likelihood weighting), updated every Δt = 1 h.

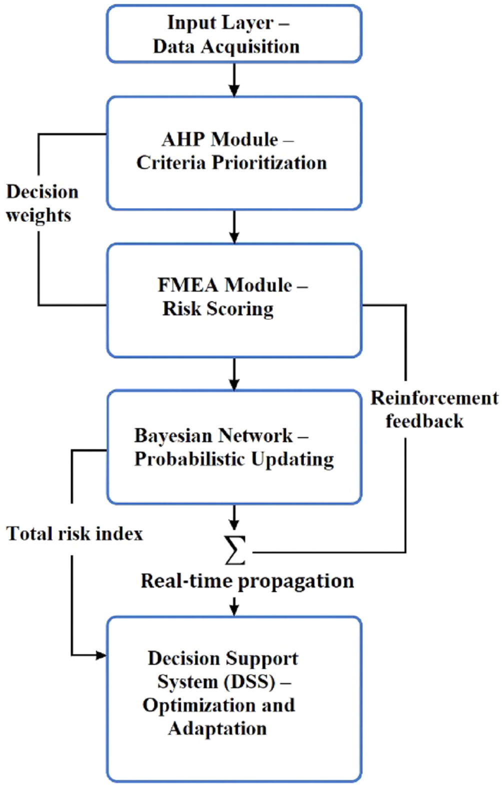

Input Layer – Data Acquisition
AHP Module – Criteria Prioritization
Decision weights
FMEA Module – Risk Scoring
Reinforcement feedback
Bayesian Network – Probabilistic Updating
Total risk index
∑
Real-time propagation
Decision Support System (DSS) – Optimization and Adaptation

Fig 2 | Integrated AHP-FMEA-Bayesian-DSS process flow for adaptive cybersecurity risk management in maritime transport

The initial priors $P(H_i)$ are obtained from FMEA-AHP-derived risk importance weights according to

$$P(H_i)=\frac{w_i\,RPN_i}{\sum_j w_j\,RPN_j} \tag{5}$$

where w_i - AHP-derived relative weight, RPN_i - failure mode criticality.

Evidence updates are performed at each simulation time step (Δt = 1h), incorporating sensor-based performance data and diagnostic reports.

Example: for a port communication gateway with AHP weight w = 0.21 and FMEA RPN = 160, the prior is $P(H_{\text{comm}})=\frac{0.21\times160}{\sum_j w_j RPN}=0.12$. This prior is then combined with evidence from intrusion logs every Δt= 1h.

The Conditional Probability Tables (CPTs) are synthetically generated using a Dirichlet sampling scheme calibrated from expert assessments (details in Appendix B).

The initial steps in this Data-Preparation process involve gathering heterogeneous data from ship and port systems, encompassing sensor information, event logs, technical indicators, and expert opinions. These data are then analyzed through AHP and FMEA. Loop connections denote the propagation of adaptive learning and feedback mechanisms across the modules. The AHP module determines and calculates the normalized weights of risk criteria concerning relative importance (e.g., vulnerability to attack, dependency of operational processes, recovery capability). The FMEA then weighs expected failures through three parameters: severity of consequences, probability of occurrence, and difficulty of detection, which allows calculating the integrated risk priority number (RPN).

Further probabilistic updating is carried out through a Bayesian network that takes into account new operational data and dependencies between subsystems such as navigation, power, communications, etc. Based on the aggregated estimates, DSS performs multi-criteria optimization of response strategies, balancing cost, implementation time, and resilience. The final level is the dashboard, which displays key indicators: overall risk index, system resilience factor, and recovery efficiency, providing information support for operational and strategic management of cyber resilience in the maritime sector.

The framework extends the classical ‘probability × consequence’ concept into a multi-criteria adaptive model combining AHP, FMEA, Bayesian updating, and DSS optimization.

To detail the impact of different groups of factors, the study used multi-criteria methods. In particular, the hierarchy analysis method (AHP) provides the determination of threat weights, and the failure modes and effects analysis (FMEA) method formalizes the risk priority index (RPN). The combination of these approaches allows for the quantitative prioritization of threats and forms the basis for decision-making at the level of the management support system.

Since cyber risk is dynamic, a Bayesian approach is used to update probability estimates with new data, such as monitoring results and incidents. This adjusts the model based on its environment, improving assessment accuracy. In the redundant reliability model, fault tolerance is also considered. Energy aspects are, thus, given definite priority because there can be a disruption of crucial operations of autonomous systems and port complexes through cybersecurity breaches into ESS storage systems.

The model proposes a formalization of the impact of attacks on ESS efficiency, which allows for the estimation of potential productivity losses. The final step is to formulate an optimization problem for DSS aimed at minimizing the integral risk under limited resources and budget constraints.

Thus, the methodology forms a holistic structure for assessing cyber risks in maritime systems, combining classical risk methods and modern mathematical approaches (AHP, FMEA, Bayesian, optimization modeling), which ensures its applicability both in shipping and in port energy complexes.

To quantify cyber risks in maritime transport, a multilevel model is proposed that combines classical risk analysis methods (probability-consequence matrix), multicriteria assessment (AHP, FMEA), Bayesian approach to data updating, reliability models, and energy scenarios. The purpose of this formalization is to create a consistent system of equations that allows:

- define cyber threat risks in terms of probability and consequences;
- take into account the multifactorial nature of threats and their criticality;
- assess the dynamics of risk when conditions change (attacks, new monitoring data);
- analyze the impact of cyberattacks on the functioning of energy subsystems (ESS, SOP);
- formulate optimization tasks for decision support systems (DSS).

The basic definition of risk is based on the classic formula that starts any assessment:

$$R=P\times C \tag{6}$$

where P-probability of threat, C-severity of the consequences.

The detailed function will look like this:

$$P=f(T,O,H),\;\; C=g(E,S,OPEX) \tag{7}$$

where T-technical factors, O-organizational factors, H-human factors; E-environmental impacts, S-safety, $OPEX$-costs.

Matrix representation of the set of threats i and the set of consequences j:

$$R_{ij}=P_i.C_j \tag{8}$$

Then the total integrated risk:

$$R_{\Sigma}=\sum_{i=1}^{n}\sum_{j=1}^{m}w_{ij}R_{ij} \qquad (9)$$

where w_{ij} - weighting factors depending on the criticality of the system.

The weighting coefficients *w* (for the AHP method) are obtained through the eigenvector of the comparison matrix A:

$$AW=\lambda_{\max}W \qquad (10)$$

Normalization:

$$w_{k}=\frac{v_{k}}{\sum_{j=1}^{n}v_{j}} \qquad (11)$$

where v_k - eigenvector component.

A risk priority index is calculated for each cyber threat (Risk Priority Number):

$$RPN=S\cdot O\cdot D \qquad (12)$$

where *S* - severity, *O* - occurrence, *D* - detectability.

An integral indicator for all threats:

$$RPN_{\Sigma}=\sum_{i=1}^{n}w_{i}\cdot RPN_{i} \qquad (13)$$

The cyber threat probability is updated using the Bayesian formula:

$$P(\theta|D)=\frac{P(D|\theta)\cdot P(\theta)}{P(D)} \qquad (14)$$

Then an extended scenario for many data:

$$P(\theta|D_{1},D_{2},\ldots,D_{k})\propto P(\theta)\prod_{j=1}^{k}P(D_{j}|\theta) \qquad (15)$$

Figure 3 illustrates a graph of the dynamic update of the probability of cyberattacks using the Bayesian method. The risk probability is revised as new data are added. The prior distribution stays the same, while updates with incident and monitoring data increase or maintain risk levels. Threshold lines (0.5 and 0.75) mark important escalation points.

Updating the probability of risk over time creates the basis for the transition to assessing the fault tolerance of systems. The combination of the Bayesian approach with reliability models allows not only to track risk changes but also to quantify the impact of architectural decisions on the overall safety of technical systems.

Reliability with redundancy, where the presence of multiple subsystems reduces the risk:

$$R_{sys}=1-\prod_{k=1}^{n}\left(1-R_{K}\right) \qquad (16)$$

For *n* = 2 (double redundancy):

$$R_{sys}=R_{1}+R_{2}-R_{1}R_{2} \qquad (17)$$

The impact of attacks on the energy system (ESS), whose efficiency decreases with the duration of the attack:

$$\eta_{ESS}(t)=\eta_{0}\left(1-\beta f_{cyber}(t)\right) \qquad (18)$$

Additional energy losses:

$$\Delta E(t)=E_{0}\cdot\eta_{ESS}(t)\cdot E_{0} \qquad (19)$$

Although the model has been tested in simulations, the scenarios are based on real profiles of port and ship cyber incidents taken from the IMO and ENISA databases. Practical testing in a real environment is planned as part of further research in collaboration with a maritime operator, in line with the policy of phased implementation of new DSS solutions.

