International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-14, Issue-6, Nov-Dec 2026
DOI: https://doi.org/10.55524/ijircst.2026.14.6.3
Article ID IRP-1801, Pages 20-29
www.ijircst.org

A Cybersecurity Integration and Supply-Chain Verification Model for Shipboard Safety-Critical Systems Complying with IACS UR E26/E27

Chen-Yu Li[1], and *Chia-Ling Chen[2]

[1] Department of Information Management, Central Police University, Taoyuan, Taiwan
[2] Department of Maritime Police, Central Police University, Taoyuan, Taiwan

Correspondence should be addressed to *Chia-Ling Chen; chiaclloyd@gmail.com

Received: 4 Oct 2026; **1st Revision:** 18 Oct 2026; **2nd Revision:** 27 Oct 2026; **Accepted:** 3 Nov 2026; **Published Online:** 13 Nov 2026

Copyright © 2026 *Chia-Ling Chen et al. This is an open-access article distributed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- Application of IACS Unified Requirements E26 and E27 in the existing vessels creates a nightmare in terms of working. It is possible that the supplier is rated highly in documentations but the ship may end up having mechanical breakdown, having been associated with a bug that is hidden within OT software. We built the Supply-chain Verified Cyber Resilience (SCV-CR) framework to deal with this gap. Ranging the perimeter of otherwise-isolated networks into view instead of physical dependencies, SCV-CR imposes separation of communication paths and physical machinery dependencies on two explicit graph structures (G N and G S) and imposes hard Boolean admission gates on signed SBOM and VEX artifacts. Our set-up of the deterministic Monte Carlo experiment took over 20,000 iterations and six representative Maritime subsystems (PMS, AMS, IAS, ECDIS, GMDSS and cargo automation). The disruption failure rates were reduced by 16.22 percent and conditional downtime reduced by 24.28 percent and the 95th-percentile recovery time reduced to 15.31 h over the simulated rollout. Because inherent physical hazard invariants are never eliminated by the framework, it appears to offer a verifiable, mathematically-underpinned, way of audit of cyber safety by shipboard engineers and classification surveyors when carrying out physical surveys of classes.

KEYWORDS- Cyber-physical systems, IACS UR E26/E27, Maritime cybersecurity, Software bill of materials, Supply-chain verification.

I. INTRODUCTION

The new commercial ship of our time is a high-level cyber-physical system (CPS). Main propulsion, power generation, auxiliary machinery, bridge navigation and automated cargo handling are operated by commands in software. And onboard operational technology (OT) can scarcely be left on clean sides of the fence. Control Field Control Loops This type of controller is normally plugged to maintenance laptops, vendor satellite controllers or common serial converters exposing critical loops of control. Nevertheless, the discovery of a software vulnerability, in one of the board-based devices does not imply mechanical damage. The physical environment is determined by network routing, protocol conduct and privilege isolation, and the intervention of an automated interlock set of safety, or an alert watchkeep crew. As such an effective maritime security assessment should be confined to realistic machinery commitments. It cannot just believe that because a device can be accessed via the network a physical hazard is existing. This is more difficult due to conditions at sea. Marine automation suites have an average life in-service of twenty to thirty years; decades after their operating systems are no longer patched with commercial (and security) patches. Sea paths are highly congested, maintenances minimal, and offshore satellite T1 is minimal and costly. The inclusion of equipment of many subcontractors and a wide range of software security practices is also typical of newbuilds. The process of checking software bills of materials (SBOM) and patch integrity becomes a paperwork. It turns into a safety necessity. The modelling of complex machinery spaces in a deterministic manner is highlighted in IMO Resolution MSC.428(98) folding cyber risk into high-level safety management systems [1], [2], but it says little of them. Unified Requirements (UR) E26 and E27 [3], [4] are a set of enforceable rules that was developed by the International Association of Classification Societies (IACS). The two collaborate. E26 and E27 includes the ship-wide system integration and figure out the capability to endure operational racism and projected component-based testing and safety features. And in practice you can hardly partition them. E27 equipment protection puts meaning to the actual network partitioning onboard, in crew routine and during emergency restoration procedures. The E26 integration, in its turn, is conditional upon the availability of field components that will ensure tamper-evident logging, as well as verified firmware updates. The mixture of both sides discloses three familiar flaws of the existing means of carrying out maritime evaluations. First, any register of statical equipment views separates but fixed equipment as islands and not the functional couplings on which steering and propulsion depend. Second, the supplier-supplier compliance certificates are kept

separately, apart, to accommodate emergency voyage repairs, the onboard technical inspection of the software, including unverified software modifications, or dry-dock overhaul could pass unnoticed. Third, the composite risk indices are likely to mitigate the lack of technical barrier by allow huge volume of paper work to overturn the situation. This brings spurious safety in classification surveys and that is perilous. To address these gaps, this paper gives Supply-chain Verified Cyber Resilience (SCV-CR) model. SCV-CR does not present some static documents as the evidences of resilience. It contains components regarding the factory manufacture, dockyard assembly and operation. Network connectability (G N) is preserved separately of the physical safety dependencies (G S) in such a way that network connectability does not become mixed with mechanical damage. The model also uses non-compensatory admission gates to signed SBOM and VEX artifacts, which actually guarantees the existence of no unnecessary code hiding behind a full set of producer documents. When the mechanisms are all placed in a form with auditable form in a ledger, the recovery behaviour is tested with 20,000 deterministic Monte Carlo trials where the six representative classes of shipboard machinery are involved.

II. BACKGROUND AND RELATED WORK

A. Healthiness and type of data in the sea

Shipping cyber risk management has had an initial approach as policy. IMO Resolution MSC.428(98) and industry guidelines by BIMCO and International Chamber of Shipping makes cyber governance a part of the existing Safety Management Systems (SMS). That encompasses the planning of the voyage, training of people on a ship and the basic network hygiene [5]. But when it comes to the end of the road with regard to the safety of a vessel, it is the way the technical protection that the machinery is really functioning that will make the vessel safe.

