Australasian Transport Research Forum 2025 Proceedings
18-21 November, Auckland, New Zealand
Publication website: https://australasiantransportresearchforum.org.au/

A maritime industry 4.0 approach to cybersecurity: A layered Digital Twin framework

Monty J Singh[1], Dr. Balwinder Sodhi[2]

[1]IIT Ropar

[2] IIT Ropar

Email for correspondence (presenting author): monty.21csz0005@iitrpr.ac.in

Abstract

The existing cyber-physical systems in the marine industry are a complex blend of IT, OT, and human-machine interfaces. These CPS can be upgraded to Digital twins by leveraging sensors, actuators, and analysis tools. Digital Twins are the backbone for applying Industry 4.0 standards to the shipping industry. They are used for real-time monitoring and control, predictive maintenance and enhanced safety, route optimisation, simulating different scenarios, etc. However, the rapid digitalisation of the marine industry has exposed the maritime asset landscape to different threats. To address this gap, this paper presents a cybersecurity risk assessment framework for marine digital twins using the MVC architecture. This framework will enable real-time threat detection, risk propagation modelling, and decision making for building a robust cyber space in complex multimodal networks. The DT layer uses Bayesian networks to model threat propagation. Probabilistic impact of cyber-attacks is assessed using Monte Carlo simulation. The controller layer uses AI-based anomaly detection and MITRE ATT&CK-based threat classification to activate mitigation responses. The view layer comprises a dashboard for threat visualisation. The approach is validated by simulating different scenarios of cyber-attacks. The proposed framework is a step forward in designing a scalable prototype for secure, intelligent maritime operations aligned with the vision of Industry 4.0.

1. Introduction

The application of industry 4.0 standards has revolutionised the marine industry. This transformation is driven by technological revolution, regulatory changes and a complex network of automated systems linking ships, ports and supply chains. A marine vessel can be considered to be an equivalent to a complex industrial plant, where different marine operations can be compared to conventional manufacturing plants. This increase in automation is facilitated using IoT, AI and intelligent software technologies like Digital Twins. Digital Twins are intelligent cyber physical systems that fuse engineering models with real-time data and digital technologies. The increasing encapsulation of marine assets with advanced digital technologies has widened the attack landscape, which has flagged serious cybersecurity concerns.

As per the World Economic Forum's Global Cybersecurity Outlook Report 2025 (Anon., 2025) "the cyber space is becoming more opaque, fragmented and unpredictable". For instance, recently, in 2024, The National Presto Industries suffered a cyberattack which operations and supply chain management; Similarly, The National Iranian Tanker Company (NITC) was targeted in 2021. The attack compromised the navigational data and disabled vessel tracking. Again in 2023, North Korea attacked South Korea with a series of cyber invasions aimed at disabling their marine logistic and defence system. These cyberattacks bring out the different geopolitical ambiguities, increasing cyber inequities and complex threat vectors in critical infrastructure that escalates the demand for a robust cyber-aware framework. As per the report, 54% of the organizations are

prone to supply chain attacks, where determining third party vulnerabilities and cyber-attack propagation are major concerns. 60% of the organizations are forced to reconsider their cyber security measures due to geopolitical issues. The advent of GenAI and AI has led to the introduction of new set of risks. 66% of the organizations have recognized the influence of cybersecurity on marine operations, while only 37% have appropriate safety measures in place. GenAI has led to an exponential increase in social engineered attacks like – phishing, ransomware, Piggybacking etc.

Table 1: Timeline of marine cybersecurity measures

Year	Security Measure	Focus Area	Standard
2002	ISPS Code	Physical Security	IMO SOLAS
2010s	Antivirus, firewalls	Basics of cybersecurity	ISO/IEC27001
2016	DNVGL RP-0496	Cyber risk resilience	DNV
2017	IMO MSC.428(98)	Cyber risk in management systems	IMO Regulations
2018	NIST CSF Recommendation	Cyber risk lifecycle	NIST Framework
2019	Cybersecurity Training	Human Factors	STCW updates
2020	MITRE ATT&CK	Threat Detection &Attacker behavior	MITRE ATT&CK
2021	Digital Twin Security	Virtual Model Integrity	ISO 23247
2022	AI/ML based anomaly detection	Predictive Cyber threat Detection	IDS/IPS
2023	Zero Trust Architecture	Access control, identity verification	NIST SP 800-207
Emerging	Blockchain, Quantum Security	Data integrity, Post Quantum Protection	PQC(NIST)

