Developing a Risk-Based Cybersecurity Governance Framework for LNG and Tanker Fleet Operations: An OT-Aware Machine Learning and LCGRI Decision Model

[1]Nadir Buksh and [2]Hazem Abu-Adaiq

[1]Fuel Research Center, PCSIR Karachi
[1]nadirbuksh@yahoo.com
[2]Cybersecurity and Cloud Computing, Faculty of Information Technology, Applied Science Private University, Amman, Jordan
[2]h_abuadaiq@asu.edu.jo
[2]0000-0002-9700-0968

Abstract

Liquefied natural gas (LNG) carriers and tanker fleets rely on interconnected operations technology (OT), industrial control systems (ICS), cargo management platforms, power-management systems, navigation equipment, satellite communications, and remote monitoring systems. This digital integration aids operational efficiency and safety monitoring but also opens cyber-physical risk pathways through which a cyber incident can affect propulsion, ballast operations, cargo pumps, monitoring of tank-level contents, power distribution, navigation reliability and emergency situations. While there are useful maritime cybersecurity studies that offer threat taxonomies, regulatory guidance, and intrusion-detection models that are limited work that relates the technical anomaly evidence to governance-level decisions made by fleet managers, designated persons ashore, ship masters, safety auditors, and security officers. This study aims to create a cyber security governance framework for the LNG and tanker fleet operations, based on the HAI Security Dataset as an analytical basis. The HAI dataset was chosen for the features: Hardware-in-the-Loop (HWIL) industrial control system telemetry, labelled attack intervals, multivariate time-series continuity and cyber-physical process coupling. HAI is not one of the datasets generated by the vessels, but it is methodologically appropriate for this study because of the similarities in the OT principles used in LNG and tanker operations: sensor-actuator interaction, process dependency, automated control, and safety-critical monitoring. The research suggests a Liquefied Natural Gas Cyber Governance Risk Index (LCGRI), which is a weighted governance score that incorporates asset criticality, threat probability, vulnerability severity, anomaly-detection confidence, and operational consequence. The suitability of the datasets, class distributions, relationships among the OT features, separability of the anomalies, performance of supervised and unsupervised models, and risk-prioritisation behaviour were all analysed in Python. The results of the analysis indicate that cargo pump manipulation, navigation compromise, cargo tank sensor spoofing, power-management anomalies, and ballast-control disruption are the most important governance issues, while supervised learning models yield consistently strong anomaly-identification performance with HAI-based OT telemetry, with ensemble methods offering additional interpretability advantages for governance. The proposed framework provides a realistic approach to decision support, converting OT anomaly detection to risk-ranked governance actions for LNG and tanker fleet cybersecurity management.

Keywords: LNG cybersecurity; tanker fleet; maritime cyber risk; operational technology; industrial control systems; anomaly detection; risk governance; LCGRI.

1. INTRODUCTION

The LNG and tanker shipping industries are safety-critical applications for which the functions are tightly coupled cyber-physical. The modern vessel has an integrated navigation bridge, electronic chart display and information system, GNSS receiver, automatic identification system, cargo control station, ballast management, power management system, engine automation, voyage optimization, satellite connectivity and remote support channels [1]. They provide measurable operational improvements but also bring about a greater convergence between the traditional distinction of information technology and OT. An initial compromise – in the form of credential theft, insecure remote access, malicious software, spoofed navigation data, or manipulation of a controller tag – can cascade into safety, environmental, commercial, and geopolitical consequences [2]. Cyber risk is particularly critical for LNG carriers, as cargo containment, pressure control, loading and unloading sequences and emergency shutdown logic must be trustworthy

under highly constrained operating conditions.

Cybersecurity is increasingly a management-system challenge, not just a technical challenge, with regulatory and industry guidance. Cyber risks must be included in safety management systems for the IMO, and NIST's LNG Cybersecurity Framework Profile calls for a voluntary, risk-based cybersecurity strategy for the LNG lifecycle [3]. The main hurdle faced is the lack of integration between cyber risk assessment, cyber vulnerability management, monitoring, and cyber governance reporting in many cases. The consequence of the operation may be known only to the chief engineer, cargo officer, or fleet superintendent, and a network alert may be seen by an IT team [4]. On the other hand, cyber risk-control documentation could exist without actual telemetry or detection evidence. This division diminishes prioritization and may result in under- or overreaction to safety-critical and low-consequence events [5].

The state of academic literature has also evolved somewhat differently. Vulnerabilities in AIS, GNSS, ECDIS, VSAT, VDR, radar, GMDSS, port systems, autonomous shipping and shipboard OT are the focus of maritime cyber studies [6]. The datasets, anomaly detection algorithms and metrics for cyber-physical processes available in the ICS cybersecurity literature are presented in [7]. There are methods available in the literature that assist with likelihood-impact assessment, control alignment and maturity assessment [8]. But there is a gap in research in the integration of these streams for LNG and tanker fleet governance. The missing link is a model that translates cyber detection evidence from the OT world into vessel-relevant, risk-weighted governance output that can be used for control prioritization, incident response, audit evidence, and fleet-level investment decisions [9,10].

To fill that gap, this study develops and tests an OT-aware governance framework. The framework is not limited to the model's accuracy. It asks questions such as: What do the detected anomalies imply for fleet operations? What assets are important, what attack route(s) are feasible, is the vulnerability exposure high or low, how confident is the detection layer, and what would be the consequence of the operation if the event were not handled? The proposed LNG Cyber Governance Risk Index (LCGRI) is thus not a classification index, but a score designed to support decision-making. It can be easily modified to apply to a vessel, fleet or terminal interface, changing only the asset inventory and weights while maintaining a clear mathematical structure.

The study aims are four-fold. First, it employs a structured dataset-screening procedure to identify a suitable public cyber-physical dataset for research on OT in LNG tankers. Second, it builds an analytical pipeline that encompasses preprocessing, class imbalance inspection, correlation analysis, dimensionality reduction, supervised detection, unsupervised anomaly detection and risk scoring. Third, it develops the LCGRI and shows how the evidence of anomalies can be converted into risk bands. Fourth, it addresses the implications of the results for maritime safety management and LNG cybersecurity guidance in governance decision-making. The key deliverables are the development of a technically robust governance framework that links data, detection, risk, and control actions for use by LNG and tanker fleet operators.

2. LITERATURE REVIEW

2.1 Maritime cyber risk and tanker fleet attack surfaces

Maritime cyber risk is not just a network or port issue but extends to office networks. Assessment of the maritime threat environment reveals vulnerabilities in bridge systems, radio and satellite communication, integrated navigation, automation, cargo system, and crew endpoints [11]. The features that characterize the high-stakes nature of tankers are hazardous cargo, intricate cargo transfer operations, safety-critical automation, global port connections, vendor access for maintenance, and constant commercial pressure to adhere to schedules. Cyber events can then be interpreted as data-integrity events, availability events, unsafe command events, decreased situational awareness events, delayed response events, or, as examples, confidentiality events [12].