IACS UR E26 and UR E27 offered an official bridge between whole-vessel architecture and subsystems engineering to the industry [3], [4]. Our evaluation framework defines the limit on evaluation in a ship that is the zone defence, recovery after an incident and incident management. UR E27 subsequently imprints developed technical skills onto board machinery controllers. The dependencies could be seen with the two being side by side. E27 offers access control on the device level in which minimal practical security is given in the event of maintenance bypass or a weak on-board local network credential. The local recording of events also becomes useless in the case where the vessel does have an automation network installed in it that is incapable of collecting, storing and correlating said telemetry in case of a degraded system. The surveyor after inspecting the bases and following the version of the class rule applicable leaves it to the surveyor to give the formal acceptance of the classes.

B. The industrial control security and constraint

Shipboard OT is quite different to a typical enterprise IT environment. The fundamental principles of industrial control security, such as zone segmentation (IEC 62443-3-3) and secure development lifecycles (IEC 62443-4-1) [6]-[8] are laid down, but are not easily applied directly to vessels, in NIST SP 800-82 Rev. 3 and the IEC 62443 series. In hybrid systems that do not follow a strict-hierarchy approach in the Purdue paradigm, it is common to find ships that combine old automation, navigation, high-voltage power control.

The zone allocations, in this instance, are viewed to be useful trust boundaries, as opposed to physical hard levels. Conducts are documents that present operational communications allowed. Instead, the dependency graph is the auxiliary services required by a machine to run safely, such as the use of continuous power, measurements of sea cooling or gyro compass. We guide our realistic attack paths relying on five viable defence-in-depth guidelines by CISA and adhering to MITRE ATT&CK (Enterprise and ICS) [9][10][11]. Nevertheless, generic taxonomies will never make you aware of when you are attacked on board. That is restricted by proprietary serial protocols, physical interlocks and the operating condition of the equipment.

C. Supply chain assurances and software-transparency

The maritime supply chains work on many levels of contraction and operators have minimal or no sight of embedded Code libraries- subcontractor code [12][13][14][15]. Software transparency frameworks have come about to minimize such blind spots. SBOM records are structured based on NTIA direction and standard machine-readable representations such as SPDX and CycloneDX to captures vulnerabilities in components, and Vulnerability Exploitability eXchange (VEX) records [16], [17], and [18]. Cryptographic signature schemes like the in-toto scheme, SLSA specification, Sigstore and TUF [20]-[23] add guarantees of provenance of artifacts and withstand of counterfeiting of artifacts during delivery. The previous priorities like CVSS v4.0, EPSS and CISA KEV thus help to prioritize vulnerabilities which are actively exploited at the moment [24]-[26].At some engineering point there must be one that is clear. A valid signature with cryptography signature informs you about the source of a given artifact. It does not tell you that the artifact has not got malfunctioning features. Likewise a static SBOM of a supplier is no longer reliable when it is changed after delivery, or when emergency dry-dock patches are not recorded. SCV-CR achieves this by ensuring signature verification is kept distinctly with operational configuration auditing as per NIST SP 800-218 (SSDF) and the continuous monitoring guideline of NIST SP 800-137 [27], [28]. The framework is not presupposed to take a malicious untested asset. Neither is it an explanation that there is no documentation as a sign of security.

D. Associated maritime CPS studies and gap in integration

How a cyber damage comes to be a physical interference, in a vessel, has garnered a fair portion of scholarly attention. Earlier studies have assessed maritime cybersecurity using general cyber-physical system (CPS) frameworks [29], looked at supervisory control weaknesses in port and logistics SCADA [30], and modelled security perimeters for autonomous ships [31]. Other more recent articles discusses the issue of autonetic attacks on autonomous surface vehicles (ASVs) with reinforcement learning pursuit models [32], and anti-hijacking schemes using blockchain technology used on maritime

autonomous surface vessels (MASS) [33]. Experiments by Chae et al. also reveal that a cyber test of a vessel is not able to omit watch keeping practice and what a human crew actual performs [34].

Irrespective of this literature, the current models have little likelihood of disruption of physical machinery dependency and verification of supply-chain that can be audited. That is the gap to be filled by SCV-CR. These risk calculations are under-ceiled as versioned asset, a seen cryptographic item along with an established chain of dependence, i.e., it permits access to uncertainty in the evidence to virulence through the public. The model is a part of the NIST Cybersecurity Framework 2.0 framework [35] that includes Identify, Protect, Detect, Respond and Recover functions within an overall Govern functional area. On the inside, in such a construct, the SCV-CR has an operational mitigation capacity regardless of formal administrative accountability necessary to receive operational risk.

III. PROBLEM FORMULATION AND DESIGN GOALS

A. Modeling of the system boundaries and its assets

In an assessment epoch t we analyze a vessel as a confined configuration 4-tuple ⟨A,Z,S,E) of the set of physical assets, security zones, supplier and verified evidence records. All safety critical OT equipment on board the analysis is included in the boundary of the analysis, and external maintenance interfaces or satellite terminals that have the capability to produce a change of state may or may not be included. Only potential exposures are modelled as shore services. Nor do we imagine them to be perched in the inside of the shipboard.

All records of assets are tuples of the form:

$$a_i = (id_i, v_i, z_i, s_i, F_i, c_i, B_i, Q_i) \quad (1)$$

Here, id_i is a persistent hardware identifier, that persists during the lifetime of the voyage. It is mapped to the installed hardware and software baseline v i, the assigned trust zone z i as well as to the vendor identities s i. F i The list of operational shipboards that an asset is used. B i indexes To records of components, which may include its cryptographic verification, such as machine-readable SBOM catalogs. An operational restriction (as of manual only bypass modes, or allowed at present during operation e.g. during port) is represented in Qi. A certain amount of operational criticality c i [0,1] regularises possible consequences in terms of life safety, environmental contaminations and manoeuvrability of a ship. This value should be proven on engineering standards that are documented otherwise normalisation can mask some severe dangers.

Table 1 collects the important mathematical terms, numbers and symbols enumerated in our formulation. The basic communication reachability can be easily mixed with mechanical damage due to industry tests. In order to prevent that, the model establishes two distinct setups of graph topologies: the cyber reachability graph GN and the operational dependency graph GD. The other affective parameters used in the asset-level security: asset-level inherent consequence listed in Table 1 as ci, exposure index measured as xi, evidential weight measured as qe and control barrier efficacy measured as eti that lead to residual operational risk Ri, and evidential uncertainty measured as Ui.