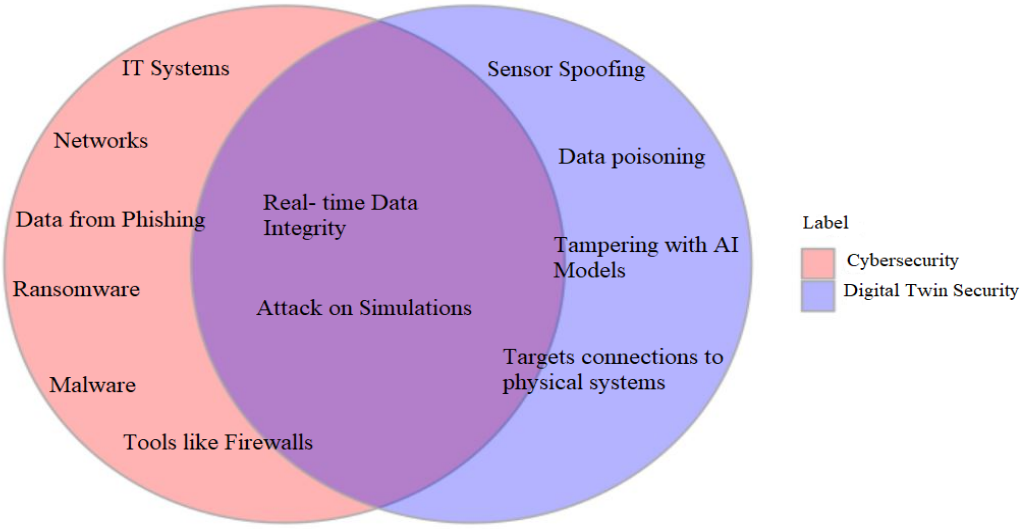
Though an extensive body of literature exists on the application of digital twin applications in the marine industry- such as for predictive maintenance, route optimisation, real-time monitoring, most of the works are application-specific, atomic and ignore associated cyber risks. To the best of our knowledge no works exists on the dynamic propagation of cyber risks across the digital twin architecture. Moreover, very few existing works use system level framework like- Model View Controller (MVC), that fulfils the primary requirements of a cyber physical system in marine industry- modularity, scalability, and maintainability. Furthermore, the conventional works have overlooked IMO guidelines, ISO27001, NIST etc., which are crucial for fulfilling regulatory scrutiny and risk fragmentation.

Table 1. defines the chronological order of security measures over the years. Traditional systems emphasised physical safety and operational efficiency that is no longer relevant considering the complex network of interconnected systems, processes, and components. These drawbacks have been addressed by the marine sector gradually, by streamlining international regulations, guidelines and leveraging emerging technological capabilities.

Though parallels can be drawn between digital twin security measures and cybersecurity standards, there exist key differences which make them different concepts. Cybersecurity is aimed at designing regulations for safeguarding IT systems, networks, software, and data, from unauthorized access or damage. It leverages tools like firewalls, intrusion detection systems and encryption algorithms to address threats like phishing, malware, ransomware, and denial of service attack. Digital Twin security

encompasses static digital assets mentioned above in addition to protecting the dynamic, real-time connection between the physical system and the virtual replica. Figure 1. shows the difference between a cyber-attack and a digital twin attack.

Figure 1: Differences between cyberattack and Digital Twin Attack



2. Literature review

(Tam, 2019) has conducted a survey on the existing risk assessment frameworks like NIST, FMEA and MaCRA in addressing maritime cybersecurity. The paper highlights the inefficiency of the existing frameworks in capturing dynamic risks and human factors. This is mainly due to the increased complexity of the marine systems and the dynamic environment in which they operate.