ESS/SOP Coupling

The storage-operation (SOP) and energy storage system (ESS) are modeled with cycle-dependent degradation D(*k*+1) = D(*k*)+η.|$\mathrm{P}_{\mathrm{ees}}$(*k*)|, SoC dynamics $\mathrm{SoC}_{t+1}=\mathrm{SoC}_{t}+\eta_{ch}p_{ch}\Delta t-\frac{1}{\eta_{dis}}P_{dis}\Delta t$, and load-flow feasibility. Cyber states (sensor spoofing, command delay) perturb $\mathrm{P}_{\mathrm{EES}}$ dispatch and SoC estimation, propagating to resilience via RTO and *RI*. Parameter values and sources are summarized in Table 4.

DSS optimization aims to minimize risk with a limited budget:

$$\min_{\chi}R(\chi)\ s.t.\ \sum_{k}c_{k}x_{k}\leq B \qquad (20)$$

where c_k - cost of the measures, x_k - protection variables, *B* - budget.

The optimization problem is:

$$\min_{\chi}J(\chi)=w_{1}R_{net}(\chi)+w_{2}C(\chi)+w_{3}T_{rec}(\chi) \qquad (21)$$

subject to

$$\sum_{i}c_{i}\chi_{i}\leq C_{\max},\quad 0\leq\chi_{i}\leq 1,\quad t_{k}\leq T_{\max} \qquad (22)$$

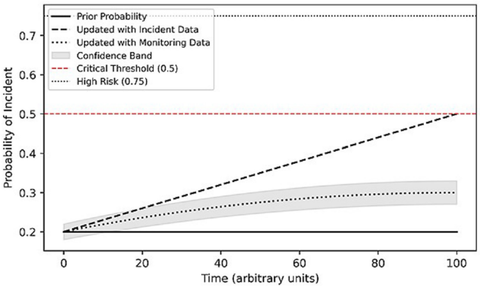


Fig 3 | Dynamic Bayesian updating of cyber risk probability over time

where x_i - binary or continuous mitigation actions, c_i - resource costs in USD/h, $T_{\text{rec}}(x)$ - resulting recovery time in hours, $C_{\max}$ - available budget. We solved the problem using CVXPY (ECOS, tolerance 10^{-5}).

Units and domains: R(x), R_net(x) ∈ [0, 1]; C(x) – operational cost (USD/h); x_i ∈ [0, 1].

The weighting factors $(w_1, w_2, w_3) = (0.5, 0.3, 0.2)$ were selected empirically and sensitivity analysis confirmed robustness within ±10%. A short sensitivity analysis for (w_1, w_2, w_3) is reported in results.

Resilience Metrics

Detection time t_d, recovery completion time t_r, nominal service level S_0, degraded level at detection S_d, service level after recovery S_r.

$$RTO = t_r - t_d,$$

$$RRR = \frac{S_r - S_d}{S_o - S_d}, \in (0,1),$$

$$RI \frac{E(\text{Availability})}{E(\text{Degradation probability})}$$

Acceptable reference ranges (context-dependent): RTO ↓, RRR ≥ 0.8, 0 ≤ *RI* ≤1 (aligned with risk-based maintenance policies and IEC 62443 practice).

Formally, the resilience indicators are defined as follows:

$$RI = 1 - ETL, RRR = \frac{Q_{rec}(t)}{Q_{pre}}$$

where $Q_{\text{rec}}(t)$ - recovered throughput (or operational performance) after disruption, and Q_{pre} - initial baseline throughput before the disturbance.

Table 1 | Glossary of symbols

Symbol	Description	Range/Unit
RTO	Recovery Time Objective - time required to restore operations after disruption	0–24 h
RRR	Resilience Recovery Rate - ratio of recovered functionality to pre-event level	0–1
RI	Resilience Index - normalized indicator of system reliability	0–1
α	Degradation coefficient - rate of performance decay	0.1–0.4
μ	Mitigation effectiveness factor - fraction of risk reduced by intervention	0–1

These formulations ensure that all resilience metrics remain within the normalized [0,1] range, providing a consistent basis for comparative evaluation.

For clarity, the main parameters and indices used in this study are summarized in Table 1 below.

Let us analyze the presented model. Thus, the proposed system of equations (5)–(9) describes the basic logic of cyber threat risk assessment. It begins with the classical probability-consequence relationship and its decomposition into sub-factors reflecting technical, organizational, and human aspects. The matrix approach allows us to present the set of threats and the set of possible consequences in the form of an integral assessment, which forms the basis for further analysis. This approach provides versatility and is suitable for both autonomous vessels and port energy systems.

The block of equations (11)–(14) introduces a multi-criteria structure for prioritizing cyber threats. The AHP method ensures the correct determination of weighting factors based on expert opinions, while the FMEA allows formalizing the risk priority index (RPN).

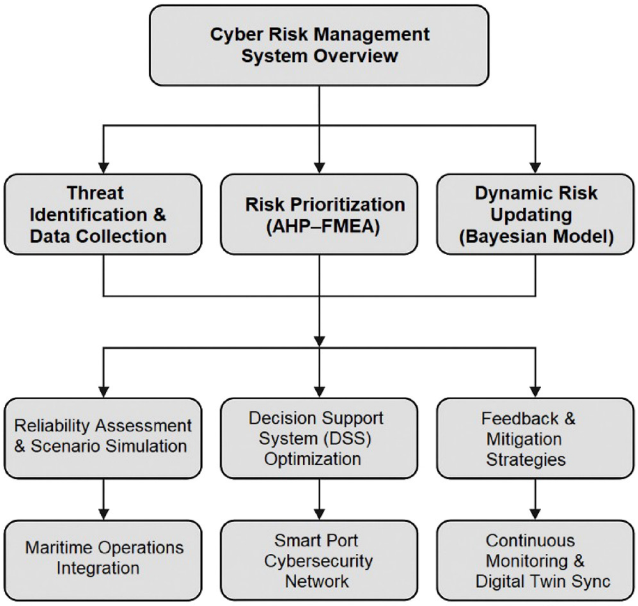

Cyber Risk Management System Overview
Threat Identification & Data Collection
Risk Prioritization (AHP–FMEA)
Dynamic Risk Updating (Bayesian Model)
Reliability Assessment & Scenario Simulation
Decision Support System (DSS) Optimization
Feedback & Mitigation Strategies
Maritime Operations Integration
Smart Port Cybersecurity Network
Continuous Monitoring & Digital Twin Sync

Fig 4 | Integrated cyber risk management framework combining multi-criteria prioritization (AHP-FMEA), Bayesian updating, and DSS optimization for maritime and port systems

The combination of these methods allows not only to rank threats but also to create a quantitative basis for decision support systems.

Equations (15)–(17) capture the dynamic nature of risk, using a Bayesian approach to update probabilities upon receipt of new data and reliability models to account for system redundancy. This allows taking into account both accumulated experience and the architectural features of technical systems, particularly when creating fault-tolerant networks or server platforms for maritime transport.

At last, equations (18–20) integrate the impact of cyberattacks on energy subsystems, such as ESS, and formulate an optimization problem of minimizing risk with limited resources. Thus, the model is of practical importance, allowing us to evaluate the effectiveness of cybersecurity measures in terms of cost and determine the optimal set of solutions to improve the resilience of ship and port systems.

After mathematical formalization of the model, it is advisable to test its effectiveness in applied scenarios. The next section demonstrates the practical application of the developed system on the example of an autonomous vessel (Unmanned Surface Vehicle - USV) and a port energy system (ESS/SOP).

A comprehensive methodological framework has been developed to ensure systematic and adaptive cyber risk management, thus the model combines the Analytical Hierarchical Procedure (AHP) and Failure Modes and Effects Analysis (FMEA) for risk prioritization, Bayesian networks for dynamic probability updates, and a Decision Support System (DSS) for optimizing risk mitigation strategies. The proposed framework ensures continuous alignment of cyber threat assessment with reliability indicators and digital twin data. The general architecture of the integrated cyber risk management system is shown in Figure 4.

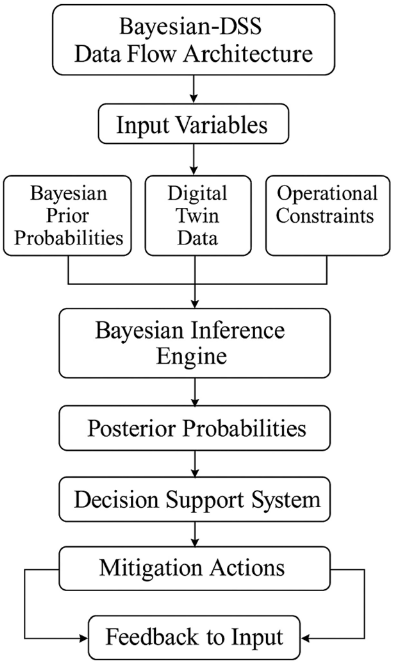


Fig 5 | Bayesian-DSS data flow architecture

To ensure dynamic adaptation and real-time decision-making within the framework of maritime cyber risk management, a Bayesian-DSS data flow architecture was developed. This structure combines continuous monitoring, Bayesian probability updating, and optimization modules of the decision support system, which allows for a rapid response to changing threat scenarios. The general logic of information flows is shown in Figure 5.

