A Holistic Risk-Informed Framework for Port Resilience Assessment

Massoud Mohsendokht

A thesis submitted to Liverpool John Moores University in partial fulfilment for the degree of Doctor of Philosophy

January 2026

ACKNOWLEDGEMENTS

This thesis represents the culmination of more than two and a half years of continuous effort, determination, and perseverance through the many ups and downs of both research and life. Along this journey, I have been fortunate to receive the support, guidance, and encouragement of several exceptional individuals, without whom this work would not have reached its present form. I would like to take this opportunity to express my sincere gratitude to them all.

First and foremost, I owe my deepest appreciation to my lead supervisor, **Professor Zaili Yang**, whose professionalism, unwavering support, and insightful guidance have been instrumental throughout my PhD journey. From him, I have learned not only how to conduct rigorous and meaningful research but also how to persevere, remain ambitious, and continuously seek improvement. Beyond his academic excellence and leadership, what has inspired me most is his humility and willingness to listen to others, even when they may be mistaken. This combination of knowledge, professionalism, and humility is the most valuable lesson I have learned from him.

I would also like to extend my heartfelt thanks to my co-supervisor, **Dr. Christos Kontovas**, an exceptional academic whose intellectual depth and open-minded perspective have enriched my work immensely. Our discussions, spanning research, academia, and life in general, have been truly stimulating and rewarding. His ability to view problems from unique angles that others might overlook has significantly strengthened the quality and depth of my research.

My sincere appreciation also goes to **Dr. Chia-Hsun Chang** and **Dr. Zhuohua Qu** for their valuable feedback and constructive suggestions, which helped refine and mature my research outcomes.

In addition, I wish to express my deep gratitude to **Dr. Huanhuan Li**, whose guidance, collaboration, and contributions to my research papers have been invaluable. She is an exceptionally talented, professional, and kind researcher, and it has been a genuine privilege to work alongside her.

Finally, I am profoundly grateful to my parents and siblings for their unwavering love, moral support, and encouragement throughout my PhD years. Despite the physical distance that separated us, their belief in me has been a constant source of strength and motivation. This achievement is as much theirs as it is mine.

ABSTRACT

Seaports are critical hubs underpinning global trade and play a significant role in ensuring economic stability through their influence on global logistics and supply chains. However, they remain highly susceptible to various disruptive events, including natural disasters, human-induced accidents, maritime terrorism, and cyber threats, each capable of causing substantial economic and operational disturbances. Given the increasing frequency and severity of these hazards, driven notably by climate change, enhancing seaport resilience has emerged as an essential focus within maritime research and practice.

This dissertation addresses critical gaps identified through a comprehensive literature review and analysis, proposing an integrated, holistic framework designed to enhance resilience in seaport operations in a holistic way. The study begins with an extensive review of existing resilience assessment methodologies, critically analysing their strengths, limitations, and applicability to maritime infrastructure. The review identifies a significant overlap among existing frameworks and highlights a persistent need for a standardized, comprehensive, and integrated approach to seaport resilience.

Building upon this foundation, the research introduces a novel maritime security risk assessment methodology specifically designed to address physical threats, particularly maritime terrorism. Utilizing a data-driven Bayesian Network (BN) model informed by empirical data from maritime terrorist incidents over two decades, this approach uncovers significant contributing factors and their interdependencies. Validation through sensitivity, performance-metric, and comparative analyses demonstrates the model's robust diagnostic and predictive capabilities, offering practical insights to stakeholders for enhancing security and preparedness.

Complementing the assessment of physical threats, the dissertation formulates a novel cybersecurity risk analysis framework. Leveraging a comprehensive dataset of maritime cyber incidents, the developed BN model facilitates the identification of critical risk factors, interdependencies, and their probabilities of occurrence. Rigorous validation further establishes the model's efficacy in diagnosing cybersecurity vulnerabilities and predicting future threats, thereby providing stakeholders with valuable information for strategic cybersecurity resource allocation.

Recognizing the complexity of socio-technical interactions within seaports, this study also employs an innovative systemic risk analysis framework grounded in the Safety-II concept. Integrating the Functional Resonance Analysis Method (FRAM) with BN, alongside sophisticated analytical techniques, the framework aids in quantitative assessment of performance variability across technological, human, and organizational functions. Applied to seaport operations, this systemic approach significantly enhances the management and quantification of risks in complex operational environments.

Further, the research develops a holistic, risk-informed resilience assessment framework using advanced simulation techniques. Addressing natural hazards as the primary focus, this simulation-based approach evaluates both direct physical impacts and indirect economic losses resulting from disruptions. Realistic hazard scenarios and historical case studies demonstrate

the framework's effectiveness in capturing a wide range of disruption scenarios, informing resilience-enhancing strategies, and optimizing recovery processes.

In synthesizing these methodologies, the dissertation provides a robust and practical holistic framework that integrates safety, security, and resilience assessments into a unified system. The resulting framework represents a pioneering advancement in maritime risk and resilience management, systematically addressing the multifaceted nature of seaport vulnerabilities. This integrated approach equips policymakers, port authorities, and maritime stakeholders with actionable insights, facilitating informed decision-making for proactive risk mitigation, operational continuity, and long-term sustainability.

Overall, this dissertation contributes significantly to maritime research and practice by delivering an innovative, holistic resilience analysis framework capable of systematically addressing the evolving landscape of threats to seaport operations. Through its integrated methodological approach, it offers critical guidance for enhancing resilience, safeguarding maritime operations, and ensuring the sustainability of critical global trade infrastructures amid increasing uncertainty and risk.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbr.	Description
ABM	Agent-Based Modelling
ABN	Augmented Bayesian Network
ACAT	Accident Causation Analysis and Taxonomy
AGV	Automated Guided Vehicles
AIC	Akaike Information Criterion
AIS	Automated Identification Systems
APP	Availability of procedures and plans
ATOS	Automated Terminal Operating Systems
ATT	Available Time and Time pressure
BN	Bayesian Network
BS	Bayesian Search
CAN	Control Area Network
CCM	Contextual Control Modes
CDF	Cumulative Distribution Function
COW	Conditions of Working
CPAF	Cognitive Process Architecture Framework
CPC	Common Performance Conditions
CPM	Critical Path Method
CPT	Conditional Probability Tables
CREAM	Cognitive Reliability and Error Analysis Method
CRS	Circadian Rhythm and Stress
CSTS	Complex Socio-Technical Systems
CWA	Central Weather Administration
DAG	Directed Acyclic Graph
DDBN	Data-Driven Bayesian Network
DDOS	Distributed Denial of Service attack
DES	Discrete Event Simulation
DS	Damage State
DSET	Dempster-Shafer Evidence Theory
DSMC	Dynamic Spatial Markov Chain
ECDIS	Electronic Chart Display and Information Systems
EPEC	Equilibrium Problems with Equilibrium Constraints
ER	Evidential Reasoning
ETA	Event Tree Analysis
FAHP	Fuzzy Analytical Hierarchy Process
FAST	Function Analysis System Technique
FCFS	First-Come-First-Served
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FPR	False Positive Rate
FRAM	Functional Resonance Analysis Method
FTA	Fault Tree Analysis
GA	Genetic Algorithms
GPS	Global Positioning Systems
GTD	Global Terrorism Database
GTT	Greedy Thick Thinning

HAZOP	Hazard and Operability
HMI	Human-Machine Interface and operational support
HRA	Human Reliability Analysis
HRI	High-Risk Influence
HTA	Hierarchical Task Analysis
IBTrACS	International Best Track Archive for Climate Stewardship
IMO	International Maritime Organization
I-O	Input-Output
IoT	Internet of Things
IT	Information Technology
ITERATE	International Terrorism: Attributes of Terrorist Events
JMA	Japan Meteorological Agency
KPTTC	Kaohsiung Port's Typhoon Command Centre
LRI	Low-Risk Influence
MaCRA	Maritime Cyber Risk Analysis
MCAD	Maritime Cyber Attack Database
MCDM	Multi-Criteria Decision Making
MCS	Monte Carlo Simulation
MCTN	Maritime Container Transport Networks
MIPT	Memorial Institute for the Prevention of Terrorism
MTS	Maritime Transportation System
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
NBN	Naive Bayesian Network
NGC	Number of Goals and Conflict resolution
NIRA	Networked Infrastructure Resiliency Assessment
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
OCR	Optical Character Recognition
PDF	Probability Density Function
PL	Plausibility Function
PRI	Port Resilience Index
PSF	Performance Shaping Factors
PSO	Particle Swarm Optimization
QSO	Quality and Support of the Organization
RAND	Research ANd Development
RBN	Rule-based Bayesian Network
RCF	Recovery Capacity Factor
RMDA	Risk Management-based Decision Analysis
RMG	Rail-Mounted Gantry
RMW	Radius of Maximum Wind
RTG	Rubber Tired Gantry crane
SADT	Structured Analysis and Design Technique
SD	System Dynamics
SHERPA	Systematic Human Error Reduction and Prediction Approach
SRIF	Security Risk Influencing Factors
STAMP	Systems Theoretic Accident Model and Processes
START	Study of Terrorism and Response to Terrorism

STS	Severe Tropical Storm
SVI	Self-contained Variability Index
TAC	Training and competence
TAN	Tree-Augmented-Naïve
TCF	Time-Cost-Functionality
TCQ	Team Collaboration Quality
TD	Tropical Depression
TNR	True Negative Rate
TEU	Twenty-foot Equivalent Unit
TIPC	Taiwan International Ports Corporation
TOPSIS	Technique for Order Preference by Similarity to Ideal Solution
TRI	True Risk Influence
TS	Tropical Storm
TY	Typhoon
ULCV	Ultra Large Container Vessel
URI	Unified Resilience Index
URMGC	Unmanned Rail-Mounted Gantry Cranes
UVI	Upstream Variability Index
VST	Very Strong Typhoon
VTY	Violent Typhoon
WITS	Terrorism Knowledge Base, the Worldwide Incidents Tracking System
WMO	World Meteorological Organization

LIST OF PUBLICATIONS

Journal papers:

1. Mohsendokht, M., Kontovas, C., Chang, C. H., Qu, Z., Li, H., & Yang, Z. (2025). Resilience analysis of seaports: a critical review of development and research directions. Maritime Policy & Management, 1–36. https://doi.org/10.1080/03088839.2025.2483410.
2. Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. (2025). Enhancing maritime transportation security: A data-driven Bayesian Network analysis of terrorist attack risks. Risk Analysis, 45(2), 283–306. https://doi.org/10.1111/risa.15750.
3. Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. (2024). Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. Ocean Engineering, 312, 119078. https://doi.org/10.1016/j.oceaneng.2024.119078.
4. Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. (2026). Systemic Risk Analysis of Complex Socio-Technical Systems through the Lens of Safety II concept. Reliability Engineering & System Safety, 270, 112200. https://doi.org/10.1016/j.ress.2026.112200.
5. Mohsendokht, M., Mokhtari-Moghadam, A, Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. (2026). A Risk-based Simulation approach to Assess Seaports Functionality and Economic Vulnerability under Cyclone Hazards. https://doi.org/10.1016/j.trd.2026.105291
6. Mohsendokht, M., Yang, Z. (2026). AI-Enhanced Bayesian Network Modelling for Security Risk Analysis of Transportation Terrorism. (Book Chapter: Artificial Intelligence in Action: Transformative Applications and Real-World Impact. CRC Press. Taylor & Francis Group)
7. Mohsendokht, M., Yang, Z. (2026). Translating Safety-II Principles into Quantitative Risk Measures via FRAM and Bayesian Networks. (Book Chapter: ERC project).

Conference papers:

1. Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. “Maritime Terrorism Risk Analysis through a Data-driven Bayesian Network Approach”. IAME conference, June 26-28, 2024, Valencia, Spain.
2. Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. “Incorporating FRAM and BN into Safety-II Principles for a Proactive Risk Assessment in Seaports”. IAME Conference, June 24-27, 2025, Bergen, Norway.
3. Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. “A Safety-II-Based Hybrid Risk Analysis Framework for Seaport Operations”. The 8th MTPC, June 17-18, 2025, Liverpool, UK.
4. Mohsendokht, M., Yang, Z. “Cyclone-Induced Risk Assessment of Seaport disruptions Using a Hybrid Deterministic-Probabilistic Approach”. 2nd Annual SRA E UK conference, November 12-13, 2025, Cardiff, UK.
5. Mohsendokht, M., H. Li, Z. Yang (2026). Risk-Based Hybrid Modelling of Seaport Resilience Against Climate-Driven Extreme Events. IAME 2026, 30 June- 3 July, 2026, Nanyang, Singapore.

Chapter 1 : Introduction

1.1 Introduction

Maritime transportation and seaport operations are vital components underpinning global trade and economic stability, accounting for approximately 80% of international trade by volume and about 70% by value (UNCTAD, 2022a). As the cornerstone of global logistics and supply chains, the continuous and reliable functioning of seaports directly influences international trade dynamics, economic growth, and supply chain reliability. Any disruption or operational failure at these crucial nodes can trigger significant economic consequences, impacting global markets and local economies alike, while creating lasting disturbances in trade networks.

Seaports face a diverse array of risks, stemming from natural hazards, intentional acts of terrorism, cyber threats, and various operational accidents. Natural hazards, including earthquakes, tsunamis, hurricanes, flooding, and storm surges, present increasingly frequent and severe threats, often intensified by climate change. Such catastrophic events can cause considerable physical damage to port infrastructure, interrupt port operations, and lead to extensive economic losses through delayed shipments, increased logistical costs, and substantial recovery expenditures. Historically, events such as the Kobe Earthquake (1995), the 2004 Indian Ocean tsunami, and Hurricane Katrina (2005) exemplify the profound economic and operational disruptions that natural disasters can impose on seaport functionality, highlighting the necessity of robust resilience planning and preparedness.

In addition to natural disasters, the evolving landscape of maritime terrorism presents significant security concerns. Although maritime terrorism comprises a small proportion of global terrorist activities, its potential impacts are severe due to the strategic importance of maritime transport and port infrastructure. Terrorist attacks targeting ships or port facilities can disrupt global supply chains, threaten economic stability, and induce environmental disasters, amplifying their adverse consequences. Moreover, maritime terrorism often targets high-profile facilities and vessels, utilizing tactics designed to maximize media exposure and political impact. For example, the 2004 bombing of the Philippine passenger ferry Superferry 14, a crowded, symbolic target on a major route, caused mass casualties and widespread media coverage, pressuring authorities to intensify counterterrorism measures and maritime security reforms. Therefore, understanding and mitigating such threats remain imperative for enhancing global maritime security.

Cybersecurity has emerged as another critical area of concern for maritime operations. As the maritime industry increasingly adopts advanced digital technologies and automated systems, such as Automated Terminal Operating Systems (ATOS), Global Positioning Systems (GPS), and Automated Identification Systems (AIS), it becomes increasingly vulnerable to cyber threats. Incidents like the 2017 NotPetya ransomware attack on Maersk, resulting in $1.2 billion loss demonstrate the extensive and disruptive nature of cyber incidents, highlighting significant financial and operational vulnerabilities (BBC, 2018). Cyber threats transcend traditional geographical and physical barriers, enabling attackers to target maritime systems remotely and unpredictably. As digital integration deepens within maritime operations,

enhancing cybersecurity measures becomes indispensable for safeguarding critical maritime infrastructure against potentially devastating disruptions.

Given these multifaceted challenges, resilience has emerged as a foundational concept in maritime industry discourse and research. Resilience refers to the capacity of seaports to anticipate, prepare for, respond to, adapt to, and swiftly recover from disruptions. It encapsulates an integrated approach to risk management, prioritizing not only prevention but also rapid recovery and adaptation in the face of disturbances. Despite its significance, the current state of resilience assessments in maritime contexts is still developing, often lacking standardized metrics and systematic evaluation methodologies capable of addressing the inherent complexities and interdependencies of seaport systems.

To bridge these critical gaps, this dissertation proposes an integrated and holistic approach towards evaluating and enhancing seaport resilience. Driven by the necessity for effective frameworks that measure, predict, and mitigate risks across multiple dimensions, the research contributes significant advancements by developing practical and robust methodologies tailored for comprehensive seaport resilience assessments. This study particularly emphasizes addressing contemporary threats, including climate-induced natural disasters, maritime terrorism, and cybersecurity vulnerabilities, utilizing empirical data to provide accurate, actionable insights.

This research ultimately aims to furnish policymakers, port authorities, and maritime stakeholders with a deeper understanding of the dynamics affecting port resilience. By systematically identifying critical vulnerabilities, evaluating risk factors, and suggesting targeted intervention strategies, the outcomes of this study support informed, proactive decision-making processes. The frameworks developed herein provide crucial guidance for enhancing resilience measures, safeguarding operational continuity, and ensuring the long-term sustainability of maritime infrastructure.

In summary, this dissertation significantly enriches existing knowledge by offering a nuanced and comprehensive examination of maritime resilience. Its integrated methodological approach not only addresses immediate practical challenges but also lays a foundation for sustained resilience improvement efforts, crucial for navigating the evolving and increasingly uncertain maritime risk landscape.

1.2 Research Aims and Objectives

By exploring the foundational aspects of safety, security, risk, and resilience within maritime infrastructure, particularly seaports, this thesis is guided by several pivotal research inquiries, emerging from an extensive review of existing knowledge:

> Q1: What are the existing methodologies for resilience analysis in seaport contexts, and what are their strengths and limitations?
> Q2: How can we effectively evaluate both physical and cyber security threats targeting maritime infrastructure, encompassing seaports and vessels?
> Q3: What methodologies can be employed to assess the safety of seaports, considering their inherent complexities and the intricate interactions among their operational components?

Q4: How can a comprehensive resilience assessment be conducted, taking into account all factors influencing seaport operations, the potential costs associated with hazards, and the subsequent recovery expenses?

Beginning with an overview of these research questions and a thorough review of the literature, this study endeavours to address these queries by establishing clear research objectives. The overarching aim of this research is to develop an innovative holistic framework using a risk-informed approach, to enhance the resilience of seaports by integrating considerations of safety, security, and their dynamic interactions. To achieve this aim, the following five objectives are formulated:

1) Conduct an exhaustive literature review to ascertain the current state-of-the-art methodologies for assessing safety, security, and resilience in maritime infrastructure.
2) Develop and validate a methodology to comprehensively assess physical and cyber security threats targeting seaports and vessels, considering both immediate impacts and long-term implications.
3) Design a robust analytical framework that captures the complex interactions within seaports, addressing safety concerns amidst operational intricacies and interdependencies.
4) Implement a holistic resilience assessment methodology that integrates all pertinent factors affecting seaport operations, including hazard impacts, potential damage costs, and recovery expenses.
5) Evaluate and refine the developed framework through case studies and simulations, demonstrating its applicability and effectiveness in enhancing seaport resilience while minimizing operational disruptions and relevant costs.

1.3 Justification of Research and its Novelties

The purpose of this study is to develop a novel holistic framework for assessing the resilience of seaports. This framework encompasses various critical aspects of safety, security, and resilience, which serve as overarching concepts for analysing the impact of undesired events on seaport operations. These aspects include, but are not limited to, reliability, availability, vulnerability, flexibility, adaptability, serviceability, restorability, and robustness. The study aims to integrate these elements into a unified approach, enabling a holistic evaluation of how seaports respond to disruptions and ensuring that all relevant factors influencing their resilience are systematically considered.

The justification for the necessity of this research stems from a significant gap identified in the literature review, where current methodologies fail to adequately address the multifaceted factors contributing to the potential disruption of seaports due to a range of hazards. These hazards include natural, technological, organizational, and human-induced risks. This gap is particularly evident when considering that the application and implementation of resilience strategies in seaports are often lagging those in other sectors of the industry. As seaports play a crucial role in global trade and transportation, the lack of a comprehensive, integrated approach to assessing and managing these diverse risks highlights the need for this research to fill that void and advance the field. In this regard, this study seeks to address these issues within the context of seaports, which serve as critical hubs in maritime transportation. The novelty of this research can be summarized as follows:

1) Building a comprehensive database of seaport-related hazards and threats: This study aims to establish a robust database that catalogues various hazards and threats relevant to seaport operations, thereby enhancing the process of risk and resilience assessment. This database will integrate both safety and security perspectives, providing a well-rounded foundation for evaluating potential disruptions from multiple viewpoints.
2) Developing an innovative framework for security risk assessment in maritime transportation: The research introduces an advanced framework for assessing security risks within the maritime transportation sector, addressing both cyber and physical threats. This approach not only highlights current security vulnerabilities but also offers solutions for mitigating the risks associated with emerging threats in both domains.
3) Proposing a new methodology for seaport safety analysis: This work presents a novel methodology for analysing seaport safety, considering the inherent complexities and interdependencies within seaport operations. It also seeks to overcome the limitations of traditional safety assessment methods by offering a more dynamic and comprehensive approach to identifying and addressing safety risks.
4) Development of a holistic risk-informed framework: An innovative, risk-informed holistic framework is developed, which integrates both simulation-based and deterministic-probabilistic resilience assessments. This framework also incorporates cost analysis, providing a more complete understanding of the economic impacts of various hazards on seaport operations, while supporting decision-making regarding risk mitigation and resource allocation.
5) Pioneering applications of advanced techniques for resilience assessment: The research pioneers the application of advanced analytical methods and techniques, such as FRAM, Bayesian Networks, Monte Carlo Simulation, evidential reasoning, Tree-Augmented-Naïve Bayesian Networks, and CREAM, to support the development of a novel and comprehensive framework for risk-informed resilience assessment. These methods collectively enhance the framework's ability to address the multifaceted challenges of seaport resilience in a dynamic and evolving risk landscape.

1.4 Structure of the thesis

This thesis is structured into seven chapters, each designed to present the research findings in a coherent and interrelated manner. The overall organization ensures a logical progression from conceptual foundations to methodological development and empirical application. It is important to note that the literature review, identification of research gaps, and methodological framework are integrated within the relevant chapters rather than confined to a single section, thereby maintaining thematic continuity and reinforcing the linkage between theoretical background, research objectives, and analytical procedures.

Chapter 1: Introduction

This chapter begins by exploring the critical importance of safety, security, and resilience in maritime transportation systems, encompassing vessels, shipping routes, and supporting maritime infrastructure, with a particular focus on seaports, with a particular focus on seaports. It emphasizes how these elements are fundamental to the effective and sustainable operation of seaports and maritime infrastructure. The chapter then presents the research questions related to these key aspects, which the study aims to address in depth. Following this, the research

aims, motivation, and objectives are systematically outlined to provide clarity on the direction and purpose of the study. Additionally, a brief background of the research is provided, highlighting the context and significance of the study, as well as the novelty and contribution of the current research to the field. The chapter concludes by outlining the structure of the thesis and summarizing the content of each chapter, offering readers a clear roadmap of the document.

Chapter 2: Literature review

This chapter presents a comprehensive survey of existing research on seaport resilience. It provides a thorough overview of advancements in the emerging field, summarizing key qualitative and quantitative methodologies developed to assess seaport resilience. The chapter employs critical literature review techniques to identify knowledge gaps and address previously overlooked questions. It also includes an extensive discussion of resilience metrics, methodologies, and strategies applied within the seaport context, highlighting their complexities and practical applications. Additionally, the chapter offers an in-depth evaluation of the strengths and weaknesses of existing approaches, identifies key challenges, and proposes potential directions for future research, contributing valuable insights to the academic community.

Chapter 3: Physical security risk assessment

This chapter focuses on the development of a new maritime security risk analysis method using real data from maritime terrorism incidents over the past two decades. The study concentrates on attacks against ships, aiming to track recent trends and identify patterns in maritime terrorism. It also examines influential factors, including vulnerable regions, high-risk countries, weapon types, and attack tactics, and explores the causal relationships between these elements. The chapter presents the first comprehensive methodology for conducting a quantitative terrorism risk analysis in the maritime sector, utilizing a data-driven Bayesian Network model. This approach, based on data from the global terrorism database, enables a thorough evaluation of the risks associated with terrorist attacks, providing valuable insights for the maritime community.

Chapter 4: Cybersecurity risk assessment

This chapter presents a novel approach to maritime cybersecurity risk analysis, addressing gaps in this context. By utilizing a comprehensive dataset of cyber incidents from the past two decades, a data-driven Bayesian Network model is trained to offer a more robust framework for evaluating cybersecurity risks in the maritime sector. The chapter highlights the creation of a refined dataset capturing key risk factors, introduces a new method for diagnosing cybersecurity risks, and tracks contemporary patterns in maritime cyber-attacks. It provides valuable insights into the dynamics of these threats, improving prediction accuracy and offering guidance for stakeholders and governmental bodies on optimized resource allocation and mitigation strategies.