(Progoulakis, 2021) integrates digital twins with security analytics and big data analytics to improve cybersecurity in iiot lifecycle by using the DT2SA model. The research considers 3 operational modes for Digital Twins- Simulation, Replication and Analytics. The Digital twin here processes different kinds of data – namely- descriptive, diagnostic, semantic, historical, and dynamic environmental data. The proposed model is validated on a microservice architecture called TWINSIGHT for intrusion detection. However, we believe more operational modes exist control (Actuation), decision support, monitoring, optimization, and prediction.

(Empl, 2023) proposes a cloud-based framework to store DT data and blockchain is used to ensure data integrity. A three-factor privacy-preserving authentication scheme is proposed for the DT environment using Elliptic curve cryptography. The framework devised by the researchers was able to address 14 different types of attacks. The work is validated using Burrows-Abadhi-Needham (BAN) logic and the real or Random (ROR) model.

(Thakur, 2023) proposed a framework that evaluates cyber security risks of Digital Twins in virtual, physical, communication, network, and application layers. Discrete-Time Markov Decision process and Markov Decision process are used to capture security aspects of DT. The defense of the system is evaluated from two perspectives- naïve attacker and skillful attacker on three defense levels- low, medium, and high. The system is implemented using the PRISM model checker. The efficiency of the framework is proved by testing it on an in-patient-healthcare monitoring system.

(Enis Karaarslan, 2021) devised a framework called Enigma to evaluate the security level of Digital Twins and provide a risk awareness training environment. ENIGMA is an integration of DT-CPS systems, a gamification platform, and an explainable AI-based DT platform. The attacks on CPS-DT have been classified into 3 types- attacks on CPS, attacks on DT and Hybrid attacks. AI agents are used as defenders, and humans are attackers. Different attack-defense scenarios are used to assess the applicability of the proposed framework.

(E. Shaikh, 2023) classifies security threats on digital twins according to the attack surface that ranges from system, communication, and data storage threats. Availability, accessibility, data Integrity and Confidentiality are a few of the aspects of security.

(Chao He, 2022) classifies threats based on layers of functionality and technologies. The adversarial approach uses the Dolev-Yao model, which examines attackers' capability of intercepting, modifying, and replaying messages between a physical object and its digital twin.

(Christian Gehrmann, 2019) proposed a digital twin-based security framework for industrial control and automation systems (ICAS). The paper highlights the requirements of the state synchronization model specifically designed for cloud-based systems. The work has been validated by connecting the adversarial approach to the Dolev-Yao model. 3 security definitions have been proposed – synchronization protection, confidentiality protection and consistency.

(Matthias Eckhart, 2018) uses digital twins for state synchronization to identify and prevent security breaches before they affect physical systems or processes. The proposed architecture leverages synchronization gateways, Intrusion Detection systems and centralized access control. This paper rightly tells us that a digital twin cannot replace a physical twin if the physical twin fails.

(Khajavi, et al., 2023) developed a new framework called CPS-Twinning to build secure virtual environments for Digital twins using engineering and domain knowledge. The virtual environment used to test the working of critical systems consists of three modules- a generator that parses the topology of the network, configuration and safety guidelines, and a virtual environment that builds a virtual environment for network infrastructure, control logic, network protocol, device types and physical equipment. Digital twins are used for testing process changes, device testing and optimizing operations. They are also used to safeguard critical systems by restricting data flow, which limits negative effects on the physical environment from threats like intrusion detection and misconfigurations. The framework is tested for different scenarios on Mininet.

(Holmes, et al., 2021) explores the threats associated with the implementation of digital twin technology. The paper uses cyber digital twins (CDT)to simulate multiple defense scenarios and security attacks for analysis without affecting the physical environment.

The existing literature highlights different aspects of integrating digital twins to enhance different operations. The works above fail to consider the risks encountered while operating a digital twin model. The difference between existing cyberattacks and these threats and risks remains unexplored. Moreover, there remains a need to evaluate the security-quality trade-off while using digital twins. This paper bridges the above gaps by proposing a mathematical framework that relates the security attributes with quality attributes. The rest of the paper is organized as follows. Section 2 is the literature review. Sections 3 explains the proposed framework in detail. Section 4 presents the case study to validate the proposed work. Section 5 presents the results followed by conclusion.