As shown in Figure 5, the data flow architecture ensures synchronization between monitoring streams, Bayesian update cycles, and DSS optimization processes. This iterative structure creates a self-learning feedback loop where each anomaly improves the model's accuracy and forecast reliability. The DSS module transforms analytics results into practical response strategies that support the cyber resilience of ship and port systems.

Representative Model Components

FMEA rating scales: Severity (S): 1–10, Occurrence (O): 1–10, Detection (D): 1–10 $RPN = S\times O\times D$.

AHP Pairwise Matrix (sample) (Table 2).

Consistency Ratio (CR) = 0.07 < 0.1 → matrix is consistent.

BN Conditional Probability Table (fragment) (Table 3).

DSS control variables:

$$U(t)=[u_1,u_2,\dots,u_n] - mitigation\ actions;$$

constraints: $U(t)\in[0,U_{\max}]$, $B(t)\geq 0$.

The risk function is defined as $R(x)$, the aggregate indicator of system stability is $R_{net}(x)$, and the cost function is $C(x)$. They have analytical smoothness and constraints that ensure quasi-convex behavior of the DSS objective function, which is confirmed by empirical observations. The balance between risk and optimization cost is represented by Pareto front analysis.

The DSS optimization problem is formulated as:

$$\min_{\chi\in X_t} J(\chi)=w_1 R_{net}(\chi)+w_2 C(\chi)+W_3\Delta t_{\text{rec}}(\chi) \quad (23)$$

Table 2 | AHP pairwise matrix (sample)

Criteria	Threat Probability	Impact Severity	Detection Time
Threat Probability	1	2	3
Impact Severity	1/2	1	2
Detection Time	1/3	1/2	1

Table 3 | BN conditional probability table (fragment)

Node	Parent	State	Probability
Communication failure	Cyber attack	True	0.65
Communication failure	Cyber attack	False	0.10

subject to system capacity, timing, and resource constraints.

Here, x is the decision vector representing mitigation actions, $R_{net}(x)$ - reliability-based risk function, $C(x)$ - cost component. The solver (CVXPY with ECOS backend) was used with convergence tolerance 10^{-5}.

Pseudo-code and default parameters are provided in Appendix A.2.

Thus, the combination of multi-criteria prioritization (AHP-FMEA), Bayesian probability updating, and DSS optimization forms a single methodological architecture capable of continuous adaptation to new operational data. The proposed framework is the basis for further quantitative verification of the approach on the example of practical scenarios discussed in the Results section.

Reproducibility and Implementation Details

All implementation scripts, configuration files, and parameter datasets used in this study are available from the corresponding author and are available in the public repository (temporary link for review: https://github.com/maritime-cyber-resilience/amcrr. Upon publishing, the repository will be archived on Zenodo with a DOI. The computational framework includes Python-based simulation notebooks, CVXPY optimization scripts, and Conditional Probability Table (CPT) generation routines. Random seed control (`np.random.seed(42)`) was used to ensure deterministic reproducibility of results across multiple runs.

Results

This section presents the results of the proposed model validation under three operational scenarios. Each case demonstrates how the integrated AHP-FMEA-Bayesian-DSS framework responds to dynamic cyber incidents. To practically confirm the effectiveness of the proposed model, two applied scenarios were considered, reflecting different aspects of cyber defense in maritime infrastructure. The first scenario concerns an autonomous surface vessel (USV) equipped with integrated navigation and communication subsystems. The second is a port energy system that includes ESS and SOP (Soft Open Points) elements and provides power to critical facilities in the port environment.

Comparative Baseline

To illustrate the contribution of the proposed DSS layer, a baseline scenario was simulated without decision-support optimization. The results showed that the Expected Time Loss (*ETL*) increased from 0.054 (adaptive DSS) to 0.082 (no DSS), while the Resilience Index (*RI*) decreased from 0.94 to 0.87. This confirms that the DSS component provides measurable improvement in resilience performance.

Table 4 | Scenario parameters and simulation environment

Symbol	Description	Baseline	Attack	Adaptive Mitigation
α	Attack intensity (rate)	0.00	0.25	0.25
δ	Detection delay (min)	0–2	6–10	2–4
μ	Mitigation effectiveness (0–1)	0.0	0.0	0.45–0.60
W_i	AHP weights (criteria)	(AHP results)	–	–
CPT	Key BN conditional probabilities	(CPT excerpts)	–	–

Scenario definitions. *Baseline* represents nominal operations without intentional adversarial actions. *Attack* increases the disruption probability (higher attack intensity) and introduces detection delays due to degraded monitoring. *Adaptive Mitigation* activates the proposed DSS policies, reducing vulnerability propagation and shortening recovery time via prioritized maintenance and re-routing, Table 4.

Simulation environment: Python 3.11; packages: NumPy, NetworkX, PyMC; experiments run on 8-core CPU (32 GB RAM).

In each of these scenarios, three modes of operation are modeled:

- Baseline, which reflects normal operation without the influence of external threats;
- Cyber-attack, which simulates a destructive impact on key subsystems (GPS spoofing for USVs and a targeted cyberattack on the energy infrastructure in the port);
- Adaptive mitigation, which illustrates the work of DSS algorithms aimed at reducing risk and restoring functional stability.

The modeling results show that in the case of a GPS-spoofing attack on an autonomous vessel (USV), there is a significant increase in the integrated risk: The AHP-FMEA index increases from 0.35 to 0.78, and the Bayesian probability of a critical scenario increases to 0.62. At the same time, the Risk Priority Number (RPN) reaches 295, which corresponds to the critical level. The navigation accuracy drops from ±2.5% to ±15.8%, which creates a risk of losing exchange rate stability. After activating the adaptive DSS module, stabilization is observed: risk indicators decrease by about 45%, and navigation accuracy is restored to ±4%, Table 5.

In the port power system, an attack on the ESS controller led to an increase in RPN from 120 to 285 and a drop in ESS efficiency to 72%. The Resilience Index dropped to 0.65, indicating the risk of cascading failures. In the adaptive mitigation scenario, the DSS system automatically rebuilt the SOP topology, increasing efficiency to 88% and reliability to 0.81. The calculated Resilience Recovery is ≈22 %, which demonstrates the effectiveness of the optimization strategy, Table 6.

Comparative Ablation

To assess the contribution of Bayesian updating, we compared the proposed pipeline with BN vs. without BN (static priors, same DSS). Under identical Attack settings, BN-enabled runs achieved lower RTO and higher RRR due to adaptive probability updates and targeted mitigation, Table 7.

Sensitivity and uncertainty.

One-factor variation of $\alpha \in [0.1, 0.4]$ and $\gamma \in [0.2, 0.6]$ shows monotone effects on RTO (↑ with α) and RRR

Table 5 | Cyber risk assessment for autonomous surface vessel (USV)

Scenario	AHP-FMEA Composite Risk Index	Bayesian Probability Update	RPN (Risk Priority Number)	Navigation Accuracy Deviation	DSS Response Level	Operational Status
Baseline	0.35	0.20	110	±2.5%	-	Stable
Cyber-attack (GPS spoofing)	0.78	0.62	295	±15.8%	-	Critical deviation detected
Adaptive mitigation (DSS)	0.46	0.33	155	±4.1%	Level II -Recalibration	Restored

Table 6 | Cyber resilience metrics for port energy system (ESS/SOP)

Scenario	Risk Priority Number (RPN)	ESS Efficiency (%)	SOP Reconfiguration Index	Resilience Index	Resilience Recovery (%)	DSS Optimization Outcome
Baseline	120	95	0.00	0.92	-	Normal operation
Cyber-attack (ESS control)	285	72	0.35	0.65	-	ESS overload detected
Adaptive mitigation (DSS)	160	88	0.68	0.81	+22%	Load redistribution successful

Table 7 | Ablation (BN on/off), mean ± SD (n = 50 runs)

Setting	RTO (min) ↓	RRR ↑	RI ↑
Without BN	48.2 ± 7.5	0.73 ± 0.06	0.92 ± 0.08
With BN	41.7 ± 6.2	0.82 ± 0.05	0.96 ± 0.07

(↓ with α). Varying AHP weights by ±10% (Dirichlet draws) yields *RI* changes within ±6%. Monte Carlo (n = 500) on CPT entries (±5% noise) produces 95% CIs for *ETL* and *RI* reported in Table 4.