Table 1: Core notation and abbreviations

Symbol or Abbreviation	Meaning
A, Z, S, E	Assets, zones, suppliers, and evidence items
G_N, G_D	Cyber reachability graph and operational dependency graph
c_i	Inherent criticality of asset i
x_i	Scenario-weighted attack-path exposure indicator
q_e	Confidence assigned to evidence item e
η_{ik}	Estimated effectiveness of control function k for asset i
U_i	Unresolved assurance uncertainty for asset i
R_i	Residual-risk indicator for asset i
H_i	Assurance score, distinct from a compliance decision
SBOM / VEX	Software bill of materials / vulnerability exploitability exchange
CPS / OT	Cyber-physical systems / operational technology
PMS / AMS / IAS	Power management / alarm monitoring / integrated automation system
ECDIS / GMDSS	Electronic chart display and information system / Global Maritime Distress and Safety System

The representative inventory is made up of six system classes. These are categories for analysis. They do not imply that every installation shares the same architecture or class scope.

Table 2: Representative ship CPS asset inventory

System	Representative function	Dependency examples to verify	Principal assurance concerns
PMS	Electrical generation and load coordination	Generator controllers, switchboard interfaces, measurement inputs	Availability, command integrity, restoration compatibility
AMS	Machinery alarm collection and presentation	Sensors, alarm servers, operator displays	Alarm integrity, event retention, loss-of-view handling
IAS	Supervisory machinery monitoring and control	Controllers, engineering workstations, process networks	Privilege separation, control changes, configuration recovery

ECDIS	Electronic navigation information and route support	Position inputs, chart updates, navigation interfaces	Update provenance, data integrity, interface restrictions
GMDSS	Maritime distress and safety communications	Communication equipment, power supplies, relevant data inputs	Configuration integrity, availability, verified maintenance
Cargo	Cargo monitoring and control, as applicable	Pumps, valves, instrumentation, supervisory equipment	Command authorization, containment, safe degraded operation

A mapping of six functional system categories to provide the primary verification pathways is constructed in Table 2 in such a way that it reflects the actual arrangements of the machinery that occur in the merchant and auxiliary fleets:

- Power Management System (PMS):

Performs automatic generator synchronisation operation, as well as high-voltage bus tie operation. Checking is conducted on the integrity of commands and quick recovery on cold-start, such that black out does not occur during manoeuvring.

- Alarm System (AMS):

Collects machinery telemetry from many channels. Audits should ensure tamper evident logging of alarms and recovery of failsafe displays in a network ridden with congestion.

- Internet-based Automation System (IAS):

Process control units (DPUs) and engineering workstations were allocated using coordinates. The key verification checks, are privilege checking and compatibility of firmware rollback.

- Electronic Chart Display and Information System (ECDIS):

Assists in navigating vital bridges. Microsoft Microsoft needs to have strict input validation of the NMEA sensor sentences, provision of secure provenance of chart updates as well as isolating the USB media.

- Global Maritime Distress and Safety System(GMDSS):

Offers compulsory emergency telecommunication. Checks that ensure power redundancy and cryptographically guaranteed firmware states.

- Cargo Control System:

Monitors automated cargo pumps, ballast valves and tank atmosphere. The audits are concerned with command authorisation and prediction of failures in case of losses of communication.

B. Reachability, dependencies, and evidence

Cyber pathways and physical operational consequences are kept apart using two directed topologies:

- Cyber Reachability Graph ($G_N = (V_N, L_N)$):

This directed graph provides mapping of the permitted communication paths in onboard OT subnets and maintenance conduits. The details of lower-layer protocols (such as (Modbus TCP) or IEC 61162/NMEA interfaces or vendor-specific serial-bus-ties) are stored in each edge, and the direction of flow is indicated, along with the credentials required and the firewall policies at the edge. Topological exposure is indicated by reachability here. It does not demonstrate that there is a compromise that is bound to happen. The IP packets do not pass through an edge, which an attacker cannot cross. Lateral movement requires fulfilment of certain preconditions, like the exploitation of an unpatched buffer exploit on an embedded controller, or the hijacking of an engineering workstation session.

- Operational Dependency Graph ($G_D = (A, L_D)$):

Where G_N encodes the digital traffic G_D documents the physical dependencies in the plant that maintain the seaworthiness of the vessel. An edge $a_j \rightarrow a_i$ indicates that asset a_i functionally requires aeuxiliary support of asset a_j in the mentioned operating modes of machinery. In a real machinery space, there are non-routable auxiliaries like sea-cooling loops to main engine jackets, 24V DC battery-backed control buses or hydraulic steering pumps, where the real loss put across as the network boundaries is propulsion off regardless of the layout of the network boundaries. Edge weights distinguish between mandatory links and redundant standby units, such that shared power distribution panels and mechanical cross-connects retain maximum weight associated with the full risk still available even when they are completely covered by an air-gap around the Ethernet backbone. Circular dependencies between auxiliaries (shaft generators with lubricating pumps etc.) might otherwise multiply the consequences indefinitely, thus they are merged into mutually dependent functional groups.

The verifiable compliance artifacts must support both topologies and thus supplier documentation is recorded as formal cryptographic evidence tuples:

$$e = \begin{pmatrix} \text{issuer, subject, version, claim, hash,} \\ \text{time, expiry, method, result} \end{pmatrix} \quad (2)$$

A record connects each release of reviewed software or firmware to a non-modifiable SHA-256 digest (or hash) that binds vendor statements to a precise binary build. This connects the integration audit of shipyards with class surveyor audit. The manner of evaluating the evidence, be it automated signature checks on SPDX manifests, observed Factory Acceptance Tests (FAT) or observed during sea trials determines the evidential confidence value $\in [0,1]$. Correlated or self-claimed, claims, which are made by one vendor are combined. By doing so, heaps of duplication of compliance documentation will never stack the security confidence on higher grounds where the physical security is not checked.