3. Proposed framework

Since the marine vessels operate in a dynamic environment, the existing cybersecurity frameworks designed for isolated , static ecosystems like manufacturing, agriculture fail to successfully address the complexity and frequency of cyber risks associated with critical

marine infrastructure. Since marine vessels are evolving into complex cyber-physical systems driven by technologies like AI,IOT, digital twins, there is a need for more robust, modular , scalable and smart architecture. In this regard, we have proposed a MVC based marine cybersecurity framework that can help in real-time risk identification, adaptive risk modelling and regulatory compliance. The proposed five-tiered framework aims to implement digital twin enabled cybersecurity risk assessment , which can provide a modular, scalable and flexible prototype of the Maritime Industry 4.0 standards. Figure 2 shows the proposed framework.

3.1 Data acquisition and preprocessing layer

This is the core layer of the proposed framework aimed at collecting, filtering and organizing raw data collected from different sensors and systems. The sources of this data can be AIS, SCADA, GPS, engine logs, port control systems etc. Data is processed and cleaned using Noise Filtering techniques like spatial filtering and machine learning. The data is then normalized in order to make it compatible with the Digital Twin model. The dataset so generated is then labelled using threat indicators like AIS spoofing, in order to train the machine learning models. This dataset can be used for detecting anomalies, predicting vessel motions or mapping cyber threats with operational anomalies.

3.2 Digital Twin model layer(model layer of proposed MVC architecture)

This layer is the backbone of the system since it can be used for predictive threat assessment, and analysing vessel behaviour in different operational scenarios. This layer is the virtual replica of the system, process or component .This is used to reflect the real-time states of the maritime asset or port operation. We have proposed the use of Bayesian Network here to reflect the probabilistic relationship between impaired systems or processes. Bayesian Networks are probabilistic graphical models that are used to represent variables and their conditional dependencies using a directed acyclic graph(DAG).

We have used it in the maritime context, since it effectively addresses the dynamic scenarios. For instance, how one event (AIS Spoofing) could lead to incorrect course heading or propulsion control. This is important for capturing real-world chain reactions that might occur in the open seas. Bayesian Networks are also capable for handling incorrect or missing entries in the data, which is common in marine sector. Additionally, Bayesian Networks generate probabilities in real-time as new data is ingested from the digital twin. This makes them ideal for continuously evolving risky situations. These probabilities are converted into quantitative risk estimations using Monte Carlo Simulations. It can help in assessing the severity and likelihood of failure under different conditions .We have preferred Bayesian networks over Rule-based trees as they overfit and lack the desired probabilistic inference.

3.3 Threat intelligence and risk assessment layer(controller layer)

This layer is used for efficient decision-making which can help in generating timely response to evolving threats. The observations made using the digital twin model are transformed into risk actions, mitigation protocols and compliance alerts.

We have used MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) to correlate real-world attack signatures like AIS Spoofing to well-known adversarial tactics. MITRE ATT&CK is a universally accessible database of real-world cyber adversary behaviour. It provides a detailed matrix of tactics and techniques used by attackers across different stages of cyberattack. “Tactics” explain the ‘why’ behind the attack. “Techniques” explores how the attacker achieves the tactics (Phishing, Lateral Movement etc).”Mitigations” analyses ways to minimize techniques. “Detections” helps in identifying

how a technique is being used. Some of the use cases are threat intelligence mapping, security monitoring and defensive gap analysis.

This has been preferred in the framework because as the marine vessels are increasingly getting digitalized, there is a need to map threat vectors to tactics, techniques and Mitigations. Moreover ATT&CK can help assess ways in which attackers can exploit model using digital twin interface. Any deviations from normal are detected using anomaly detection techniques. Alarms and warning are triggered based on the vulnerability and degree of damage expected from the attack.