Chapter 5: Systemic risk analysis based on Safety-II concept

This chapter introduces an integrated framework for systemic risk analysis in seaports, aligned with the Safety-II concept. The methodology combines FRAM and Bayesian Networks with

advanced analytical tools, including Monte Carlo simulation, probabilistic methods, statistical modelling, evidential reasoning, Dempster-Shafer theory, and the CREAM methodology. The chapter outlines the analysis of seaport elements such as technological, human, and organizational functions individually to assess their performance variabilities. It also examines the interactions among related functions, tracking their upstream-downstream effects and impacts on the overall system. The framework allows for both retrospective and prospective risk analysis, providing decision-makers with actionable insights to address risks. By quantifying variabilities, the framework supports risk-based decision-making, enabling the prioritization of interventions and targeted risk management measures.

Chapter 6: Risk-informed resilience assessment

This chapter presents a simulation-based resilience analysis framework aimed at estimating both the physical and economic impacts of natural hazards on seaport operations. The framework extends existing research by offering a risk-informed resilience analysis that considers a broad range of disruptions, including natural hazards, cyber-attacks, security breaches, and accidents, with a primary focus on climate-related risks. It enables port authorities and stakeholders to better understand potential risks, assess their capacity to withstand these threats, and design effective strategies for adaptation and recovery. By using realistic data and advanced simulation techniques, the framework provides a powerful tool for enhancing the long-term sustainability and reliability of seaports in the face of climate change.

Chapter 7: Conclusion

This chapter wraps up the PhD thesis by highlighting the key academic contributions aligned with the research aims and objectives. It also discusses the limitations encountered throughout the study and proposes potential areas for future research, offering new directions that could further advance the field.

Chapter 2 : Literature review

2.1 Summary

This chapter provides a comprehensive review of existing studies on seaport resilience. It begins by examining recent review papers on maritime infrastructure resilience to understand the current state of knowledge and to identify gaps that remain insufficiently explored. Building on this foundation, a systematic literature review is undertaken to identify and refine relevant studies specifically focused on seaport resilience, while excluding unrelated works through well-defined eligibility criteria. The remaining studies form the core of this analysis.

Drawing from these sources, the chapter offers an integrated overview of progress in this emerging research field, summarizing both qualitative and quantitative approaches used to evaluate seaport resilience. Through critical examination, it highlights existing knowledge gaps, conceptual challenges, and methodological limitations that warrant further attention. The discussion extends to resilience metrics, frameworks, and strategies employed in seaport studies, emphasizing their complexities, applicability, and practical implications.

Overall, this chapter critically assesses the strengths and weaknesses of existing approaches, identifies key challenges facing researchers and practitioners, and outlines promising directions for future investigation. It thus establishes the conceptual and methodological foundation for the subsequent chapters and guides the research toward addressing the identified gaps.

2.2 Introduction

Maritime transportation and seaport operations serve as the fundamental pillars of global trade and the international economy. In this respect, the continuous operation of seaports as the heart of maritime transportation is essential. Any failure or disruption would significantly hinder the flow of goods and disrupt supply chains, both domestically and internationally. The key principles for evaluating seaport performance include reliability, vulnerability, robustness, survivability, safety, and security. These terms cover several technical aspects related to evaluating the functionality of seaport operations but differ in their primary objectives and perspectives. Among these concepts, resilience stands out for its significance and emblematic nature. It has the capacity to cover a wide range of port operation assessments and is of utmost importance in facilitating seamless and effective functioning while maintaining its integrity. Resilience refers to a port's ability to withstand, adapt to, and recover from various shocks and stresses. This involves understanding conceivable hazards, assessing their potential consequences, and implementing measures to enhance the port's capacity to resist and mitigate the adverse effects of disturbances and recover from them.

This chapter aims to serve as a comprehensive survey of existing research on resilience studies in seaports. Over the past years, there has been a significant surge in attention surrounding the notion of resilience, making it a topic of interest for this review. Regarding maritime resilience, the existing literature is rather scant. Madhusudan and Ganapathy (2011) conducted a review study on the resilience of transportation infrastructure and seaports in the face of relevant disasters. They concluded that a universally agreed-upon metric for assessing

the resilience of transportation infrastructure across various modes of transportation has not yet been established. Wendler-Bosco and Nicholson (2020) conducted a literature review of existing research on the impacts of seaport disruptions on the maritime supply chain. They reviewed a variety of scholarly research and industry sources to gain insights into the impacts of port disruptions on various dimensions of the supply chain, including transportation, inventory management, and customer service. Gu and Liu (2023) conducted a comprehensive literature analysis that specifically examined the notion of resilience in the realm of maritime transportation. Additionally, a bibliometric study was undertaken, providing insights into the elements that contribute to maritime resilience. Recent studies have explored resilience in the context of maritime transportation. Lau et al. (2024) employed bibliometric analysis and a systematic literature review to examine a broad range of issues related to maritime transport resilience. It discusses resilience in maritime transport systems and freight networks, ports and supply chains, and the effects of climate change on port resilience. Liu et al. (2024) also utilized bibliometric analysis and a literature review but focused specifically on the implications of maritime transport resilience for international trade. This study emphasizes the need for more comprehensive economic evaluations using analytical models and simulations to assess the costs and benefits of resilience strategies. Additionally, it identifies a significant gap in research concerning geopolitical risks and their impacts on maritime transport resilience and trade. While both recent papers provide valuable insights into maritime transport resilience, they are limited by their reliance on bibliometric analysis. Although bibliometric analysis is useful for understanding the research landscape, it does not offer in-depth insights into the content, quality, or practical implications of the studies reviewed. This reliance may lead to conclusions that reflect publication trends rather than substantive advancements in the field. Additionally, bibliometric data can sometimes overemphasize certain research areas based on publication volume rather than actual impact or innovation. As a result, the papers face several limitations: a lack of sufficient discussion and categorization of resilience analysis methodologies from an engineering perspective, insufficient exploration of practical implementation of resilience strategies in seaports, and inadequate analysis of the resilience of seaport networks.

In this respect, it is imperative to conduct a comprehensive review study that provides a thorough overview of the advancements in the emerging field of seaport resilience. This study includes a summary of the existing body of knowledge, with particular emphasis on the qualitative and quantitative methodologies that have been developed. Furthermore, it consolidates the findings from various research papers, highlighting future research directions and recognising the current methodological challenges.

To achieve the objectives, a comprehensive critical review with a focus on seaport resilience is conducted, leading to the following significant contributions:

(1) Extensive coverage: A broad array of journal papers published over the past two decades is meticulously surveyed, providing a comprehensive and in-depth review, with the most relevant and research-worthy studies chosen through a rigorous screening process.

(2) Critical analysis: Critical literature review techniques have been employed to facilitate the exploration of previously unaddressed questions in existing research, thereby uncovering significant knowledge gaps in this field.

(3) Extensive discussion on resilience metrics and methodologies: A comprehensive examination of the resilience concept, along with the existing measures, methodologies, and strategies specifically applied within the seaport context, has been carried out, highlighting their complexities and practical applications.

(4) In-depth evaluation: This work extends beyond simple exploration, providing an in-depth evaluation that highlights both the strengths and weaknesses of the topics covered. It also identifies and discusses key challenges, while proposing potential directions for future research, offering valuable insights to the academic community.

The rest of this chapter is structured as follows: Section 2.3 presents the research methodology and the process of literature identification. Section 2.4 provides the concept, definition, application, and purpose of resilience assessment in the context of seaports. Section 2.5 particularly concentrates on the methodologies and approaches applied in the resilience analysis of individual seaports. Section 2.6 discusses the resilience of seaport networks, focusing on how disturbances might affect the interconnectedness and overall functionality of port networks. The discussion for existing challenges, policy implications and future research directions, as well as the insights and summary, are provided in Sections 2.7 and 2.8, respectively.

2.3 Methodology

To conduct an in-depth examination of resilience research within the seaport field, a critical review approach has been employed to find relevant publications for evaluation. This approach consists of four phases: 1) the use of online platforms for research studies retrieval and exploration, 2) the systematic evaluation and selection procedure employed to assess the suitability and credibility of sources, 3) the eligibility assessment, and 4) concluding the incorporation of research studies. The relevant studies have been gathered through a search performed using Clarivates's Web of Science, which is known for its robust search capabilities and well-acknowledged reputation for trustworthiness throughout the scientific world. While SCOPUS is widely utilized for research, its citation analysis tools are less robust compared to the Web of Science, offering only basic features. Web of Science's meticulous quality control, including manual indexing, assures researchers of database accuracy. Thus, choosing the Web of Science for locating seaport resilience papers is preferred due to its reliability and comprehensive citation analysis capabilities.

The procedure to search records started by using a combination of keywords as follows: ("seaport" or "sea port" or "port") AND ("resilience" or "resilient" or "resiliency") for the resilience analysis of individual seaports, and ("seaport" or "sea port" or "port") AND ("Network") AND ("resilience" or "resilient" or "resiliency") for the resilience analysis of seaport networks. The investigation was conducted throughout the timeframe spanning from 2000 to 2024 and yielded a total of 1131 records. Initially, it was decided that our investigation to be limited to only peer-reviewed publications, given that the peer-review process is often regarded as the most reliable means of securing acceptance within the scientific community. To this end, our study purposefully omitted conference proceedings, editorial articles, white papers, and book chapters since these sources are likely to provide retrospective perspectives on the topic matter. Furthermore, the screening process included reviewing the titles and

abstracts of the identified articles, and in some cases, doing a cursory reading or scanning of the content. In this phase, a substantial portion of the initially identified research papers were eliminated (967 out of 1131), with a retention rate of only 14% (164 papers) being maintained. In the literature review, stringent screening criteria were applied. The term 'resilience' encompasses various disciplines, necessitating the selection of studies directly addressing seaport resilience. Numerous papers explored related areas, such as supply chain and shipping network resilience, while others focused on broader concepts like economic and coastal community resilience. Additionally, papers from computer science, centred on different 'port' contexts, were excluded. These measures ensured the review's precision, resulting in a refined collection of studies specifically contributing to our understanding of seaport resilience assessment, while mitigating the inclusion of tangential or unrelated research.

In the phase of the eligibility assessment process, the screened records underwent further analysis through full-text review, leading to the elimination of 36 records. Consequently, only 128 publications were deemed to have the possibility for inclusion in our review. In this phase, we used a set of criteria to assess the significance of selected papers. These criteria included inquiries into the papers' pertinence to the overarching objective and their potential for deriving novel outcomes. For instance, in several cases, resilience was seen only as a sub-topic or a superficial designation. It is noteworthy that in addition to the aforementioned procedure, some papers were identified using reference tracking, which included examining relevant review studies and highly cited research papers. This methodology facilitated the inclusion of an additional 14 records in our comprehensive literature review.

Figure 2.1 illustrates the overall demonstration of the implemented procedure. Following the above four steps, all major studies are included in the analysis.

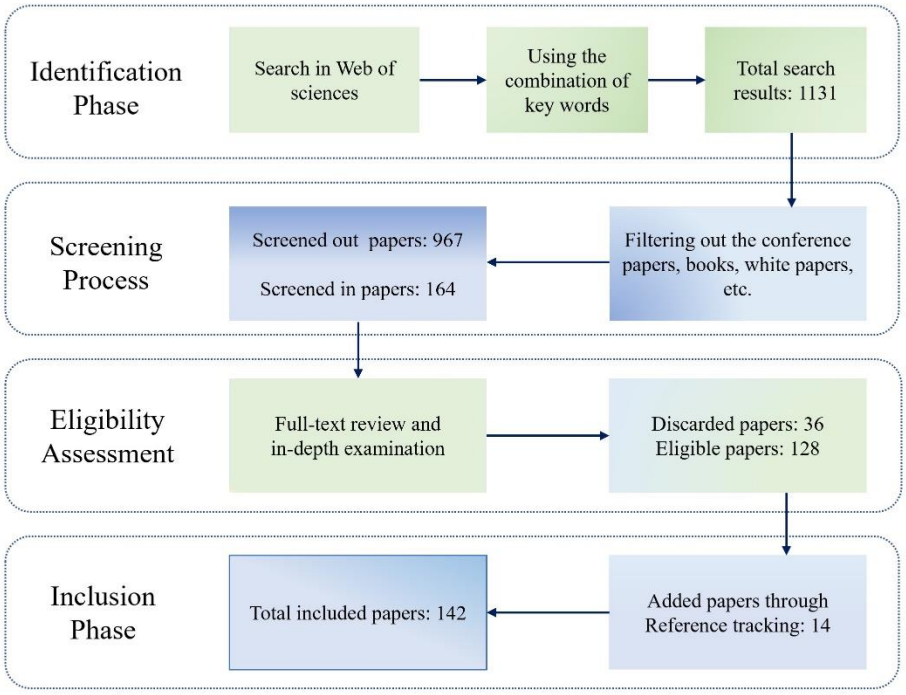

Figure 2. 1: The flowchart of the different phases in the literature review.

2.4 The concept of resilience in seaports

2.4.1 Definition and terminology

Resilience in many application fields is subject to varying viewpoints and definitions. Within the realm of engineering systems, and specifically in the domain of infrastructures, the concept of resilience encompasses several dimensions and viewpoints, resulting in the absence of a universally applicable definition. For instance, the National Infrastructure Advisory Council ("Critical infrastructure resilience: Final report and recommendations.," 2009) provided a definition of infrastructure system resilience, characterizing it as the capacity to predict, absorb, adapt, and/or quickly recover from a disruptive event such as natural disasters. (Hosseini et al., 2016) conducted a comprehensive literature review, including research publications that explore the definition, conceptualization, and measurement of resilience across many academic fields, with particular emphasis on engineering systems. Wan et al. (2018) conducted a thorough analysis of prior scholarly investigations, focusing on the elucidation and fundamental attributes of transportation resilience. Out of all relevant resilience definitions, this research aligns with the prevailing viewpoint within the maritime community and the term 'seaport resilience' is defined as the capacity of a port to effectively withstand disturbances, preserve its fundamental structure and operations, adapt to the existing situation, and then restore its service to a satisfactory level within an acceptable timeframe and financial constraints after the occurrence of disruptions.

According to the above-mentioned definitions, the features of resilience may be delineated using several terminologies, including, but not limited to, reliability, robustness, redundancy, vulnerability, flexibility, adaptability, and recoverability, among others. In this regard, Biringer et al. (2013) proposed three capacity categories of basic system features that contribute to infrastructure resilience and act as defence layers against disruptive events. These categories, namely absorptive, adaptive, and restorative capabilities, serve as a classification framework for different elements of resilience. Figure 2.2 illustrates the three resilience capacities and their respective elements in the context of seaport operations.

The 'absorptive capacity', as its name suggests, refers to the inherent capability of a system to absorb or endure the effects of any disturbances that pose a risk to its functioning, while also mitigating the resulting repercussions. As an endogenous characteristic of the system, this capacity is widely recognized as the primary mechanism for mitigating the impacts of disruptive events. The analysis of relevant scholarly sources has led us to identify five key components that contribute to this particular capability. These components include reliability, robustness, redundancy, diversity, visibility, and preparedness.

The 'adaptive capacity', as the second line of defence, is the ability of a system to adjust and reorganize itself in response to post-accident scenarios, while using non-standard operating approaches that require more resources and expenses, with the aim of minimizing the impacts of interruptions. Four elements of resilience that can be attributed to the adaptive capacity are identified as follows: flexibility, agility, collaboration, and communication.

The concept of 'restorative capacity' is presented as the last line of defence, denoting a system's capability to undergo repair, recovery, and restoration in a prompt and efficient manner in a way that the repaired system will function at the same level as its original condition. Given the

vast array of operations involved in this capacity, including services, methods, procedures, and technologies (resourcefulness), it necessitates a substantial amount of effort and financial investment compared to other capacities. Table 2.1 presents the definition of the terms related to seaport resilience.

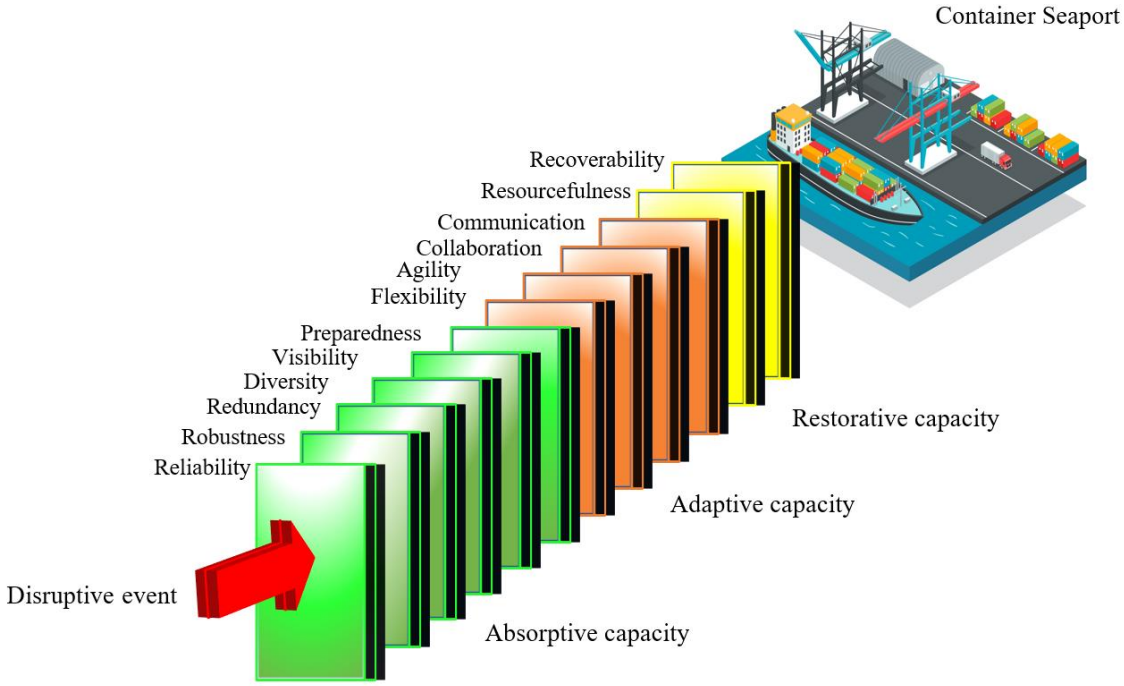

Figure 2. 2: Seaport resilience structure.

Table 2. 1: Seaport resilience terminology.

Term	Definition	Reference
Absorptive capacity	The ability of a system to absorb or withstand the impacts of any disruptions threatening its operation as well as minimizing the subsequent consequences.	*(Biringer et al., 2013)*
Adaptive capacity	The ability of a system to adapt itself to post-accident situations (reorganization) and employ unconventional operational strategies with extra effort and cost to mitigate the effects of disruptions.	*(Biringer et al., 2013)*
Restorative capacity	The ability of a system to be repaired, recovered, and restored quickly and efficiently, although requiring the greatest effort and cost.	*(Biringer et al., 2013)*
Reliability	The probability of a system to successfully operate at its optimum level of functionality under specific conditions and within a specified period.	*(Modarres et al., 2016)*
Robustness	The inherent characteristics of a system to withstand and absorb the stress of perturbations and disturbances while maintaining its functionality.	*(Faturechi and Miller-Hooks, 2015)*
Redundancy	The ability of a system to substitute its failed components or even sub-systems with the reserved embedded ones to take over the same functions in the same way.	*(Modarres et al., 2016)*
Diversity	Having multiple independent systems or components that can fulfill the same function, while possessing distinct attributes, to reduce the possibility of common cause failure.	*(Modarres et al., 2016)*

Visibility	Visibility refers to the ability to systematically monitor different operations such as tracking shipments and the corresponding supply *of* information throughout the entire process.	*(Kim et al., 2021)*
Preparedness	The ability to be prepared against disruptions through proactive implementation of specific measures prior to their occurrence.	*(Kwesi-Buor et al., 2019)*
Flexibility	The capacity to adjust, adapt, reorganize, and reconfigure in response to a disruptive occurrence, via the implementation of contingency strategies. The connotations associated with flexibility differ from those associated with robustness in the context of preserving system performance, rather than specifically preserving system structure.	*(Lagoudis et al., 2010)*
Agility	The capacity to promptly address disruptions with the aim of mitigating the extent of suboptimal performance.	*(Adam et al., 2016)*
Collaboration	The capacity of multiple groups to collectively view and participate in the process of decision-making together, to effectively address the disruptions.	*(Wang et al., 2023)*
Communication	The process of effective exchange of information for mitigating the consequences of disruptions among relevant groups of decision-makers, both prior to, during, and after such events.	*(Wang et al., 2023)*
Resourcefulness	Resourcefulness is described as the state or quality of having access to a sufficient quantity of materials, supplies, and personnel in order to effectively restore or maintain functionality.	*(Reggiani, 2013)*
Recoverability	The capacity to efficiently recover from disruptions and restore the normal functioning within a reasonable timeframe, while minimizing expenses and resource utilization.	*(Baroud et al., 2014)*
Vulnerability	The deficiency or susceptibility in the structure, design, functioning, and/or administration of a seaport, which makes it prone to damage or a considerable reduction in capacity in the face of disruptive events or diminishes its ability to return to a state of stability.	*(Pan et al., 2021)*
Survivability	Survivability refers to the ability of a seaport to resist various stressors, disturbances, or adverse events while maintaining essential functions and minimizing the impact on its overall stability and functionality.	*(Lagoudis et al., 2010)*
Rapidity	Rapidity is a measure of how quickly the system can restore its critical functions and resume regular activities after facing a disruption. A seaport with high rapidity can bounce back swiftly and efficiently from disruptive events, minimizing downtime and negative impacts to supply chains and customer service.	*(Baroud et al., 2014)*

2.4.2 Temporal phases of seaport resilience

To enhance understanding and facilitate the assimilation of the concept of resilience, as well as to see the role of resilience elements during disruptions, Figure 2.3 depicts the hypothetical performance level of a seaport and its fluctuations across three distinct temporal phases: pre-disruption, during the actual disruption, and post-disruption. The diagram follows the 'Resilience Triangle' concept (Fan et al., 2024) and aims to integrate the essential characteristics of resilience elements to depict the time-dependent representation of seaport performance. Over the pre-disruption period, a port's functionality depends on factors such as the design configuration, the reliability of its systems, sub-systems, and associated components, as well as the prevailing operating conditions. For simplicity, the system's functionality is represented by a linear model, assuming a steady state and disregarding any transitory deviations from the original state.

Upon the occurrence of disruptive events within the system, namely at time t_e, the absorptive capacity is triggered. This time may be divided into the following two distinct phases: In the

first phase, the system demonstrates its ability to withstand the effects of disruptive events by using redundant or diversified capabilities. This enables the system to uphold a minimal threshold of performance, demonstrating that it only fulfils the most basic requirements. In the second phase, depending on the severity of the disruptive event, functionality reduction persists beyond the complete exhaustion of redundant capabilities, resulting in continuous deterioration until time t_d, when the adverse effects of the disruption are fully manifested.

In this scenario, the system's functionality is at its lowest point, determined by the level of systems' robustness. In other words, the extent to which functionality decreases reflects the degree of vulnerability in the system, indicating a lack of robustness. The level of vulnerability shown by a system inversely correlates with the degree of its robustness. Following the point of maximum functional deterioration, denoted as time t_d, a series of adaptive and restorative mechanisms are initiated with the aim of restoring the system's functioning to a stable condition by time t_r.

It is important to acknowledge that the new state does not necessarily have to be at the same level as the initial state. This is because the new state has the potential to attain an alternative equilibrium level, which might be either an enhanced state (i.e., enhanced functionality) or a partially restored state (i.e., reduced functionality). During the recovery phase, the presence of various factors such as the availability of resources (human, technology, budget), agility, flexibility, effective communication, and efficient collaboration are of utmost importance. In the resilience diagram, the red dashed line indicates the presence of a highly resilient system, which implies that the system's functioning may see considerable improvement in comparison to its initial state. A stronger absorptive capacity not only reduces the vulnerability but also prolongs the occurrence of minimal functionality ($\Delta t_1' > \Delta t_1$). Furthermore, with enhanced adaptive and restorative capabilities, there can be an observed rise in the rate of recovery, suggesting a more rapid process of repair (see the slope of the recovery line, ($\Delta t_2' < \Delta t_2$)). It is worth mentioning that, following a disruption, the system's functionality may increase to a higher degree and its resilience against future occurrences may be enhanced due to the adoption of advanced adaptive capabilities and the incorporation of lessons learned from prior experiences or during the disruption. All in all, this observation indicates that systems encountering disruptive events and possessing higher resilience exhibit superior performance compared to those with lower resilience when facing the same disruptions.