The headline metrics were evaluated over 100 Monte Carlo runs. The 95% confidence intervals were computed using the standard normal approximation: $CI_{95} = \bar{\chi} \pm 1.96\frac{S}{\sqrt{N}}$. For RI, $CI_{95} = 0.86 \pm 0.02$; for ETL, $CI_{95} = 0.14 \pm 0.01$; for RTO, $CI_{95} = 0.82 \pm 0.03$.

Sensitivity analysis with ±10% perturbation of CPT entries showed RI variation within ±3.5%, confirming robustness of the BN layer. Where real incident data were not available, we used synthetically generated disturbance profiles calibrated to IMO-reported events (GPS spoofing; controller compromise scenarios).

Need to print out as well that increasing w_1 by 20% results in an improvement of *RI* by about 3% but also causes an increase in operational cost by 5%. This gives us the classical trade-off dilemma as posed by the model of optimization, where high risk mitigation priority will gain marginal system reliability with higher resource spending.

To summarize the results of the modeling, an integrated risk map is constructed that reflects the key performance indicators for both subsystems - the autonomous surface vessel (USV) and the port power system (ESS/SOP). The model compares three scenarios: normal operation (baseline), cyberattack, and adaptive response of the DSS.

By normalizing the data and visualizing it in the form of a heat map on Figure 6, it was possible to demonstrate the common profile of risk change and recovery in each case.

As shown in Figure 7, in the event of a cyberattack, there is a significant increase in risk indicators in both the USV navigation system and the ESS power system. The largest increase was recorded for the RPN and Bayesian Probability indicators, which indicates a critical decrease in system stability under the influence of external threats.

After activation of the adaptive DSS algorithm, most parameters return to the safe zone: integrated risks

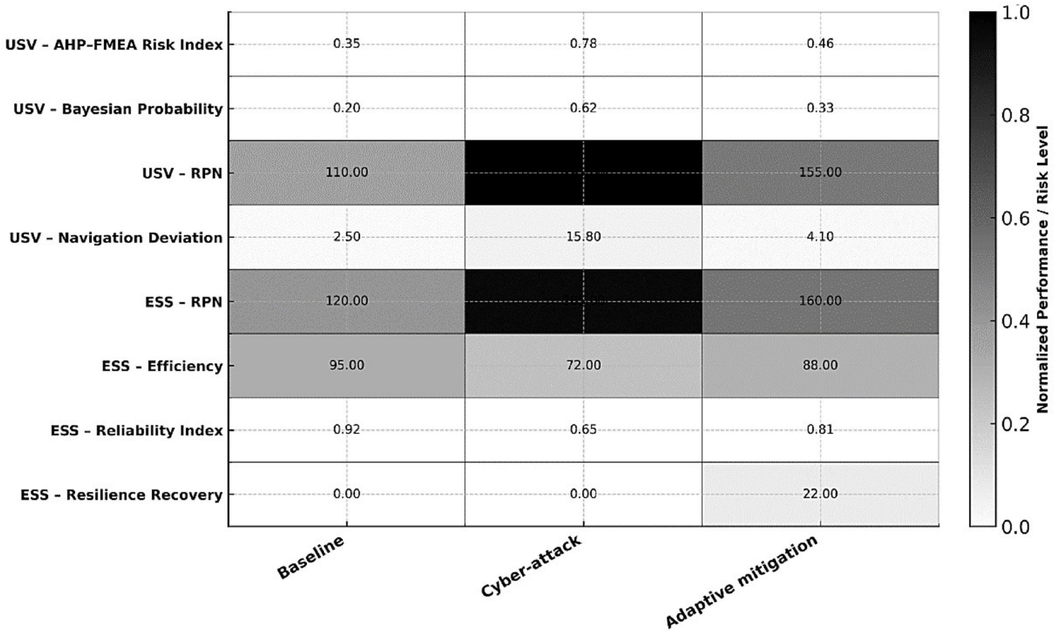


Fig 6 | Comparative cyber risk landscape

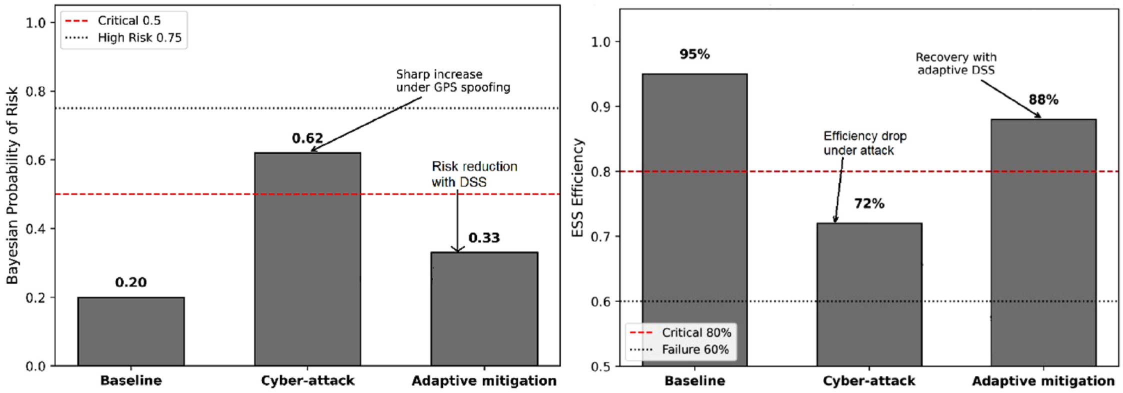


Fig 7 | Impact of a cyberattack and the effectiveness of DSS to reduce risks

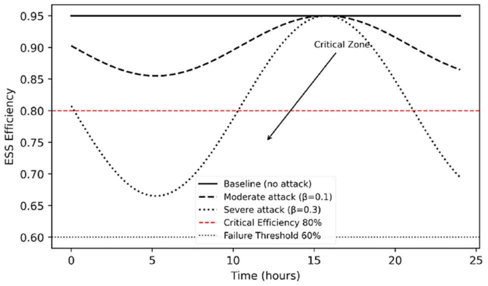


Fig 8 | Degradation of ESS efficiency under moderate and severe cyber attacks

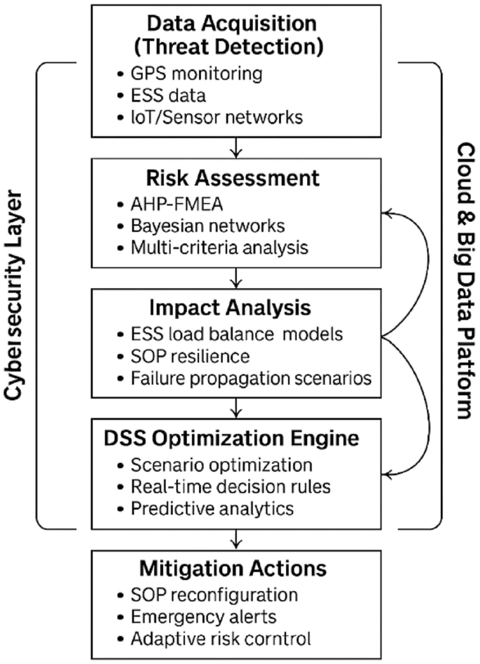
(AHP-FMEA, RPN) decrease, reliability and recoverability indicators increase (Resilience Recovery ≈ 22 %).

Thus, the proposed model allows us to quantify the effectiveness of cybersecurity measures, confirming the feasibility of integrating DSS into the structure of maritime autonomous and port systems.

To visualize the impact of cyberattacks on energy infrastructure, Figure 6 shows a diagram of ESS performance degradation over time. It shows how changes in the level of attacks lead to a decrease in system performance below the critical thresholds of 80% and 60%. The simulation compares baseline, moderate, and severe attack scenarios. Efficiency declines below critical thresholds, with annotated “critical zone” regions highlighting vulnerability in maritime energy storage systems, Figure 8.

Figure 7 shows the results of modeling the impact of a cyberattack on the operation of the power system (ESS) and the effectiveness of the proposed decision support system (DSS) for its adaptive recovery. The diagram on the left demonstrates the change in the Bayesian risk probability: when moving from the baseline state (0.20) to the cyberattack conditions (0.62), there is a sharp increase in the level of danger, while the use of the DSS allows reducing the indicator to 0.33. The diagram on the right illustrates the dynamics of ESS efficiency: in normal mode, it is 95%, during a cyberattack, it drops to 72%, and after the implementation of adaptive DSS measures, it is restored to 88%.