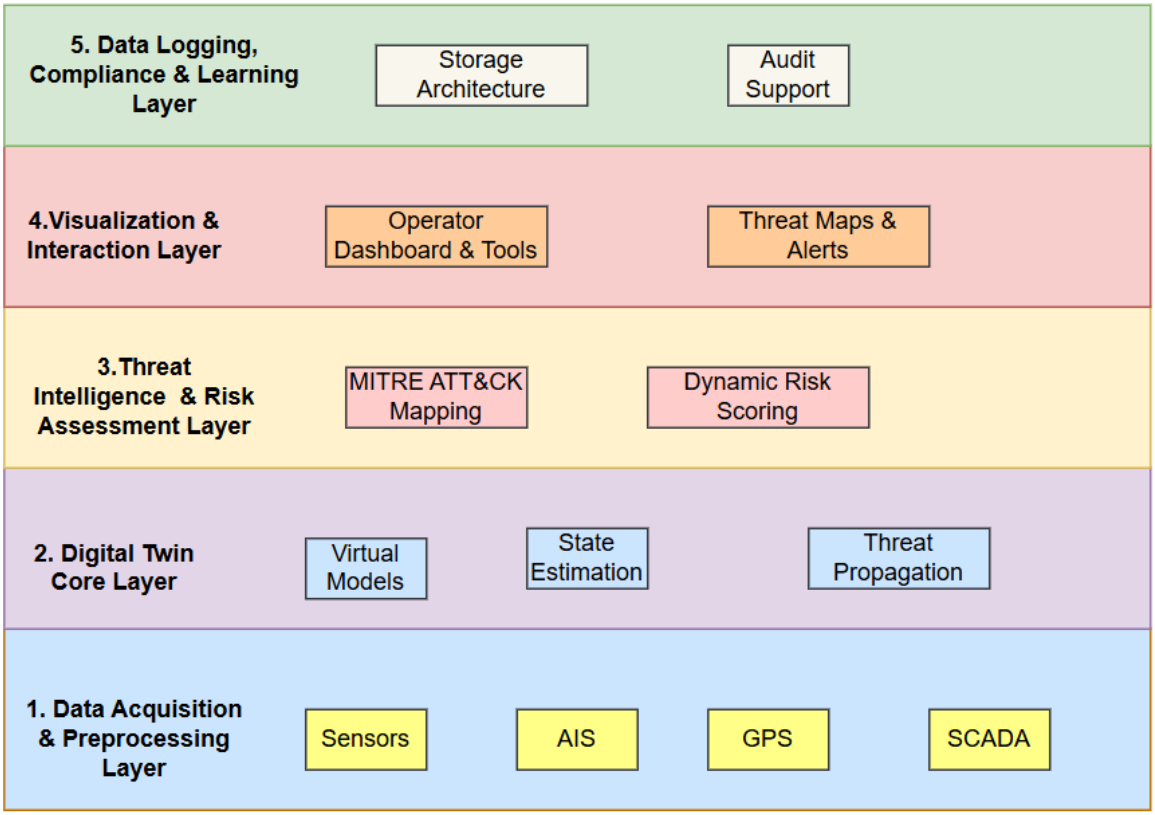
3.4 Visualization & interaction layer(view layer)

This layer is the machine-user interface like a dashboard which can help in promoting situational awareness to act quickly and efficiently in the event of an encountered threat. Dashboards can be used to provide real-time updates on states of the vessel, threat levels, analyse warning signals etc. Timelines could be created to generate chronological sequence of events and the mitigation strategies used.

3.5 Data logging, compliance & learning layer

This layer is used to store historical data, support compliance to existing regulatory standards like NIST, IMO, ISO27001 and improvise the model efficiency using continual learning approaches. This data can also be used for post-incident inspection.

Figure 2: Proposed framework



4. Case study

A case study was conducted to evaluate the validity of the proposed five-tiered digital twin based cybersecurity risk assessment framework. We simulated a cyber-attack on vessel's navigation system. The experiment was performed using a digital twin model of a small scale

digital twin model of a cargo ship. The model was equipped with virtual representations of its physical components, communication system and control software.

5.1 Scenario

A threat scenario was simulated where an unauthorized user attempted to manipulate engine performance parameters .The attack was aimed at disrupting voyage stability and reduce propulsion efficiency. This attack mirrors the Tactics and Techniques from the MITRE ATT&CK for ICS(e.g., T0831- Unauthorized command message, T0803- Control Manipulation,T0858- Spoof Alert Message).