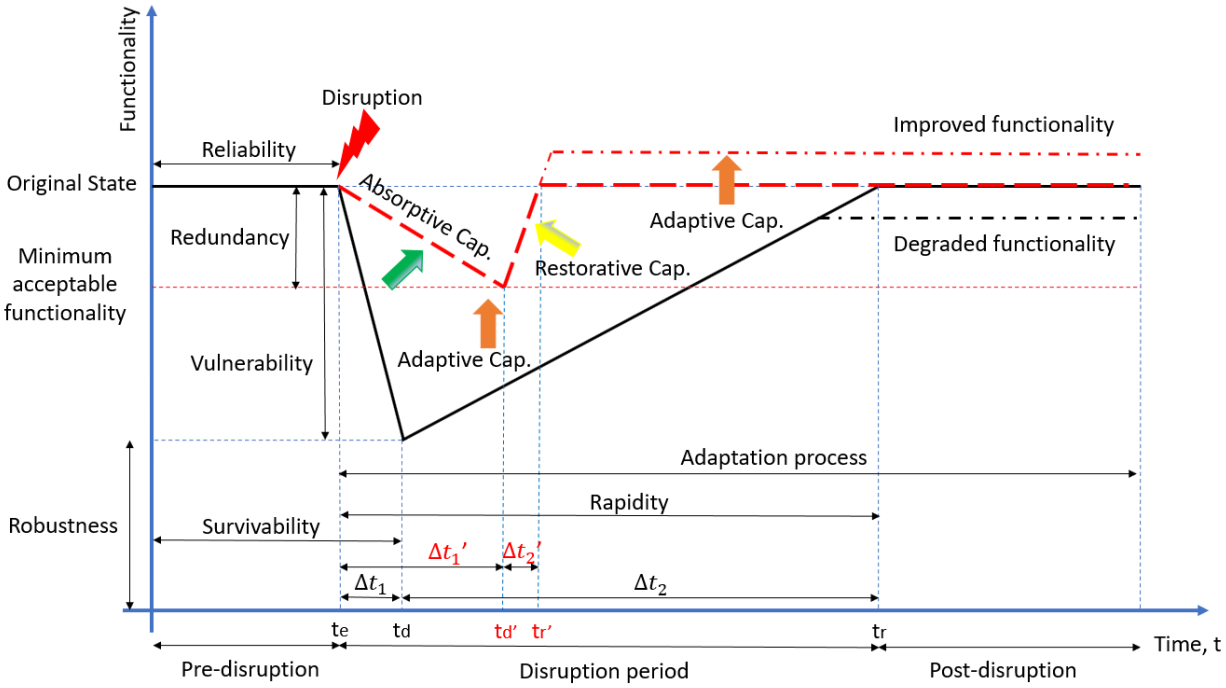

Figure 2. 3: Schematic representation of seaport functionality with consideration of resilience capacities.

2.4.3 Seaport disruptive scenarios

Maritime supply chains in general, and seaports in particular, are subject to numerous sources of risk, resulting in moderate to severe interruptions. There appears to be a growing recognition among academic researchers and industry stakeholders that seaports should not be viewed as merely another set of nodes in the supply chain. Instead, they should be seen as interconnected components and as central components of the maritime transportation system (MTS), with serious repercussions if they fail (Wendler-Bosco and Nicholson, 2020).

Given the interconnected operation of different parts in MTS, any disruption in any part will immediately propagate throughout the system, having an immediate impact on supply chains. In this regard, attempting to identify all possible types of hazards threatening the functionality of such important infrastructures is essential. Using lessons learned from research on safety and reliability in other critical fields such as aviation, nuclear, and chemical industries, potential disruptive scenarios in the context of seaports can be identified and classified using a data-driven approach or a qualitative process. In the former, hazards are detected and documented through a systematic process using historical events, allowing for traceability and additional analysis, and in the latter, discussions, interviews, and brainstorming from experts, academics and stakeholders are applied. Due to the nature of ports, the location they are built, the complex systems they consist of, and the sociological environment they operate in, a wide range of risks could impact their functionality. Mansouri et al. (2010) stated that hazards to ports can be classified into four main groups: natural disasters, organizational factors, technological failures, and human errors. Each group can also be attributed to different underlying causes originating from either external disturbances or internal perturbation of the ports' boundaries. To enrich the above list of classification, one might introduce the following disruptive scenarios which have received less attention but are critical in a case of occurrence, which are economic factors, land/ marine access disruptions, and network disturbances (Grainger and Achuthan, 2014). There are several noteworthy studies aiming at analysing the impact of different hazards on the seaports and discussing their subsequent consequences. With the help of the Automatic

Identification System (AIS), Verschuur et al. (2022) analysed 141 cases of port disruptions caused by natural disasters in 74 different ports throughout the world. Based on the empirical evidence they provided, they concluded that multiple ports at the same time, could be disrupted and even shutdown in case of extreme natural disasters, putting the reserve capacity at potential alternative ports at risk. Cao and Lam (2018) developed a novel framework based on the simulation of seaport operations, historical events and actual data logs to estimate the financial consequences of two major types of catastrophes that occur in ports, namely, natural disasters and human-induced hazards. Adam et al. (2016) conducted a systematic analysis of maritime disruptive scenarios over a period of six decades from 1950 to 2014 to evaluate their scale, time span and subsequent impacts on UK ports and the related areas. They categorized the disruptions into seven major sources, including human errors, technological failures, poor visibility, rough seas, snow and ice, storm surges and windstorms. Lam and Su (2015) provided a comprehensive assessment of port interruptions in East and South Asia from 2001 to 2011. They concluded that natural disasters and labour strikes are the two most frequent reasons for port interruptions, with natural disasters having the most damaging impact on supply chains. In Figure 2.4, a comprehensive analysis of the existing literature has been compiled to identify and categorize seven primary disruptive scenarios and their corresponding sub-factors that pose significant risks to the efficient operations of seaports.

Figure 2. 4: Seaport disruptive scenarios classification.

2.4.4 Seaport resilience strategies

Seaport resilience strategies are a crucial set of protective actions and contingency plans, including both reactive and proactive measures, with the objective of improving the ability of seaports to manage disruptions and swiftly bounce back from adverse events. These strategies encompass various features that are commensurate with the resilience capacities and elements. Figure 2.5 demonstrates the overall structure of seaport resilience and the relevant strategies. It is to be noted that the resilience strategies are not limited to the examples in Figure 2.5 and may be customized to the unique features of individual ports and their challenges against various disruptions. In this regard, we have compiled the different resilience strategies adopted in the selected papers in Table 2.2.

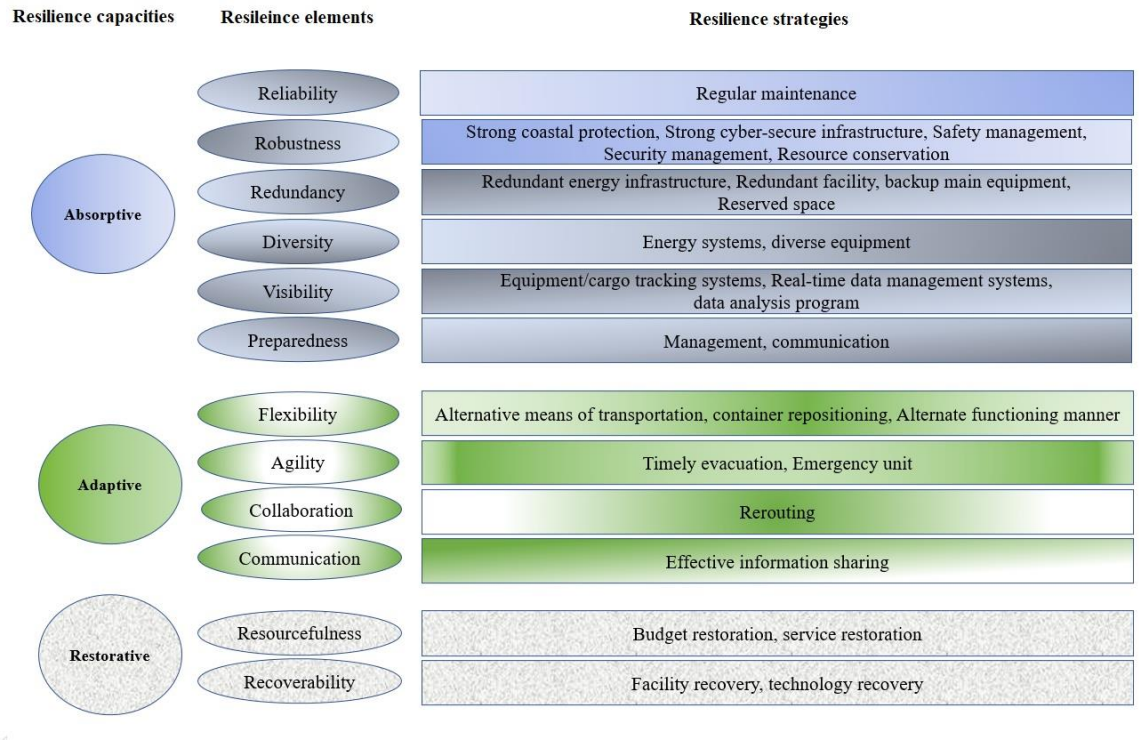

Figure 2. 5: Seaport resilience capacities, elements, and strategies.

Table 2. 2: List of resilience capacities, elements, and strategies in representative studies.

Study	Resilience capacity	Resilience elements	Resilience Strategies
(Hossain et al., 2019)	Absorptive	Redundancy, Robustness	Strong coastal protective measures, Energy redundant facilities, Safety management, Emergency response team
	Adaptive	Adaptability	Quick evacuation, Repositioning, mode flexibility
	Restorative	Resourcefulness	Resource restoration, budget restoration
(Hosseini and Barker, 2016)	Absorptive	Reliability, redundancy, robustness	Supportive utility systems, additional controlling equipment, Storm surge protection, Communication, Space utilization, maintenance, skilled labor management
	Adaptive	Adaptability	Quick evacuation, Repositioning, mode flexibility
	Restorative	Resourcefulness	Resource restoration, budget restoration
(Wang et al., 2023)	Readiness Response	Redundancy, robustness, visibility, agility, flexibility, recovery	Facility, technology and manpower restoration, alternative operation mode, real-time data management system, extra capital equipment, safety management, quick evacuation, alternative transportation mode, emergency response team, redundant facilities, and energy infrastructure
(Kim et al., 2021)	Absorptive	Robustness, redundancy, visibility	Situational operation manual, Emergency workforce mobilization plans, establishing backup offloading and transportation machinery, establishment of systematic inspection protocols, the modernization and visualization of IT systems for port operations, the use of cutting-edge technology, such as digital twins.
	Adaptive	Flexibility, collaboration, agility, and information sharing	Implementation of alternative operation strategies using big data, machine learning, etc., communication of the port's strategic objectives, consistent identification of client demands, personnel instruction on how to swiftly respond to emergencies, and information exchange for the development of collaborative response systems.

	Restorative	Response, recovery	Creating crisis-specific organizational and monitoring structures, Emergency preparedness instruction, devising strategies for funding the recovery of port functions during emergencies, the assessment of the viability of emergency plans preparations using simulation.
(León-Mateos et al., 2021)	Absorptive	Diversity, redundancy	Alternative sources of energy, new infrastructures,
	Adaptive	Information sharing, flexibility, collaboration,	Adaptive management, digitalization, transport improvement, Collaboration with insurance providers, consideration of the impacts and costs of the different adaptive plans, long-term proactive strategies, development of strategies to ensure uninterrupted functioning of infrastructure and facilities, relocation.
	Restorative	Response, recovery	Facility and technology recovery, service restoration.
(Omer et al., 2012)	Absorptive	Redundancy, robustness, diversity, modularity, capacity tolerance,	Alternative road transportation, increasing the port reserved capacity.
	Adaptive	Information sharing, collaboration, resource allocation, preparedness	Allocation of trains, trucks, and personnel
(Mansouri et al., 2010)	Prevention	Redundancy, vulnerability	Redundant information systems, redundant infrastructure systems, implementation of security monitoring systems,
	Recovery	Support and maintenance	Designing efficient maintenance strategies for the infrastructures
(John et al., 2014b)	Absorptive	Robustness, redundancy, modularity, visibility	Hardening infrastructure systems, constructing systems that can be attached and detached easily, enhancing the use of vessel traffic management systems, deploying floating harbor cranes, investing in container tracking technology, making infrastructure systems more cognitive,
	Adaptive	Collaboration, resource allocation, information sharing,	Proper allocation of resources to enhance operation, collaborative efforts between stakeholders for an efficient information flow
	Restorative	Resourcefulness,	Increasing staffing in critical areas, consideration of high-capacity tolerance of the systems
(Mutombo et al., 2017)	Preparedness	Robustness,	Incorporating projected climate forecasts into the planning and construction of port infrastructure.
	Adjusting	Redundancy, diversity,	Rerouting cargoes to a back-up port, using rail line and road interchangeably
	Rebounding back	resourcefulness	Consideration of efficient operations and timely implementation of sophisticated supply networks
(Cho and Park, 2017)	Preparedness	Robustness	Allowance capacity, substitution by nearby ports
	Recovery	Rapidity, resourcefulness	Allocating enough resources for repairing and recovery

2.5 Seaport resilience assessment methodologies

In this section, the primary emphasis is placed on deliberating upon all relevant aspects of resilience assessment in seaports. Utilizing an extensive examination of the relevant literature and following the classification of resilience assessment methods presented in (Hosseini et al., 2016), the research of seaport resilience may be approached in a similar manner. The approaches to evaluating the resilience of seaports against the above-discussed disruptive scenarios can be classified into three primary categories, namely qualitative, semi-quantitative, and quantitative approaches. The qualitative approaches deliver a general comprehension of

the definition of resilience, the interaction between the resilience elements, the identification of causal relationships between various influencing factors in resilience, and the establishment of an overarching framework to categorize resilience strategies based on resilience elements. As guiding principles and roadmaps, qualitative approaches can assist stakeholders in understanding resilience and recognizing the relevant strategies adopted to improve resilience. However, when it comes to addressing the multitude of variables and discerning precise quantitative correlations between them, qualitative approaches are not sufficient, and there arises a need for a complementary approach. This necessity can be explained by the fact that managers or decision-makers tasked with devising strategies require a solid justification for their decision-making process to optimize resource allocation for strengthening system resilience, a need that qualitative approaches alone cannot fulfil. In this regard, quantitative approaches have the potential to address the aforementioned limitations and offer more compelling and cogent insights. The following sections introduce and discuss the different resilience assessment methodologies developed and applied in the context of seaports and their related superstructures.

2.5.1 Qualitative approaches

The qualitative approaches in the literature can be further categorized into conceptual frameworks and empirical studies.

2.5.1.1 Conceptual frameworks

The qualitative assessment of seaport resilience is predominantly carried out through the utilization of conceptual frameworks. This approach deals with a wide range of concept-related subjects, such as terminologies, attributes, conceptual foundations and modelling. The study by Mansouri et al. (2010) is considered a seminal study in introducing conceptual frameworks within the realm of seaport resilience. The authors developed a risk management-based decision analysis (RMDA) framework consisting of three main phases, namely vulnerability assessment, resilience strategies development, and cost-effectiveness analysis, to provide the seaport stakeholders with a tool to select the best available policies for the improvement of port infrastructure resilience.

The issue of fragmented information flows among multiple stakeholders in seaports has been widely recognized as a significant barrier to coordinated responses during disruptive events. Various researchers have developed conceptual frameworks to address this challenge, each offering distinct approaches to improving seaport resilience. These frameworks can be categorized into different thematic areas, including decision-making processes, stakeholder engagement, information sharing, and organizational resilience.

In terms of decision-making and process architecture, Mostashari et al. (2011) introduced the Cognitive Process Architecture Framework (CPAF). This framework aims to support the effective perception of changes and events, facilitate the analysis of operational scenarios, enable informed decision-making by accounting for trade-offs, and ensure continuous monitoring of the implementation of selected actions. This approach highlights the need for a dynamic and adaptive framework that evolves with the complexities of seaport operations, making it particularly relevant in scenarios where rapid responses are required. Almutairi et al. (2019) adopted a different approach, emphasizing the fluctuating interests and influences of different stakeholders over time. Their framework integrates stakeholder mapping and disruption scenario modelling to address varying levels of stakeholder participation in response to disruptive scenarios. By recognizing that stakeholders' priorities may shift depending on

economic, environmental, and social factors, this framework allows for more strategic planning initiatives aimed at enhancing resilience. Shaw et al. (2017) tackle the issue of information sharing between key seaport stakeholders, including managers, shipping firms, and logistics businesses. Their multi-level case study methodology led to an information-sharing model that leverages both supplier and customer perspectives. The key insight here is that subjective information, when shared effectively, can enhance seaport resilience by enabling stakeholders to act promptly and allocate resources more efficiently. This approach provides a practical solution for optimizing limited resources, emphasizing the operational benefits of improved communication channels among stakeholders during disruptions. Vanlaer et al. (2022), developed a framework that categorizes resilience-building activities into three key phases: anticipation, coping, and adaptation. Their model applies these phases across the policy, economic, and operational domains, offering a comprehensive approach to seaport resilience. By focusing on these domains, the framework ensures that resilience is not only a reactive measure but also a proactive process, embedded within the broader organizational strategy of seaports. This holistic approach suggests that resilience must be built at multiple levels, from policy planning to day-to-day operations, to be effective.

Categorizing the above-mentioned approaches reveals two major focuses: process-driven frameworks (such as CPAF and the information-sharing model) and stakeholder-centric frameworks (as demonstrated in the stakeholder mapping by Almutairi et al. and the organizational resilience model by Vanlaer et al. (2022)). Both categories highlight the importance of collaboration and communication, but each addresses different aspects of resilience: process frameworks prioritize efficiency and optimization, while stakeholder frameworks emphasize the need for inclusive and flexible engagement strategies.

Despite the merits of conceptual approaches, such as providing a structured methodology for understanding seaport resilience and helping researchers and practitioners systematically evaluate various dimensions of resilience, their theoretical foundation and limited reliance on quantitative data can weaken the persuasiveness of their conclusions, potentially leading to an incomplete representation of the overall picture.

2.5.1.2 Empirical studies

Moving away from conceptual approaches, there also exist some survey-based studies that aim to analyze port resilience. Empirical studies provide valuable, data-driven insights into seaport resilience by focusing on real-world events and gathering the perspectives of those directly involved in port operations. These studies offer practical, grounded recommendations for improving resilience, such as identifying common disruption patterns or developing risk management models.

Trepte and James (2014) research found that US seaport disruptions typically last 6 to 20 days. They analyzed cargo concentration, disruption duration, and capacity requirements to reduce port bottlenecks. Additionally, *Rice and Trepte (2012)* gathered insights from stakeholders, concluding that ports are resilient to daily fluctuations and minor disruptions. However, their study showed that the maritime transportation system lacks sufficient resilience when facing large-scale disruptions, highlighting a gap in preparedness for significant challenges. These works capture the firsthand experiences and perspectives of various stakeholders, such as port managers and users. This provides a comprehensive understanding of port resilience from the viewpoint of those directly involved in operations. The involvement of multiple stakeholders ensures that empirical studies reflect the practical challenges faced during disruptions, making the findings highly relevant to real-world applications. A similar approach, conducted by *Loh and Thai (2015a)*, classified the port-related supply chain disruption threats into four

categories, namely, infrastructure threats, manpower threats, planning threats and security threats, through interviewing the professional port managers as well as port users. They also proposed a management model to improve the resilience of seaports regardless of their specific cargo handling types, regions, or stages of development. The strength of empirical research lies in its ability to connect theory to practice, validating resilience frameworks through actual disruptions and stakeholder input. However, empirical studies also face challenges. The limited scope of data, potential lack of generalizability, and difficulty in addressing large-scale, complex disruptions present notable drawbacks. Moreover, the reliance on stakeholder interviews and qualitative data can introduce subjectivity, which might hinder the development of universally applicable strategies.

2.5.2 Semi-quantitative approach

A semi-quantitative methodology seeks to furnish a structured framework for assessing resilience by harmonizing the depth of qualitative understanding with the precision of quantitative analysis. An often-used strategy in semi-quantitative resilience evaluation involves assigning scores or rankings to various resilience indicators or elements. These assessments may draw upon a blend of qualitative assessments, expert insights, and quantitative data.

A semi-quantitative measurement framework to evaluate the resilience of seaports was established by Kim et al. (2021), drawing upon an extensive review of pertinent scholarly literature. This framework was empirically validated through the implementation of both exploratory and confirmatory factor analyses, utilizing a sample of 199 individuals representing various stakeholders within the port industry in South Korea. Based on the findings of the study, they came to this conclusion that the Korean ports possess a certain degree of adaptive and absorptive capabilities for encountering adverse circumstances. However, they exhibit a relatively limited level of restorative capability to respond to such circumstances when they do occur. Mutombo et al. (2017) introduced a novel approach that uses resilience scores to assess the resilience of port infrastructure against climate-related hazards. By providing the scores, this approach delivers clear and actionable results. These scores can highlight areas of strength (e.g., adaptive and absorptive capabilities) and weakness (e.g., limited restorative capabilities), helping stakeholders prioritize actions. The weighted scoring system, where preparedness is given a higher priority, allows decision-makers to focus on crucial adaptive measures.

While semi-quantitative methods aim to harmonize qualitative and quantitative aspects, reliance on expert insights and qualitative assessments introduces a level of subjectivity. Additionally, assigning weights and scores, though useful for decision-making, can sometimes oversimplify the complexities of resilience. As a result, the mathematical formulas used to calculate resilience may overlook nuanced factors or interdependencies between resilience elements, potentially leading to an incomplete picture.

2.5.3 Quantitative approaches

This section provides a discussion of various quantitative methodologies for assessing the resilience of seaports. Based on the literature review, we have identified four major approaches used in the relevant studies: Bayesian Networks (BN), multiple criterion decision making, simulation, mathematical modelling and optimization. It's worth mentioning that certain

additional approaches have been identified which do not fall into the previously established categories. As a result, they are all addressed under the miscellaneous category heading.

2.5.3.1 Bayesian Networks

BN is a formal probabilistic methodology that is utilized to represent the causal relationships between random variables through the utilization of conditional probabilities. With a diverse array of functions in the domain of risk, reliability and in particular, resilience engineering, as well as its capability to combine various pieces of information, including objective and subjective data, BN has emerged as an advanced tool for uncertainty modelling in the realm of seaport resilience assessment.

Hosseini and Barker (2016) applied BN to assess the resilience of the Port of Catoosa against various disruptions, focusing on the "Triple Resilience" capacities: absorptive, adaptive, and restorative. They developed strategies for each capacity and validated their model through sensitivity, forward, and backward propagation analyses. Similarly, Hossain et al. (2019) devised a five-phase BN-based resilience assessment for the Port of Pascagoula, incorporating disruptions like natural disasters and cyber-attacks. Their sensitivity analysis highlighted the importance of maintenance practices, alternate routing, and manpower allocation in enhancing port resilience. Building on this, Hossain et al. (2020) expanded their research by integrating interdependencies into a BN model, recognizing geographic, service provision, and repair access as key factors. All the above-mentioned studies emphasize the utility of BN for resilience assessment, highlighting maintenance, interdependencies, and adaptive strategies as essential to enhancing port infrastructure resilience under various disruptive scenarios. The approaches underscore the significance of interconnectedness in port operations and supply chain management.

Wang et al. (2023) developed a circular four-stage research framework using a BN model to assess the resilience of Shanghai Yangshan Deepwater Port. They categorized resilience capabilities into two main areas: readiness (pre-event actions) and response (post-event actions). To validate their model and gain insights, they conducted sensitivity analysis along with forward and backward inference analyses.

In line with relevant studies, Panahi et al. (2022) developed a BN model to measure the resilience of Hong Kong’s Kwai Tsing Container Terminals in the face of the Covid-19 pandemic. They applied similar approaches in BN models, such as sensitivity and propagation analyses, to extract useful insights. The results indicated that the primary variables contributing to the enhancement of seaport infrastructure resilience are port connectivity, training, and service improvement.

It goes without saying that BN offers a powerful framework for analysing seaport resilience by modelling causal relationships, handling diverse scenarios, and incorporating interdependencies. The ability of BN to blend qualitative and quantitative data makes it a versatile tool in assessing resilience across multiple dimensions, from infrastructure to human factors. However, the success of BN models depends heavily on data quality and the expertise of those building and interpreting the models. To maximize the benefits of BN in seaport resilience analysis, ongoing refinement of models and broader data collection efforts are essential, along with improving accessibility for non-experts in the field.

2.5.3.2 Multiple Criterion Decision Making

In the realm of seaport resilience assessment, the intricate nature of systems and the multitude of factors at play, necessitate the consideration of diverse techniques, including expert judgment, cost-benefit analysis, collaborative design and modelling of the system. This has resulted in an enhanced assortment and abundance of tools for decision-making, leading to the emergence of Multi-Criteria Decision Making (MCDM) tools. In this regard, the MCDM framework encompasses the integration of qualitative and quantitative data, along with the implementation of suitable resilience strategies, to mitigate the potential impact of disruptive scenarios and improve the overall resilience of seaports. Some illustrative examples of adopting MCDM for seaport resilience analysis can be tracked in the following works. John et al. (2014b) proposed a framework combining the Fuzzy Analytical Hierarchy Process (FAHP) and fuzzy TOPSIS to select optimal resilience strategies for seaports, using nine criteria (e.g., cost, safety, reliability) and analysing 11 strategies. FAHP was used to assign weights, while TOPSIS ranked the strategies. Sensitivity analysis examined the impact of weight variations on rankings. Similarly, Cao and Lam (2019) applied fuzzy Evidential Reasoning (ER) and fuzzy TOPSIS to assess port vulnerability post-2015 Tianjin Port explosion, offering insights into port resilience by addressing both pre- and post-disruption vulnerabilities in uncertain scenarios.