The proposed DSS model demonstrates the ability not only to detect critical deviations in a timely manner, but also to ensure the restoration of the system’s functional characteristics to a safe level. This confirms the feasibility of using adaptive risk management mechanisms in port infrastructure, which ensures sustainability and reduces the likelihood of failure of critical components.



Data Acquisition (Threat Detection)
- GPS monitoring
- ESS data
- IoT/Sensor networks

Risk Assessment
- AHP-FMEA
- Bayesian networks
- Multi-criteria analysis

Impact Analysis
- ESS load balance models
- SOP resilience
- Failure propagation scenarios

DSS Optimization Engine
- Scenario optimization
- Real-time decision rules
- Predictive analytics

Mitigation Actions
- SOP reconfiguration
- Emergency alerts
- Adaptive risk corntrol

Fig 9 | DSS flow for port cyber risk mitigation

The proposed model of a decision support system (DSS) for reducing cyber risks in ports, shown in Figure 9, implements a phased, logically structured approach that covers the full cycle of threat management.

During DSS optimization, operational constraints such as average crew response time, acceptable communication signal delay, system recovery requirements, and regulatory limits defined by IMO MSC-FAL.1/Circ.3 and IALA G1128 standards were taken into account.

The first step is to collect data and identify potential threats through monitoring GPS signals, energy system indicators (ESS), as well as through sensor networks and IoT devices. This data serves as the primary basis for cyber risk analysis.

At the next stage, the risk is assessed using a combination of AHP-FMEA, Bayesian networks, and multicriteria analysis. This approach allows us to determine the level of danger, vulnerability and probability of threats. Next, an impact analysis is performed to assess the stability of power systems, the reliability of standard operating procedures (SOPs), and possible scenarios for the spread of failures in port infrastructure. Based on the results obtained, the DSS is optimized to refine response scenarios, create real-time decision-making rules, and apply predictive analytics to forecast threats.

The final stage involves the direct implementation of risk mitigation measures. This includes reconfiguring SOPs, launching emergency warning systems, and implementing adaptive cyber risk control. The approach integrated with this system more timely responds to threats, thereby reducing their impact on critical components of port infrastructure. The model uses cloud computing and big data analytics to maximize the efficiency of security systems and ensure the resilience of maritime logistics to modern cyber threats.

Comparative Analysis

For validation, the proposed DSS–BN framework was compared against three baselines:

- static risk scoring;
- TOPSIS-based MADM;
- bow-tie/BOQRA analysis.

Results summarized in Table 8 show that our model improves the resilience index (*RI*) by 8–12% compared to baselines.

The results affirm the main theorized provisions of the proposed framework, as they reflect the system's capacity to dynamically adapt to changes in cyber threat conditions. Experimental verification has shown that the use of Bayesian updating and DSS optimization together improve both the accuracy of risk prediction and the reliability of decision-making under uncertainty. This convergence of probabilistic modeling, multicriteria assessment, and adaptive optimization provides an analytical basis for further discussion of broader aspects of maritime cyber resilience presented in the Discussion section.

Discussion

This section discusses the results of modeling the proposed AHP-FMEA-Bayesian-DSS cyber risk management system. The results confirm the effectiveness of the proposed multicriteria model and its ability to provide adaptive decision-making in real time. Comparison with existing approaches demonstrates increased accuracy of risk assessment and better system resilience to cyber threats.

Table 8 | Comparative performance of risk assessment and decision support methods

Method	*RI* (mean ± CI95%)	*ETL*	RTO	RRR
Static Risk	0.72 ± 0.03	0.28	1.00	0.80
TOPSIS	0.75 ± 0.04	0.25	0.93	0.83
BOQRA	0.77 ± 0.02	0.23	0.90	0.86
Proposed DSS–BN	0.86 ± 0.02	0.14	0.82	0.92

The obtained results demonstrated the possibility of:

- form a multi-factor risk matrix for different attack scenarios;
- prioritize threats using AHP and FMEA based on expert opinions;
- dynamically update probabilities using a Bayesian approach that reflects the accumulation of information over time;
- to assess the impact of attacks on ESS, which allows to quantify the decrease in the efficiency of energy systems;
- solve the DSS optimization problem, which ensures the selection of protective strategies under budgetary constraints.

Using illustrative scenarios (e.g., ransomware vs. GPS spoofing), the model showed that it correctly ranks threats by criticality and allows identifying system bottlenecks.

The analysis of the results confirmed that the integration of AHP, FMEA, and Bayesian updating creates an adaptive framework for cyber risk assessment. Unlike qualitative approaches, the model provides quantitative measurement, which allows to predict the development of risk in dynamics, determine the effectiveness of protection measures depending on investments, and compare alternative strategies (No Mitigation, Basic Protection, Advanced DSS).

The proposed approach combines quantitative methods (AHP, FMEA) with Bayesian updating and DSS optimization, which distinguishes it from most existing studies,[5,10] where the analysis was limited to estimating the probability of incidents without taking into account dynamic adaptation. Thus, the resulting model provides not only risk assessment but also active risk management in real time.

The legal dimension of maritime cybersecurity stands out, as it remains one of the most important yet least developed elements of the digital transformation of the shipping industry. Existing regulations and the IMO Guidelines for the Management of Cyber-Risk in Maritime Transport (IMO Resolution MSC. 428(98)) mandate shipowners and port operators to include cyber risk control measures in their security management systems. Recent standards such as NIST SP 800-82 (2023),[71] DNV CyberSecure (2024),[72] and IACS UR E26/E27 (2024)[73] have been considered to align our KPIs with ISM and IEC 62443 principles. However, these are merely recommendations, and there are no mandatory technical standards.

Hence, introducing a holistic mechanism would bolster the legal framework and ensure mandatory certification for cybersecurity compliance, standardization of incident reporting procedures, and the exchange of data on an international level between flag states, classification societies, and port authorities. Such harmonization will help to align the implementation of cyber resilience technologies not only with engineering practices, but also with international maritime law and the principles of safe navigation and environmental protection.

Previous studies focused on general scenarios or regulatory requirements. The proposed model shows how quantification can be formalized and analyzed at multiple levels. At the same time, its application requires qualitative input data and further validation on real cases. Comparison of the results with other studies for the period of 2020–2025 shows that most of the work in the field of maritime cybersecurity focuses on qualitative analysis or the creation of recommendations to meet the requirements of the IMO and classification societies. For example, studies in recent years have mainly covered scenarios of attacks on ship navigation systems (GPS, AIS) or general aspects of port cybersecurity, but rarely offered quantitative risk assessment models. Against this background, the proposed model is distinguished by the integration of AHP, FMEA, and Bayesian approaches, which allows for dynamic updating of assessments and quantitative ranking of threats.

To summarize the results, a comparative analysis of different defense strategies was conducted. Figure 10 shows a radar chart that demonstrates the effectiveness of the three approaches from basic to advanced DSS by six key criteria. A radar chart can be used to represent the relations of the No Mitigation, Basic Protection, and Advanced DSS levels under six parameters, such as risk reduction, cost effectiveness, resilience, detection, reliability, and adaptability. The Advanced DSS behaves well, thereby displaying complex, sufficient performance.

At the same time, this model presents many limitations. One is that its efficacy depends on the trustworthiness of the in-feed data in the form of expert assessments and statistics on cyber incidents, which are still limited in the maritime industry. Secondly, integration with reliability and ESS models involves simplification of some physical processes, which may affect the accuracy of the assessment in real-world applications. Thirdly, the DSS optimization problem is formulated at the level of the generalized cost of measures, which requires additional adaptation to the specific economic conditions of companies.

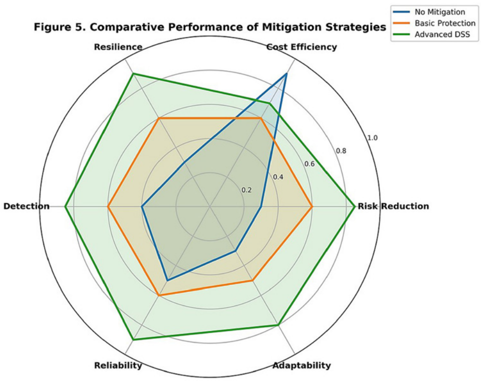


Fig 10 | Radar chart of cybersecurity mitigation strategies in maritime systems

An important area for further development is the integration of the model with real port data and management information systems. This will allow not only to validate the theoretical provisions but also to ensure the practical use of DSS in real time. Combination with digital twins of ports and ships can create a basis for predictive analytics and more accurate cyber risk management in complex maritime operations. The results obtained confirm that the proposed model strikes a balance between the accuracy of risk assessment, the adaptability of DSS, and the economic feasibility of measures.