C. Assurance and risk goals.

Given operational threat scenario $h \in H$, let p_h represent the scenario occurrence weight and L_h the estimated physical loss post-mitigation. Residual risk is modeled as:

$$R = \sum_{h \in \mathcal{H}} p_h \, L_h \quad (3)$$

Unless empirical baseline probabilities and standard financial or safety metrics have been professed, the use of equation (3) ought to be in the form of a comparative engineering indicator. Scenario paths that intersect must be constrained with Fréchet inequalities, in order to ensure that there is no overestimation of occurrence rates.

The next audit that is carried out is evidential uncertainty in comparison to modelled risk and this is important. Unresolved assurance uncertainty Ui of asset i can be defined as:

$$U_i = 1 - \frac{\sum_{e \in E_i} w_e q_e}{\sum_{e \in E_i} w_e} \quad (4)$$

In which E_i is the admissible evidence that is bound to asset i, q_e is the estimated confidence and $w_e > 0$ provides a relative weight to each claim of verification. When the asset has no admissible documentation ($E_i = \emptyset$), $U_i = 1$ default. Measurement of incompleteness of the evidence is in equation (4). It is not a probability of exploits.

The engineering goal is to determine an admissible control set $u \in U$ such that the risk minimization cost is a compromise with the evidential certainty:

$$\min_{u \in \mathcal{U}} [R(u) + \lambda \sum_i c_i U_i(u)] \quad (5)$$

timing constrained, operational availability constraints and verification gates. The weighting factor lambda i sanctions key elements with no evidence that is verifiable, and by so doing, attempted uncertified affirmations by a supplier formally becomes barred in a fleet foundation.

D. Design objectives and auditing.

SCV-CR works to five operational design objectives:

- Operational Safety Invariance: There are no mitigations that can impair the control-loop response time, availability of a system or machinery safety limits.
- Verifiability: The artifacts should be cryptographically implicated. Second party warranties are not taken.
- Non-Compensatory Gating: But even the completest administrative documentation would not numerically compensate unverified critical upgrades or unproven technical security measures.
- Lifecycle Continuity: Reassessment will automatically begin when the firmware is being built, and a change of network paths or physical dependency paths has occurred during an overhaul.
- Reproducible Audit Trails: The inputs of the model boundary conditions and artifact hashes as well as the surveyor decisions are stored forever so that the classes can be checked.

Audits may be bi-directional. An IACS requirement theme can be followed by a surveyor to its physical cryptographic artifact, or a score of risks can be reassembled based on the underlying network configuration. The evaluation is fed by signed SBOM and VEX artifacts, but neither replaces nor substitutes surveyor inspection. The last score is a summation of technical evidence recorded. Not statutory classification approval and no standing out of class society procedures.

IV. THE SCV-CR MODEL

A. Architectural Overview and Assurance Boundary

The supply-chain Verified Cyber Resilience (SCV-CR) model unites technical exposure, safety dependencies, supplier evidence and operational recovery into a single versioned assurance model. Not a vessel under measurement, but a willed ship configuration, not a vessel under subject of the perceived isolated located software code, equipment, interfaces and maintenance procedures. Both of the assessments determine the configuration base line, the operational mode, the date on which evidence ceased to be cut and the edition of rule being applied to the classification (see the below figure 1).

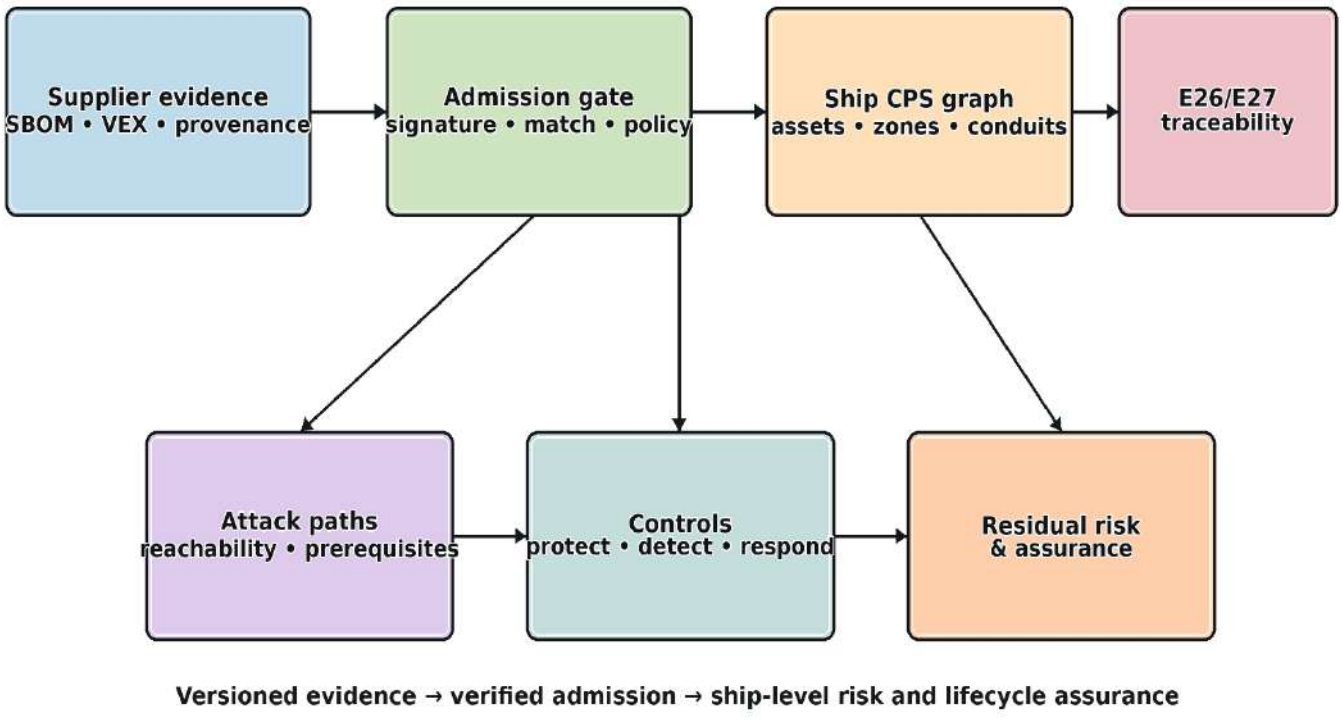


Figure 1: SCV-CR model linking the supplier evidence, proven admission, ship CPS dependencies and lifecycle assurance

The architecture has six layers that are connected to each other:

- Asset and dependency layer: lists security-relevant safety-relevant functional relationships and cyber-physical assets.
- Zone and conduit layer: exhibits credible limits, authorized communications and service paths.
- Supply-chain evidence layer: this links equipment and components to provenance evidence and vulnerability data that is authentic.
- Threat and exposure layer: identifies the possible attack paths that can be taken and in what conditions.
- Control and resilience layer: documentation prevention, detection, response and recovery capabilities.
- Risk and assurance layer: calculates the conditioned risk by scenarios and, independently, measures the evidence-supported assurance.