The MCDM approach offers a comprehensive framework for quantitative analysis by integrating both qualitative and quantitative data, enabling a well-rounded assessment of seaport resilience. Additionally, the method can be tailored to various criteria and scenarios, making it adaptable to different contexts and needs. Techniques such as FAHP and TOPSIS provide systematic ways to rank resilience strategies based on multiple factors. However, the process of assigning weights and performing sensitivity analyses can be time-consuming and complex. Furthermore, expert judgment and the selection of criteria introduce subjectivity, which may negatively influence the results.

2.5.3.3 Simulation

The evaluation, design, and configuration of resilience strategies in seaports pose significant challenges due to various factors such as the geographical characteristics of the port, the unpredictable and diverse nature of disruptive events, the management of investments and allocation of resources, as well as the complex interactions among numerous other variables. In this respect, simulation could be a useful approach to deal with the complexity of the process by executing numerous iterations and experiments to investigate the responsiveness of a model to various scenarios and inputs. Several studies have applied simulation models to assess port resilience, as detailed below.

Folkman et al. (2021) developed a simulation model to examine the adverse impacts of hurricanes on Houston port operations, demonstrating how natural disasters affect TEU throughput and port efficiency. This approach allows stakeholders to explore the effects of disruptions on various aspects of port operations, providing valuable insights into both pre- and post-disruption scenarios. However, the accuracy of simulations depends heavily on the data and assumptions used. Their model may be limited by the availability and precision of real-

world data regarding port operations, and the assumptions about recovery timelines and infrastructure capacity can affect the validity of the outcomes.

Zhou et al. (2021) established a decision support system that utilizes digital-twin modelling to assess the resilience of a port in the face of three power supply disruption scenarios with specific levels of power shortage as well as determine the most suitable course of actions to be taken following the disruptions. The findings of the research indicate that neglecting ordinary operational uncertainties in port models can lead to a substantial overestimation of resilience levels, which subsequently will result in misleading conclusions for port operators, falsely indicating that their port possesses a high level of resilience.

Loh and Thai (2015b) conducted simulations to ascertain the importance of ports in the context of supply chain disruptions. The research aimed to establish a comparative analysis of costs associated with various scenarios, namely, no disruption, waterway accidents, 12-hour delay, and port shutdown resulting from a strike. The findings indicated that the escalation in expenses during an unfavourable occurrence is primarily ascribed to elevated warehousing storage costs, inventory storage costs, labour costs, and transportation costs. The limitations of their study can be succinctly described as the absence of a sensitivity analysis and the exclusive examination of disruption effects on a single category of cargo.

Shafieezadeh and Ivey Burden (2014) proposed a comprehensive framework for assessing port resilience through simulation analysis. Their developed framework was specifically designed to evaluate the seismic performance of a hypothetical seaport terminal located on the West Coast of the United States, considering both the during and post-hazard phases. While the study gives port operators insight into vulnerabilities, particularly how berths are more affected than cranes, and highlights the long recovery timelines after significant seismic events, it may not account for other types of disruptions, such as economic or environmental shocks.

Based on the above studies, it can be concluded that simulation is a powerful tool for analysing seaport resilience due to its ability to model complex real-world scenarios and test responses to various disruptive events. However, its effectiveness is limited by the quality of data, assumptions made during model construction, and the potential omission of key variables or scenarios. To fully maximize the benefits of simulation in resilience assessments, models should be continuously refined with updated data, broader risk considerations, and the inclusion of sensitivity analyses.

2.5.3.4 Mathematical modelling and optimization

In the context of port resiliency, mathematical modelling-based approaches are well-established and frequently used methods which in conjunction with optimization techniques, are usually employed to optimize the resilience for achieving the maximum effectiveness. Zhen et al. (2022) sought to evaluate the resilience of a seaport by quantifying the resilience of its traffic-electric power coupled system. They developed a two-stage stochastic mixed-integer nonlinear mathematical model within the constraints of a predetermined budget. The two-stage entail making a decision regarding the implementation of preparedness measures in the initial stage, and the implementation of appropriate recovery measures for the power system in the second stage. The result indicated that simultaneous implementation of the pre-event preparedness measures and post-event recovery measures yields greater advantages in

enhancing and sustaining port resilience. León-Mateos et al. (2021) introduced a Port Resilience Index (PRI) to evaluate seaport resilience by associating it with perceived indicators. Using a multi-stage approach, they identified climatic risks, analysed resilience factors, and incorporated expert opinions to derive normalized scores. A case study at the port of Galicia, Spain, revealed a PRI of 52%, highlighting the port's vulnerability to climate change impacts, especially concerning its infrastructure, facilities, and operations.

Mathematical modelling and optimization approaches provide a powerful framework for assessing and enhancing seaport resilience by enabling the quantification and optimization of relevant strategies such as preparedness and recovery. These models are particularly useful for handling complex, coupled systems and allow for structured, scenario-based decision-making. However, their effectiveness can be compromised by data scarcity, simplifying assumptions, and the potential subjectivity involved in indicator-based models. To maximize their usefulness, mathematical models should be continuously refined with updated data, and efforts should be made to reduce bias in indicator selection and weighting.

2.5.3.5 Miscellaneous methodologies

In addition to the aforementioned methodologies, several other approaches that do not fit into the previously discussed categories have been utilized in the literature. For instance, Galbusera et al. (2018) put out a theoretical framework based on Boolean networks to analyse the complex interdependencies and dynamic nature of a multidomain port infrastructure network. The construction of the model is grounded in the use of directed functionality graphs, whereby the nodes symbolize infrastructure components, and the edges symbolize the interdependencies between them. This study aims to examine the performance of a seaport under stressful conditions and analyse its recovery profile using resilience metrics. These metrics include functionality measurements, systemic impact, total recovery effort, and departure from desired system performance levels. Cho and Park (2017) developed a framework for port infrastructure resilience assessment using system dynamics. Their framework evaluates the resilience of port systems by considering various factors such as disruption, recovery actions, and long-term effects. In addition, the model further integrates socioeconomic aspects, such as fluctuations in freight demand and financial conditions. Table 2.3 provides an overview of relevant research along with their outputs.

Table 2. 3: Seaport resilience assessment methodologies.

Approach	Methodology	Remarks	Representative Studies
Qualitative	Conceptual framework	Conceptual frameworks are concerned with describing the resilience elements and identification of their causal links. They benefit the stakeholders and managers with a general framework as a guiding principle.	*(Almutairi et al., 2019; Mansouri et al., 2010; Mostashari et al., 2011)*
	Empirical studies	Empirical studies in resilience assessment entail collecting real-world data via observation or experimentation to comprehend and assess the resilience of a given system.	*(Loh and Thai, 2015a; Rice and Trepte, 2012; Trepte and James, 2014)*
Semi-quantitative	Scoring systems, Ranking methods	The semi-quantitative approaches focus on constructing resilience elements and assessing their characteristics based on expert elicitation on a number or percentage scale.	*(Kim et al., 2021; Mutombo et al., 2017)*

Quantitative	Bayesian Network	BN has the ability to accurately represent the cause-and-effect connections among different variables, handle both objective and subjective data and allow for probabilistic resilience analysis.	*(Hosseini and Barker, 2016; Panahi et al., 2022; Wang et al., 2023)*
	Multiple criteria decision-making	MCDM is concerned with the consideration of both qualitative and quantitative elements simultaneously to address the complexity of port resilience assessment. A combination of fuzzy techniques such as FAHP and TOPSIS could be a good example of the MCDM approach.	*(Cao and Lam, 2019; John et al., 2014b)*, *(Wan et al., 2024)*
	Simulation	The simulation approach enables the evaluation of the performance of ports in different scenarios and investigates their behavior under specified conditions.	*(Folkman et al., 2021; Shafieezadeh and Ivey Burden, 2014; Zhou et al., 2021)*
	Mathematical modeling	This methodology relies on mathematical models and ideas for the definition of resilience elements and quantification of relevant items.	*(León-Mateos et al., 2021; Zhen et al., 2022)*
	Miscellaneous	There are other resilience analysis procedures that do not align with the aforementioned particular categories, while providing innovative ways to quantitatively address the concept of seaport resilience.	*(Cho and Park, 2017; Galbusera et al., 2018)*

2.6 Network resilience assessment of seaports

In the previous sections, the papers were examined on the resilience of ports within their physical boundaries and their individual capacity to withstand various disruptions. However, it is important to note that seaports are not confined to their physical boundaries, but are part of various interconnected networks, collectively known as port networks. From this perspective, a port's overall performance, despite all preventative, mitigative and recovery measures implemented within its operational zone, is contingent upon the efficacy of other ports within the network. This is because an individual port with suboptimal functionality may significantly impair the overall system performance. To illustrate this point, consider a hypothetical incident occurring at an arbitrary port, which impacts its capacity to efficiently manage and execute a certain volume of goods or services within a given time frame. A lack of berth capacity for incoming vessels will lead to delays in the movement of vessels to subsequent locations, resulting in queues and increased congestion both upstream and downstream. The presence of a disruption is clearly linked with subsequent disruptions that spread throughout the network, causing negative consequences for the functioning of other ports and the overall performance of the network system. Given this situation, it is crucial to examine, measure, and improve the resilience of port networks in relation to the systemic risk concept. This analysis should take a broader perspective, considering the repercussions of any disturbances that may impact the interconnectedness of port networks.

In this regard, a modest number of studies conducted over the past decade have focused on investigating the impacts of disruptions on the operation of seaport networks. In the work conducted by Mansouri et al. (2009), they aimed to conceptualize and analyse maritime transportation systems as a 'System of Systems' (SoS). 'Systems Thinking' is employed to examine key attributes of a SoS, including resilience and security, in response to disruptions within a complex network of ships, seaports, intermodal links, waterways, and users. Rose and

Wei (2013) proposed a systematic approach that integrates demand-driven and supply-driven input-output (I-O) analyses for assessing the overall financial ramifications due to a port service interruption, taking into account various key dimensions of resilience. Olalla (2012) constructed and applied attacker-defender network interdiction-optimization models to assess the global maritime network resiliency against manmade disruption caused by either piracy or political issues at critical chokepoints of maritime routes. From the perspective of seaport network resiliency, numerous studies have proposed approaches for modelling resilience in the broader maritime network. These approaches can be categorized into two main groups: centralised and decentralised approaches. The former assumes that investment decisions for network resilience improvement can be centrally determined with the full cooperation of all ports for the collective benefit, disregarding business competition among ports. In contrast, decentralised approaches align more closely with real-world scenarios. They assume that ports operate in a competitive and cooperative manner, striving to enhance their individual market shares. The predominant focus in the existing literature on the subject of seaport network resilience, revolves around centralised approaches, which have employed a range of methodologies, including graph theory (Cui and Notteboom, 2018), mathematical optimization (Peng et al., 2016), empirical analysis (Poo et al., 2024), and system dynamics (Omer et al., 2012), among others.

However, in recent years, a few studies have put forth a co-opetitive optimization scheme, which combines competition and collaboration, as an alternative to centralised decision-making for improving the port networks resilience. Their argument is predicated on the belief that pooling substantial capital investment and exchanging crucial information among diverse entities or nations that own port facilities is considered impractical and unattainable. The idea of co-opetition was first presented by Nalebuff et al. (1996) within the realm of business management. Drawing on this concept, Asadabadi and Miller-Hooks (2018) put up a conceptual framework in which individuals involved with the port, assuming the roles of participants in a game, engage in collaborative efforts through cross-port investment. The aim of this collaboration is to enhance throughput during a disaster event, while simultaneously engaging in competitive activities to secure business opportunities. The dynamics of co-opetition observed among ports are addressed by employing a bi-level multiplayer game theoretic framework, in which, each individual port makes strategic investment decisions aimed at protecting its interests, while also considering the potential reaction of the typical market-balancing shipping mission problem within the affected network. Games were modelled to simulate a range of cross-port investment plans, including unrestricted (where ports may invest arbitrarily), limited (where ports only invest in themselves), and semi-restricted (where certain ports can invest across borders while others will only self-invest). Asadabadi and Miller-Hooks (2020) further expanded their analytical approach to evaluate the resilience of a port network in the face of various natural hazard events. Similarly, using the concept of Equilibrium Problems with Equilibrium Constraints (EPECs), Li et al. (2022) conceptualized a framework to investigate the potential benefits in terms of resilience, return on investment and demand fulfilment rates that can be achieved through port coalitions. In these coalitions, individual ports have the opportunity to invest in the protection of coalition member ports, and the members can also pool their resources during times of catastrophic occurrences. Based on the results, it is indicated that the overall resilience of the network is enhanced through mutual investment and capacity sharing in the face of significant disruptions. Although there might be a slight drop in the level of resilience of individual ports, particularly

those that engage in capacity investment or collaboration with other ports. Table 2.4 provides a modest compilation of relevant studies on the resilience of port networks. They have been organized according to their classification and the different types of disruptive scenarios they analysed.

Table 2. 4: List of studies on port network resilience assessment.

Approach	Methodology	Disruption scenario	Research output	Literature
Centralized	conceptualized qualitative framework	Natural hazards	Developing a novel risk framework to analyze the impacts of weather and climatic related events on three layers of port networks, including critical infrastructure, hinterland, and maritime networks and to provide different resilience strategies against identified systemic risks.	*(Verschuur et al., 2022)*
	Network optimization problem, System dynamics	Natural and anthropogenic hazards	Proposing a framework called Networked Infrastructure Resiliency Assessment (NIRA) to optimize maritime network performance. The proposed framework treats the problem as a network optimization task, with the objective of maximizing the overall flow on the network links. In this respect, three MTS resiliency metrics (tonnage resiliency, time resiliency and cost resiliency) are suggested.	*(Omer et al., 2012)*
	Complex networks, Graph theory	Climate disasters	Developing a multi-stage framework based on the integration of climatic risk variables, centrality evaluation, and an optimized model of shipping routes to address the related vulnerabilities and to analyze the resilience of the global shipping networks.	*(Poo and Yang, 2022)*
	Empirical study, Graph theory	Earthquake, malicious attack, hurricane	Studying and analyzing the local ports' resilience against the impacts of the selected shocks based on a spatiotemporal scale.	*(Rousset and Ducruet, 2020)*
	Fuzzy logic, Bayesian Networks, Evidential reasoning	Operational risks	Establishing a comprehensive methodology for evaluating the resilience of maritime container transport networks (MCTNs), assessing the hazards associated with container shipping activities as well as the significance of individual shipping routes across MCTNs. Network centrality measures are employed to assess the susceptibility of individual shipping routes across the network.	*(Wan et al., 2019)*
	Graph theory	Seismic hazards, political conflicts	Modeling the impacts of both natural and anthropogenic disruptive scenarios on a multi-port system and liner shipping networks through quantification of port and route capacity reduction. A cost-based container assignment model is also implemented to minimize the total system-wide cost.	*(Achurra-Gonzalez et al., 2019)*
	Complex network theory	Intentional attacks, random failure	Developing a framework to assess the robustness of the global shipping networks against failure of nodes (ports).	*(Angeloudis et al., 2013)*

	Mathematical model	Unpredictable disasters	Developing a two-stage stochastic program to allocate optimized limited resources to seaports against undesired events for minimization of total loss.	*(Peng et al., 2016)*
De-centralized	Game theory, Mathematical model	Earthquake, Flooding	Developing a co-opetitive protective investment problem for port network protection against natural disasters and improving their resilience.	*(Asadabadi and Miller-Hooks, 2018)*
	Game theory, Mathematical model, optimization technique	Tsunami, Earthquake, Flooding	Modeling a stochastic optimization program for finding optimal investment strategies to improve reliability and enhance the resilience of ports in a network against natural disasters.	*(Asadabadi and Miller-Hooks, 2020)*
	Game theory, mathematical model,	Hurricane, Tsunami, Earthquake, Flooding	Developing an EPEC for improving the resilience of individual ports and the network they are in, based on resource pooling in protective plans of action through coalition idea.	*(Li et al., 2022)*
	Conceptual qualitative framework	Climate disasters	Developing a standard set of guidelines based on a multi-stage methodology to enhance the resilience of individual ports and the larger network they represent.	*(Python and Wakeman, 2016)*
	Dynamic spatial Markov Chain (DSMC)	Financial crises, Epidemics, Environmental and ecological risks, Traffic congestion, Trade disputes and conflicts	The resilience analysis of regional container port networks, identifying key factors influencing resilience and proposing strategies to enhance network adaptability amid external shocks and internal risks.	*(Chang et al., 2024)*

2.7 Discussion and research gap identification

This section provides a concise, evaluative examination of the previously discussed topics, exploring their shortcomings and challenges, as well as potential avenues for future research.

2.7.1 The concept of seaport resilience analysis

The primary focus on resilience in the context of seaports is attributed to their capacity to withstand and recover from a disruptive scenario. In terms of measuring seaport resilience, numerous research investigations have addressed the concept of resilience by examining the fluctuations in functionality over a period of time. Some studies consider the ratio of the degraded system functionality to its original state, while others express it as the ratio of recovery to loss of functionality. However, resilience is a comprehensive concept that encompasses various scales and dimensions, requiring evaluation from diverse perspectives and throughout different time periods, including pre-disruption, during disruption, and post-disruption.

A partial assessment of capabilities or phases would not deliver a thorough evaluation of seaport resilience, as most of the articles reviewed in this study fail to fulfil this requirement. In this regard, it is strongly recommended that resilience metrics designed for seaports should extend beyond a partial temporal stage and should also encompass various dimensions of resilience, including reliability, vulnerability, resourcefulness, cost-effectiveness, and even

safety culture. An additional significant aspect that has been overlooked by the majority of research studies is the assessment of the vulnerability of main components which contribute significantly to maintaining the seaport functionality. Unlike the reliability assessment of engineering systems, which includes the identification of critical components as an essential aspect, little research has been conducted to identify the vulnerable components and measure their criticality level based on the resilience of the whole seaport. A holistic approach not only helps in addressing the vulnerabilities of a seaport but also contributes to a deeper understanding of the trade-offs involved in achieving both efficient resource allocation and increased resilience. With the use of quantitative metrics, it enables the comparison and evaluation of various resilience strategies to determine the optimal outcomes. Therefore, the formulation of a systematic framework to evaluate the resilience of seaports, factoring in the aforementioned items, presents a significant area for future investigation.

2.7.2 Disruptive scenarios and resilience strategies

Figure 2.6 shows the distribution of the disruptive scenarios in 142 seaport resilience papers that we have analysed. 32% of them deal with environmental-related disruptions, and 27% of them are related to human-induced ones. This is unsurprising, as the majority of disruptive events are linked to the geographical locations of seaports and the significant engagement of human activities. However, it is important to acknowledge that some sub-factors within the realm of the aforementioned factors, such as climate change and cyber-attacks, continue to be sources of concern and require more scrutiny from academics. In contrast, there is a significant lack of analytical frameworks that specifically examine the concept of seaport resilience in relation to access and network factors.

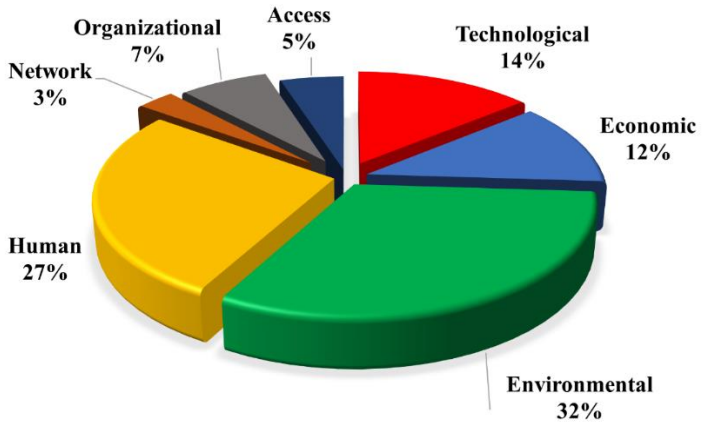

Figure 2. 6: Percentage distribution of disruptive scenarios in seaport resilience studies.

One notable aspect of the disruptive scenarios is the presence of interdependent multi-hazards. This term refers to a situation where multiple disruptive events, whether natural or anthropogenic, occur simultaneously, consecutively, or partially overlap. As a result, this situation introduces greater potential for adverse effects on seaport functionality and increases the complexity of response and recovery operations. A historical example that exemplifies the concept of interdependent multi-hazards and their repercussions on seaports is the case of Sendai port in Japan (Kazama and Noda, 2012). In 2011, a massive earthquake followed by a subsequent tsunami led to substantial structural damage to port infrastructure, such as cranes, quays, piers, and storage facilities, as well as the inundation of the port zone by the resulting

tsunami waves. An additional layer of complexity was also added to the disaster by the release of radioactive materials from the damaged Fukushima Daiichi Nuclear Power Plant, located relatively close to the port. This practically hampered the response and recovery efforts due to radiation concerns. In light of this matter, which has been overlooked by the existing studies, it is imperative to explore interdependent multi-hazards within the seaport environment and advance corresponding resilience models in future research investigations.

Concerning resilience strategies, as discussed in section 2.4.4, effective approaches typically involve a blend of proactive risk reduction, adaptive capacity-building, and flexible response methods. However, the existing literature lacks an extensive exploration of diverse resilience strategies and their impact on seaport resilience. Hence, future research should prioritize understanding various resilience strategies, their influence on resilience components, and the development of innovative quantitative evaluation methods. To facilitate this, a comprehensive list of applicable resilience strategies for seaports, along with detailed descriptions and applications, is provided in Table Ap.1 in the appendix.

2.7.3 Methodologies developed for seaport resilience assessment

The prevailing methodologies used for assessing resilience in the context of seaports include conceptual frameworks, semi-quantitative approaches, BN, simulation, MCDM, mathematical modelling and optimization techniques. Figure 2.7 shows the distribution of the methodologies utilized by the studies reviewed in this article. As can be seen, simulation approaches constitute the majority of approaches, accounting for 31%, followed by conceptual frameworks (23% of the reviewed studies).

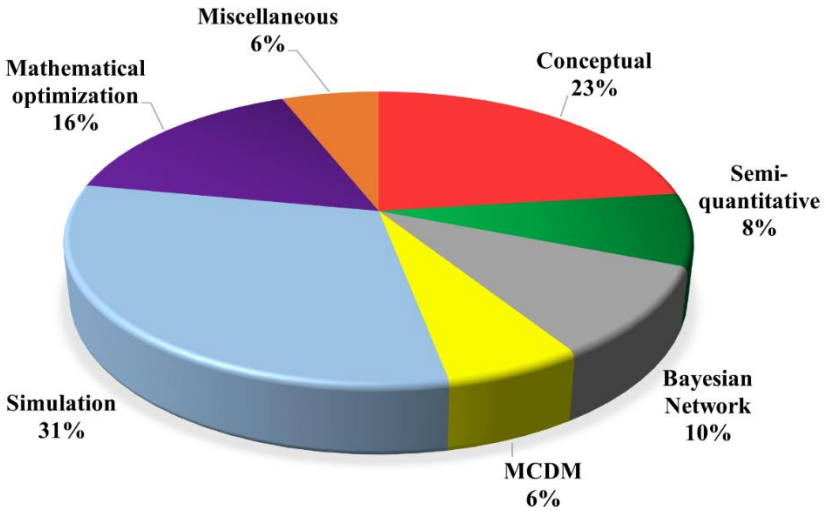

Figure 2. 7: Percentage distribution of different methodologies adopted for seaport resilience assessment.

To get a deeper insight into the capabilities of these methodologies, Table 2.5 presents a detailed overview of their advantages and disadvantages.

Table 2. 5: Strengths and limitations of different resilience assessment methodologies.