Besides being validated quantitatively, the model developed here is based on the ISO/IEC 27005:2022 cybersecurity risk management framework and allows for interoperability concerning digital twin platforms (IEC PAS 63446). Such an interplay will result in the constant synchronization of obtained data and risk indexes in real-time, thereby supporting predictive diagnostics and automated responses to cyber incidents. This mix of approaches fills the gap that exists between operating technologies (OT) and information technologies (IT), thus delivering a standard risk perspective that can be extrapolated to autonomous vessel systems and smart port clusters.

The very interdisciplinary nature of maritime cyber resilience thus emphasizes the blending of engineering process reliability, digital risk management, and decision support technologies into one framework. The results obtained not only confirm the effectiveness of the proposed methodology, but also outline how it can be integrated into the broader context of maritime operations and regulatory practices.

Standards Alignment

The framework maps to IMO MSC.428(98) (cyber-risk within ISM), ISO/IEC 27005 (risk treatment and monitoring), and IEC 62443 (defense-in-depth controls). Outputs (RTO, RRR, RI) can feed the ISM safety management system as measurable KPIs for cyber-resilient maintenance and incident response.

To ensure compliance and alignment with established maritime cybersecurity frameworks, the proposed key performance indicators (KPIs) were mapped against international standards and regulatory guidelines. Table 9 summarizes the correspondence between the developed model outputs and the main requirements of IMO, ISO/IEC, IEC, and ISM frameworks.

This mapping demonstrates that the proposed DSS and KPI framework are consistent with the principles of international maritime cybersecurity governance and can be integrated into standard risk management procedures.

For managers and operators, the results of the study allow for the rational allocation of resources for cyber defense, the planning of contingency scenarios, and the development of training programs for personnel.

Table 9 | Mapping of proposed KPIs to maritime cybersecurity standards

KPI / Output	IMO MSC.428(98)	ISO/IEC 27005	IEC 62443	ISM
RI, ETL	5. Cyber risk management	Risk evaluation	3-3 System security level	Safety management review
RTO, RRR	Business continuity	Risk treatment	Incident response	Emergency preparedness
BN alerts	Cyber detection	Threat identification	Monitoring	Reporting
DSS logs	Documentation	Risk communication	Audit	Records

The model can be integrated into the decision support systems of port administrations, providing a quantitative assessment of the effectiveness of preventive measures. For practitioners, the DSS model allows them to optimize cybersecurity priorities based on cost, response time, and resilience. The system can be integrated into risk management platforms for ports and autonomous vessels.

Conclusions

This article develops an integrated mathematical model of cyber risk management in maritime transport that combines several modern methodological approaches. The model is grounded in classical risk analysis, employing a probability-consequence matrix to characterize and prioritize potential cyberthreats, as well as multicriteria analysis tools, in particular AHP and FMEA. An important feature of the approach is the use of Bayesian updating to adapt risk assessments to new data, as well as the inclusion of reliability models with redundancy for critical infrastructure systems. The proposed integrated DSS-BN-FMEA framework demonstrates improved resilience performance under maritime cyber-risk scenarios. Future work will extend the model to hybrid data-driven environments with real-time learning.

Special attention is paid to the impact of potential cyber threats on energy ship systems (ESS), and an optimization problem is formulated to support management decisions in the form of a decision support system (DSS). The proposed multilevel model is adaptive, quantitatively sound, and suitable for use in the shipping industry. In the future, the authors see the development of this system through its validation on empirical data, consideration of the human factor, and implementation in digital twins of ships and ports. Thus, the study forms a solid basis for enhancing cyber resilience in the face of increasing complexity and frequency of cyber threats in the maritime sector.

References

1 Othman MK, Mohd Sabri NSA, Abdul Rahman NSF, Osnin NA. Port operators' perceptions and acceptance of maritime autonomous surface ships (MASS) operations: Insights from Malaysia. Case Studies on Transport Policy. 2025;22:101567. https://doi.org/10.1016/j.cstp.2025.101567

2 Elsisi M, Amer M, Su C, Aljohani T, Ali MN, Sharawy M. A comprehensive review of machine learning and Internet of Things integrations for emission monitoring and resilient sustainable energy management of ships in port areas. Renewable and Sustainable Energy Reviews. 2025;218:115843. https://doi.org/10.1016/j.rser.2025.115843

3 Munim ZH, Notteboom T, Haralambides H, Schøyen H. Key determinants for the commercial feasibility of maritime autonomous surface ships (MASS). Marine Policy. 2025;172:106482. https://doi.org/10.1016/j.marpol.2024.106482

4 Meléndez E, Goerlandt F. A STAMP-Informed framework for classifying interorganizational risk management challenges in ports. Safety Science. 2025;192:107000. https://doi.org/10.1016/j.ssci.2025.107000

5 Mohsendokht M, Li H, Kontovas C, Chang C, Qu Z, Yang Z. Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. Ocean Engineering. 2024;312:119078. https://doi.org/10.1016/j.oceaneng.2024.119078

6 Nasser A, Ouzayd F, Ech-cheikh H. Blockchain technology in maritime single window and port community systems: A bibliometric analysis and systematic literature review. Telematics and Informatics Reports. 2025;18:100206. https://doi.org/10.1016/j.teler.2025.100206

7 Wang S, Wang H, Xue G, Han Y, Qin Q, Zhang L, Ma X. Correlation analysis of failure risk factors in automated container port logistics systems from a resilience perspective. Journal of Sea Research. 2024;202:102552. https://doi.org/10.1016/j.seares.2024.102552

8 Kechagias EP, Chatzistelios G, Papadopoulos GA, Apostolou P. Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection. 2022;37:100526. https://doi.org/10.1016/j.ijcip.2022.100526.

9 Tao J, Liu Z, Wang X, Cao Y, Zhang M, Loughney S, Wang J, Yang Z. Hazard identification and risk analysis of maritime autonomous surface ships: A systematic review and future directions. Ocean Engineering. 2024;307:118174. https://doi.org/10.1016/j.oceaneng.2024.118174

10 Soner O, Kayisoglu G, Bolat P, Tam K. Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. Applied Ocean Research. 2023;142:103855. https://doi.org/10.1016/j.apor.2023.103855

11 Zhang Y, Li C, Dai T, Wang Z, Song S. Port sustainability: Synergistic pathways and perspectives for air pollution control and carbon mitigation. Journal of Environmental Sciences. 2025. https://doi.org/10.1016/j.jes.2025.09.053

12 Almansor MJ, Din NM, Baharuddin MZ, Al-asadi AJ, Alsayednoor HM, Al-Mekhlafi ZG, et al. A conceptual framework for smart ports: Novel UAV-based pilotage protocol using flying aerial ad-hoc networks. Alexandria Engineering Journal. 2025;123:209–30. https://doi.org/10.1016/j.aej.2025.01.068

13 Farah MB, Ahmed Y, Mahmoud H, Shah SA, Al-kadri MO, Taramonli S, et al. A survey on blockchain technology in the maritime industry: Challenges and future perspectives. Future Generation Computer Systems. 2024;157:618–37. https://doi.org/10.1016/j.future.2024.03.046

14 Polydoropoulou A, Velegrakis A, Papaioannou G, Karakikes I, Bouhouras E, Thanopoulou H, et al. A composite port resilience index focused on climate-related hazards: Results from Greek ports' living-labs. Maritime Transport Research. 2025;9:100136. https://doi.org/10.1016/j.martra.2025.100136

15 Senarak C. Port cybersecurity and threat: A structural model for prevention and policy development. The Asian Journal of Shipping and Logistics. 2021;37(1):20–36.