An evidence ledger crosscuts across all levels and links all derived results with input records, and calculating version, assumptions and approval record. Because of this difference, there will always be no good numeral score which can correspond to an obligatory need that was not addressed.

Evidence ledger is put along with all the layers. The configuration changes, new vulnerabilities releases, supplier changes and recovery exercises are reflected by feedback arrows. Its products include a risk register, a requirements traceability, a list of open assurance findings and update admission decisions.

SCV-CR steals a Purdue-like hierarchy to aid in organising the analysis. It does not mention that ship networks are a duplication of a manufacturing structure. The operational and safety requirements may be of propulsion, cargo systems, automation and communications systems and navigation. It does not belong to some level that a system is in some zone, but rather, its functionality, access requirements and dependencies that it allows.

B. Representation Repository, Network, and Safety-Dependency

Let V denote the set of inventoried assets. Two separate graphs describe the distinct cyber and physical relationships:

$$G_N = (V, E_N), \qquad G_S = (V, E_S) \tag{6}$$

The directed network, G_N is the directed network, and the possible communication paths lie in the directed network. The protocol, direction and the points of enforcement as well as the operating modes and pre-requisites are contained in all the edges. The safety-dependency graph, G_S, is operational relevant dependencies of which the edge $i \to j$ denotes that a failure of struggle of the safety component of asset j is directly due to the degradation of asset i. The fact that the network is accessible does not mean that there is a dependency on safety and that an operational dependency does not presuppose a network relationship.

Each profile of assets is:

$$a_i = \langle id_i, fun_i, z_i, ver_i, sup_i, crit_i, deps_i, if_i, rec_i, evid_i \rangle \tag{7}$$

where $crit_i$ signifies documented consequence criteria, which pertains to personnel safety, vessel operation, of environmental protection and continuity of service.

This is possible because some dependency (i.e. shared auxiliary power, gyro feeds or workstations, etc.) means that a count will be counted twice. In order to avoid this dependency adjusted criticality is defined as:

$$\tilde{c}_i = \underset{j \in \mathrm{REACH}_S(i) \cup \{i\}}{\mathrm{MAX}} \left[c_j \underset{p: i \rightsquigarrow j}{\mathrm{MAX}} \prod_{(u,v) \in p} h_{uv} \right] \tag{8}$$

where $h_{uv} \in [0,1]$ is the conditional dependency-transfer factor and the empty path evaluates to unity. Cyclic dependencies are treated as mutually dependent groups to prevent unbounded consequence recursion.

C. Evidence Objects, gate to admission, and Software

Written records written evidence artifacts:

$$\text{EvidenceRecord} = \langle \text{id,asset_id,comp_id,type,issuer,key_id,digest,sig,valid_until,ver,conf,method,result} \rangle \tag{9}$$

In evidence artifact, a signed Software Bill of Materials (SBOM), a Vulnerability Exploitability eXchange (VEX) statement, a type-approval certificate or a FAT/SAT test record are evidence artifacts. Provenance and integrity are assured with a valid cryptographic signature. It fails to give the assurance that the software is not insecure.

The imperfection of a very essential kind may be masked by compensatory scoring. This way until any software update is installed on board it has to go through compulsory, non-compensatory admission gates:

$$\mathrm{Admit}(u) = \mathrm{SigOK}(u) \wedge \mathrm{DigestOK}(u) \wedge \mathrm{IdentityOK}(u) \wedge \mathrm{Applicable}(u) \wedge \mathrm{Authorized}(u) \wedge \mathrm{SafetyReviewOK}(u) \wedge \mathrm{RecoveryReady}(u) \tag{10}$$

If any predicate fails, admission is blocked. Rollback to earlier firmware is not assumed intrinsically safe, as downgrading may reintroduce known CVEs or break interface dependencies.

D. Control Effectiveness and Remaining risk and Threat Scenarios.

Threat scenarios consider entry points, adversary capability, and prerequisite paths. For attack edge e, the conditional success parameter given preventive barrier effectiveness b_e is $p_e^* = p_e(1 - b_e)$. The overall path success probability is:

$$P_\pi = \prod_{e \in \pi} P\,(e \text{ succeeds} \mid \text{preceding path conditions}) \tag{11}$$

When common credentials or shared maintenance conduits create dependencies, conservative Fréchet bounds are applied: $\max_\pi P_\pi \le P_{\text{access}} \le \min(1, \sum_\pi P_\pi)$.

Operational controls are aligned with NIST CSF 2.0 (Identify, Protect, Detect, Respond, Recover). Letting d_s denote early detection probability and k_s successful containment probability, the disruption probability becomes:

$$P_{\text{disruption},s} = P_{\text{access},s}(1 - d_s k_s) \tag{12}$$

Conditional downtime D_s incorporating recovery effectiveness ρ_s is modeled as:

$$D_s = D_{\min,s} + \left(D_{\text{unmit},s} - D_{\min,s}\right)(1 - \rho_s) \tag{13}$$

Total residual risk across mutually exclusive scenarios $s \in \mathcal{H}$ over horizon T is:

$$R(T) = \textstyle\sum_{s \in \mathcal{H}} P_s\,(T) \cdot \mathbb{E}[L_s \mid s] \tag{14}$$

Concurrently, assurance score A is tracked separately to ensure documentary completeness does not obscure high-exposure operational nodes.