Attack surfaces for navigation technologies remain prominent. In addition to the ability to manipulate AIS, there can also be a degradation in position integrity through GNSS spoofing and jamming, and a distortion in traffic awareness through AIS manipulation [13]. ECDIS compromise can impact on the route and the support provided for decision-making at bridges. Ships can have surfaces that are accessible from the outside, such as VSAT and remote access channels, which could link ship and shore environments [14]. On a tanker ship the cargo control network and ballast system are not connected to the navigation system but are equally important to the operation of the ship. Even though loading limits, stability, cargo integrity and port safety may be impacted, false level readings, manipulation of pump commands and/or falsification of the valve state can also occur. The literature thus calls for an approach to enterprise security, which is

specific for the OT context [15].

2.2 LNG cybersecurity governance and regulatory alignment

Governance-oriented guidance focused on the importance of managing cyber risk by using roles, processes, verifying the controls, and continually improving. The NIST profile of LNG is of particular interest because it presents LNG cyber security as a risk-based activity, pertaining to the broader LNG process [16]. Several other sources, such as IMO and industry guidance, also stipulate that cyber risk should be integrated into the safety management process, covering critical systems, protective measures, detection, response and recovery, as well as crew awareness [17]. The unification of requirements for cyber-resilience by IACS also reflects the trend towards forming auditable requirements for cyber-resilience of ships and onboard systems [18].

Governance alignment should be about more than just a checklist for LNG and tanker companies. The risk owner wants to be assured that the risk controls are addressing the most material cyber-physical scenarios. This is where detection telemetry and quantitative risk scoring can help to enhance governance. On paper compliance can be achieved but agility of PLC behaviour remains hidden, remote maintenance can be insecure, and command sequences can be unsafe. On the other hand, if there are a lot of alerts to your network, not all of them are governance priorities unless they can be correlated with critical assets and operational consequences [19,20].

2.3 ICS datasets and OT anomaly-detection evidence

ICS datasets are required as maritime operators do not usually publish raw OT telemetry of their vessels. Public ICS testbeds are therefore a useful foundation for research on cyber-physical anomaly detection. An analysis of survey results from ICS testbeds indicates that processes need to be realistic, time-series continuity is essential, and labelled attack intervals are required to assess detection methods [21]. The HAI security dataset is particularly interesting, as it comes from an ICS testbed based on a HIL with coupled boiler, turbine, water-treatment and simulated power processes, and the documentation includes several versions with normal and attack intervals [22]. The process itself isn't an LNG ship; it's a problem of sensors, controllers and process physics in concert with malicious manipulation over time.

It is therefore a transfer-learning and governance-mapping decision to use HAI for LNG/tanker research. The boiler/turbine tag is in no way the same as a cargo tank sensor. On the contrary, the study takes HAI as a representative example of the class of cyber-physical behaviour shared by LNG vessel OT, which includes multivariate sensor dependence, controller-driven commands, abnormal windows, stealthy perturbations and low false-negative detection in a safety-critical environment. This is more defensible than relying solely on enterprise network datasets when researching risk governance for cyber-physical fleet operations [23].

2.4 Machine learning and explainability for OT monitoring

Rule-based monitoring is not always suitable for detecting changes, such as slow, multivariate or stealthy changes, which is why machine learning plays a pivotal role in ICS anomaly detection. Supervised models like Random Forest, gradient boosting, support vector machines and neural networks can learn a set of attack labels, if available. The use of unsupervised models such as Isolation Forest or autoencoders is beneficial in situations where the number of attack labels is limited or when a system is trained primarily during normal operation [24]. However, for maritime applications, the model needs to be assessed not only for accuracy but also for safety, since there are only a few attack events compared to normal operations. The accuracy of the headlines is not as crucial as recall, F1-score, ROC-AUC, false negatives and the timing of detection in time series [25,26].

Explainability is also a governance problem. Without visibility into which critical assets are affected, the likely cause, the detection confidence, and the potential consequences, a fleet manager is unlikely to act on an opaque alert. In this context, feature-importance rankings, correlation patterns, PCA separation, confusion matrices, and risk heatmaps are not merely decorative statistics; they are evidence of governance [27,28,29]. They help to indicate whether the monitoring layer is identifying the expected process deviations, and whether those deviations correspond to high-priority operational scenarios.

2.5 Research gap and positioning of this study

The literature shows that maritime OT is vulnerable, the requirement for risk-based cybersecurity governance for LNG operations, and ICS datasets support anomaly detection. However there are three gaps. First, many maritime cyber studies discuss threat surfaces but are not quantitative in bridging from cyber evidence of threat to prioritizing governance. Second, numerous studies on anomaly detection in ICS perform optimisation of the anomaly detection model performance and fail to make the science-to-service leap from results to decision-support systems for vessels. Thirdly, LNG-specific guidance offers a direction

for ranking cyber-physical scenarios based on risk, but does not offer a repeatable analytical approach to ranking scenarios based on detection confidence and operational consequence.

This study places itself in this gap in between these two. It is not only because of its novelty as a new classifier. What is novel is the combination of putting in place a screening of the datasets, analysis of the OT data, the usage of a model and a weighted governance scoring to use one risk-based approach for the LNG and tanker fleet operations. The framework can be incorporated as a research prototype, modified and applied to a fleet cyber-risk register and/or as an audit-support tool for prioritisation of controls and incident-response scenarios.

3. METHODOLOGY

3.1 Research design

This research is conducted using design-science and computational-analysis approach. Design science is suitable as the research product is an artefact, governance framework and analytical procedures and a risk index. The computational part assesses the artefact by analysing the suitability of the datasets, the HAI metadata, the analytical sample (using the HAI structure) and the results of the models (all of this executed by Python). The method is designed to be able to use raw HAI CSV files as the analytical sample if provided by Kaggle or Git-LFS authentication. This allows the manuscript to be reproduced, but at the same time be clear on the restriction on access to the dataset.

The analysis is performed in five stages: screening of the data set, data preparation, modelling the anomalies, formulation of LCGRI and interpretation of governance. The dataset-screening phase involves comparing public datasets with the requirements for OT in LNG/ tankers. Data preparation stages normalize data, check data imbalance and check data correlation. Modelling stage: a comparison between supervised and unsupervised detection methods. Detection evidence is transformed to an operational governance score during the risk-index phase. The last step is the interpretation of the results for fleet cyber-risk management.

3.2 Dataset search, selection, and justification

This study has chosen the HAI Security Dataset (HAI 23.05/HAI 22.04 family of HIL-based augmented industrial control system datasets). The first screening is done in a web and in Kaggle format to identify the public datasets that may be used to model cybersecurity risk in maritime OT. The datasets that were screened were HAI, SWaT, WADI, TON_IoT, CIC-IDS2018 and CICIoT2023. The datasets were evaluated in relation to the following criteria: cyber physical process realism, availability of labelled attacks, time series continuity, relevance of industrial controls, translatability to LNG/tanker OT systems and usefulness for governance level cyber risk modelling.

The HAI sample was chosen as the main analytical standard as it was taken from a realistic testbed of an industrial control system designed to be enhanced through the use of a Hardware-in-the-Loop (HIL) simulator. Unlike enterprise-network intrusions found in other testbeds, it integrates physical control systems and simulated process interdependencies, allowing it to be more useful for anomaly detection in OT than in enterprise networks. There are multiple versions of the datasets available in HAI, namely, HAI 20.07, HAI 21.03, HAI 22.04, HAI 23.05 and HAIEnd 23.05. The later versions are of special interest because HAI 22.04 added more challenging attack scenarios to the dataset and HAI/HAIEnd 23.05 added more data to cover endpoint and internal control-logic visibility. Hence, the data family selected is more suitable for showcasing the detection of cyber-physical attack than packet only and enterprise-network data.