Methodology	Strengths	Limitations
Conceptual framework	Provides a structured and organized methodology that facilitates an overall	Because of the theoretical foundation of conceptual frameworks and due to

	understanding of seaport resilience, outlines the key components and essential elements that contribute to a port's resilience, and finally assists researchers and practitioners in conducting a systematic evaluation of various dimensions of resilience.	their limited reliance on quantitative data, the conclusion may lack persuasiveness, thereby failing to provide a comprehensive representation of the whole picture.
Semi-quantitative	Leverages both quantitative data and qualitative insights and allows for the incorporation of qualitative input from experts and stakeholders when quantitative data is unavailable.	The presence of biases has the potential to exert an influence on one's judgment. The utilization of expert judgments is hindered by the insufficient comprehension and management of biases, giving rise to various challenges.
Bayesian Network	Being able to model uncertainties, dependencies and inter-dependencies between various factors in complex systems, to integrate different types of data, including quantitative data from historical records, expert elicitations, and qualitative insights, to simulate different scenarios and to conduct sensitivity analysis.	The utilization of BN necessitates a substantial volume of data, and its analysis and computation entail intricate processes. Moreover, developing BN is a challenging task that requires substantial effort and expertise. Therefore, only the network's designer may utilize causal effects.
MCDM	Capable of handling both quantitative data and qualitative insights, where a combination of quantifiable measures and expert judgments is necessary, mitigating biases and promoting judgments by assigning weights to criteria.	The effectiveness of the methodology could be contingent upon the precision and comprehensiveness of the employed data. Moreover, the inclusion of subjective criteria and the utilization of fuzzy logic may introduce a certain degree of uncertainty into the decision-making process.
Simulation	Provides a dynamic and quantitative approach for examining various disruptive scenarios; effectively capturing the dynamic behaviors of a system and offering valuable insights into the propagation of disruptions; tests different resilience strategies and assists in optimizing resource allocation to boost seaport resilience.	Despite its utility, this evaluation methodology demands a significant investment of time and resources, as well as a limited scope of testing that only encompasses specific case scenarios.
Mathematical modeling and optimization	Facilitates a more evidence-based and data-driven decision-making by evaluating the decisions and strategies based on measurable criteria; assists the decision-makers to quickly evaluate the potential consequences of different strategies by integrating mathematical models and real-time data; helps to understand the system's behavior by representing interactions and dependencies mathematically; optimizes the resource allocation by considering various constraints and objectives.	Mathematical models are usually based on specific assumptions and scenarios, and there are certain factors that are not accounted for. Therefore, their applicability in real-world contexts may be limited.

2.8 Conclusion

This chapter represents an inaugural, critical and comprehensive assessment of current studies on seaport resilience using the Web of Science database. Through this study, the approaches, models, and techniques that have been developed for the resilience analysis of seaports were identified, categorised and analysed. Furthermore, an extensive inventory of disruptive scenarios, as well as the relevant resilience strategies pertaining to these scenarios, were compiled. The findings of this study reveal a limited body of research on the topic of seaport resilience, despite the high degree of importance associated with this important infrastructure. Moreover, the methodologies that have been established in this context are still in their infancy and possess significant potential for improvement. It is believed that the incorporation of additional quantitative techniques would enhance the robustness and perception of the methodologies developed for the investigation of seaport resilience. This study also contributes significantly to identifying research gaps in enhancing seaport resilience and exploring potential avenues for future investigation. The outcomes established in this review serve as a critical cornerstone for further research, offering valuable insights for both academic scholars and industry practitioners. Moreover, this review article not only provides practical approaches for implementation but also furnishes essential references for managing seaport disruptions, whether at the individual or network level.

While this study endeavours to shed light on methodologies pertinent to the analysis of seaport resilience, it is imperative to recognize some limitations that warrant discussion. Foremost among these limitations is the omission of research pertaining to seaports within the broader intermodal transportation network, known as maritime supply chain resilience. The complex dynamics of the maritime supply chain, which involves the interplay of various transportation modes such as railways and roads is required to be addressed for the sake of a holistic resilience analysis. However, it is noted that this absence stems from the primary focus of this study, which prioritizes methodologies directly relevant to the examination of seaport resilience. Secondly, this review study draws upon papers from reputable journals as its main source for identifying relevant literature. While this is a standard practice for conducting a critical review paper, the decision to exclusively rely on it for literature selection means that potentially valuable studies, including conference papers, white papers, technical notes, and relevant reports, are neglected. Consequently, there may be some degree of literature omission, which could have influenced the comprehensiveness of the findings and the overall scope of the review.

In summary, seaport infrastructures are vulnerable to a diverse array of disruptions, necessitating further efforts in the development of innovative approaches to assess and enhance their resilience against these threats.

Chapter 3 : Physical security risk assessment

3.1 Summary

This chapter develops a novel maritime security risk analysis framework grounded in empirical data from maritime terrorism incidents over the past two decades. Given the low-frequency yet high-consequence nature of such events, the chapter addresses the critical need for research that manages inherent uncertainty and compensates for the limited body of literature in this area.

Focusing specifically on attacks targeting ships, the chapter investigates recent trends and recurring patterns in maritime terrorism. It explores key influencing factors, such as vulnerable regions, high-risk countries, weapon types, and attack tactics, and examines the causal relationships among these variables. Through this analysis, the chapter introduces a comprehensive quantitative approach to terrorism risk assessment in the maritime domain, built upon a data-driven Bayesian Network (DDBN) model. Utilizing information from the Global Terrorism Database, this method enables systematic evaluation of terrorism-related risks, offering a structured means to identify critical contributing factors, analyse their interdependencies, and determine the likelihood and consequences of diverse terrorist scenarios.

The developed DDBN model undergoes extensive verification and validation, including sensitivity, metric-based, and comparative analyses, and is further tested using real-world case studies to demonstrate its applicability in both retrospective and predictive contexts. By integrating diagnostic and prognostic capabilities, the model provides actionable insights into the propagation of terrorism risk within the maritime sector. The findings of this chapter offer valuable contributions for industry stakeholders and governmental bodies alike, enhancing the understanding of maritime terrorism dynamics and supporting the formulation of more effective preventive and emergency management strategies.

3.2 Introduction

Due to the immense significance of global maritime trade, constituting over 80% of worldwide trade in goods, there are notable concerns regarding the potential impact of terrorist attacks. Given the vast expanse and relatively unregulated environment of seas and oceans, maritime transportation has emerged as an appealing target for terrorist groups. However, in comparison to incidents on land, acts of maritime terrorism represent a minimal proportion of overall armed violence and terrorist attacks, as indicated by Asal and Hastings (2015). The Global Terrorism Database (GTD) reports that less than 0.2% of the total attacks have occurred at sea in the last five decades (“START,” 2023). Nonetheless, this statistical rarity does not warrant overlooking or underestimating the potential consequences of maritime terrorism. Before further discussing the intricacies of maritime terrorism, it is essential to establish a clear definition of the term. It should be noted that, similar to terrorism, there is no universally accepted definition for maritime terrorism (Zelenkov et al., 2022). The GTD defines a terrorist attack as “the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation” (“GTD,” 2021). Nevertheless, given that maritime terrorism falls within the broader category of terrorism, its general definition should align with that of terrorism. However, when considering the specific

aspects of the definition, it is important to acknowledge that maritime terrorism possesses distinct features of its own. The term "maritime terrorism" is employed to encompass acts of terrorism that arise from the complexities associated with maritime security.

According to Nincic (2005), maritime terrorism is defined as "*any illegal act directed against ships, their passengers, cargo or crew, or against seaports with the intent of directly or indirectly influencing a government [or] group of individuals*". Joyner (1989) has presented a somewhat different definition that extends to encompass threats originating from a vessel associated with terrorist activities. It describes maritime terrorism as "the systematic use or threat to use acts of violence against international shipping and maritime services by an individual or group to induce fear and intimidation in a civilian population in order to achieve political ambitions or objectives." Concerns regarding methodological approaches to defining "maritime terrorism", the potential threats posed by maritime terrorism, and strategies to address its challenges are also discussed in (Asal and Hastings, 2015), (Farrell, 2007), (Nincic, 2005), and (Knyazeva and Korobeev, 2015). Drawing insights from an extensive collection of papers, it can be inferred that maritime terrorism essentially entails a manifestation of political violence employing a strategic approach aimed at destabilizing or disrupting maritime transportation processes to attain specific political objectives.

Within the realm of maritime terrorism, a plethora of maritime targets exist, including but not limited to a variety of ship types such as oil tankers, cargo ships, fishing boats, LNG carriers, ferries, naval crafts, and civilian vessels. In terms of infrastructure, container seaports and harbours with oil and LNG terminals, refineries, petrochemical installations, underwater pipelines, seabed-crossing cables, and offshore facilities pose attractive targets for terrorist groups. In this context, it is important to highlight the susceptibility of maritime targets. Actions such as armed assaults against passenger vessels, detonating oil tankers, abducting ship crew, or hijacking cargo vessels could prove quite impactful, capturing global media attention and providing terrorists with a significant advantage. Events like the destruction of a refinery or a major port, the sinking of a ship, and the obstruction of maritime chokepoints can hold considerable political value for terrorists and have the potential to inflict substantial economic losses at both national and international levels.

From a different perspective, terrorists require substantial funds to fuel their nefarious objectives. One lucrative avenue for acquiring financial resources involves hijacking cargo ships and kidnapping crew members, subsequently demanding ransom. Additionally, it is crucial to consider the potential for engaging in activities that could result in environmental harm. This includes attacking containers transporting hazardous materials such as nuclear waste, contaminated materials, or other chemical-related substances (Rajput, 2022). Such actions not only pose security threats but also have the potential to cause significant environmental damage, as demonstrated by the most heinous incidents, such as Achille Lauro in 1985 and the USS Cole in 2000 ("START," 2023). In contrast to maritime incidents driven by factors such as human errors, equipment failure, or environmental conditions, maritime terrorism poses a distinct challenge. It involves intelligent human actors or actors who take extreme risks and do not follow standard procedures, can bypass security measures, and are notably driven by the desire to attract media attention. Nevertheless, documented incidents indicate that while the tactics employed by terrorists have experienced minimal change, there has been a consistent expansion in the range of targets they choose to attack.

This chapter, therefore, aims to develop a new maritime security risk analysis method. It will use real data from maritime terrorism incidents over the past two decades to train a Data-Driven Bayesian Network (DDBN) model. Note that the scope of this study is limited to attacks against ships rather than infrastructure such as seaports or offshore facilities. It seeks to track recent trends in maritime terrorism and identify potential patterns. The chapter also pinpoints influential factors in maritime terrorism, such as vulnerable regions, high-risk countries, types of weapons, and attack tactics and aids to discern the causal relationships between these factors. The approach relies on a DDBN, and leverages information accumulated over the last two decades from the GTD. This methodology facilitates a comprehensive evaluation of the risks linked to terrorist attacks, providing a robust foundation for in-depth analysis.

The rest of the chapter is organized as follows. Section 3.3 offers a comprehensive critique of the current literature on maritime terrorism and the utilization of the technique. In Section 3.4, the specifics of the chosen methodologies are investigated, encompassing the procedures of data collection, BN structure learning, and model validation. Section 3.5 presents the analysis results and deliberates on the model's outputs. Lastly, the conclusions are drawn in section 3.6.

3.3 Literature review

The persistent challenge of international terrorism remains a concern, with ongoing reports underscoring its high impact on maritime activities. An extensive examination of the literature indicates that studies on maritime terrorism predominantly focus on theoretical frameworks and definitions (Chalk, 2008; Ganor, 2002; Schwenkenbecher, 2012), governmental and legal perspectives (Asal and Hastings, 2015; Hong, 2012; Rajput, 2022; Schneider, 2013; Shah, 2013; Tan, 2012), general and private security challenges (Greenberg et al., 2006; Knyazeva and Korobeev, 2015; Nincic, 2005; Richardson, 2004; Tertia and Perwita, 2018; Tilly, 2004), enhancements to operational systems (Knyazeva and Korobeev, 2015; Kuhn et al., 2023), and other qualitative research (Hacaga, 2020; Schneider, 2020; Zelenkov et al., 2022). The majority of past investigations into maritime terrorism have primarily employed a qualitative perspective, with only a limited number delving into the identification of security risk factors that impact maritime terrorism. In research carried out by Nelson (2012), the study identified factors that distinguish maritime terrorism from piracy and also examined whether the individuals responsible for these activities are collaborating with each other. A quantitative assessment of the effects of terrorism and piracy was conducted on maritime-related economic activities in the Niger Delta region of Nigeria (Eberechukwu Onwuegbuchunam et al., 2021). Using the Linear Regression Analysis model, the authors identified a noteworthy inverse relationship between the chosen maritime-related economic activities and incidents of maritime terrorism and piracy. Statistically examining the period from 2010 to 2017, Schneider (2020) conducted an analysis of terrorist attacks on maritime targets. This research investigates the current patterns in global maritime terrorism, the attributes of the perpetrators and their attacks, the geographical regions of the incidents, and the types of weapons and methods used.

While quantitative studies in the maritime industry related to terrorism are scarce, other domains have employed a diverse range of quantitative analysis models to scrutinize terrorism (Dillon et al., 2009; Li and Yang, 2023; Liang et al., 2024; Monroe et al., 2018; Regens et al., 2015; Rezazadeh et al., 2019). Ezell et al. (2010) investigated various methodologies for analysing security risks of terrorism, with a focus on probability and decision-making

frameworks. The methods explored included fault/attack/success tree analysis, event tree analysis, and game theory. Nevertheless, these approaches exhibit weaknesses in modelling terrorist risk. They struggle to handle uncertainties associated with influential factors and cannot clearly pinpoint the causal interrelationship among these factors (Zhu et al., 2020). Moreover, they face challenges in addressing questions regarding the specific impact and level of influence that different factors have on the varied attack risks posed by individual perpetrators. Given the drawbacks highlighted earlier, BN emerges as a promising method for overcoming these limitations. BN has the capability to incorporate information from multiple sources, assess the likelihood of events, forecast the outcomes of diverse scenarios, account for both objective and subjective data, address variables with multiple states, handle multiple outputs, and identify causal relationships among contributing factors leading to the top event. BN also possesses a robust theoretical foundation and is well-suited for handling incomplete data. Additionally, it exhibits the ability to incorporate new data, updating the probabilities of events accordingly (Kabir and Papadopoulos, 2019; Wei, 2022). When employing BN for risk assessment in safety or security, the initial step involves constructing the BN model, which includes multiple interdependent risk factors. Various methods can be utilized for this purpose, such as literature review, expert judgment, data learning, or a combination of these approaches. In the realm of maritime risk assessment, Bouejla et al. (2014) and Pristrom et al. (2016) employed expert judgment along with data sourced from the International Maritime Organization (IMO) to establish a BN structure for assessing the risk of piracy attacks on ships. Similarly, Jiang and Lu (2020) utilized a combination of statistical data and expert knowledge for BN structure learning, applying this approach to analyse maritime piracy in Southeast Asia.

While expert knowledge remains crucial for BN development, particularly in situations with incomplete or unavailable data, it is acknowledged that this approach introduces subjectivity and potential uncertainty. To mitigate such subjective elements, there is a growing trend in the academic community towards DDBN approaches. This methodology becomes particularly popular when there is a wealth of data available, allowing for the construction of BN models based on learning from the data itself. The utilization of a data-driven approach is evident in various maritime risk assessment studies. Some researchers employed a DDBN model to simulate global maritime risk analysis (Li et al., 2023), investigate collision risk analysis (Li et al., 2024a), explore the dynamic accident evolution (Li et al., 2024b), and conduct maritime severity analysis (Zhou et al., 2024). Fan et al. (2022) developed a DDBN model to explore the joint impact of risk factors on different types of maritime accidents within restricted waters. In another instance, Liang et al. (2022) conducted an analysis of influential risk factors affecting theft-related accidents in freight supply chains. They constructed a BN using a data-driven approach to predict the likelihood of the occurrence of such events.

In summary, the main research gaps identified from the literature review are summarized as follows:

1) Predominance of qualitative studies: Most previous research on terrorism broadly, and maritime terrorism specifically, has predominantly focused on qualitative analysis. These include theoretical frameworks, governmental and legal viewpoints, and overall security challenges. There is a noticeable lack of quantitative analysis of the specific security risk factors affecting maritime terrorism.

2) Limitations with current quantitative approaches: Conventional approaches for assessing terrorism-related security risks, including fault/attack/success tree analysis, event tree analysis, and game theory, have notable limitations. These techniques have difficulty managing uncertainties and are not adept at uncovering causal interrelationships among the various influential factors.
3) Incompleteness of maritime terrorism studies: Many current studies in this field fail to encompass the spatial-temporal aspects of recorded attacks. This results in an incomplete understanding of the actual events.
4) Shortage of data-driven approaches: There is a growing trend towards DDBN approaches in risk science, which are particularly useful when there is a wealth of data available. These approaches can construct BN models based on data learning, reducing the subjectivity associated with expert judgment. Although DDBN models hold promise, their use in maritime security risk assessment is still limited, presenting opportunities for further investigation.

Building upon prior research and the research gaps identified, this chapter endeavours to pioneer the application of data-driven learning in constructing a Tree Augmented Naïve Bayes (TAN)-based model for the analysis of maritime terrorism. To achieve this objective, the GTD database is used to extract information on terrorist incidents involving ships over a 22-year period from 2000 to 2021. The outcomes of this study aim to provide a substantial contribution to the comprehension of maritime terrorism. Additionally, the research seeks to enhance understanding of the risk characteristics associated with terrorist attacks in this domain, filling a gap that, to the best of the authors' knowledge, exists in the current literature.

3.4 Methodology

In this research, a DDBN technique is employed to uncover the security risk influencing factors (SRIFs) affecting terrorist incidents in maritime transportation. The primary goal is to assess the significance of these factors and gain a more profound insight into the workings of maritime terrorism. This methodology comprises of four primary stages, namely data acquisition and processing, model construction and development, model validation, and model output. Figure 3.1 depicts the comprehensive framework of the proposed methodology.

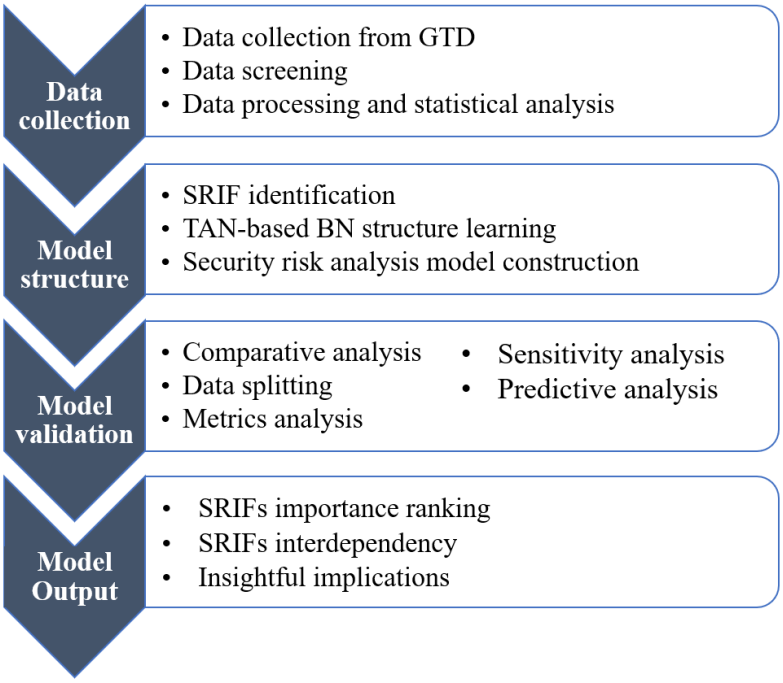

Figure 3. 1: The proposed methodology framework.

3.4.1 Data collection, exploration and processing

This study utilizes the GTD as its main source for documenting terrorist incidents. Initially, alternative terrorist databases were considered, including the National Memorial Institute for the Prevention of Terrorism (MIPT) Terrorism Knowledge Base, the Worldwide Incidents Tracking System (WITS), the Research ANd Development (RAND) Database of Worldwide Terrorism Incidents, and the International Terrorism: Attributes of Terrorist Events (ITERATE). Nevertheless, the GTD is notable for being the most extensive repository of terrorism incidents because of the following reasons: a) the prior databases have been discontinued for a considerable duration of time; b) they do not possess the metadata accumulated by the GTD compilers; c) Different databases offer varying definitions of terrorism. Contrary to other databases, GTD is an extensive compilation of reported terrorist activities worldwide, encompassing over 200,000 incidents since 1970. The data is sourced from the United States (US) National Consortium for the Study of Terrorism and Response to Terrorism (START), an esteemed department of Homeland Security of Excellence located at the University of Maryland in the United States ("START," 2023). The first step involved extracting the pertinent data on maritime terrorism from the GTD for the period from 2000 to 2021. It should be noted that the GTD has not recently updated its database over the past two years, but it is still the most comprehensive database available. Out of the 204 identified occurrences, 160 cases are specifically linked to acts of terrorism targeting ships and other marine vehicles. The remaining incidents consist of terrorist assaults targeting seaports and other fixed infrastructure, which have been excluded from the analysis.

The GTD encompasses a multitude of characteristics pertaining to terrorist occurrences, such as the nature of terrorism, the regions most affected by terrorism, the nations where the incidents took place, and the dates of the incidents. There are numerous aspects related to terrorism that prompt us to analyse the spatial-temporal distribution of maritime terrorism. As

depicted in Figure 3.2, the frequency of terrorist attacks on ships does not exhibit a discernible pattern. Nevertheless, there has been a general increase in the number of incidents over the last ten years, reaching a peak in 2016. Figure 3.3 illustrates the distribution of terrorism occurrences by month, revealing that the first and last three months of the year witness the highest incidents. Five main global locations are focal points for maritime terrorist activity, as depicted in Figure 3.4. Southeast Asia and Sub-Saharan Africa are particularly identified as high-risk regions. An additional noteworthy aspect is the variety of maritime vessels susceptible to terrorism. Figure 3.5 shows that fishing boats and tankers are the primary targets for terrorist activities. Following closely are cargo and commercial ships. It is important to note that various vessels may be vulnerable to different types of terrorist attacks, a topic that will be explored in the subsequent sections.

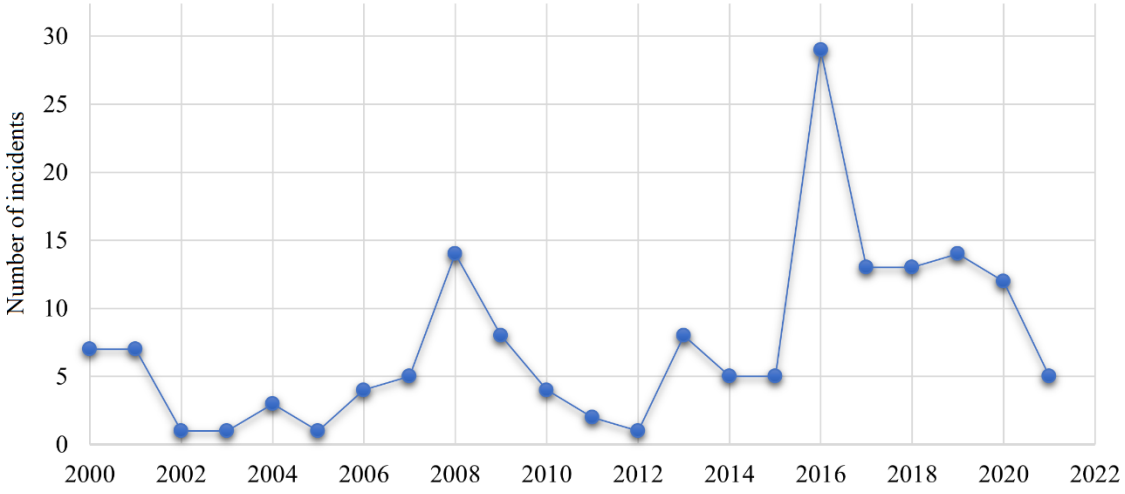

Figure 3. 2: The distribution of terrorist attacks for maritime vessels over 22 years (GTD).

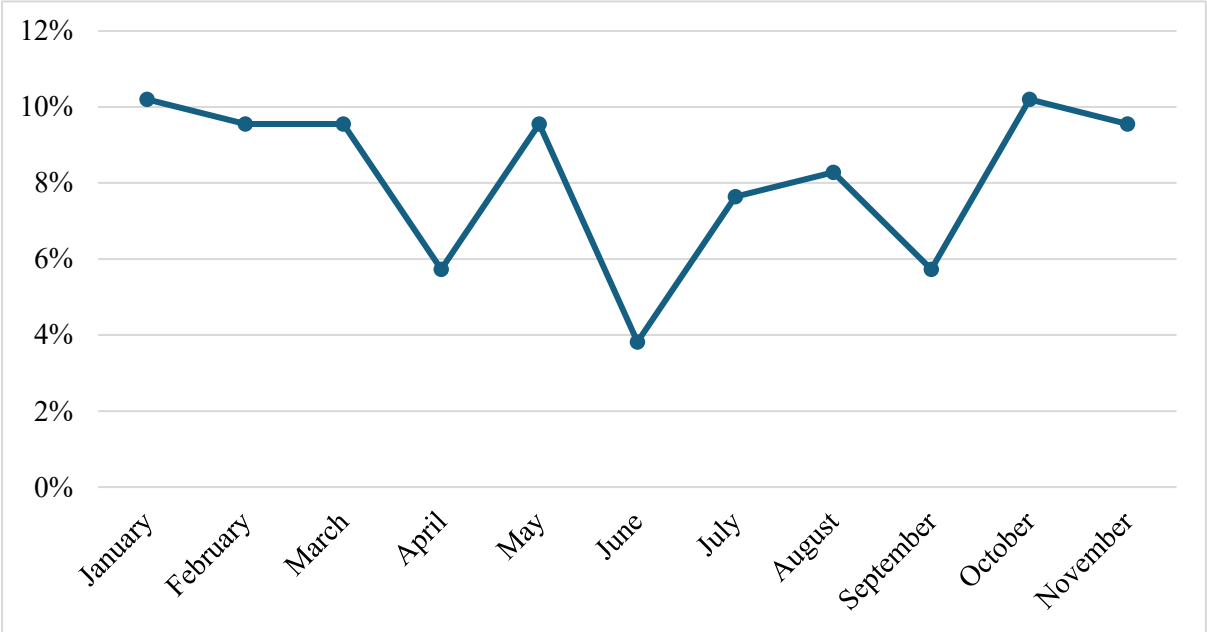

Figure 3. 3: The percentage of incidents over months of year (GTD).