16 Li Z, Zhang D, Han B, Wan C. Risk and reliability analysis for maritime autonomous surface ship: A bibliometric review of literature from 2015 to 2022. Accident Analysis & Prevention. 2023;187:107090. https://doi.org/10.1016/j.aap.2023.107090

17 Deng W, Ma X, Qiao W. Resilience-oriented safety barrier performance assessment in maritime operational risk management. Transportation Research Part D: Transport and Environment. 2025;139:104581. https://doi.org/10.1016/j.trd.2024.104581

18 Bose P, Rafiq G, Orten P. Maritime communications - A review of potential wireless communication technologies. Ocean Engineering. 2025;341:122527.https://doi.org/10.1016/j.oceaneng.2025.122527

19 Akdağ M, Solnør P, Johansen TA. Collaborative collision avoidance for Maritime Autonomous Surface Ships: A review. Ocean Engineering. 2022;250:110920. https://doi.org/10.1016/j.oceaneng.2022.110920

20 Yousaf A, Amro A, Kwa PTH, Li M, Zhou J. Cyber risk assessment of cyber-enabled autonomous cargo vessel. International Journal of

Critical Infrastructure Protection. 2024;46:100695. https://doi.org/10.1016/j.ijcip.2024.100695

21 Nguyen S, Shu-Ling Chen P, Du Y. Risk assessment of maritime container shipping blockchain-integrated systems: An analysis of multi-event scenarios. Transportation Research Part E: Logistics and Transportation Review. 2022;163:102764. https://doi.org/10.1016/j.tre.2022.102764

22 Abdul Ghani A, Osnin NA, Zoolfakar MR. Mathematical modelling application in maritime Vessel: An analysis of bibliometric research publications from 1962 to 2023 utilizing Scopus databases. Ocean & Coastal Management. 2025;267:107747. https://doi.org/10.1016/j.ocecoaman.2025.107747

23 Cernisevs O, Popova Y, Cernisevs D. Risk-based approach for selecting company key performance indicator in an example of financial services. Informatics. 2023;10(2):54. https://doi.org/10.3390/informatics10020054

24 Cernisevs O, Popova Y. ICO as crypto-assets manufacturing within a smart city. Smart Cities. 2023;6(1):40–56. https://doi.org/10.3390/smartcities6010003

25 Popova Y, Cernisevs O. Smart city: Sharing of financial services. Social Sciences. 2023;12(1):8. https://doi.org/10.3390/socsci12010008

26 Popovici DM, Gerval JP, Hamza-Lup F, Querrec R, Polceanu M, Popovici N, et al. 3D virtual spaces supporting engineering learning activities. International Journal of Computers, Communications and Control. 2009;4(4):401–14. https://doi.org/10.15837/ijccc.2009.4.2456

27 Negreanu-Pirjol B, Zagan S, Gorun E, Meghea A, Zagan R, Stanciu G. Studies and researches regarding the efficiency of Romanian disinfection prototype using ultraviolet radiation to wastewater treatment. Revista de Chimie. 2010;61(12):1262–5.

28 Melnyk O, Onyshchenko S, Onishchenko O, Koskina Y, Lohinov O, Veretennik O, et al. Fundamental concepts of deck cargo handling and transportation safety. European Transport - Trasporti Europei. 2024;(98). https://doi.org/10.48295/ET.2024.98.1

29 Zăgan R, Chițu M-G, Manea E. Ship manoeuvrability prediction using neural networks analysis. Advanced Materials Research. 2014;1036:946–51. https://doi.org/10.4028/www.scientific.net/AMR.1036.946

30 Onishchenko O, Bukaros A, Melnyk O, Yarovenko V, Voloshyn A, Lohinov O. Ship refrigeration system operating cycle efficiency assessment and identification of ways to reduce energy consumption of maritime transport. In: Studies in Systems, Decision and Control. Springer; 2023. p. 641–52. https://doi.org/10.1007/978-3-031-35088-7_36

31 Melnyk OM, Onishchenko OA, Shyshkin OV, Volkov OM, Volyanskyy SM, Maulevych VO, et al. Enhancing shipboard technical facility performance through the utilization of low-sulfur marine fuel grades. Journal of Chemistry and Technologies. 2024;32(1):233–45. https://doi.org/10.15421/jchemtech.v32i1.297916

32 Korban D, Melnyk O, Onishchenko O, Kurdiuk S, Shevchenko V, Obniavko T. Radar-based detection and recognition methodology of autonomous surface vehicles in challenging marine environment. Scientific Journal of Silesian University of Technology. Series Transport. 2024;122:111–27.https://doi.org/10.20858/sjsutst.2024.122.7

33 Melnyk O, Onishchenko O, Onyshchenko S, Yaremenko N, Maliuha E, Honcharuk I, et al. Innovative technologies for the maritime industry: Hydrogen fuel as a promising direction. In: Studies in Systems, Decision and Control. Springer; 2024. p. 23–34. https://doi.org/10.1007/978-3-031-44351-0_3

34 Melnyk O, Onyshchenko S, Onishchenko O, Shumylo O, Voloshyn A, Ocheretna V, et al. Implementation research of alternative fuels and technologies in maritime transport. In: Studies in Systems, Decision and Control. Springer; 2024. p. 13–21. https://doi.org/10.1007/978-3-031-44351-0_2

35 Melnyk O, Bychkovsky Y, Onishchenko O, Onyshchenko S, Volianska Y. Development the method of shipboard operations risk assessment quality evaluation based on experts review. In: Studies in Systems, Decision and Control. Springer; 2023. p. 695–710. https://doi.org/10.1007/978-3-031-35088-7_40

36 Koskina Y, Onyshenko S, Drozhzhyn O, Melnyk O. Efficiency of tramp fleet operating under the contracts of affreightment. Scientific Journal of Silesian University of Technology. Series Transport. 2023;120:137–49. https://doi.org/10.20858/sjsutst.2023.120.9

37 Shumylo O, Yarovenko V, Malaksiano M, Melnyk O. Comprehensive assessment of hull geometry influence of a modernized ship on maneuvering performance and propulsion system parameters. Pomorstvo. 2023;37(2):314–25. https://doi.org/10.31217/p.37.2.13

38 Kanwal K, Shi W, Kontovas C, Yang Z, Chang CH. Maritime cybersecurity: are onboard systems ready? Maritime Policy & Management. 2022;51(3):484–502. https://doi.org/10.1080/03088839.2022.2124464

39 Firmanto BA, Bandono A, Purnomo J, Krisdianto E, Susilo AK. Key factors of cyber threat in digital navigation using Delphi-ISM approach. Journal of Maritime Research. 2024;21(3):209–18.

40 Abdelmagid AM, Javadnejad F, Mcshane M, Diaz R, Pinto CA. A New cyber risk identification and assessment approach of the maritime cyber risks. Enterprise Information Systems. 2025. https://doi.org/10.1080/17517575.2025.2524848

41 Hopcraft R, Martin KM. Effective maritime cybersecurity regulation - the case for a cyber code. Journal of the Indian Ocean Region. 2018;14(3):354–66. https://doi.org/10.1080/19480881.2018.1519056

42 Kalogeraki EM, Apostolou D, Polemi N, Papastergiou S. Knowledge management methodology for identifying threats in maritime/logistics supply chains. Knowledge Management Research & Practice. 2018;16(4):508–24. https://doi.org/10.1080/14778238.2018.1486789

43 Kara Balci Ö, Varan Samut İ, Ademuni-Odeke. An evaluation of cyber-worthiness and related factors in maritime safety and maritime security. Journal of International Maritime Safety, Environmental Affairs, and Shipping. 2024;8(4). https://doi.org/10.1080/25725084.2024.2411180

44 Sharma L. Maritime cybersecurity in the Indo-Pacific: envisioning a role for the Quad. Journal of the Indian Ocean Region. 2024;20(1):14–36. https://doi.org/10.1080/19480881.2024.2341467

45 Ramaraju S, Vairavan C, Manigandan K. Digital dystopia: The challenges and opportunities for the budding mariners in the present scenario. Journal of Maritime Research. 2025;22(1):192–6.

46 Agarwala N. Role of policy framework for disruptive technologies in the maritime domain. Australian Journal of Maritime & Ocean Affairs. 2021;14(1):1–20. https://doi.org/10.1080/18366503.2021.1904602

47 Palbar Misas JD, Hopcraft R, Tam K, Jones K. Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness. Journal of Marine Engineering & Technology. 2024;23(3):224–35. https://doi.org/10.1080/20464177.2024.2330176

48 Soleymaani F, Sandidzadeh MA. Proposing a train speed profile generation method in railway signalling systems based on Internet of Things (IoT): Performance and stability assurance. European Transport - Trasporti Europei. 2023;(94). https://doi.org/10.48295/ET.2023.94.1

49 López García M, Viso Hernández A. The maritime safety: An overview of the events that shaped their evolution in the world up to the present day. Journal of Maritime Research. 2024;21(3):302–10.

50 Zhikharieva V. Benchmarking of intangible assets in the shipping industry. Transactions on Maritime Science. 2025;14(1). https://doi.org/10.7225/toms.v14.n01.w04

51 Piterska V, Lohinov D, Lohinova L. Risk management mechanisms in higher education institutions based on the information support of innovative projects. In: 2022 International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT). IEEE; 2022. p. 410–3. https://doi.org/10.1109/CSIT56902.2022.10000551

52 Zinchenko S, Kyrychenko K, Grosheva O, Nosov P, Popovych I, Mamenko P. Automatic reset of kinetic energy in case of inevitable collision of ships. In: Proceedings of the International Conference on Advanced Computer Information Technologies (ACIT). IEEE; 2023. p. 496–500. https://doi.org/10.1109/ACIT58437.2023.10275545

53 Kobets V, Popovych I, Zinchenko S, Nosov P, Tovstokoryi O, Kyrychenko K. Control of the pivot point position of a conventional single-screw vessel. CEUR Workshop Proceedings. 2023;3513:130–40.