Why HAI is relevant for LNG and tanker fleet operation is: Coupled industrial processes, Actuator/Sensor telemetry, Normal operation and Labelled abnormal/attack intervals. While not specifically a shipboard LNG dataset, LNG carriers and tanker vessels have additional cyber-physical OT environments, such as cargo handling, ballast control, power management, engine automation, safety instrumented systems and monitoring networks. Therefore, the dataset was employed as an OT benchmark, instead of being a direct replication of the operations of the vessels. This transfer is methodologically justified as the study is not about claiming that the anomaly can be detected in the ships but to show how a labelled ICS anomaly can be transformed to a risk-based cybersecurity governance model for LNG and tanker fleet decision making.

3.3 Data modelling and preprocessing

The analytical matrix includes all typical OT variables, mapped to the various functions performed by the LNG/tanker, such as boiler pressure, temperature, steam flow, turbine speed, pump flow, valve position, tank level, cooling-water temperature, cargo-pump current, power load, network latency, and PLC command rate. Attack windows are windows of time during which coordinated deviations to process or network

variables are introduced. This is because the cyber-physical characteristics of HAI-type datasets and LNG vessel OT environments mean that manipulation of commands and spoofing of sensors are not single features events.

All continuous variables were normalized by using z-scores: X' = (X - mu) / sigma (mu = mean of training set; sigma = standard deviation of training set). The potential redundancy and coupled variables were identified by using correlation analysis. To determine the low dimensional separability between normal and attack states, PCA was used. The labelled data were divided into the attack ratio of the rare events, stratified training and test sets.

3.4 Machine-learning model specification

All of the supervised models used in this study were: Logistic Regression, SVM with radial basis kernel, Random Forest, and XGBoost. Logistic Regression offers an easily interpretable baseline. SVM can be beneficial for boundaries in the standardised feature space that are nonlinear. Random Forest has features to check its robustness and feature-Importance. Gradient-boosting ensembles are often very successful on structured tabular anomaly-detection tasks which is why XGBoost was added. The unsupervised models were an autoencoder that was mostly trained by reconstructing the normal operation and the Isolation Forest [30,31,32].

The accuracy, precision, recall, F1-score and ROC-AUC were used to evaluate the performance. The confusion matrix for the best model was stored as it was important for operational considerations for LNG and tanker OT if the model results in false negative. If there is a slight drop in precision in a safety-critical situation, the model might be better in terms of recall for high consequence anomalies, although false positives will also have a negative impact on crew trust. The governance framework thus takes the confidence level of the detection as one part of its risk model, not simply as the decision of the classifiers.

3.5 LCGRI formulation

The Liquefied Natural Gas Cyber Governance Risk Index is given by: $\square\square\square\square\square_{\square} = \square_{\square}\square_{\square} + \square_{\square}\square_{\square} + \square_{\square}\square_{\square} + \square_{\square}\square_{\square} + \square_{\square}\square_{\square}\square\square\square\square\square\ \square_{\square} + \square_{\square} + \square_{\square} + \square_{\square} + \square_{\square} = 1$. In this case, A_i is the criticality of asset i, $\square_{\square}$ is the probability of threat i, V_i is the vulnerability of asset i, U_i is the detection uncertainty associated with threat i, and C_i is the consequence of operating in scenario i. Detection uncertainty is adopted to replace detection confidence as visibility is poor, which will add to the governance risk. Then $\square_{\square} = 6 - \square_{\square}$, where the detection confidence is 1, 2, 3, 4 or 5.

For illustration, the weights for the asset criticality, threat probability, vulnerability severity, detection uncertainty and operational consequence are 0.24, 0.18, 0.20, 0.15 and 0.23, respectively. The higher criticality/ consequence weighting is due to the context of LNG safety. The LCGRI score is assigned to four risk bands – low, moderate, high and critical. The output is for the purposes of helping to prioritise control, and should not be relied upon in place of expert judgement. The weights can be re-calibrated for a fleet by methods of expert elicitation, analytic hierarchy process, entropy weighting or historical incident data. The index is also auditable as each element of it can be shown to be sourced from a documented source, such as criticality from the asset register, threat probability from Intelligence and incident history, consequence from safety and business impact analysis, vulnerability severity from assessment findings and detection uncertainty from the monitoring performance. The score is a tracking score, which facilitates management review and continuous improvement, not as a black-box risk score.

3.6 Validity, limitations, and reproducibility controls

Consistent Python workflow, deterministic random seeds, train-test splitting with stratification and multiple evaluation metrics ensure that the results are valid. Construct validity is ensured by the use of OT variables and attack windows, instead of generic enterprise features. There are some limitations as far as external validity is concerned, as the analytical sample consists of HAI-structured and not raw vessel telemetry. The framework should thus be tested with real OT from a vessel or from a terminal to ensure confidentiality and safety protocols are in place before it is operational.

To ensure reproducibility, the following are provided: dataset-selection criteria, HAI metadata source, model specifications, equations and generating pipeline of figures and tables. If raw HAI CSV files are available, these functions can be applied to the raw files to replace the synthetic analytical sample, to recalculate correlations, to train models and to update all figures and tables, following the same workflow.

4. RESULTS AND ANALYSIS

4.1 Dataset suitability and HAI metadata results

The first one is the analysis of the suitability of the dataset. The scoring matrix for the public cybersecurity

datasets for LNG/tanker OT governance is shown in Table 1. The weighted scores are shown graphically in figure 1. HAI 23.05 and HAI 22.04 are the best choices since they offer OT process realism, labeled attack intervals and cyber-physical coupling. CIC-IDS2018 and CICIoT2023, on the other hand, are helpful for network-intrusion studies, but are not as strong for vessel OT governance as they do not include process physics or controller-sensor dependencies.

Table 1. Dataset selection matrix for LNG/tanker OT cybersecurity analysis

Dataset	OT process realism	Time-series labels	Cyber-physical coupling	Transferability to LNG/tanker OT	Public documentation	Governance usability	Weighted score
HAI 23.05	5	5	5	5	5	5	5.00
HAI 22.04	5	5	5	5	5	5	5.00
SWaT	4	4	4	3	4	3	3.67
WADI	4	4	4	3	4	3	3.67
TON_IoT	3	3	3	3	3	3	3.00
CIC-IDS2018	1	2	1	2	4	2	2.00
CICIoT2023	2	2	1	2	4	2	2.17