Figure 3: Digital Twin Model of the marine vessel

5.2 Implementation

The digital model of the ship generated real-time emulated sensor data (temperature, RPM, shaft, torque, 6 degrees of freedom etc) as shown in Figure 3. Bayesian Networks was used to identify the most probable cyber intrusion sources and compromised nodes, given the observed anomalies in RPM. Monte Carlo Simulations were used to simulate thousands of possible cascading effects (shaft damage, voyage delay, wind readings) under different operational scenarios.

5.3 Validation process

Bayesian network evaluation: Impaired nodes were identified with 90.8% accuracy using probabilistic inference technique. This is an improvement over the conventional static data based alerts that ignored context relevant information. These probabilities were updated in real-time as new data was fed to the digital twin model. This can help prioritize real-time threats. It is computed using the below formula:

$$P(X_1, X_2, ..., X_n) = \prod_{i=1}^{n} P(X_i \mid \text{Parents}(X_i))$$

This shows how the complete probability distribution of the system is factored into local conditional probabilities.

Monte Carlo simulation results: Risk distribution across multiple iterations revealed 13-37% range in operational downtime. This can help the controller layer to generate pre-defined mitigation strategies such as isolation and re-routeing instructions. Monte Carlo Simulations are computed using the below equation.

$$\hat{E}[C] = \frac{1}{N}\sum_{i=1}^{N} C_i$$

Here, C_i is the cost impact from the i^{th} simulation

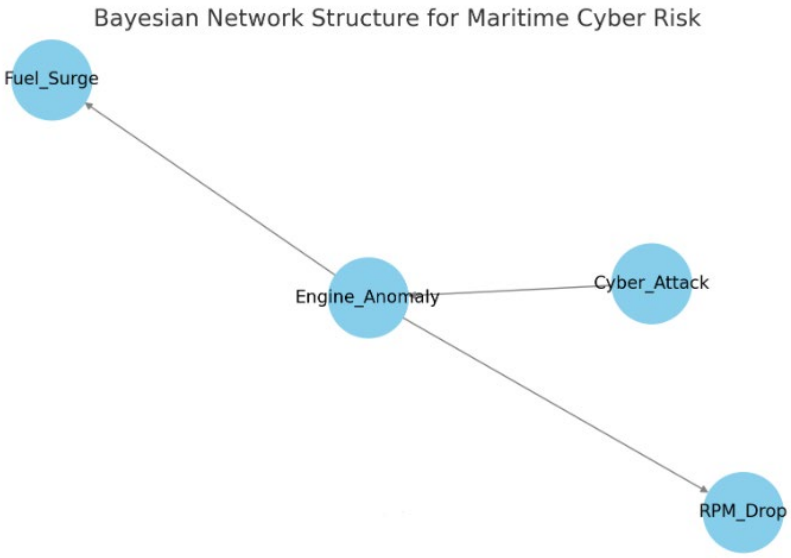
N is the number of simulations

MITRE ATT&CK mapping efficiency: The detection and mapping engine successfully correlated attack sequence with MITRE techniques. This validates the fact that integrating MITRE ATT&CK framework has helped in developing standards for threat interpretation layer which can aid in decision-making and operability.

6. Results

The Bayesian Networks in this case study consider the precipitating effect of multiple cyber-on critical marine infrastructure. The different nodes of the Bayesian Network are EngineAnomaly, CyberAttack, RPMDrop and FuelSurge as shown in Figure 4. These nodes map the relationship from its origin to mechanical consequences. The application of the Bayesian Networks shows that the event of occurrence of cyber-attack increases the posterior probability of EngineAnomaly from 30% to 70%. This validates the fact that Bayesian Networks can successfully capture and measure independent risks which are difficult to detect using static models.

Figure 4: Different Nodes of Bayesian network



Monte Carlo simulations are uses to evaluate the operational and financial implications of the cyberattack. Synthetic parameters were used to simulate 10000 iterations to evaluate downtime distribution, hourly cost rate and resulting total cost. Figure 5 shows the downtime distribution. As can be seen from the Figure, 6 hours is the average downtime for cyber

events, which have a mean deviation of 2 hours. The graph is skewed towards the right which shows that short interferences are common, it is the occurrence of long downtimes though rare, which pose serious threat.