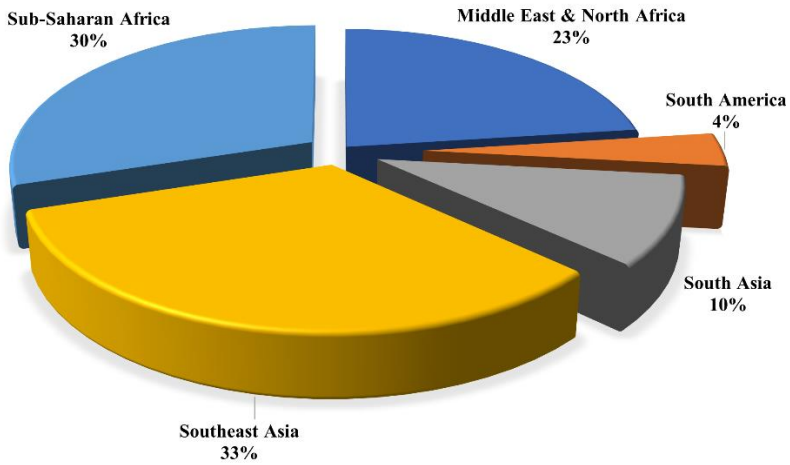

Figure 3. 4: The distribution of incidents over critical regions of the world (GTD).

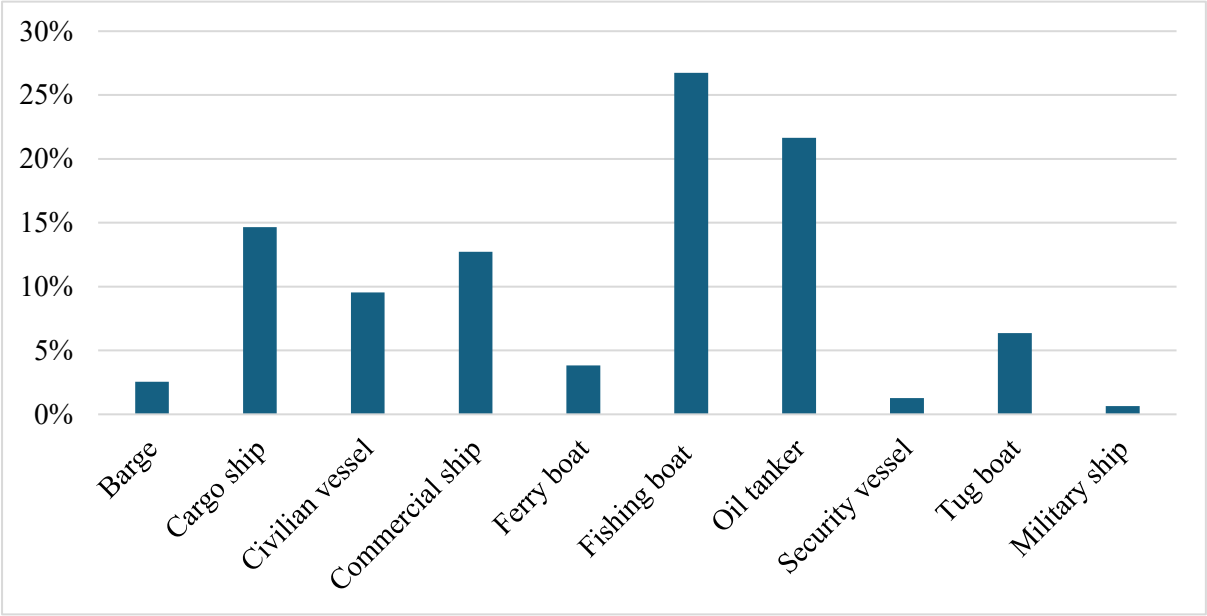

Figure 3. 5: The percentage of incidents for different types of vessels (GTD).

3.4.2 Analysis of SRIF on maritime terrorist attacks

In this study, the security-affecting factors are referred to as SRIFs. These factors are determined by analysing data from the GTD, integrating with the information obtained from the literature review to categorize and compile the relevant indicators. To accurately evaluate the risk level of terrorist attacks and identify the factors involved, it is necessary to carefully investigate elements such as the date, location, methods of attack, types of weapons employed, casualties, degree of damage, and the overall impact of the incidents. Following the outlined procedures, a total of 12 distinct SRIFs were identified, including factors such as the type of attack, ship category, weapon employed, region, country, flag state, year, perpetrator, success of the attack, property damage, ransom, and casualties.

Table 3.1 provides details on various terrorist attack types, while Table 3.2 delineates the remaining SRIFs, offering descriptions and the associated states linked to each.

Table 3. 1: Types of terrorist attacks against maritime transportation ("GTD," 2021).

Attack type	Description
Assailment	A deliberate attack with the intention of leading to physical harm or causing death to others using weapons, incendiary devices, or sharp implements (such as knives). It also includes attacks involving particular categories of explosive devices, such as grenades, projectiles, and unidentified explosive devices thrown, as well as weapons, incendiaries, or cutting tools.
Explosion	This refers to attacks utilizing unstable materials that rapidly release energy, creating a pressure wave that causes physical harm to the environment. This release can result from chemical reactions, high pressure, or other processes, leading to a sudden and forceful release of energy, often causing damage to its surroundings. It covers both high and low explosives, including dirty bombs, but excludes nuclear devices.
Hijacking	Hijacking refers to a deliberate action with the objective of taking control of a marine vessel in order to divert its course or achieve political objectives. Although ransom may not be the only purpose, it could be present in conjunction with other stated objectives. Hijacking pertains to the act of forcibly taking control of a ship, as opposed to hostage taking, which mostly involves the abduction of individuals rather than the vehicle itself.
Hostage taking (Kidnapping)	Kidnappings are defined as the deliberate act of taking hostages with the aim of achieving political objectives or causing disruption to regular activities. Kidnappings differ from Barricade Incidents in that they entail the act of forcibly moving and confining individuals against their will. The main objective is to achieve political goals by either making concessions or disrupting regular activity for a specific reason. Occasionally, a ransom may be also demanded.

Table 3. 2: Description of SRIFs and their states.

Node number	SRIFs	States	Description
1	Ship type	Cargo ship, Civilian vessel, Commercial ship, Fishing boat, Tanker, Tugboat, Other	"Other" encompasses barges, military vessels, security ships, and ferries. Tankers refer to oil, gas, and chemical carriers.
2	Weapon type	Bomb, Combinatory, Explosive laden-boats, Firearms, Projectile, Unknown	"Bomb" encompasses naval mines, suicide bombers, time fuses, dynamite/TNT, sticky bombs, pipe bombs, and other unidentified explosive types. "Combinatory" refers to employing a combination of weapons, for instance, utilizing projectiles to damage ships, followed by employing firearms to attack them. "Explosive-laden boats", often referred to as suicide boats or explosive boats, are watercraft that have been loaded with explosives with the intention of being used as a weapon. These boats loaded with explosives can be operated either by individuals onboard (Suicide mission) or controlled remotely from a distance. "Firearms" include all portable weapons such as automatic or semi-automatic rifles, handguns, rifles/shotguns, and any other unclassified gun types. "Projectile" refers to various items like rockets, mortars, RPGs, and missiles.

3	Region	Middle East & North Africa, South America, South Asia, Southeast Asia, Sub-Saharan Africa	These are the sole regions globally where terrorist attacks against maritime transportation have been documented.
4	Country	Cameroon, Colombia, Congo, India, Iraq, Libya, Malaysia, Mozambique, Myanmar, Nigeria, Philippines, Saudi Arabia, Somalia, Sri Lanka, Yemen, Other	Countries where the terrorist attacks occurred fewer than three times are grouped into the "other" category.
5	Flag state	China, Colombia, Congo, Egypt, Greece, India, Indonesia, Iran, Iraq, Italy, Japan, Liberia, Malaysia, Mozambique, Multinational, Myanmar, Netherlands, Nigeria, Pakistan, Philippines, Romania, Russia, Saudi Arabia, Sierra Leone, South Korea, Spain, Sri Lanka, Thailand, Turkey, United States, Vietnam, Yemen, Other	The ship's flag state is the nation where the ship is registered, which may not align with the location of the incident. "Other" denotes flag states that have experienced fewer than two attacks.
6	Year	2000-2021	-
7	Perpetrator	AA, ALQ, ALS, AMC, ASG, BIFM, FARC, HE, LTTE, ME, MEND, MMCM, NDV, NPA, Other, Unknown	Terrorist groups are denoted by acronyms, with their complete names accessible on the GTD website. This study features the perpetrators recorded at least twice, while the remaining are grouped as "other." Instances exist where no responsible perpetrator was identified, labeled as "unknown."
8	Successful attack	Yes, no	A successful attack is based on immediate impact, not broader goals; a bomb exploding, even without major consequences, counts as success.
9	Property damage	Yes, no	The presence of property damage is indicated by a "Yes." If "Property Damage" is affirmative, one of the following three categories describes the extent of damage: 1 = Catastrophic (probably $\geqslant$ \$1 billion) 2 = Major (probably $\geqslant$ \$1 million but < \$1 billion) 3 = Minor (probably < \$1 million) For simplicity, we only consider whether property damage exists or not.
10	Ransom	Yes, no	In cases of hijacking or hostage-taking incidents, ransom denotes the monetary demand required for the release of kidnapped individuals or the return of hijacked vessels.
11	Casualty	Yes, no	Casualties refer to the total count of confirmed fatalities and injuries resulting from the incident, encompassing both victims and attackers who perished directly due to the event.

3.4.3 BN structure learning

In building the BN model, there are mainly two approaches: one involves data-free modelling, relying on expert judgment, introducing uncertainty and bias, while the other employs data-driven methods. The latter utilizes empirical data to steer the search-based learning process,

yielding objective results. In this study, the focus of BN structure learning is to unveil a Directed Acyclic Graph (DAG) structure that effectively represents the relationships between SRIFs, which are variables derived from the collected data. These relationships encompass dependencies, interdependencies, or even independence among influential factors.

Various DDBN approaches exist in the literature, including NPC algorithm, K2 algorithm, Naive Bayesian Network (NBN), Augmented Bayesian Network (ABN), Bayesian Search (BS), Greedy Thick Thinning (GTT) and Tree Augmented Naive Bayes (TAN), each with its own strengths and weaknesses, contingent upon factors such as the volume of data, data sources, number of nodes, and model validation (Meng et al., 2022). This study has opted for using the TAN approach, an improved version of NBN, to investigate the BN structure learning. In a standard Naive Bayes classifier, it is assumed that all features (influencing factors/variables) are conditionally independent when given the class variable, a simplification that leads to its characterization as "naive." The TAN algorithm departs from the assumption of feature independence by introducing dependencies among features, yet it adheres to a tree structure for these relationships. TAN holds an edge over the standard Naive Bayes by effectively capturing particular interconnections between features (Friedman et al., 1997). This capability enhances classification accuracy, particularly in scenarios where Naive Bayes' independence assumption proves overly limiting. It therefore witnesses the rising profile of using TAN-trained BN in maritime-related risk/safety analysis (Li et al., 2023). The essential steps in TAN modelling can be succinctly outlined as follows (Fan et al., 2020): a) Selecting a target node, typically the class variable, as the initial point for tree construction; b) Creating a Maximum Weight Spanning Tree to form connections among the remaining nodes. The edge weights are determined by measuring mutual information between features; c) Defining conditional dependencies: Identifying the parent of each feature within the tree. Each feature in the spanning tree structure is conditionally dependent on its parent node and the class variable, given the root node; d) Learning parameters: After establishing the structure, calculate conditional probability distributions for each node based on available data.

This study employs the TAN Bayes algorithm, a data-driven approach among existing methods for constructing BN. TAN establishes a tree structure among features, with each node representing a feature and edges denoting dependencies between features. Typically, this tree is formed by designating the feature with the highest mutual information with the class variable as the node, followed by the addition of edges between features based on their mutual information with the class variable. TAN is designed to capture more realistic dependencies between features, offering greater flexibility compared to the conventional Naive Bayes model, while still maintaining computational efficiency. This algorithm is especially advantageous in scenarios where strong dependencies among features cannot be adequately addressed by the stringent independence assumption of Naive Bayes networks (NBN).

To elucidate this concept, a straightforward demonstration illustrating the disparity between NBN and TAN can be observed in Figure 3.6. In NBN, attribute nodes are devoid of edges, thus capable of representing zero conditional dependencies. However, the assumption of conditional independence is overly rigid for real-world scenarios. When confronted with intricate attribute dependencies, this can lead to classification bias. For instance, in our scenario, the target node is defined as cyber threats with other attributes linked to it. Under the NBN framework, there are no interdependencies between the region and the year, thereby

overlooking spatial-temporal considerations. TAN relaxes this independence assumption, extending NBN from a zero-dependence tree to a dependent maximum weighted spanning tree, purportedly enhancing classification performance compared to NBN.

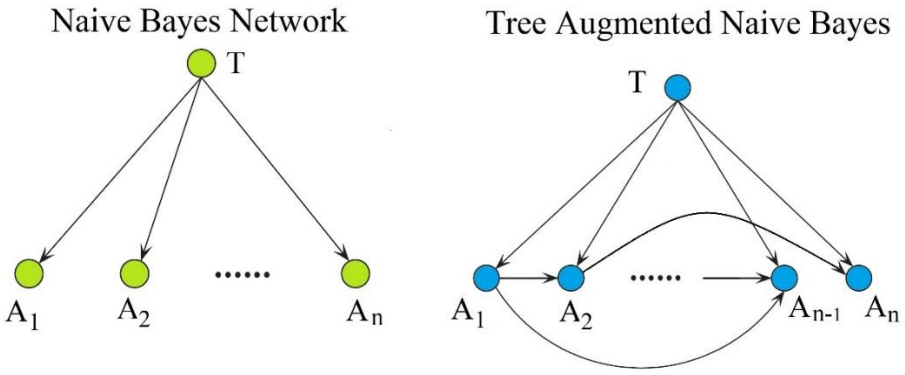

Figure 3. 6: The illustrative comparison between NBN and TAN structure learning.

To summarize the advantages of the TAN technique over alternative training methods, it can be analysed from three distinct perspectives. Firstly, regarding interpretability, the tree structure in TAN offers a clear graphical representation of feature dependencies. This clarity facilitates the interpretation of model predictions and enhances the understanding of variable relationships. Secondly, in terms of robustness, TAN demonstrates greater resilience to irrelevant features compared to other techniques like traditional Naïve Bayes or general BN. Its tree structure aids in filtering out extraneous information, focusing instead on pertinent feature dependencies, thereby improving model performance and mitigating overfitting. Lastly, in terms of efficiency, despite its increased complexity relative to Naïve Bayes, TAN remains relatively quick to learn. This efficiency renders it suitable for datasets with moderate to large numbers of features, where fully learning the joint distribution could be computationally cumbersome, time-consuming, and costly (Wu, 2018) (Jiang et al., 2012) (Ren and Guo, 2023).

The conceptual foundation of this approach is detailed in the work of Friedman et al. (1997). To succinctly outline the fundamental steps in TAN learning, the process involves several key stages (Fan et al., 2020) which are demonstrated in Figure 3.7. Its application in the context of maritime cybersecurity risk is detailed in the ensuing section.

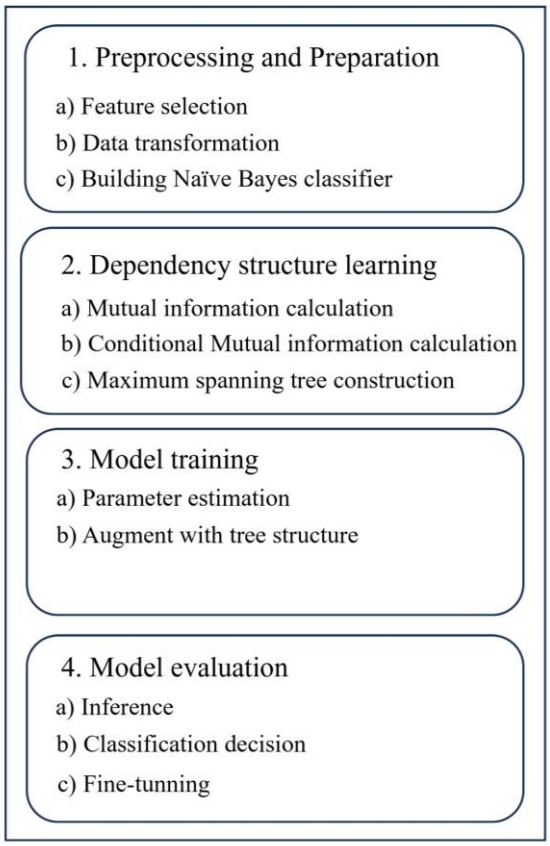

Figure 3. 7: TAN structure learning process.

Initially, the data is categorized into different classes known as SRIFs as represented in Table 3.2. Subsequently, data cleansing is performed, involving the removal of irrelevant entries and identification of missing data. Following this, the target node, representing the class variable for classification and serving as the starting point for tree modelling, is selected. The qualitative structure of the TAN network is then established based on the mutual information between different nodes. Mutual information measures the statistical dependence between two variables. In the context of TAN, mutual information is used to quantify the relationship between each attribute and the class variable (target node). The mutual information between two variables X and Y is calculated as the reduction in uncertainty about X when the value of Y is known, and vice versa. It is commonly defined using entropy, a measure of uncertainty in a random variable. The mutual information between two discrete random variables X and Y is given by (Cover and Thomas, 2005):

$$I(X;Y) = \sum_{x \in X} \sum_{y \epsilon Y} P(x,y) Log \frac{P(x,y)}{P(x)P(y)} \qquad (3.1)$$

where P(x,y) is the joint probability mass function of X and Y, and P(x) and P(y) are the marginal probability mass functions of X and Y, respectively. This process is also carried out for all other nodes in the network concerning the target node.

Furthermore, with the class variable established, the relationships among various pairs of variables are discerned by computing conditional mutual information. This helps identify the most informative parent variable for each attribute in the network.

The conditional mutual information between two discrete random variables X and Y given Z is given by (Shannon, C.E., 1949):

$$I(X;Y/Z) = \sum_{x\in X}\sum_{y\in Y}\sum_{z\epsilon Z} P(x,y,z)log\frac{P(x,y/z)}{P(x/z)P(y/z)} \qquad (3.2)$$

After obtaining the pairwise conditional mutual information, the maximum spanning tree algorithm is utilized to build a tree structure over the attributes in TAN. This typically involves employing heuristic algorithms like Prim's or Kruskal's algorithm, aiming to connect all attributes while maximizing the total weight of edges and minimizing network complexity (Cormen, 2009). Subsequent connections are made by calculating conditional mutual information among the remaining variables, ensuring that the tree structure reflects the most significant informational relationships.

The parameter learning phase is executed to determine the conditional probability table for each node. Commonly employed methods for parameter learning and CPT acquisition in TAN encompass Maximum Likelihood Estimation, Bayesian Estimation, Expectation-Maximization, Markov Chain Monte Carlo, Structural EM, and others (Ji et al., 2015). The selection of a specific method hinges on factors such as the data's characteristics, computational resources, and assumptions regarding the data's underlying distribution. In this study, Bayesian estimation is chosen due to the completeness of the database, the absence of missing data, and the method's recognized accuracy and efficiency. While Bayesian estimation may introduce sensitivity to prior specification and entails slightly higher computational effort compared to purely data-driven methods such as maximum likelihood estimation, these effects are mitigated in this study by the availability of a complete dataset and the use of non-informative priors, resulting in stable and robust CPT estimates. The final stage encompasses model evaluation through three sub-steps: inference, classification decision, and fine-tuning. Inference calculates joint probabilities using the trained TAN model, guiding classification. Class labels are assigned based on the highest probability. Fine-tuning adjusts parameters to enhance predictive accuracy and robustness, ensuring optimal TAN model utilization in real-world scenarios.

Overall, the process of constructing the BN tree structure entails identifying the most informative dependencies while ensuring that it remains acyclic, and the mutual information measure assists in assessing the strength of linkages between variables. TAN achieves a middle ground by combining the simplicity of Naive Bayes with the complexity of fully linked BNs.

3.4.4 Model validation

Model validation is the evaluation of the effectiveness and reliability of the constructed BN model. The objective is to guarantee that the model precisely represents the fundamental connections in the data and may provide trustworthy predictions or inferences. In this study, the constructed model undergoes validation using a range of methods, which encompass a)

comparative analysis, b) data splitting, c) metrics analysis, d) sensitivity analysis, and e) real-world scenario analysis.

3.4.4.1 Comparative analysis

A comparative analysis involves assessing the performance and characteristics of a developed BN model by comparing it to other existing models or benchmarks. Various approaches can be employed for this purpose. For example, the BN model is juxtaposed with other models known for their robust performance in analogous tasks. This process facilitates an evaluation of the relative strengths and weaknesses of the BN model compared to other well-established methodologies. Additionally, the BN model may be contrasted with conventional approaches or algorithms commonly utilized in the industry, providing valuable insights into its performance against widely accepted standards.

In this study, given the limited existing research on maritime terrorism and the scarcity of BN-based models in this domain, the findings are compared with the initially collected statistical data. In this regard, the predicted probabilities for the states of the target node are contrasted with their associated statistical ones. Greater consistency in the results serves as an indicator of the reliability of the established model (Fan et al., 2020).

3.4.4.2 Data splitting

The data splitting process in DDBN aids in creating a more reliable, generalizable, and well-validated predictive model by enabling effective training, testing, and hyperparameter tuning. It replicates the model's performance on data that it has not been exposed to during the training phase. This aids in the detection of potential problems such as overfitting, which occurs when the model exhibits good performance on the training data but fails to generalize to new data. The overall procedure entails splitting the given dataset into two or more distinct subsets: a training set and a validation (or testing) set. The bulk of the dataset, typically 90 percent of it, is assigned to the training set, where the model is developed and trained. This allocation enables the model to understand the core patterns and relationships within the data. On the other hand, a minor portion of the dataset, usually the remaining 10 percent, is designated for the validation set. The performance of the model is subsequently assessed on this set to determine its ability to generalize to new, not-observed data. However, the process of selecting testing data is crucial. Random selection alone may not yield optimal performance. Techniques like k-fold cross-validation address this by splitting the dataset into k subsets (Refaeilzadeh et al., 2009). The model is trained k times, each time using a different subset as the testing set and the remaining data as the training set. This approach provides a more reliable estimate of the model’s performance and reduces the risk of overfitting. Conversely, underfitting occurs when the model is too simple to capture the underlying patterns in the data. Validating the model on different subsets helps identify and mitigate underfitting issues. Through this data splitting process, the model learns a wider variety of patterns, making it more robust and less sensitive to fluctuations in the data. The higher accuracy rate of the prediction denotes the validity of the model.

3.4.4.3 Metrics analysis

Metrics analysis is an essential approach for validating BNs as it offers a quantitative evaluation of the model's performance. This approach entails employing diverse measures to assess the degree of alignment between the BN model and the actual data or desired outcomes. In this context, specific metrics have been chosen to assess the performance of the model. The confusion matrix serves as a tabular representation, dividing predictions into categories such as true positives, true negatives, false positives, and false negatives. Figure 3.8 illustrates the basic idea of a confusion matrix.

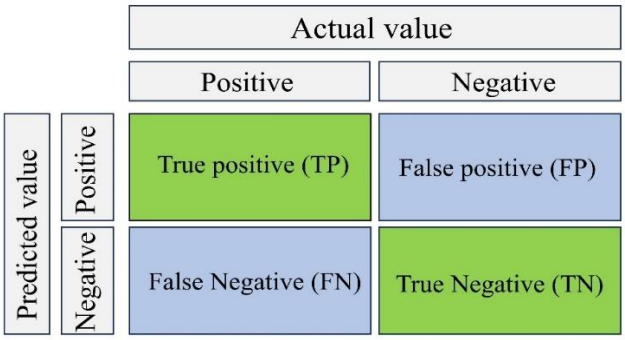

Figure 3. 8: The basic illustration of a confusion matrix.