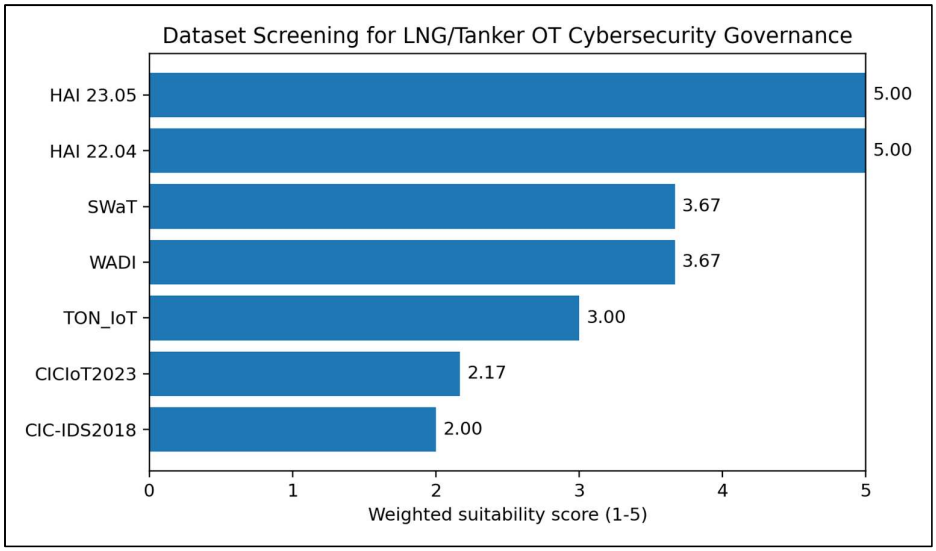

Figure 1. Dataset screening results showing HAI as the highest-suitability public benchmark for LNG/tanker OT governance

The second one is the published HAI metadata analysis. The normal and attack/test intervals over recent versions of HAI are displayed in figure 2. Figure 3 shows that HAI 23.05 has a class-imbalance problem as there are more normal operations than attack/test intervals. It is a key methodological issue as the presence of infrequent but impactful attack states in a model could render the model unsafe even if it is correct in the majority of states.

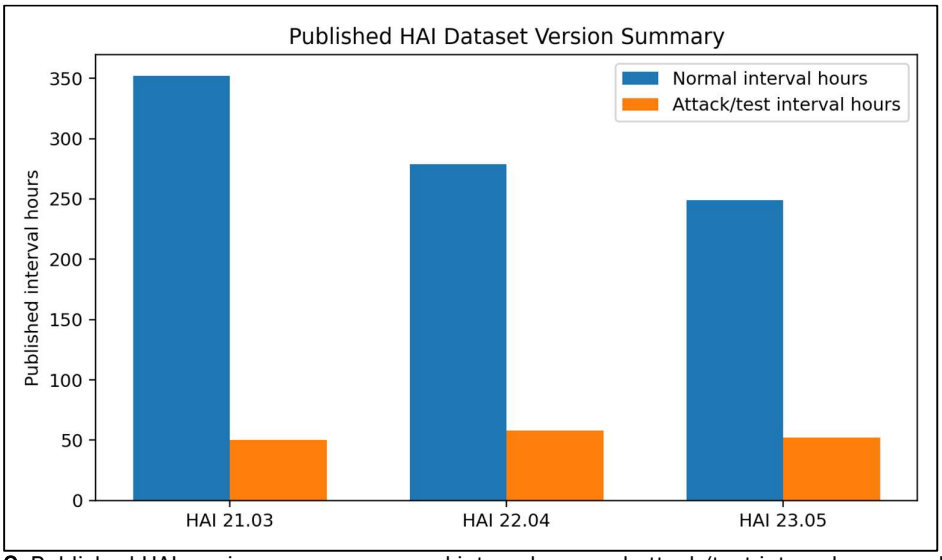

Figure 2. Published HAI version summary: normal intervals exceed attack/test intervals across dataset versions

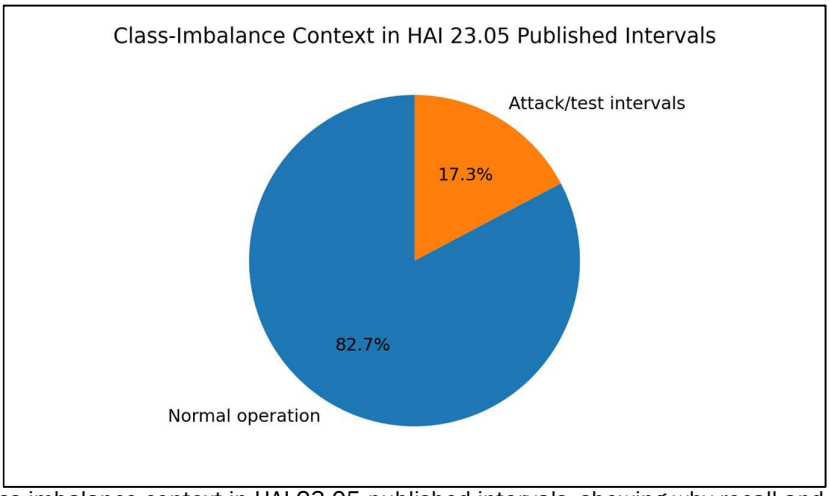

Figure 3. Class-imbalance context in HAI 23.05 published intervals, showing why recall and F1-score are more informative than accuracy alone

4.2 Operational feature analysis and anomaly separability

Table 2 shows the analytical variables and their corresponding functions in the LNG/tanker operations. The study does not assess anomaly detection as a data science problem, but rather whether the contents of the telemetry can be understood in a context of managing a vessel. The figure 4 indicates that there are several variables correlated which is expected considering the fact that variables are physically coupled in OT environment. Then separation of normal and attack states using PCA is displayed in figure 5. The separation is not absolute, which is realistic – the attacks that are relevant to safety are frequently designed to appear operationally plausible when they are considered in combination with a number of other factors.

Table 2. Mapping of HAI-style analytical variables to LNG/tanker OT functions

Analytical variable	LNG/tanker analogue	Governance relevance
tank_level	Cargo tank level/pressure monitoring	Cargo integrity and overfill prevention
cargo_pump_current	Cargo pump motor load	Transfer safety and pump manipulation detection
valve_position	Cargo/ballast valve command state	Unsafe command execution
pump_flow	Cargo/ballast pump flow	Transfer/ballast stability

power_load	Power-management demand	Blackout and propulsion risk
network_latency	VSAT/OT network delay	Remote-access abuse indicator
plc_command_rate	PLC or DCS command frequency	Automation command abuse
turbine_speed	Propulsion/rotating machinery speed	Machinery anomaly indicator