V. COMPLIANCE MAPPING TO IACS UR E26/E27

SCV-CR links the ship-level requirements of UR E26 with the system and equipment capabilities of UR E27 through structured verification artifacts. At ship level the concern is overall integration, network segmentation, incident response and operational recovery. At equipment level it is secure development lifecycle evidence, firmware integrity, local access control and diagnostic telemetry.

Table 3: SCV-CR Traceability to IACS UR E26/E27 Core Themes

Theme	Ship-Level E26 Assurance Focus	Equipment-Level E27 Assurance Focus	SCV-CR Artifacts	Verification & Acceptance Evidence
Asset Inventory	Installed topology, interfaces, boundaries	Firmware version, hardware IDs, SBOM	Asset registry, SBOM catalog	Drawing reconciliation, physical audit
Network Segmentation	Zones, conduits, boundary controls	Available interface restrictions, VLANs	G_N matrix, conduit rules	Traffic filtering tests, boundary audit
Secure Configuration	Maintained ship configuration baseline	Secure boot, hardening guidelines	Baseline manifest, crypto digests	Version check, hardening inspection
Access Control	Roles, remote vendor access policies	Account authentication, least privilege	Role matrix, remote access logs	Credential review, authentication tests
Malware Protection	Vessel network filtering, USB policy	Application whitelisting, code signing	Admission logs, update gate checks	Code signature checks, isolation drills
Logging & Monitoring	Centralized event collection & review	Standardized syslog generation	Telemetry schema, NTP audit	Alert path verification, clock checks
Incident Recovery	Continuity plans, restoration drills	Image backups, factory fallback	Recovery playbooks, backup digests	Restoration drills, cold-start tests
Supply Chain Assurance	Integration evidence, patch authorization	Component provenance, VEX reports	VEX repository, supplier ledger	Signature checks, version matching, vulnerability review

Every traceability requirement is stored as a structured claim tuple:

$$r_k = \langle id_k, \text{source}_k, \text{scope}_k, \text{evidence}_k, \text{status}_k \rangle \quad (15)$$

Where status k can only take the values satisfied, partially supported, not demonstrated, justified N/A. the status can only be one of these discrete values to avoid having unverified claims included in compliance ratings, or even metrics that use documentation as a basis.

Table 3 introduces a mapping of ship-level operational resilience of the IACS UR E26 lines with UR E27 technical capabilities of equipment. Under the eight core themes of compliance:

- Asset Inventory as well as Network Segmentation: The SBOM inventory at the equipment level is required to assist a topology and zone boundaries of the ship at the ship level (E26). These are confirmed through drawing of reconciliation and boundary tests traffic.
- Configuration, Access & Malware Controls: Baseline configurations, role matrices and code-signing gates can be audited through cryptographic digests and update admission logs. This extends the shipboard policy to the least-privileged at device-level and to secure boot.
- Logging, Monitoring & Incident Recovery: A typical syslog schema, verified recovery images means that the activity of each device is available to be stitched together to create situational awareness of a ship and to allow cold-start continuity tests.
- Supply Chain Assurance: Patch authorisation by integrator under E26 directly relates to component provenance in terms of cryptographically signed VEX reports and supplier ledger entries under E27. The combination can offer an end-to-end trail of evidence.

VI. EXPERIMENTAL EVALUATION AND DISCUSSION

A. Synthetic Monte Carlo Simulation Setup

Experiments with real vessels, machinery or safety of navigation were not desired, and the model was experimented through a synthetic, deterministic Monte Carlo simulation. It was tested on six representative systems of safety critical mission on board of Power Management System (PMS), Alarm Monitoring System (AMS), Integrated Automation System (IAS), Electronic Chart Display and Information System (ECDIS), Global Maritime Distress and Safety System (GMDSS) and Cargo Control at 20,000 trials ($N = 20{,}000$).

Two settings that we have compared:

- Base line Mode: Normal marine deployments, when no verbal supplier assertion is involved, patching and performing the recovery processes, which are not related to any other process at all, are performed manually.
- SCV-CR Mode: supports cryptographic admission gating, network segmentation (dependencies taken into account), and demonstrating SBOM/VEX provenance.

A trial represents one abstract cyber-risk opportunity affecting a target system. The overall mean downtime $\overline{D}_m$

and conditional mean downtime $\overline{D}_{m|Y=1}$ satisfy the relation $\overline{D}_m = \hat{p}_m \overline{D}_{m|Y=1}$, where $Y \in \{0,1\}$ indicates disruption occurrence.

B. Methodological Comparison and Novelty of SCV-CR

When compared to current industrial cybersecurity, software supply-chain assurance and maritime risk frameworks, it is evident that SCV-CR leaves them behind in practice. An overview is presented in Table 4. There are some problems in the shipboard machineries as per the current practices. The classical OT models such as the Purdue hierarchy or IEC 62443 give pre-defined perimeter delimitations. However, when adjacency on the network is considered physical consequence, benign communication paths cause false alarm, and vital dependencies having no network at all, such as an auxiliary supply of a shared 24 V (or shared cooling loop) are detected. Software transparency programs (SBOM/SPDX, SLSA and Sigstore, among others) do just the opposite. They authenticate the provenance of the build, and the cryptographic signatures but are not aware of the operation of the vessel itself. A signature of an update in the firmware may be perfectly valid, yet create serious timing latency, or when manoeuvring may cause latent weaknesses that are unknown to anyone. And compensatory weighted averages in risk scoring systems (CVSS or NIST SP 800-30, say) permit much of the paperwork numerically to justifiate a disastrous single-point technical failure. SCV-CR would resolve such conflicts through the three main architectural practices of:

First, our formulation explicitly isolates cyber reachability (G_N) from physical safety dependencies (G_S) via a dual-graph model. This ensures that critical mechanical dependencies remain audited even when field equipment operates completely air-gapped from the ship's Ethernet backbone. Second, the model enforces non-compensatory Boolean admission gating ($Admit_u$, Eq. 10). Documentation completeness cannot offset unverified code; any failed cryptographic digest or unverified supplier statement results in an immediate deployment block. Third, under Equation (4), unverified supplier claims directly incur an explicit uncertainty penalty (U_i). This mathematically prevents assessors from treating missing vulnerability disclosures as confirmed onboard safety.