This matrix forms the foundation for calculating several crucial metrics (Simsekler and Qazi, 2022). The overall accuracy metric quantifies the proportion of correctly predicted instances relative to the total number of instances, providing a general measure of the model's classification performance. Precision measures the reliability of positive predictions by indicating the proportion of true positives among all instances predicted as positive. Recall, also referred to as sensitivity, evaluates the model's ability to correctly identify all relevant instances by representing the proportion of true positives among all actual positives. While precision reflects the correctness of positive classifications, recall captures the completeness of positive instance detection. The "F1 Score", a metric that strikes a balance between "Precision" and "Recall", is computed as the harmonic mean of the two. The harmonic mean is used to assess the overall average distribution. This metric is especially valuable when handling imbalanced class distributions. "Specificity" measures the proportion of correctly predicted negative samples out of all actual negative samples. A higher "Specificity" value indicates a better result. Finally, the "False Positive Rate (FPR)", which is inversely related to "Specificity", a lower FPR value indicates better performance. The calculation formulas of the above six indicators are shown in Eqs. (3.3)-(3.8).

$$Overall\ accurracy = \frac{T_P + T_N}{T_P + F_P + T_N + F_N} \tag{3.3}$$

$$precision = \frac{T_P}{T_P + F_P} \tag{3.4}$$

$$recall = \frac{T_P}{T_P + F_N} \tag{3.5}$$

$$F - measure = \frac{2 * precision * recall}{precision + recall} \quad (3.6)$$

$$Specificity = TNR = \frac{T_N}{F_P + T_N} \quad (3.7)$$

$$FPR = 1 - TPR = \frac{F_P}{F_P + T_N} \quad (3.8)$$

TP represents the positive samples correctly predicted as positive, and TN denotes the negative samples correctly predicted as negative. FP refers to the negative samples incorrectly predicted as positive, while FN represents the positive samples incorrectly predicted as negative. TNR, also known as Specificity, indicates the true negative rate. Together, these metrics provide a comprehensive evaluation of the model's performance, considering aspects such as accuracy, precision, recall, and the balance between precision and recall (Hu et al., 2016). This selection enables a thorough assessment of the model's effectiveness in making correct predictions across different categories and addressing potential challenges posed by imbalanced class distributions.

3.4.4.4 Sensitivity analysis

In the context of BN analysis, sensitivity analysis refers to the examination of how changes or uncertainties in the probabilities or values assigned to the variables in the network impact the output or results of the model. It is a technique used to assess the robustness and reliability of the BN in the face of variations in the input data. Moreover, it aids in pinpointing the SRIFs that wield the most influence on the target node, enabling the strategic selection of cost-effective measures to alleviate potential consequences. Various approaches exist for executing sensitivity analysis in BN, such as mutual information, joint probability, True Risk Influence (TRI), and minor variation testing.

"Mutual information", originating from entropy theory, serves as a metric for evaluating the relationship between two random variables within the BN, quantifying the extent of dependence or shared information between them. Calculating the mutual information provides insights into the relative significance of relevant SRIFs concerning the target node. Typically, a higher mutual information value indicates a stronger association between the variables, offering a gauge of their interdependence.

As commonly practiced in traditional sensitivity analysis, different values are assigned to the states of the nodes under investigation while maintaining the states of other nodes unchanged. This method is generally suitable for nodes that possess only two states. However, when dealing with nodes in a BN model that have multiple states, it becomes challenging to discern how altering one state affects the other states. To address this challenge, a novel method known as TRI, introduced by Alyami et al. (2019) and rooted in joint probability, is employed. The joint probability refers to the probability of a specific combination of states occurring across multiple random variables in the network. The joint probability distribution provides a comprehensive description of the simultaneous occurrences of different states for all the variables in the network. TRI operates in the following manner: Initially, the High-Risk

Influence (HRI) is calculated by raising the probability of the state of an investigated node with the most substantial impact on the target node to 100%. Following this, the Low-Risk Influence (LRI) is computed similarly, but the selected state is the one that contributes to the lowest risk stake of the target node. Ultimately, the TRI value for the examined SRIF is determined as the average of HRI and LRI. This procedure can be systematically employed for all SRIFs. A higher TRI value indicates a more pronounced impact of the respective SRIF on the target node. In simpler terms, the target node exhibits greater sensitivity to the SRIF associated with the higher TRI value.

Beyond the sensitivity analysis methods discussed earlier, an additional approach is available for consideration. This method relies on two specified principles (Zhang et al., 2013):

Principle 1: A marginal increase or decrease in the prior probabilities of each tested node should result in a proportional increase or decrease in the posterior probability of the target node.

Principle 2: The cumulative impact of incorporating probability variations from the evidence should be at least as significant as the impact from a subset of the evidence.

In adherence to these principles, slight modifications to variables are implemented. Following the mutual information results, SRIFs are prioritized, and the updates commence from the less influential nodes, progressively reaching the target node. This process is iteratively carried out for the remaining nodes while retaining the previous outcomes.

3.4.4.5 Real-world scenario analysis

To address this matter, several steps are taken. First, a real case scenario is collected from outside of the GTD database to accurately represent the variables within the BN. This data should cover a diverse range of scenarios and conditions. Next, the BN model is applied to make predictions or determinations based on real-world empirical data. This involves estimating probabilities, predicting outcomes, or making determinations based on the model's structure and parameters. Subsequently, the accuracy of predictions is assessed by comparing them to actual outcomes. The evaluation involves scrutinizing the extent to which the model's predictions align with the observed results in real-world data. This comparison entails assessing both projected probabilities and observed outcomes, ensuring a comprehensive evaluation of the model’s performance.

3.5 Results and discussion

3.5.1 TAN modelling

The TAN model is created utilizing data gathered from the GTD database; wherein pertinent details are extracted to identify the SRIF as outlined in Table 3.2. The model designates the attack type as the target node, and the Netica software (“Netica (Version 607).,” 2019) is employed to facilitate the construction process. Netica allows in-depth analytical and statistical assessment of networks with its generous bin capacity. It places no restrictions on the number of nodes and supports dynamically changing values. The graphical interface provides numerical outputs, allowing users to visualize statistics, and offers the flexibility of selecting value ranges as evidence (George and Renjith, 2021). In Figure 3.9, the depicted process

involves the construction of the TAN network, followed by a crucial step in the parameter learning phase. Specifically, this step focuses on refining the parameters associated with the Conditional Probability Tables (CPTs) for different nodes within the network. The refinement process is achieved by incorporating relevant prior data through the Bayesian estimation method. This method adds a layer of sophistication to the learning process, allowing the model to adapt and improve its understanding of the causal relationships and probabilities associated with each node. Essentially, after the TAN network is established, the model undergoes a data-driven enhancement, fine-tuning its predictive capabilities through the incorporation of historical data.

As previously noted, the "attack type" is selected as the target node and is therefore directly connected to all other nodes. The rationale behind the constructed connections between different nodes can be interpreted to some extent through expert judgement. Regarding the connection between the target node and success rate, the type of attack can significantly impact the likelihood of success. For instance, certain attack types may have higher success probabilities due to their nature (e.g., explosions might be more successful than hijackings in certain situations). Additionally, the type of attack directly affects the number of casualties, with assailment generally resulting in more casualties compared to hijackings.

In terms of connections between the other nodes, the following examples illustrate the rationality of the constructed model. “Successful attacks”, “property damage” and “ransom” are all interconnected. If an attack succeeds, the probability of significant property damage and subsequent ransom demands increases, particularly in cases of explosions and hostage-taking situations. “Casualties” are linked to “weapon”, “region”, “country”, “perpetrator”, and “year”. This multifaceted connection indicates that the lethality and destructiveness of an attack depend on various factors, including its success and nature. The type of weapons used by various perpetrators in different countries and regions worldwide significantly affects the number of deaths and injuries among seafarers or people on ships. For instance, the most dangerous scenarios with high casualties typically involve armed assaults rather than explosions, particularly in the Middle East and Northern Africa. The nationality of a ship (flag) is connected to the perpetrator, suggesting that certain flags might be more susceptible to attacks from specific terrorist groups due to political reasons. By following the connections in the model, it can be seen that it reflects real-world relationships between various factors involved in terrorist attacks. These connections are crucial for building a comprehensive security risk assessment framework. Each arrow represents a logical dependency that enhances our understanding of the factors contributing to the likelihood and impact of terrorist activities.

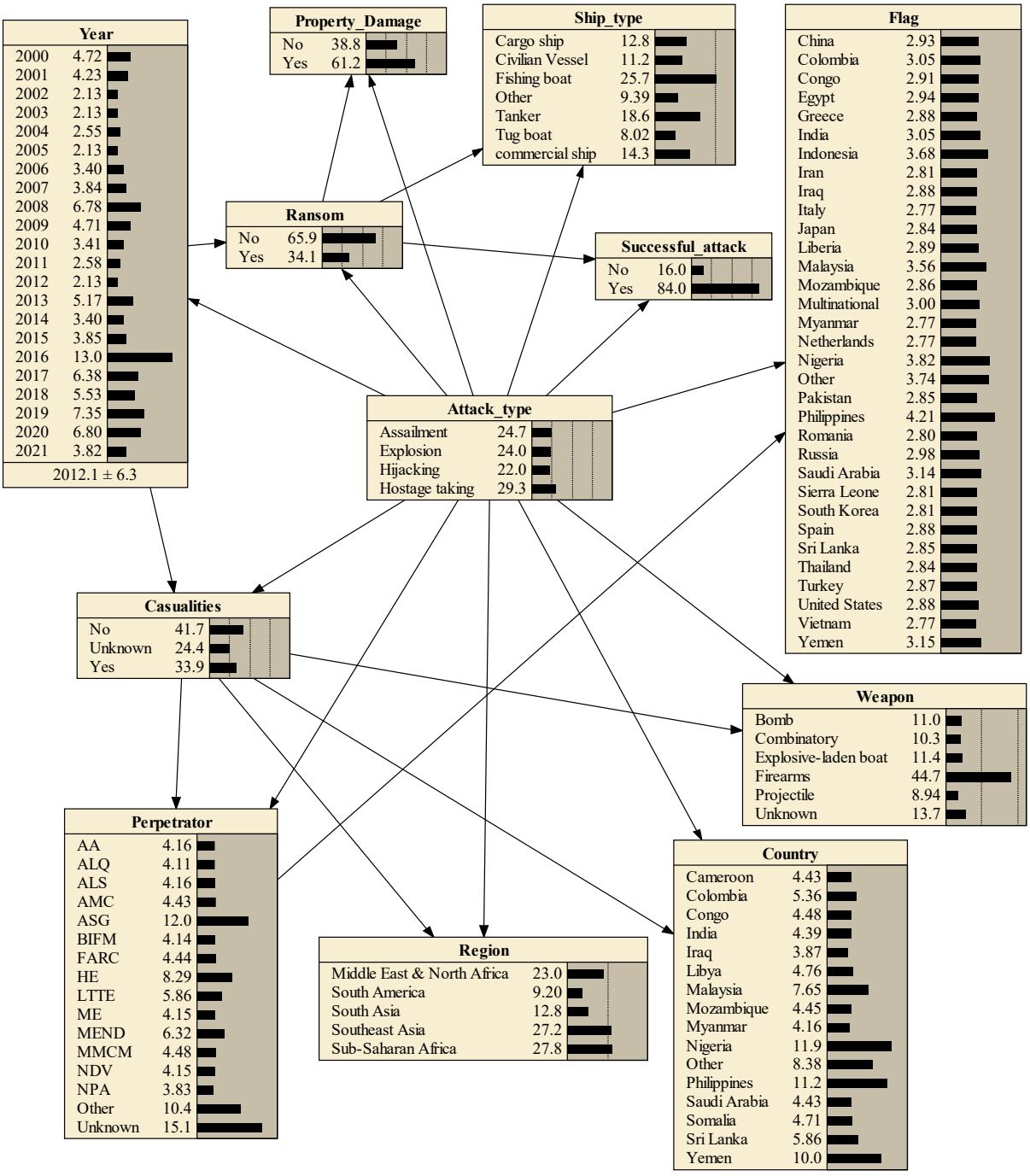

Figure 3. 9: The TAN-based BN model of terrorist attacks against maritime transportation.

3.5.2 Model validation

In accordance with section 3.4.4, a variety of approaches are employed to assess the accuracy of the constructed model. These can help determine whether the security risk prediction outcomes accurately correspond to the actual occurrences of maritime terrorism.

3.5.2.1 Comparative analysis

The TAN model's results, as detailed in Table 3.3, demonstrate a noteworthy level of consistency and reliability in comparison to historical data. The robustness of the model's predictions is particularly evident, with only minor variations observed. These minor variations between the historical data and TAN results can be explained by two reasons. First, during the data-splitting procedure, 10 percent of the data was reserved for alternative validation methods, and the model was constructed using the remaining 90 percent. Second, the TAN model extends the Naive Bayes classifier by incorporating limited dependencies between features, represented as a maximum spanning tree. This approach maintains a balance between simplicity and effectiveness, enhancing computational efficiency and ease of interpretation. Although this can lead to minor discrepancies, such as a 0.2% error between the model's probabilities and actual data, such errors are typically acceptable, as evidenced by (Fan et al., 2020; Yang et al., 2018). The result reveals that hostage taking is the predominant form of terrorist acts, followed by assailment, explosions, and hijackings. The data not only identifies the order of occurrence but also emphasizes the relative frequency of each type, contributing to a comprehensive understanding of the terrorism landscape. It therefore provides much more insights than the simple statistics revealed by the historical data. It is important to acknowledge that different regions of the world may see distinct patterns of terrorist acts. The above findings only reflect a global viewpoint and cannot be generalized to all regions. For instance, hostage-taking tends to be more prevalent in Southeast Asia, whereas explosions are more frequently observed in the Middle East and North Africa. Based on the results, it can be inferred that BN outperforms basic statistical analysis by adeptly capturing intricate relationships and dependencies among variables, yielding a comprehensive system understanding. Furthermore, BN is exceptional at handling uncertainty, incorporating prior knowledge, and continuously updating beliefs. This capability improves decision-making by providing nuanced insights that are often missed by more straightforward statistical methods.

Table 3. 3: Comparative analysis of historical and TAN results

Attack type	Historical data (%)	TAN results (%)	Accuracy rate (%)
Assailment	24.5	24.7	99.2
Explosion	23.9	24.0	99.6
Hijacking	22.1	22.0	99.5
Hostage taking	29.5	29.3	99.3

3.5.2.2 Data splitting and metrics analysis

In order to enhance the thorough evaluation of the model and accurately assess its predictive capabilities, a deliberate decision was made to randomly set aside 10% of the original database. This reserved portion, strategically chosen, was then utilized to rigorously test the model's performance. This testing phase took place after the model undergoing training, allowing for a comprehensive examination of how well the model generalized to new data and accurately predicted outcomes beyond its training set. As outlined in Table 3.4, the confusion matrix shows that the overall accuracy of the model stands impressively at 94.1%. Notably, when it comes to predicting assailment, the accuracy is slightly lower at 75%. However, for the prediction of other types of attacks, the model achieves a perfect accuracy rate of 100%. This high accuracy across various attack types highlights the robustness and reliability of the developed model in accurately classifying and predicting different forms of attacks.

Table 3. 4: Confusion matrix of predicted results

		Actual					Accuracy rate (%)
		Assailment	Explosion	Hijacking	Hostage taking	Total	
Predicted	Assailment	3	1	0	0	4	75.0
	Explosion	0	4	0	0	4	100
	Hijacking	0	0	4	0	4	100
	Hostage taking	0	0	0	5	5	100
	Total	3	5	4	5	17	94.1

In accordance with the details outlined in section 3.4.4, Table 3.5 presents various performance metrics for each attack type based on the analysis of the confusion matrix. The “Precision” of the model is exceptionally high, registering 100% for all attack types except for explosions, where it stands at 80%. Regarding “Recall”, assailment exhibits a value of 75%, while other attack types achieve a perfect 100%. F-measure, a composite metric of “Precision” and “Recall”, exceeds 85% across all categories. Notably, higher Specificity contributes to enhanced model robustness. Specifically, assailment, hijacking, and hostage taking boast a specificity of 100%, while explosions, though slightly lower at 92%, still indicate substantial robustness. The FPR, inversely related to Specificity, aligns with its patterns. An examination of these performance metrics underscores the commendable reliability and robustness of the developed model.

Table 3. 5: Performance results for each SRIF

	Precision (%)	Recall (%)	F-measure (%)	Specificity (%)	FPR (%)
Assailment	100	75	86	100	0
Explosion	80	100	89	92	8
Hijacking	100	100	100	100	0
Hostage taking	100	100	100	100	0

An additional metric employed to evaluate the model's reliability is the “Kappa coefficient”, also referred to as Cohen's kappa (Cohen, 1960). This metric measures the agreement between two raters or observers categorizing items. In our context, it quantifies the agreement between the predicted and actual results. Using the values derived from the confusion matrix (with the expected proportion of agreement equating to 0.25 and the observed proportion of agreement, representing overall accuracy, equalling 0.94), the Kappa coefficient is determined to be 0.92. As a well-established criterion suggests, a model is deemed nearly perfect when the Kappa coefficient exceeds 0.8 (Landis and Koch, 1977). In our case, the model demonstrates robust consistency given its Kappa coefficient of 0.92, indicating a high level of agreement beyond what would be expected by chance.

3.5.2.3 Mutual information

The mutual information between the attack types, acting as the target node, and other SRIFs has been computed and is illustrated in Table 3.6, along with the associated entropy reduction percentage and variance of beliefs. A higher mutual information value implies a more substantial impact of the respective SRIF on the attack type. Notably, the analysis reveals that the weapon type exerts the most significant influence on the attack types, accounting for nearly 11%. Following closely are the year, ship type, region, country, and perpetrator, contributing

entropy reduction percentages of 7.21%, 5.56%, 5.19%, 4.45%, and 3.61%, respectively. This insight underscores the varying degrees of impact these factors have on determining the nature of attacks, with the weapon type playing the most pivotal role.

Table 3. 6: Mutual information between attack type and SRIFs.

Node	Mutual information	Percentage (%)	Variance of belief
Attack type	1.99184	100	0.5589422
Weapon	0.21278	10.7	0.0215904
Year	0.14370	7.21	0.0166978
Ship type	0.11074	5.56	0.0141138
Region	0.10341	5.19	0.0112710
Country	0.08856	4.45	0.0109211
Perpetrator	0.07184	3.61	0.0096693
Property damage	0.05053	2.54	0.0055830
Successful attack	0.03175	1.59	0.0027943
Casualties	0.01969	0.988	0.0017811
Ransom	0.01835	0.921	0.0015514
Flag state	0.00955	0.479	0.0010733

3.5.2.4 The joint probability and TRI calculation

Additional sensitivity methods are employed to validate the developed model and pinpoint the most influential SRIFs in determining the likelihood of various attack types against maritime ships. The joint probability of the SRIFs and the target node is computed, as outlined in section 3.4.4. By incrementally setting the probability of each state of each node to 100%, the corresponding values for the states of the target nodes are obtained. Table 3.7 illustrates the results of the joint probability for the top six SRIFs identified from mutual information analysis. It is evident that, for different SRIF states, the values for target node states undergo changes compared to the original values. Examining the results in Table 3.7, the highest and lowest values for each attack type corresponding to the SRIF states are highlighted in bold for use in TRI calculation. Valuable insights can be derived from these results. For instance, the probability of an explosion is highest when explosive-laden boats are used in terrorist attacks. For fishing boats, the likelihood of hostage-taking is highest, particularly in the Southeast Asia region and in the country of Malaysia.

Table 3. 7: The joint probability.

	Assailment	Explosion	Hijacking	Hostage taking
Weapon				
Bomb	21.6	47.9	13.0	17.5
Combinatory	**34.1**	25.7	17.4	22.8
Explosive-laden boats	**14.0**	**60.5**	**12.4**	**13.0**
Firearms	29.4	**3.44**	25.6	**41.5**
Projectile	17.9	49.5	15.9	16.7
Unknown	17.9	23.4	**32.9**	25.8
Ship type				
Cargo ship	**16.6**	26.8	**40.9**	**15.7**
Civilian vessel	**41.8**	19.2	16.7	22.2
Commercial ship	20.8	24.0	36.2	19.1
Fishing boat	21.5	16.6	11.3	**50.6**
Other	36.3	32.0	**10.4**	21.4
Tanker	22.9	**34.5**	20.9	21.6

Tug boat	21.2	**16.2**	24.2	38.4
Perpetrator				
AA	21.5	20.9	26.4	31.2
ALQ	21.7	34.7	20.0	23.5
ALS	21.5	20.9	26.4	31.2
AMC	26.6	19.6	24.9	28.9
ASG	14.5	**11.9**	25.1	**48.5**
BIFM	**35.8**	21.0	19.9	23.4
FARC	33.0	19.6	18.6	28.9
HE	**14.3**	**53.0**	**13.3**	19.4
LTTE	25.1	34.2	18.7	22.0
ME	28.4	20.9	19.9	30.8
MEND	23.3	18.4	17.4	40.9
MMCM	26.3	19.4	18.4	35.9
NDV	28.4	20.9	19.9	30.8
NPA	23.3	30.0	21.5	25.2
Other	22.3	24.8	**34.4**	**18.4**
Unknown	34.9	19.3	20.1	25.7
Country				
Cameroon	26.6	19.6	24.9	28.9
Colombia	27.3	16.2	20.5	36.0
Congo	26.3	19.4	18.4	35.9
India	26.8	19.8	31.3	22.0
Iraq	23.1	22.5	21.3	33.1
Libya	18.8	18.3	28.9	34.1
Malaysia	22.9	**11.4**	**10.8**	**54.9**
Mozambique	20.0	19.5	24.7	35.8
Myanmar	21.5	20.9	26.4	31.2
Nigeria	**34.2**	12.3	20.9	32.6
Other	31.3	34.3	23.0	**11.5**
Philippines	**18.4**	20.3	29.5	31.8
Saudi Arabia	26.6	33.0	18.6	21.8
Somalia	18.9	18.4	**35.0**	27.6
Sri Lanka	25.1	34.2	18.7	22.0
Yemen	20.7	**52.2**	11.0	16.1
Region				
Middle East & North Africa	**21.0**	**48.8**	**12.6**	17.6
South America	27.9	18.4	21.0	32.7
South Asia	27.0	30.0	27.2	**15.9**
Southeast Asia	21.2	17.3	21.3	**40.3**
Sub-Saharan Africa	**29.0**	**9.23**	**28.4**	33.3
Year				
2000	18.0	44.6	8.64	28.7
2001	30.2	9.96	38.5	21.3
2002	20.0	39.6	19.2	21.2
2003	20.0	39.6	19.2	21.2
2004	16.7	49.6	16.0	17.7
2005	39.9	19.8	19.1	21.2
2006	25.0	12.4	36.0	26.6
2007	33.3	22.0	21.2	23.5
2008	37.6	12.4	30.0	20.0
2009	36.1	17.9	17.3	28.7
2010	24.9	24.7	23.9	26.5

2011	32.9	16.3	15.8	35.0
2012	**39.9**	19.8	19.1	21.2
2013	24.7	32.6	7.88	34.9
2014	25.0	12.4	36.0	26.6
2015	33.1	32.8	10.6	23.4
2016	16.4	13.0	22.0	**48.7**
2017	13.3	**6.60**	**44.7**	35.4
2018	23.1	**53.3**	**7.36**	**16.3**
2019	28.9	11.5	16.6	43.0
2020	**12.5**	49.6	18.0	19.9
2021	22.3	22.1	32.0	23.6

In the context of TRI calculation, which is based on the insights from section 3.4.4 and the outcomes of the joint probability analysis, the specific TRI values corresponding to all SRIFs have been computed and are presented in detail in Table 3.8. To shed light on the calculation process, this study focuses on TRI for the region, particularly in the case of explosions. Referring to the information in Table 3.7, it is observed that the Middle East and North Africa region contributed the most to the explosion, with a probability of 48.8%, while Sub-Saharan Africa has the lowest contribution at 9.23%. When comparing these values with the original probability estimate for explosion (24%), the subsequent calculations for HRI and LRI are determined as 24.8% and 14.77%, respectively. The TRI value, derived by averaging these calculated values, is computed to be 19.79%. The influence of various SRIFs on maritime terrorism is clearly dependent on the specific type of attack. Analysing the average TRI across all attack categories reveals that the year emerges as the most significant factor, followed by weapon type, country, perpetrator, ship type, and region. Figure 3.10 illustrates the ordering of TRI values for SRIFs. This comprehensive approach to TRI not only highlights the varying contributions of different SRIFs but also provides a more detailed assessment of their impact on specific attack types, enhancing the interpretability of the model's findings.

Table 3. 8: TRI of SRIF for different attack types.