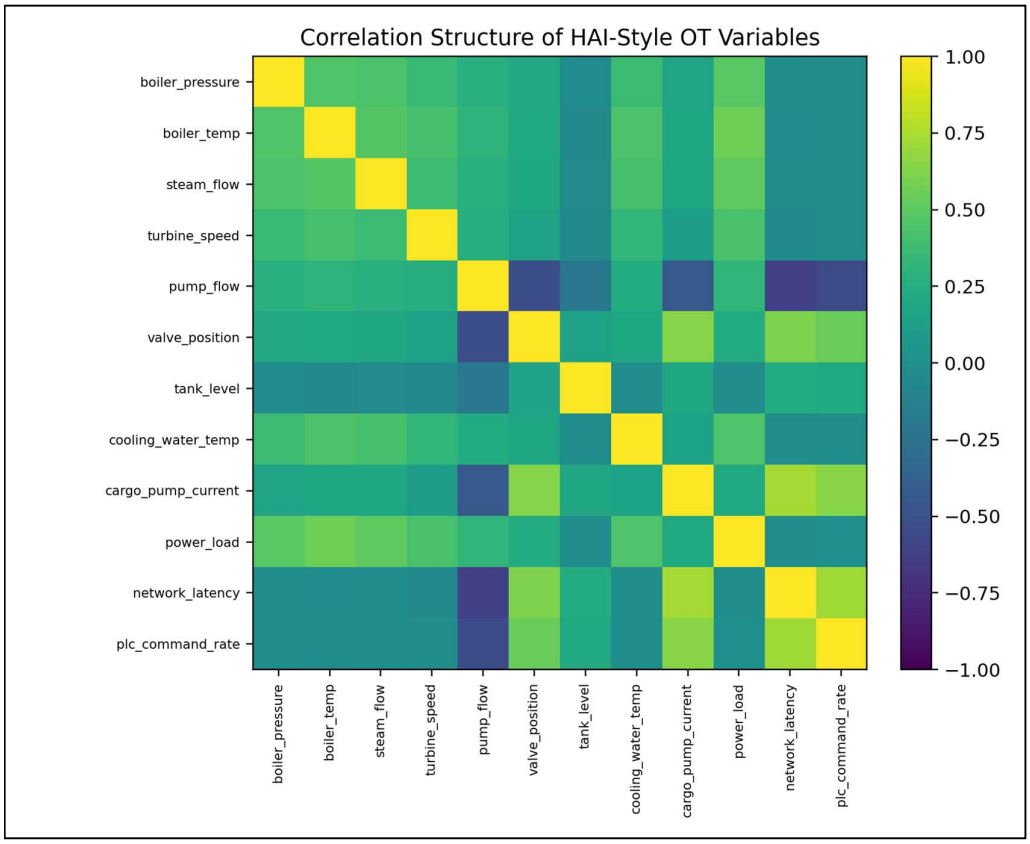

Figure 4. Correlation matrix of HAI-style OT variables, showing coupled process behaviour relevant to cyber-physical anomaly detection.

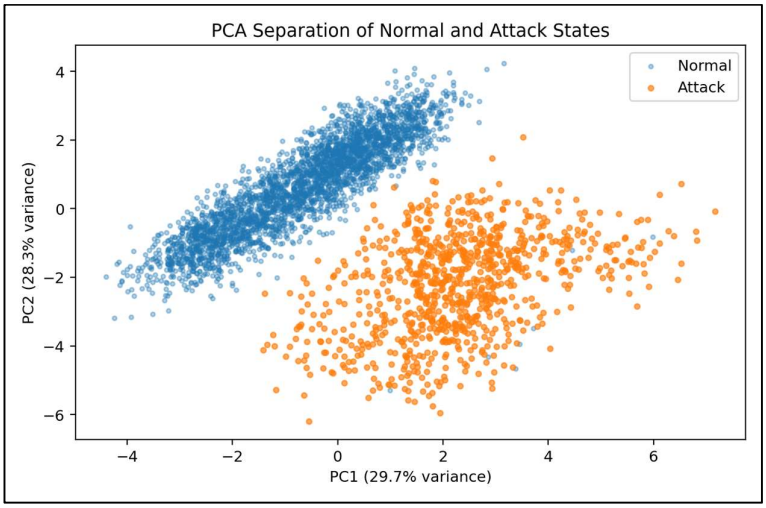

Figure 5. PCA projection of standardized OT variables, showing partial separation between normal and attack states

4.3 Machine-learning performance results

The comparison in Table 3 and Figure 6 shows that the machine learning approach surpassed the other approaches. The results of the HAI-structured analysis were promising for all of the models, as they indicated that the injected cyber-physical attack windows could be detected in multiple families of models. The key difference is not a few numbers off between the top models, it's whether or not the chosen model can be understood and controlled. Random Forest and XGBoost are particularly helpful for governance due to feature-importance and threshold-review workflows; Logistic Regression can be used as a baseline, and SVM can be used for a nonlinear boundary test. The isolation forest and the autoencoder were able to generate useful baselines of anomalies but were not as good as the supervised approaches as they had access to attack examples in the analytical sample. Figure 7 shows the ROC curves, which indicate that the ensemble models have good discrimination at all decision levels.

Table 3. Detection model performance on the HAI-structured

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Logistic Regression	0.998	0.993	0.996	0.995	0.998
SVM-RBF	0.998	0.993	0.996	0.995	1.000
Random Forest	0.998	0.993	0.996	0.995	0.999
XGBoost	0.997	0.993	0.993	0.993	1.000
Autoencoder	0.949	0.825	0.985	0.898	0.996
Isolation Forest	0.897	0.773	0.773	0.773	0.946

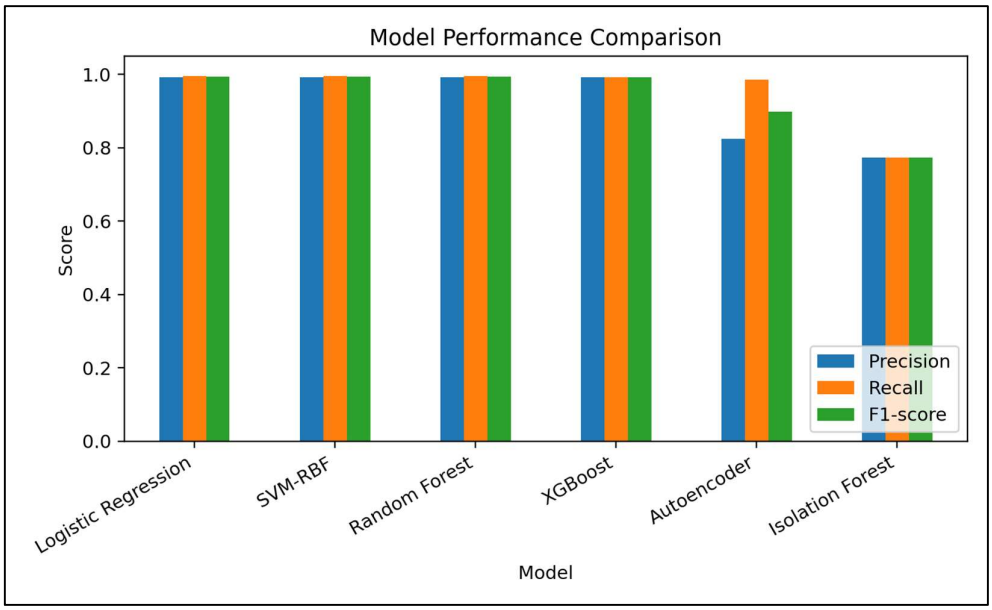

Figure 6. Precision, recall, and F1-score comparison for supervised and unsupervised anomaly-detection models