Table 4: Comparison of SCV-CR with Existing Cybersecurity and Supply-Chain Methods

Feature / Dimension	**Traditional OT Security (e.g., IEC 62443, Purdue)**	**Software Supply-Chain Frameworks (e.g., SBOM, SLSA, in-toto)**	**General Risk Scoring (e.g., CVSS v4.0, NIST SP 800-30)**	**Proposed SCV-CR Model**
Primary Scope	Static network zoning and perimeter boundary controls.	Build pipeline integrity and artifact provenance signing.	Component vulnerability severity and weaponization metrics.	Unified lifecycle assurance linking equipment provenance to ship-level safety.
Reachability vs. Safety Dependency	Conflates network reachability with physical hazard potential.	Disregards physical runtime and functional dependencies entirely.	Considers target exposure without operational dependency modeling.	Explicitly decouples Cyber Reachability (G_N) from Safety Dependency (G_S).
Treatment of Supply-Chain Evidence	Assumes static vendor compliance without cryptographic binding.	Provides cryptographic attestation but lacks operational integration.	Treats vendor claims as qualitative input parameters.	Cryptographically binds signed SBOM/VEX to operational asset baselines.
Decision & Evaluation Rules	Compensatory or heuristic qualitative review.	Binary build-admission without runtime risk evaluation.	Compensatory weighted-average scoring (masks critical flaws).	Non-compensatory admission gates (Eq. 10) preventing compensatory scoring.
Handling of Missing Evidence	Often treats lack of evidence as acceptable or assumes baseline security.	Fails build pipeline; lacks explicit uncertainty quantification.	Interpolates missing inputs or relies on subjective defaults.	Formulates evidential uncertainty (U_i) as an explicit optimization penalty (Eq. 5).
Regulatory Alignment	General industrial systems; indirect maritime mapping.	General enterprise software; not tailored to maritime classification.	Generic IT/OT environments.	Direct, auditable traceability mapping to IACS UR E26 and UR E27 (Table 3).

C. Simulation Results and Quantitative Comparison

Table 5 gives the overall simulation results for the two operational modes.

Table 5: Quantitative Experimental Results from 20,000 Monte Carlo Trials

Metric	**Baseline**	**SCV-CR**	**Relative Change / Interpretation**
Monte Carlo Trials	20,000	20,000	Identical sample size ($s = 20261024$)
Disruptive Event Count	376	315	61 fewer disruption incidents observed
Event Rate (p)	0.01880	0.01575	16.22% relative reduction
Mean Downtime (All Trials, h)	0.215960	0.136987	36.57% total operational downtime reduction

Conditional Mean Downtime ($D \mid Y = 1$, h)	11.487244	8.697572	24.28% relative reduction
95th-Percentile Downtime ($D \mid Y = 1$, h)	20.776741	15.306389	26.33% reduction in upper-tail outage duration
Supplier Exposure Score (x)	0.497000	0.213334	57.08% reduction in unverified components
Detection Effectiveness (d)	0.416345	0.714701	71.66% improvement in early anomaly detection
Recovery Effectiveness (ρ)	0.310089	0.705894	127.64% increase in restoration efficiency
Conditional Impact Indicator (I)	1.125371	1.123273	Negligible change (-0.19%, physical invariant)

D. Key Findings and Sensitivity Analysis

- Physical Invariance Consequence Severity:

The statistics reveals just one certain fact in marine engineering. The rate of events being disrupted dropped by 16.22% and conditional mean downtime dropped by 24.28% but the conditional severity impact indicator did not change much (1.125371 vs. 1.123273). Cyber controls can put boundaries on the extent of an exploit and can accelerate the recovery following an incident. There is an outcome of loss of propulsion or steering during a critical port manoeuvre which they cannot change. When physical machinery fails, it remains the same regardless of the level of software assurance.

- Upper-Tail Recovery Outage Suppression:

The 95th-percentile downtime dropped sharply from 20.78 h to 15.31 h—a 26.33% reduction. On an actual ship, this could be a reflection of proven backup manifests and dependency-sensitive recovery-playbooks, without long-term restoration deadlocks as are prone to occur when human operators debug using manual, non-coordinated work when an offshore blackout occurs.

- *Sensitivity to Upstream Evidence:*

Sweeping the supplier-evidence reduction factor across $r \in [0,0.8]$ via the empirical relation:

$$rate(r) = 0.01880(1 - 0.72r) \qquad (16)$$

Depends on an uninterrupted smooth decrease on the operational disruptions as unverified third-party libraries are eliminated. This implies that strict supply-chain gating at the initial design, at the shipyard, is a safety payback many times over throughout the working life of the ship.

VII. CONCLUSION

To satisfy IACS UR E26/E27 it is not sufficient to be dependent on vendor paperwork. The SCV-CR architecture presented below corresponds to the provenance of component-level software provenance in fact to the survivability of ship-level hardware. Because the concept of reachability of communication is divided in terms of physical control channels, there is no chance to counterbalance a large number of documents with unproven failures in firmware numerically. The run simulation of 20,000 shows clear improvement in engineering: the disruptive outages were minimized by 16.22 to 15.31 h and the worst-case recovery windows were minimized by 20.78 to 15.31 h. Equally, physical consequence invariants that hold true everywhere in conditions of critical manoeuvring that are controlled by the admission software adds value towards the recovery without discounting physical engineering risks. It can be utilized with the evidence ledger, to offer an easy audit base to the shipyards, class societies and operators that are destined to undergo obligatory E26/E27 inspections.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] International Maritime Organization, “Maritime cyber risk,” IMO Guidance Document, 2021. Available from: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[2] International Maritime Organization, “Maritime cyber risk management in safety management systems,” Resolution MSC.428(98), Jun. 2017. Available from: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[3] International Association of Classification Societies, “UR E26: Cyber resilience of ships,” Unified Requirements, Electrical and Electronic Installations, 2023. Available from: https://iacs.org.uk/resolutions/unified-requirements/ur-e

[4] International Association of Classification Societies, “UR E27: Cyber resilience of on-board systems and equipment,” Unified Requirements, Electrical and Electronic Installations, 2023. Available from: https://iacs.org.uk/resolutions/unified-requirements/ur-e