Figure 5: Distribution Downtime for Monte Carlo Simulations

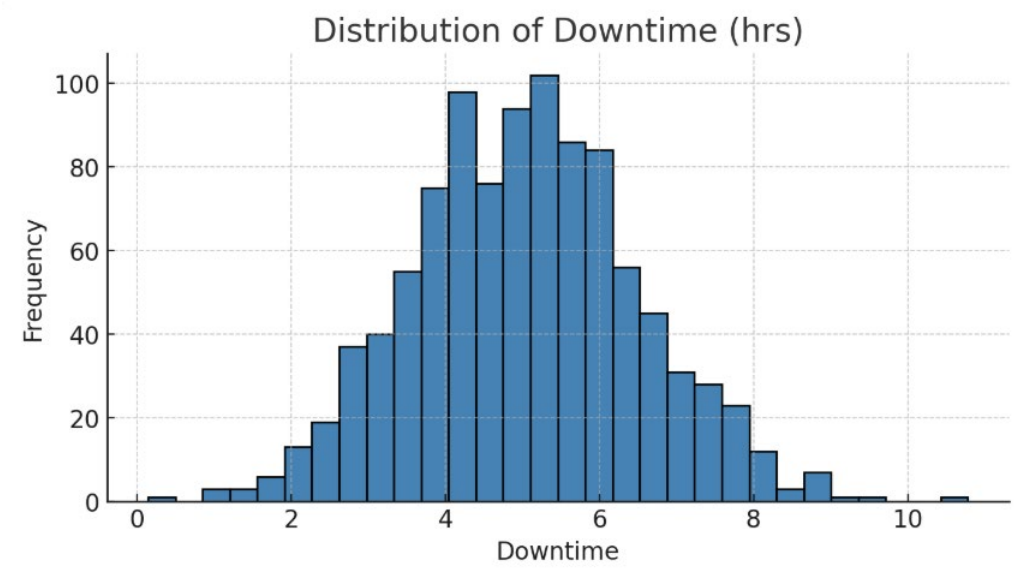


Figure 6 shows the Cost Rate distribution where average cost is $5000 per hour with variations to accommodate different weather scenarios. The results how moderately deviated cost profile, which is relevant for fuel-intensive commercial vessels.

Figure 7 shows Total Cost Distribution which is obtained by multiplying downtime and cost rate. Results show variations in the range of $25000-$40000, with outliers at $70000. These variations highlight the importance of proactive security investments to overcome high risk events.