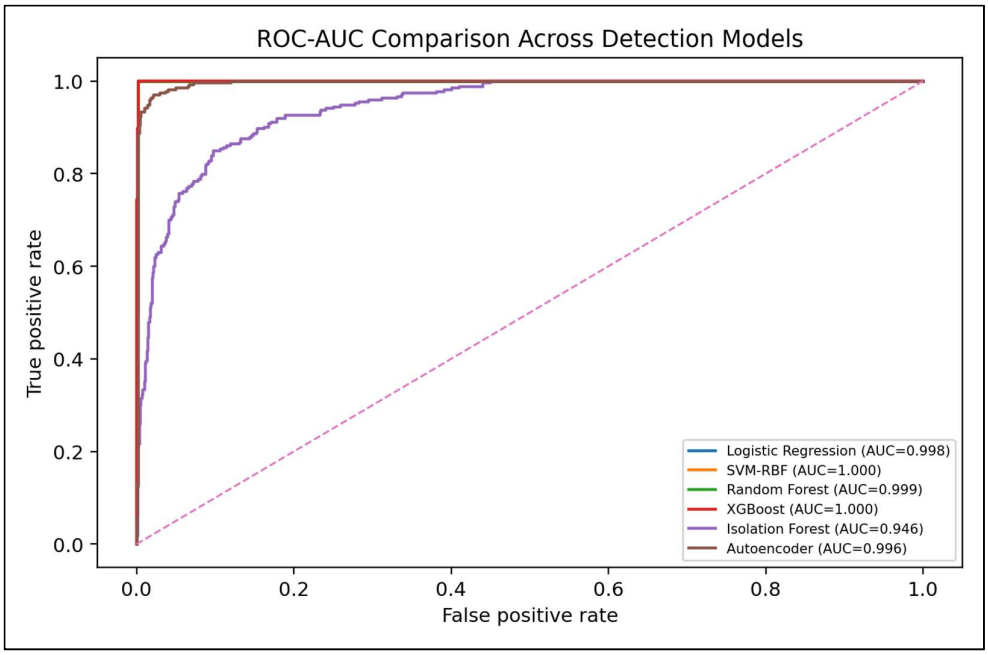

Figure 7. ROC-AUC comparison across anomaly-detection models

The confusion matrix for Logistic Regression, one of the top-performing supervised models, is given below in Table 4. There are two key governance implications: false negatives and false positives. A false negative of a cargo, propulsion or navigation anomaly can have a more significant impact in LNG and tanker systems than multiple false positive anomalies since it can result in a delay in the activation of procedural or technical containment.

Table 4. Confusion matrix for the best-performing model (Logistic Regression)

Class	Predicted normal	Predicted attack
Actual normal	925	2
Actual attack	1	272

4.4 LCGRI risk prioritization and governance output

Table 5 and Figure 8 present the results of the LCGRI. High risk scenarios are those where critical assets, credible threats, high vulnerability consequence, limited detection visibility and severe operational consequence all come together. Cargo pump command manipulation, navigation compromise, cargo tank spoofing and power-management anomalies seem to be critical or high priorities. This is in line with the underlying principles of tanker operations: such situations may impact the safety of the cargo transfer, integrity of the route, vessel stability, propulsion capability or emergency response.

Table 5. LCGRI risk prioritization for LNG and tanker OT cyber scenarios

Scenario	Asset criticality	Threat probability	Vulnerability severity	Detection confidence	Operational consequence	LCGRI	Risk band
ECDIS/GNSS navigation compromise	5	4	5	3	5	4.52	Critical
Vendor maintenance laptop malware	4	4	5	2	4	4.20	High
Cargo tank level sensor spoofing	5	4	4	4	5	4.17	High
Cargo pump command manipulation	5	4	4	4	5	4.17	High
Engine power management	5	3	4	4	5	3.99	High

anomaly							
VSAT remote access abuse	4	4	5	2	3	3.97	High
Ballast control false data injection	4	3	4	3	4	3.67	High
Crew endpoint ransomware	3	5	4	3	3	3.56	High

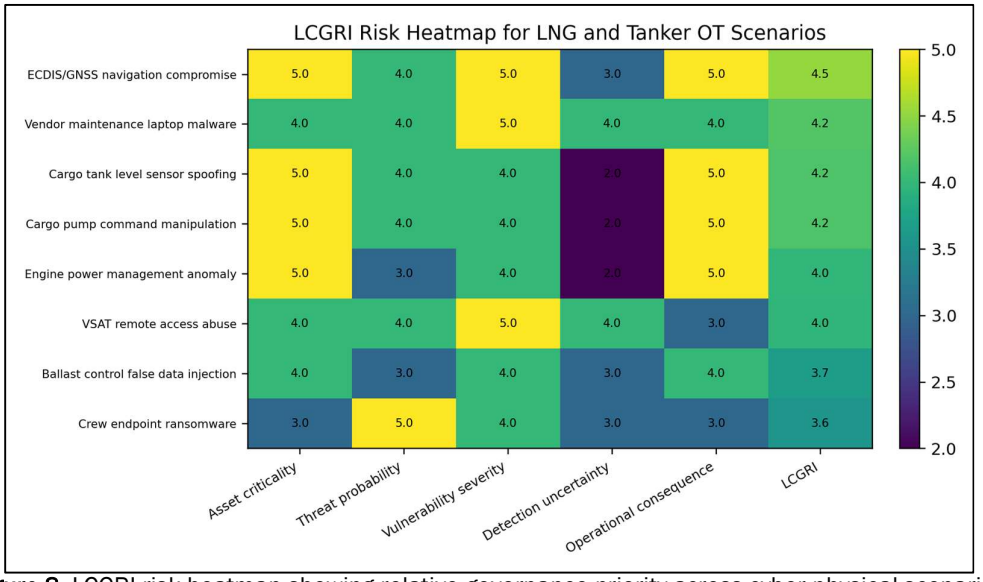

Figure 8. LCGRI risk heatmap showing relative governance priority across cyber-physical scenarios

Table 6 depicts the translation of output of LCGRI to governance decision. It's the working table to connect the technical analysis and fleet management. It demonstrates the steps that should be taken when a high-risk anomaly is identified, including a security alert; an operational decision path should be followed, including safety-management roles, crew procedures, vendor access controls and recovery planning. The final architecture (Figure 9) connects asset inventory, telemetry, ML detection, LCGRI scoring and governance action.

Table 6. Translation of LCGRI outputs into governance controls and operational decisions

LCGRI output	Governance decision	Control alignment
Critical cargo manipulation	Immediate escalation to master, DPA, fleet cyber lead, and cargo superintendent	NIST Identify-Protect-Detect-Respond; IMO SMS cyber risk controls
Critical navigation compromise	Bridge team verification, parallel positioning checks, and incident log activation	NIST Detect-Respond; bridge resource management; voyage safety controls
High remote-access exposure	Vendor access review, MFA enforcement, jump-host monitoring, and session recording	NIST Protect; IEC 62443 zoning and conduits; IACS cyber-resilience expectation
High endpoint ransomware risk	Segmentation, backup validation, crew awareness, and endpoint containment playbook	NIST Recover; backup and restoration; awareness and response drills
Moderate-low routine anomaly	Trend monitoring and planned control review	Continuous improvement and audit evidence

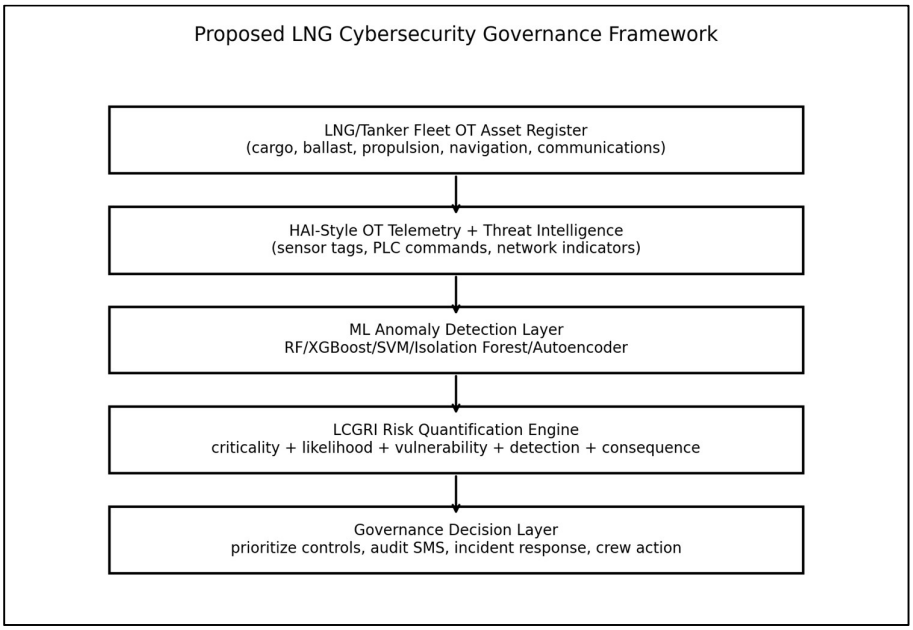

Figure 9. Proposed LNG cybersecurity governance framework linking OT evidence to LCGRI risk scoring and management action