[5] BIMCO, International Chamber of Shipping, and collaborating organizations, *The Guidelines on Cyber Security Onboard Ships*, Version 4. Copenhagen: BIMCO, 2020. Available from: https://www.ics-shipping.org/publication/the-guidelines-on-cyber-security-onboard-ships/

[6] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, “Guide to operational technology (OT) security,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-82 Rev. 3, 2023. Available from: https://csrc.nist.gov/pubs/sp/800/82/r3/final

[7] International Electrotechnical Commission, *Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels*, IEC 62443-3-3:2013, 2013. Available from: https://webstore.iec.ch/

[8] International Electrotechnical Commission, *Security for Industrial Automation and Control Systems—Part 4-1: Secure Product Development Lifecycle Requirements*, IEC 62443-4-1:2018, 2018. Available from: https://webstore.iec.ch/

[9] Cybersecurity and Infrastructure Security Agency, “ICS recommended practices,” CISA Industrial Control Systems, 2023. Available from: https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

[10] The MITRE Corporation, “ATT&CK: Enterprise matrix,” MITRE ATT&CK, 2023. Available from: https://attack.mitre.org/matrices/enterprise/

[11] The MITRE Corporation, “ATT&CK: ICS matrix,” MITRE ATT&CK, 2023. Available from: https://attack.mitre.org/matrices/ics/

[12] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, “Cybersecurity supply chain risk

management practices for systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-161 Rev. 1, 2022. Available from: https://csrc.nist.gov/pubs/sp/800/161/r1/final

[13] Joint Task Force, "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-53 Rev. 5, 2020. Available from: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[14] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30 Rev. 1, 2012. Available from: https://csrc.nist.gov/pubs/sp/800/30/r1/final

[15] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber-resilient systems: A systems security engineering approach," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-160, vol. 2, Rev. 1, 2021. Available from: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

[16] National Telecommunications and Information Administration, "The minimum elements for a software bill of materials (SBOM)," U.S. Department of Commerce, Report, 2021. Available from: https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

[17] Cybersecurity and Infrastructure Security Agency, "Minimum requirements for Vulnerability Exploitability eXchange (VEX)," CISA Guidance, 2023. Available from: https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex

[18] SPDX Project, "SPDX specification version 2.3," Linux Foundation, 2022. Available from: https://spdx.github.io/spdx-spec/

[19] OWASP Foundation, "CycloneDX specification overview," OWASP Standard, 2023. Available from: https://cyclonedx.org/specification/overview/

[20] S. Torres-Arias, H. Afzali, T. K. Kuppusamy, R. Curtmola, and J. Cappos, "in-toto: Providing farm-to-table guarantees for bits and bytes," in *Proc. 28th USENIX Security Symposium*, 2019, pp. 1393–1410. Available from: https://www.usenix.org/conference/usenixsecurity19/presentation/torres-arias

[21] OpenSSF, "Supply-chain Levels for Software Artifacts (SLSA) specification v1.0," OpenSSF Standard, 2023. Available from: https://slsa.dev/spec/

[22] Linux Foundation, "Sigstore documentation: Software signing and transparency," 2023. Available from: https://docs.sigstore.dev/

[23] J. Samuel, N. Mathewson, J. Cappos, and R. Dingledine, "Survivable key compromise in software update systems," in *Proc. 17th ACM Conference on Computer and Communications Security*, 2010, pp. 61–72. Available from: https://doi.org/10.1145/1866307.1866315

[24] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System version 4.0: Specification document," FIRST, 2023. Available from: https://www.first.org/cvss/v4.0/specification-document

[25] Forum of Incident Response and Security Teams, "Exploit Prediction Scoring System (EPSS) user guide," FIRST, 2023. Available from: https://www.first.org/epss/

[26] Cybersecurity and Infrastructure Security Agency, "Known exploited vulnerabilities (KEV) catalog," CISA, 2023. Available from: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[27] M. Souppaya, K. Scarfone, and D. Dodson, "Secure Software Development Framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-218, 2022. Available from: https://csrc.nist.gov/pubs/sp/800/218/final

[28] K. Dempsey, N. Chawla, A. Johnson, R. Johnston, A. Jones, A. Orebaugh, M. Scholl, and K. Stine, "Information security continuous monitoring (ISCM) for federal information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-137, 2011. Available from: https://csrc.nist.gov/pubs/sp/800/137/final

[29] I. Progoulakis, D. Nikitakos, and D. Dalaklis, "Cyber physical systems security for maritime assets," *Journal of Marine Science and Engineering*, vol. 9, no. 12, p. 1384, 2021. Available from: https://www.mdpi.com/2077-1312/9/12/1384

[30] E.-M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, "A novel risk assessment methodology for SCADA maritime logistics environments," *Applied Sciences*, vol. 8, no. 9, p. 1477, 2018. Available from: https://www.mdpi.com/2076-3417/8/9/1477

[31] S. Katsikas, "Cyber security of the autonomous ship," in *Proc. 3rd ACM Cyber-Physical System Security Workshop*, 2017, pp. 55–56. Available from: https://doi.org/10.1145/3055186.3055191

[32] E. Liu, S. Dong, Z. Wu, and S. Zhang, "A PPO-based robust target pursuit framework for ASVs under cyberattacks," in *Proc. 2026 41st Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, 2026, pp. 1270–1275. Available from: https://doi.org/10.1109/YAC71005.2026.11615513

[33] M. Gao *et al.*, "Swarm of MASSs cyber-security for anti-hijack system based on blockchain and chaotic-steganography using VRF-PBFT and encoder-decoder deep neural networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 12, pp. 21758–21768, 2025. Available from: https://doi.org/10.1109/TITS.2025.3616187

[34] C. Chae, I. Kim, R. Baumler, and Y. Ahn, "Ship cybersecurity risk assessment for safe operation with human involvement: An experimental case study," *WMU Journal of Maritime Affairs*, vol. 24, no. 4, pp. 515–543, 2024. Available from: https://doi.org/10.1007/s13437-024-00353-6

[35] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024. Available from: https://www.nist.gov/cyberframework