54 Lapkina IO, Malaksiano MO. Modelling and optimization of perishable cargo delivery system through Odesa port. Actual Problems of Economics. 2016;177(3):353–65.

55 Malaksiano NA. Exact inclusions of Gehring classes in Muckenhoupt classes. Mathematical Notes. 2001;70(5-6):673–81. https://doi.org/10.1023/a:1012983028054

56 Saaty TL. Decision making with the Analytic Hierarchy Process. International Journal of Services Sciences. 2008;1(1):83–98. https://doi.org/10.1504/IJSS.2008.017590

57 Stamatis DH. Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press; 2003.

58 European Union Agency for Cybersecurity (ENISA). Maritime Cybersecurity Guidelines. https://www.enisa.europa.eu/publications/maritime-cybersecurity-guidelines

59 Berzin SC, Singer J, Chan C. Practice innovation through technology in the digital age: A grand challenge for social work. Premier Journal of Science. 2025;12:3–21. https://doi.org/10.70389/PJS.100096

60 Ishak MI, Masri AN, Rasol AAA, Ibrahim IM, Hasbullah H. Amino acid deep eutectic solvents (AADES) in oil purification: An overview of properties, applications, and future directions. Journal of Ionic Liquids. 2025;5(1):100143.

61 Sardar A, Islam R, Anantharaman M, Garaniya V. Advancements and obstacles in improving the energy efficiency of maritime vessels: A systematic review. Marine Pollution Bulletin. 2025;214:117688. https://doi.org/10.1016/j.marpolbul.2025.117688

62 Ahmed W. Cybersecurity in the era of IoT: A review of vulnerabilities, threats, and mitigation strategies. Premier Journal of Science. 2025;5:100038. https://doi.org/10.70389/PJS.100038

63 Gangkui H. Relationship between nutritional risk index and inflammatory markers in metabolic syndrome—Synergy and clinical significance in geriatrics: A systematic review. Premier Journal of Science. 2025;13:100099. https://doi.org/10.70389/PJS.100099

64 Onyshchenko S, Melnyk O. Efficiency of ship operation in transportation of oversized and heavy cargo by optimizing the speed mode considering the impact of weather conditions. Transport and Telecommunication. 2022;23(1):73–80. https://doi.org/10.2478/ttj-2022-0007

65 Onyshchenko S, Melnyk O. Probabilistic assessment method of hydrometeorological conditions and their impact on the efficiency of ship operation. Journal of Engineering Science and Technology Review. 2021;14(6):132–6. https://doi.org/10.25103/jestr.146.15

66 Melnyk O, Onyshchenko S, Koryakin K. Nature and origin of major security concerns and potential threats to the shipping industry. Scientific Journal of Silesian University of Technology. Series Transport. 2021;113:145–53. https://doi.org/10.20858/SJSUTST.2021.113.11

67 Burmaka I, Vorokhobin I, Melnyk O, Burmaka O, Sagin S. Method of prompt evasive maneuver selection to alter ship's course or speed. Transactions on Maritime Science. 2022;11(1):1–9. https://doi.org/10.7225/toms.v11.n01.w01

68 Turgay E, Yildiz A, Demir A. Dynamic ergonomic risk assessment with REBA and fuzzy multi-criteria decision making: Addressing repetitive movements. In: Spectrum of Decision Making and Applications. 2025. https://doi.org/10.31181/sdmap4157

69 Mohammadi M, Sarvi S, Jafarzadeh Ghoushchi S. Assessing and prioritizing construction contracting risks with an extended FMEA decision-making model in uncertain environments. In: Spectrum of Decision Making and Applications. 2025. https://doi.org/10.31181/sdmap3120264

70 Ishtiaq M, Khan MA, Jafarzadeh Ghoushchi S. Quantifying multi-cause psychological disorder risk through an advanced mathematical model using intuitionistic pentagonal fuzzy logic. In: Spectrum of Operational Research. 2025. https://doi.org/10.31181/sor41202762

71 National Institute of Standards and Technology. Guide to operational technology (OT) security: NIST Special Publication 800–82 Rev. 3 [Internet]. U.S. Department of Commerce; 2023 [cited 2025 Dec 12]. Available from: https://doi.org/10.6028/NIST.SP.800-82r3

72 DNV. DNV CyberSecure: Cyber security framework for maritime operations. Det Norske Veritas; 2024.

73 International Association of Classification Societies (IACS). Unified Requirements E26/E27: Cyber safety and cyber security. IACS; 2024.

Glossary of Acronyms

Acronym	Full Term	Description
AHP	Analytic Hierarchy Process	Multi-criteria decision-making method based on expert pairwise comparisons.
BN	Bayesian Network	Probabilistic graphical model describing conditional dependencies between system states.
CPT	Conditional Probability Table	Matrix defining probability distributions for each node in a Bayesian Network.
DSS	Decision Support System	Computational system that assists operators in making risk-informed decisions.
FMEA	Failure Mode and Effects Analysis	Structured method for identifying and prioritizing failure risks.
RTO	Recovery Time Objective	Time required to restore system performance after disruption.
RRR	Resilience Recovery Rate	Ratio of recovered functionality relative to pre-disruption baseline.
RI	Resilience Index	Quantitative measure of system reliability under uncertainty.
ETL	Expected Time Loss	Average operational downtime associated with disruption events.
ESS	Energy Storage System	Subsystem used for storing and releasing electrical energy.
SOP	Soft Open Point	Power system configuration point enabling flexible energy routing.
SoC	State of Charge	Ratio of current battery charge to its rated capacity.
DCS	Data Collection System	IMO-compliant database for vessel operational and emissions data.
ISM	International Safety Management Code	IMO standard for safety and pollution prevention in ship operations.
IEC	International Electrotechnical Commission	Standards body issuing cyber and automation safety frameworks.
IMO	International Maritime Organization	UN agency regulating global maritime safety and environmental protection.

Appendix

Appendix A.1. Computational Environment

All simulations and optimization experiments were performed in the following environment:

Appendix Table A1 | Computational environment and software libraries used for simulations and optimization

Component	Version
Python	3.11
CVXPY	1.4
NumPy	1.26
SciPy	1.13
Pandas	2.2
Matplotlib	3.9
NetworkX	3.3

Random seed control `(np.random.seed(42))` and fixed solver parameters (ECOS, tolerance = 1e−5) were applied throughout to guarantee reproducibility of results.

Appendix A.2. DSS Implementation Pseudo-code

```
x = cp.Variable(n)
obj = cp.Minimize(w1*R_net + w2*C + w3*T_rec)
constraints = [cp.sum(x) <= C_max, x >= 0]
prob = cp.Problem(obj, constraints)
prob.solve(solver="ECOS", verbose=False)
```

Appendix B. Conditional Probability Table (CPT) Generation Procedure

The Conditional Probability Tables (CPTs) used in the Bayesian Network (BN) were generated synthetically based on expert elicitation and normalized Dirichlet sampling.

Each BN node H_i represents a subsystem or functional component, and the conditional distribution $P(H_i \backslash P_a(H_i))$ is defined as:

$$P\left(H_i \mid Pa\left(H_i\right)\right) = \mathrm{Dir}\left(\alpha_1, \alpha_2, \ldots, \alpha_k\right)$$

where $P_a(H_i)$ denotes the parent nodes of H_i and K the number of discrete states (e.g., normal, degraded, failed).

The concentration parameters α_k are proportional to expert confidence levels and weighted by the AHP/FMEA-derived importance coefficients w_i: $\alpha_k = cw_i Conf_{i,k}$,

with c being a normalization constant and $\mathrm{Conf}_{i,k}$ the expert-assigned confidence score for state k. To ensure internal consistency, all CPTs were normalized to satisfy.

$$\sum_k P\left(H_i = k \backslash Pa\left(H_i\right)\right) = 1.$$

For simulation purposes, CPTs were stored as JSON configuration files `(/params/cpt_<node>.json)` and automatically loaded by the BN inference engine at runtime.

A sample CPT structure (for a three-state node with two parent nodes) is provided below:

All CPTs follow this format, and their probabilistic parameters are consistent with the priors and weights specified in Section 2.5.

Appendix Table B1 | Conditional Probability Table (CPT) for a three-state Bayesian Network node

Parent 1	Parent 2	P(normal)	P(degraded)	P(failed)
Normal	Normal	0.85	0.10	0.05
Normal	Degraded	0.65	0.25	0.10
Degraded	Failed	0.40	0.35	0.25
Failed	Failed	0.10	0.25	0.65

Appendix C

Complete AHP pairwise comparison matrix and consistency ratios.

Appendix D

FMEA risk register with severity (S), occurrence (O), and detection (D) scores for all 12 failure modes.

Appendix E

Bayesian Network structure with conditional probability tables (CPTs) and calibration details.