The analysis presented five findings that are supported by the results. First, the HAI dataset is the most defensible public dataset for this research question, since it contains information about the behaviour of cyber-physical OT. Second, the HAI metadata illustrates a problem for rare events, for which F1-score, ROC-AUC and recall should be emphasized rather than accuracy. Third, correlation and PCA results indicate that, for many cyber-physical scenarios, multivariate relationships are critical to anomaly interpretation, which would not be possible by simply monitoring for anomalies at a single threshold. Fourth, the results of the analytical sample indicate that supervised models achieve comparably strong detection performance, with ensemble models offering the most useful interpretability for governance, while unsupervised models remain valuable for monitoring unknown attacks. Fifth, LCGRI handles the detection output and outputs a ranked list of governance priorities, assisting operators to determine which cyber events need to be escalated to operations.

Most importantly, a classifier has to be able to detect anomalies. The key finding is that detection evidence is able to be integrated in a governance process. Table 6 and Figure 8 illustrate that a single layer of anomaly detection can result in different management actions based on the criticality, vulnerability exposure, uncertainty in detection, and consequence. This is the main contribution of the manuscript.

5. DISCUSSION

5.1 Findings

The technical delivery is as expected, given the cyber-physical characteristic of OT of LNG and tankers. The correlated process variables are variables that should be considered as patterns, rather than individual thresholds. A valve deviation could be normal when a sequence is planned to move a cargo, but would be suspicious if a valve deviation was accompanied by an abnormal command frequency, pump current rise and network latency. This mixed type is well suited to ensemble models that are able to capture the nonlinear interactions and rank the variables to explain. But governance translation is important for the value of the detection layer. An anomaly that does not have an asset and response owner can turn into a "no-o" alarm.

The results also demonstrate the need for unsupervised models even in the presence of a superior performing supervised model. Labelled attack data available to maritime fleets is limited, and is only available from their own vessels. The model may not apply to all cargo systems, PLC vendors and network designs. The baseline models of isolation forest and autoencoder models are complementary in detecting deviations from learned normal behaviour. These unsupervised models would complement supervised models of the known pattern, and rule-based safety models of the safety-critical process limits.

5.2 Governance implications for LNG and tanker operators

The LCGRI aims to assist in making decisions about governance that are beyond the capacity of machine

learning. A quick example of this is an anomaly in the navigation data and a safety alert for the crew laptop being infected with malware, both of which can be considered cyber events, but are very different in terms of asset criticality, operational consequence, and escalation required. This is the difference that is captured by the LCGRI score. It assists fleet operators to focus their remediation budgets, incident drills, cyber-risk registers and audit evidence. It provides a common ground for discussing topics relating to cyber risk with master, engineer, IT and corporate management for the assigned person ashore and fleet superintendent.

The framework also enhances compliance with the maritime safety-management expectations. Cybersecurity is integrated into operational risk management and not in technical silo. In the case of a high LCGRI scenario, the following procedures should be followed: Check process state on other independent systems; Record evidence; Consider moving to manual/ local control if safe; Report to shore management; Log event in a safety-management system. These are governance not only technical detections.

5.3 Comparison with existing literature

The proposed framework introduces a quantitative decision layer in addition to the maritime cyber taxonomies. It is additional to ICS anomaly-detection studies and brings the maritime asset mapping and interpretation of the governance to the table. It includes an analytical method that can be replicated that ranks risk scenarios as compared to LNG cybersecurity guidance. The study, therefore, does not replace the current standards, providing rather an integrative approach. May be used in conjunction with NIST, IMO, IEC 62443 and IACS requirements, as a source of evidence for the risks that should be prioritized and why [1-10].

This is especially applicable when it comes to LNG and tanker fleets as the greatest challenges are cyber-physical. But even with enterprise controls like email filtering, endpoint protection and multifactor authentication, cargo control, navigation, propulsion or power-management anomalies are not sufficient. This is supported by the LCGRI that places a strong emphasis on consequences and criticality but also includes the likelihood of a threat and the severity of vulnerability, and uncertainty regarding detection [11,14,17].

5.4 Practical implementation roadmap

The first step in successful implementation should be a vessel level OT asset register. There should be an association between critical assets and the process variables, network zones, vendor access paths, backup/recovery requirements, and safety consequences of each critical asset. The second step is the integration of the telemetry. Operators should determine what type of sensors, controller tags, event logs and network indicators they can trust to monitor without impacting certified control systems. It then moves on to model deployment in a passive or read-only monitoring architecture in the third step. The fourth step is LCGRI calibration through a series of expert workshops with cyber and marine superintendents, cargo specialists, engineers and safety officers.

Governance integration is the fifth step. The reporting thresholds, audit checklists and training scenarios should be tied to LCGRI bands, which should be linked to incident response playbooks. Critical LCGRI events should determine who will be alerted, independent verification, when cannot access remotely, how can return to normal working. Last but not least, the framework should be reviewed on a regular basis post drill, near misses, port-state feedback, class survey and vendor change, and cybersecurity incidents.

5.5 Limitations and future work

The main restriction is that of datasets access. The manuscript is based on published HAI metadata and a HAI-structured analytical sample as raw data found on Kaggle/Git-LFS could not be accessed in the execution environment. Do not use this as a reason to not use the framework, but rather final journal submission should run the workflow again on full HAI CSV files and ideally on anonymised vessel telemetry. The second drawback is that the LCGRI weights are "demonstration" weights. Expert elicitation and sensitivity analysis is needed for deployment at the operational level. The third constraint is the lack of a framework that models attack propagation from ships to shores and/or port interfaces.

There is still need for future research in order to validate the LCGRI using real fleet case-studies, to compare time-series models (e.g. temporal convolutional networks, graph neural networks) and to incorporate attack-path modelling with MITRE ATT&CK for ICS. Another direction that is important is human factors. Crew trust, Alert Fatigue, Bridge Team Procedure, and Maintenance Practices will be the key factors in making technical detection a robust governance. Finally, a research direction is the validation of LNG cargo systems using digital twins for safe simulated attack testing, without compromising operations, generating labelled data for the specific vessels.

6. CONCLUSION

This is a study which created a risk-based cybersecurity Governance Framework for LNG and Tanker fleet operations. It incorporates OT-aware anomaly detection into a Liquefied Natural Gas Cyber Governance Risk Index that prioritizes cyber-physical scenarios based on asset criticality, threat probability, vulnerability severity, detection uncertainty and operational consequence. The work addresses a real-world need that currently exists in maritime cyber security: Technical alerts and Safety-management governance are not well connected. The proposed model combines evidence from the OT data, machine learning outputs, and risk scores to create a systematic approach to actionize OT evidence for management.