Figure 6: Cost Rate Distribution

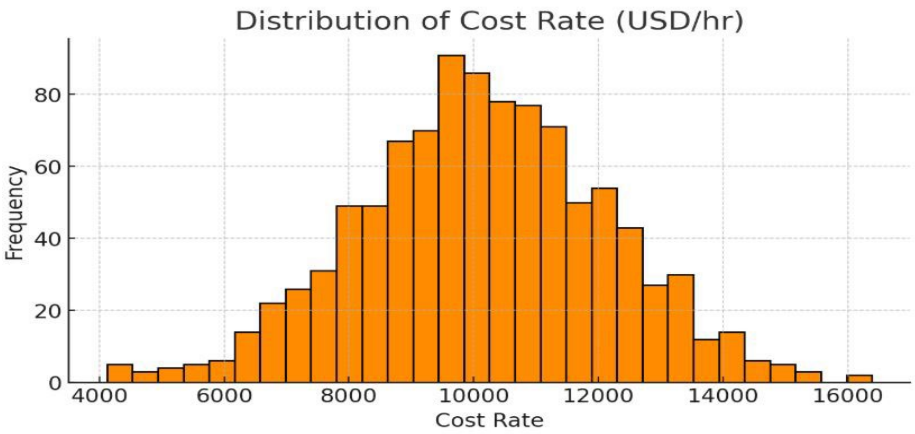
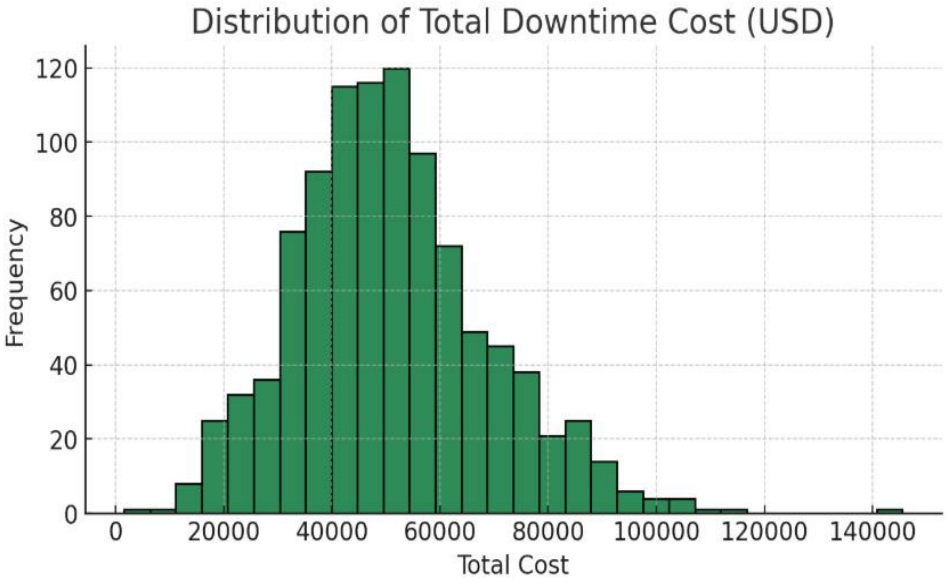


Figure 7: Total Downtime Distribution = Cost Rate Distribution X Downtime



7. Conclusion

The marine industry is responsible for carrying out 90% of the global trade by volume. The future of marine navigation lies in the adoption of technologies like IOT, AI and Digital Twins. But the adoption of these technologies poses new cybersecurity risks that the existing frameworks fail to address. This paper proposed a novel five-tiered framework that integrates digital twin models with cybersecurity modelling using Bayesian Network for establishing causal relationships and Monte Carlo simulation for cost-impact analysis. The framework was validated successfully using a case study to showcase the propagation of security events across layers varying from physical assets to AI powered decision engines.

8. References

Anon., 2025. *World Economic Forum - Global Cybersecurity Outlook.* [Online] Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ [Accessed 2025].

Chao He, T. H. L. R. L. Z. S. M. D., 2022. Security and Privacy in Vehicular Digital Twin Networks: Challenges and Solutions. *IEEE Wireless Communications,* 30(4), pp. 154 - 160.

Christian Gehrmann, M. G., 2019. A Digital Twin Based Industrial Automation and Control System Security Architecture. *IEEE Transactions on Industrial Informatics ,* 16(1), pp. 669-680.

E. Shaikh, A. R. A.-A. S. M. N. M. a. F. A., 2023. Security Analysis of a Digital Twin Framework Using Probabilistic Model Checking. *IEEE Access,* Volume 11, pp. 26358 - 26374.

Empl, P. a. G. P., 2023. Digital-Twin-Based Security Analytics for the Internet of Things. *Information,* 14(2).

Enis Karaarslan, M. B., 2021. *Digital Twin Security Threats and Countermeasures: An Introduction.* Ankara, Turkey, IEEE.

Holmes, D. et al., 2021. *Digital Twins and Cyber Security – solution or challenge?.* Preveza, Greece, IEEE.

Khajavi, S. H. et al., 2023. Digital Twin for Safety and Security: Perspectives on Building Lifecycle. *IEEE Access,* Volume 11, pp. 52339 - 52356.

Matthias Eckhart, A. E., 2018. *Towards Security-Aware Virtual Environments for Digital Twins.* s.l., ACM.

Progoulakis, I. R. P. a. N. N., 2021. Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering ,* Volume 9.

Tam, K. a. J. K., 2019. *Factors affecting cyber risk in maritime.* Oxford, UK, IEEE.

Thakur, G. P. K. S. J. A. K. D. a. Y. P., 2023. An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment. *IEEE Access,* Volume 11, pp. 26877 - 26892.