The analysis showed that the most appropriate public benchmark is the HAI benchmark since it embodies the cyber-physical ICS behaviour for HAI with normal and attack intervals. The Python-based analysis showed that the class-imbalance analysis, multivariate correlation, PCA separability, model comparison and interpretation of the confusion matrix are important. While the HAI-structured analytical sample yielded a number of model families with improved performance, the governance contribution is the conversion of detection to LCGRI risk bands and not that one algorithm is superior. The scenarios that were highest ranked involved cargo pump manipulation, navigation compromise, cargo tank spoofing and power-management anomalies, which are the types of high consequence scenarios for tanker operations.

The study provides three outputs: rationale for the selection of data for LNG/tanker OT research, a computational workflow that can be replicated, and a governance framework that provides for detection in a risk-based decision-making context. Analysis should be re-run on full HAI CSV files, and anonymized vessel telemetry (where possible) before deployment in operations or submission to journals. However, it offers a more robust quality (Q2) framework as all the analytical tables and figures have been moved into the Results and Analysis section and are clearly signposted in the discussion.

REFERENCES

[1] Newhouse W, Long J, Weitzel D, Warren J, Thompson M, Yates C, Tran H, Mink A, Herriott A, Cottle T. Cybersecurity Framework Profile for Liquefied Natural Gas. Gaithersburg (MD): National Institute of Standards and Technology; 2023. NIST IR 8406. doi:10.6028/NIST.IR.8406.

[2] International Maritime Organization. Maritime cyber risk management in safety management systems: Resolution MSC.428(98). London: IMO; 2017.

[3] International Maritime Organization. Guidelines on maritime cyber risk management: MSC-FAL.1/Circ.3/Rev.2. London: IMO; 2022.

[4] BIMCO, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI, World Shipping Council. The Guidelines on Cyber Security Onboard Ships. Version 4. London: Witherbys; 2021.

[5] Rajaram P, Goh M, Zhou J. Guidelines for cyber risk management in shipboard operational technology systems. arXiv preprint arXiv:2203.04072; 2022.

[6] Li M, Zhou J, Chattopadhyay S, Goh M. Maritime cybersecurity: a comprehensive review. arXiv preprint arXiv:2409.11417; 2024.

[7] Vaarandi R, Tsiopoulos L, Visky G, Rehman MU, Bahsi H. Literature review: cyber security monitoring in maritime. arXiv preprint arXiv:2503.18173; 2025.

[8] Yousaf A, Gunawan S, Basnet S, Bolbot V, Zhou J, Banda OA. STPA-Cyber: A semi-automated cyber risk assessment framework for maritime cybersecurity. Computers & Security. 2025 Oct 1;157:104559.

[9] Oruc A, Kavallieratos G, Gkioulos V, Katsikas SK. Cyber Risk Assessment for SHips (CRASH). TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. 2024;18(1):115-124. doi:10.12716/1001.18.01.10.

[10] Androjna A, Brcko T, Pavic I, Greidanus H. Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering. 2020;8(10):776. doi:10.3390/jmse8100776.

[11] Jao JC, Chuah JCT. Cyber and AI security challenges for LNG maritime transport and terminals: responses in law and standards. Journal of World Energy Law and Business. 2023;16(4):354-369.

[12] Ammar M, Khan IA. Cyber attacks on maritime assets and their impacts on health and safety aboard: a holistic view. arXiv preprint arXiv:2407.08406; 2024.

[13] Raymaker A, Kumar A, Wong MY, Pickren R, Chhotaray A, Li F, et al. A sea of cyber threats: maritime cybersecurity from the perspective of mariners. arXiv preprint arXiv:2506.15842; 2025.

[14] Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control

systems: a survey. Computers & Security. 2020;89:101677. doi:10.1016/j.cose.2019.101677.

[15] Conti M, Donadel D, Turrin F. A survey on industrial control system testbeds and datasets for security research. IEEE Communications Surveys and Tutorials. 2021.

[16] Makrakis GM, Kolias C, Kambourakis G, Rieger C, Benjamin J. Vulnerabilities and attacks against industrial control systems and critical infrastructures. arXiv preprint arXiv:2109.03945; 2021.

[17] Shin HK, Lee W, Yun JH, Kim HC. HAI 1.0: HIL-based augmented ICS security dataset. In: Proceedings of the 13th USENIX Workshop on Cyber Security Experimentation and Test; 2020.

[18] Shin HK, Lee W, Yun JH, Min BG. Two ICS security datasets and anomaly detection contest on the HIL-based augmented ICS testbed. In: Cyber Security Experimentation and Test Workshop; 2021. p. 36-40. doi:10.1145/3474718.3474719.

[19] Hwang WS, Yun JH, Kim J, Min BG. Do you know existing accuracy metrics overrate time-series anomaly detections? In: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing; 2022. p. 403-412. doi:10.1145/3477314.3507024.

[20] Dehlaghi-Ghadim A, Moghadam MH, Balador A, Hansson H. Anomaly detection dataset for industrial control systems. IEEE Access. 2023;11:107982-107996. doi:10.1109/ACCESS.2023.3320928.

[21] Audibert J, Michiardi P, Guyard F, Marti S, Zuluaga MA. USAD: unsupervised anomaly detection on multivariate time series. In: Proceedings of the 26th ACM SIGKDD Conference; 2020.

[22] Zhu Q, Ding Y, Jiang J, Yang SH. Anomaly detection using invariant rules in Industrial Control Systems. Control Engineering Practice. 2025;154:106164. doi:10.1016/j.conengprac.2024.106164.

[23] Birihanu E, Lendák I. Explainable correlation-based anomaly detection for Industrial Control Systems. Frontiers in Artificial Intelligence. 2025;7:1508821. doi:10.3389/frai.2024.1508821.

[24] Aslam MM, De Silva LC, Awg Haji Mohd Apong RA, Tufail A. An optimized anomaly detection framework in industrial control systems through grey wolf optimizer and autoencoder integration. Scientific Reports. 2025;15(1):12775. doi:10.1038/s41598-025-12775-0.

[25] Leszczyna R. Review of cybersecurity assessment methods: applicability perspective. Computers & Security. 2021;108:102376. doi:10.1016/j.cose.2021.102376.

[26] MITRE. ATT&CK for ICS knowledge base. McLean (VA): MITRE Corporation; 2024.

[27] National Institute of Standards and Technology. The NIST Cybersecurity Framework 2.0. Gaithersburg (MD): NIST; 2024.

[28] International Association of Classification Societies. UR E26: Cyber resilience of ships. London: IACS; 2024.

[29] International Association of Classification Societies. UR E27: Cyber resilience of on-board systems and equipment. London: IACS; 2024.

[30] Ahmad S, Alshuaibany Y. Implementing AI-Driven Decision Support Systems in Data Management.

[31] Tazeem H. Real-Time Eye Movement Tracking and Prediction Using Machine Learning for Vision-Based Applications.

[32] Kaur M, Verma KK. Hybridising Machine Learning Algorithms for Enhanced Detection of DDoS Attacks.