	Assailment	Explosion	Hijacking	Hostage taking	Average
Year	13.70	23.35	18.67	16.20	17.98
Weapon	10.05	28.53	10.25	14.25	15.77
Country	7.90	20.40	12.10	21.70	15.53
Perpetrator	10.75	20.55	10.55	15.05	14.23
Ship type	12.60	9.15	15.25	17.45	13.61
Region	4.00	19.79	7.90	12.20	10.97

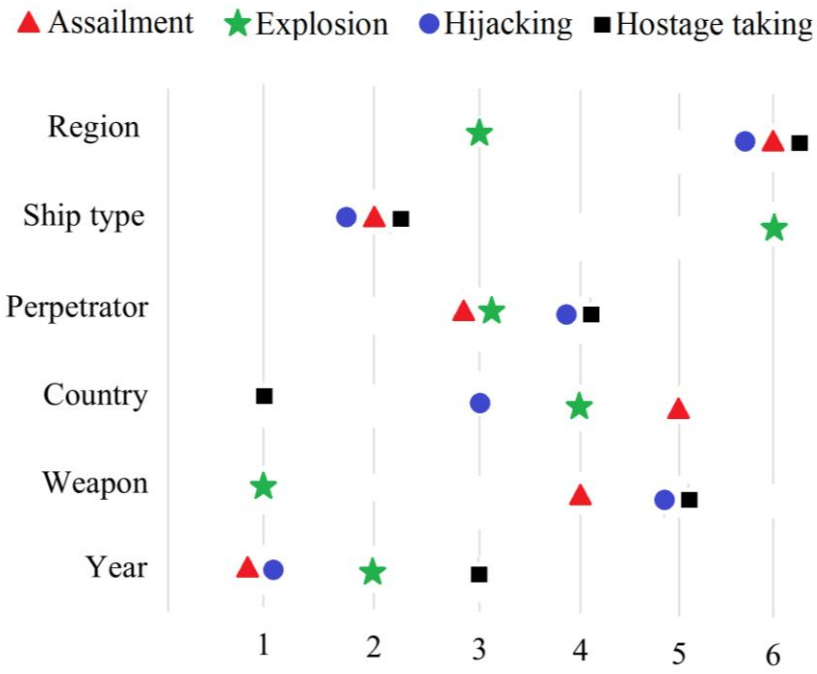

Figure 3. 10: The ranking of SRIFs for different types of attacks based on TRI value.

3.5.2.5 Model verification

To validate the model further and adhere to the two principles outlined in section 3.4.4, minor adjustments of 2% in the positive direction are applied to the prior probabilities of the most important identified variables. This adjustment is made in accordance with their importance levels determined through mutual information ranking. Subsequently, the changes in the probability of the target node are observed. In Table 3.9, the initial probability of attack types is presented in the second column, while the subsequent columns depict their cumulative probabilities following an increase in the prior probabilities of other nodes. Notably, elevating the prior probabilities of SRIF nodes leads to a corresponding rise in the posterior probabilities of the target node. These outcomes align entirely with the specified principles, underscoring the robust validity of the TAN-based BN model designed for analysing maritime terrorism.

Table 3. 9: The output of minor changes in SRIFs.

Perpetrator	-	+2%	+2%	+2%	+2%	+2%	+2%
Country	-	-	+2%	+2%	+2%	+2%	+2%
Region	-	-	-	+2%	+2%	+2%	+2%
Ship type	-	-	-	-	+2%	+2%	+2%
Year	-	-	-	-	-	+2%	+2%
Weapon	-	-	-	-	-	-	+2%
Assailment	24.7	25.1	25.4	25.6	26.1	26.6	27.0
Explosion	24.0	24.8	25.7	26.5	26.9	27.9	29.1
Hijacking	22.0	22.4	22.9	23.2	23.9	24.7	25.1
Hostage taking	29.3	29.9	30.8	31.3	32.0	32.7	33.3

3.5.2.6 Real-case scenario analysis

To reinforce the model's accuracy, two terrorist attack scenarios, which occurred recently and were not initially included in the original database, have been selected for testing. This deliberate selection of new, unseen data enhances the model's credibility by assessing its predictive capabilities on previously unencountered scenarios. The procedure operates by initially identifying specific SRIFs based on detailed information from reported incidents. These identified SRIFs are assigned a state with a probability of 100%. Subsequently, the probabilities of states for the target node are updated to reflect the predictive attack type.

On September 8, 2023, a terrorist attack unfolded in Mali, located in the Sub-Saharan Africa region, targeting a civilian marine vessel. The perpetrators, identified as the al-Qaeda-linked group, executed the attack using a combination of rockets and firearms. The incident took place on the river Niger as the boat travelled from Gao to Mopti. At least three rockets were launched at the vessel, specifically targeting its engines, resulting in the immobilization of the boat on the river. The military promptly initiated evacuation procedures for the passengers amidst an exchange of gunfire with the assailants. Unfortunately, the attack led to the death of 49 civilians and 15 soldiers. The terrorist attack was simulated using the constructed BN model, as depicted in Figure 3.11. The outcome indicates a remarkably precise prediction, with the incident probability accurately estimated at 95.4%.

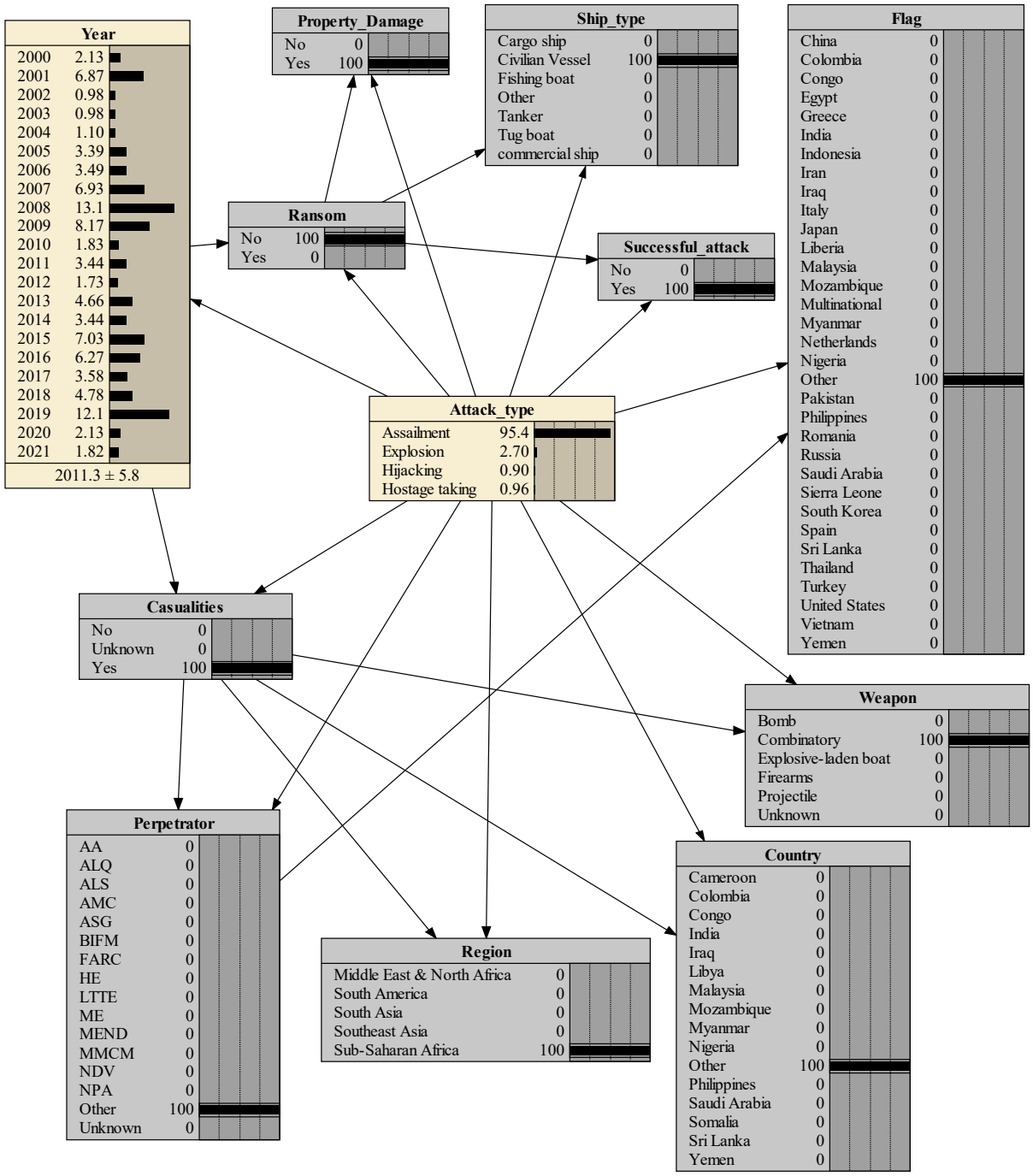

Figure 3. 11: The first real-case scenario analysis.

In another case, on March 10, 2021, an Iranian cargo ship fell victim to what has been described as a "terrorist" attack in the Mediterranean Sea. The vessel, owned by an Iranian state-run company, was on its route from Iran to Europe when it was targeted by an explosive device, identified as a naval mine. The blast caused damage to the ship's hull, resulting in a small fire that was swiftly extinguished. Despite the intentional attack, there were no reported casualties. The initial findings suggest that the cargo ship was intentionally targeted by an unknown source, marking a deliberate act of violence against maritime transportation interests in the North Africa region. By assimilating the data from the report into the BN model, the model

yielded a 96.7% probability of the occurrence of an explosion-type attack, as demonstrated in Figure 3.12. This outcome underscores the model's precision in making highly accurate predictions.

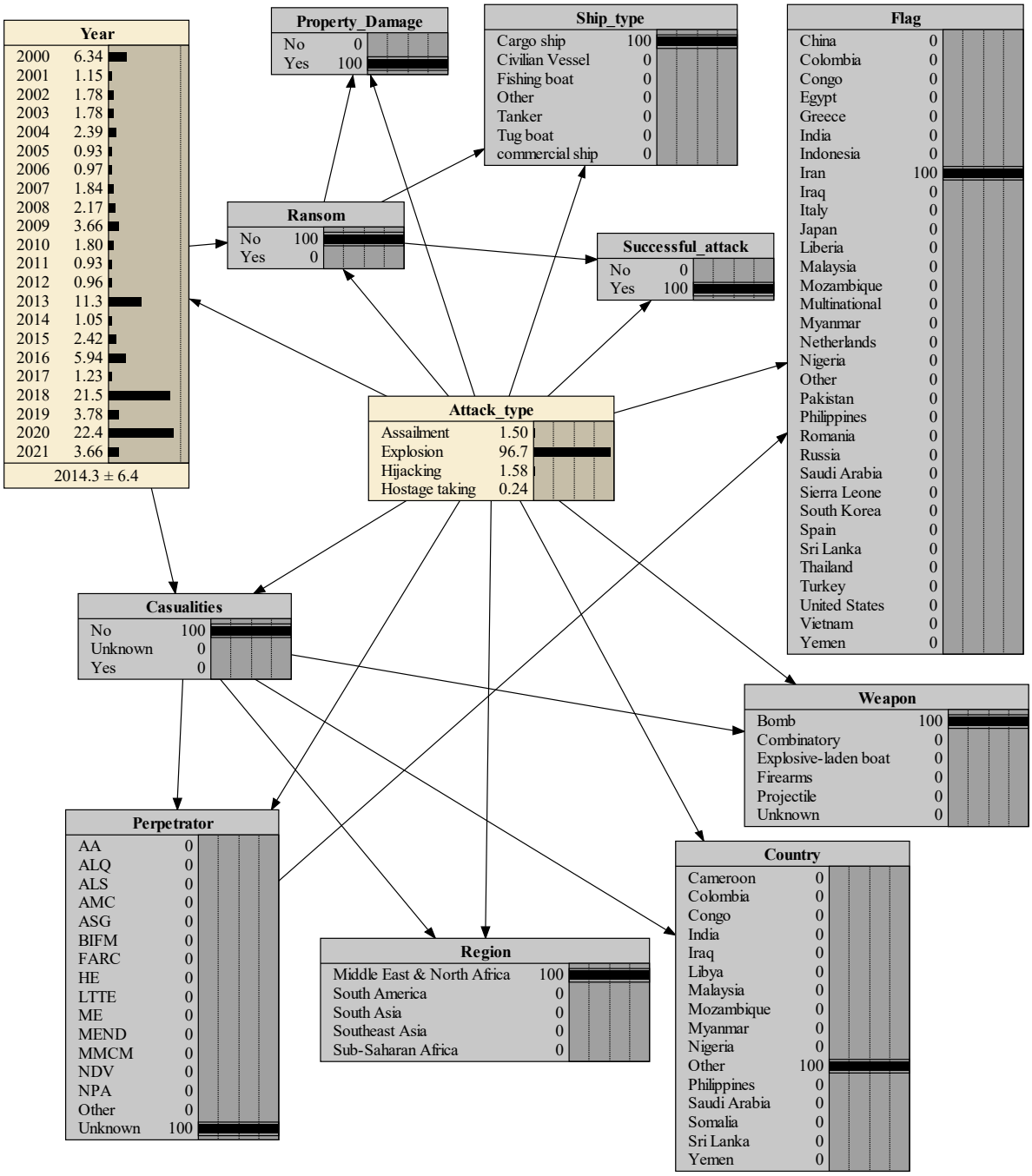

Figure 3. 12: The second real-case scenario analysis.

3.6 Analytical discussion and Implications

3.6.1 Attack types

The findings of the study led the authors to determine that each maritime transport region possesses unique characteristics related to maritime terrorism, categorizing them into types such as assailment, explosion, hijacking, and hostage taking. Utilizing the constructed model and employing scenario analysis to investigate the influence of particular conditions on the target node allows for the extraction of valuable information. As an illustration, setting the explosion state in the target node to 100% can unveil the most probable scenario for an explosion incident. As depicted in Figure 3.13, several nodes show increased probabilities, indicating their contribution to this outcome. Regarding the type of weapon, explosive-laden boats overwhelmingly precede other types, such as various bombs and projectiles, in terms of frequency of use. In reaction to the type of vessels, tankers are the most frequently targeted. Concerning high-risk regions and countries, the Middle East, and North Africa region, particularly Yemen as a country, emerge as the most perilous locations for the occurrence of explosion scenarios. This serves as a reminder of the tragic attack on the USS Cole, a U.S. Navy ship, in this region in 2000. The heightened risk can be attributed to the presence of HE (Houthi extremists) terrorist group with specific expertise in bombing tactics.

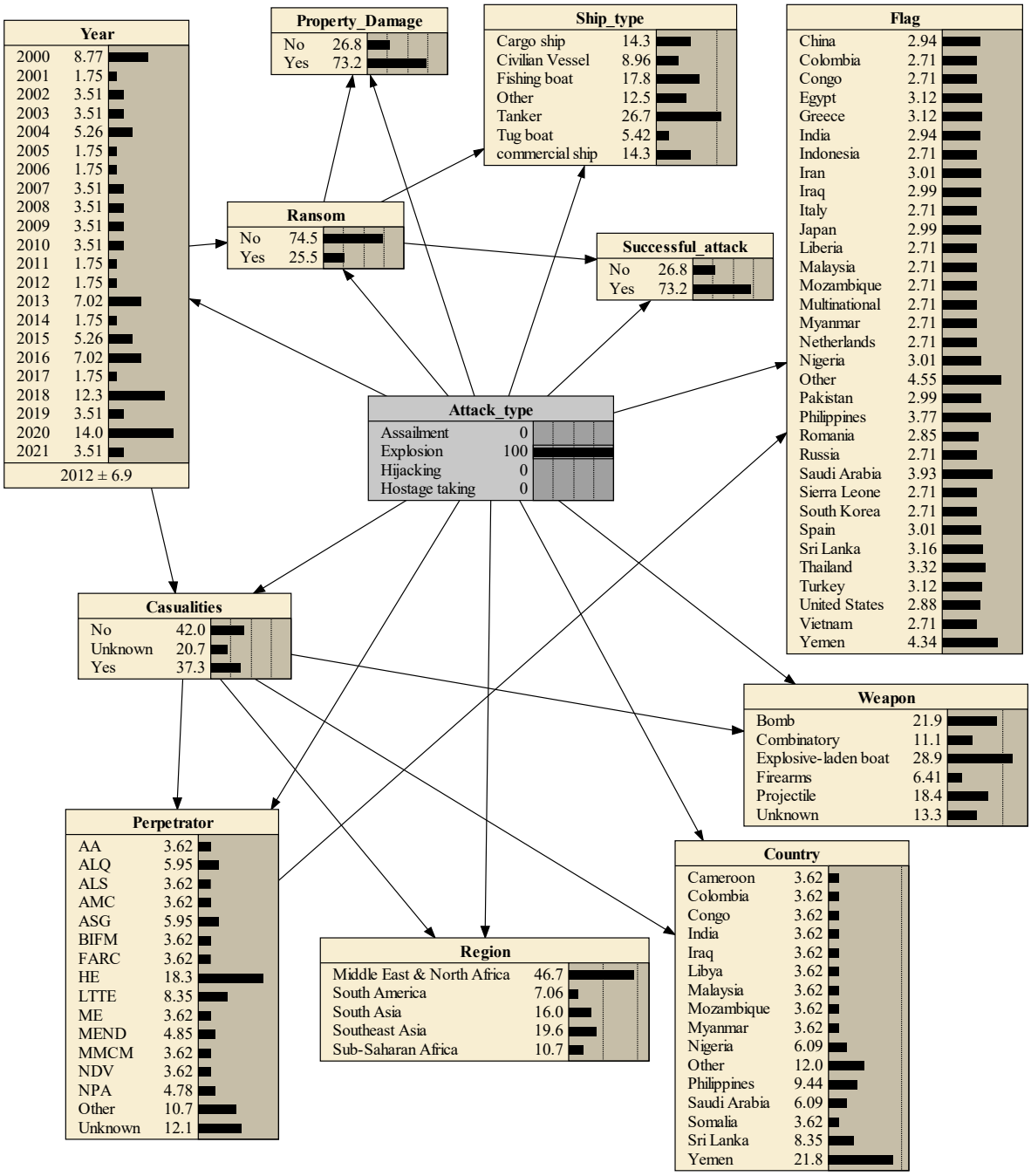

Figure 3. 13: Explosion scenario.

Similar data can be derived for various scenarios. In the context of hostage-taking incidents, firearms are the predominant weapons used. Southeast Asia and Sub-Saharan Africa emerge as the two high-risk regions, with Malaysia, Philippines, and Nigeria representing them, respectively. Fishing boats are commonly the preferred target for hostage-taking scenarios. Regarding the perpetrating groups, ASG (Abu Sayyaf Group) is predominantly responsible for these incidents in Southeast Asia, showcasing meticulous expertise in both hostage-taking and hijacking of vessels. Based on historical incidents, vessels flagged with Malaysia, Indonesia, and the Philippines are among the most frequently targeted by these groups, a trend not surprising given the geographical location of these ships in the mentioned region.

3.6.2 Top SRIFs

According to the findings presented in Table 3.8, the top six SRIFs with the highest average TRI, listed in order, are “year”, “weapon type”, “country”, “perpetrator”, “ship type” and “region”. The designation of "year" as the most influential risk factor suggests that the temporal dimension, specifically the particular year of an event, significantly influences the probability of maritime terrorist incidents. This designation can be viewed from multiple perspectives. Temporally, distinct periods of heightened and reduced terrorist activities have been observed over the past two decades. For instance, in 2016, more than 18 percent of all incidents took place, marking the year with the highest occurrence. Conversely, in 2002, 2003, 2005, and 2012, only one incident was recorded. Thus, certain years demonstrate discernible patterns or trends in the frequency of maritime terrorist incidents. From the standpoint of policy changes, it can be contended that post-2016, the reinforcement of the military's defence strategy to prevent highly violent crimes in Philippine waters has contributed to a decline in the number of ASG members and the weakening of its units. This has resulted in a zero hostage-taking rate in 2022. Another noteworthy aspect in this context is the progression of technology, encompassing both defensive and offensive capabilities, which has the potential to shape the methods and efficacy of terrorist attacks. Tracking the evolution of technology over time becomes crucial for anticipating potential threats. For instance, there is the possibility of retrofitting aquatic drones to operate as remotely controlled or autonomous waterborne improvised explosive devices, offering a discreet means to launch attacks against ships. Conversely, the development of advanced monitoring and detection security systems can play a pivotal role in mitigating the adverse impacts of such weaponry.

The type of weapon stands out as the second crucial SRIF with a substantial impact on the target node. It is evident that firearms play a pivotal role in most attack types, with a contribution of 60 percent, particularly in instances of hijacking and hostage-taking. Regarding explosions, explosive-laden boats, and in the case of assailment, combinatory weapons and projectiles emerge as the most influential states. This insight underscores the importance of early detection of weapon types, achievable either through intelligent services and coast guards, or security monitoring devices on ships that can detect suspicious approaching boats. Such early detection measures can significantly contribute to neutralizing or, at the very least, mitigating the impact of these incidents.

The inclusion of “country” and “region" as the third and sixth top SRIFs underscores the pivotal role of these geographical aspects play in shaping the likelihood of diverse types of terrorist attacks. The recognition of country as a risk factor acknowledges that the geopolitical landscape of a specific nation can exert a substantial influence on the occurrence and nature of maritime terrorist incidents. Notably, Yemen is recognized as a notorious country for explosion scenarios, the Philippines for hostage-taking, and Nigeria for armed assault and hijacking. Various factors contribute to the varying risk profiles across countries, including political stability, governance effectiveness, and counterterrorism measures. These elements fluctuate widely, impacting the overall susceptibility of a country to maritime terrorism. The distinct geopolitical characteristics of each nation highlight the need for tailored security strategies that account for these specific contextual factors. Similarly, the region in which maritime activities unfold emerges as a critical factor. A nuanced understanding of regional dynamics is crucial

for customizing security measures and response strategies to effectively address the specific challenges posed by maritime terrorism.

The identification of perpetrator groups as the fourth significant SRIF underscores their substantial impacts on various types of terrorist attacks. Distinct motivations, tactics, and capabilities among different perpetrators influence target selection, methods of attack, and overall implications for maritime security. Notorious terrorist groups, including ASG in the Philippines, HE in Yemen, LTTE (Liberation Tigers of Tamil Eelam) in Sri Lanka, and MEND (Movement for the Emancipation of the Niger Delta) are active in the context of maritime terrorism. Understanding the unique characteristics and behaviours of these groups is crucial for the development of targeted counterterrorism strategies.

The fifth SRIF is linked to the type of ships involved. Distinct ship categories face varying vulnerabilities, influencing the potential nature of attacks. Tankers, encompassing oil, gas, LNG, and chemical tankers, are particularly susceptible to explosive incidents, garnering widespread media attention. Cargo ships become targets for hijacking due to their valuable cargoes, serving as potential funding sources for terrorists. Fishing boats, characterized by easy accessibility, are prone to hostage-taking scenarios. Civilian vessels, vulnerable to armed assaults, are targeted for heinous attacks with firearms. Addressing these diverse threats requires the implementation of tailored security measures, rules, and regulations across different maritime sectors.

3.6.3 Implications

The generated implications highlight the need for a multi-faceted approach involving various stakeholders to enhance maritime security and counter the evolving challenges posed by maritime terrorism, including the following:

1) Governments and security agencies should recognize the significance of the temporal dimension (the specific year) in influencing the probability of maritime terrorist incidents. They should allocate resources and manpower, accordingly, focusing on factors associated with years exhibiting discernible patterns of heightened activity.

2) Policy changes and strategies should be adaptable based on temporal trends. For example, if certain years show increased activity, governments may need to reinforce defense strategies or law enforcement efforts during the years with those patterns which may be repeated in the future.

those periods.

3) Continuous monitoring of technological advancements is vital for anticipating potential threats. Governments should invest in intelligence and research capabilities to stay ahead of evolving technologies that could be used in maritime terrorist attacks.

4) The type of weapon used in attacks plays a significant role. Shipping companies should invest in advanced security measures, such as intelligent services, coast guards, and monitoring devices, to detect and respond to different weapon types, especially explosive-laden boats, and firearms.

5) Companies operating in different regions should conduct thorough risk assessments. In fact, understanding the geopolitical landscape of specific countries can help in tailoring security measures and response strategies to mitigate potential threats.

6) Early detection of suspicious approaching boats is critical for the maritime industry. Companies should, therefore, invest in advanced monitoring and detection security systems to neutralize or mitigate the impact of incidents.

7) Understanding the motivations, tactics, and capabilities of different perpetrator groups is essential. Counterterrorism agencies should focus on intelligence gathering and profiling of terrorist groups active in maritime terrorism.

8) Targeted counterterrorism strategies that account for the unique characteristics and behaviours of specific terrorist groups should be developed. This includes tracking their activities, funding sources, and recruitment methods.

9) Promote international collaboration and information sharing to combat maritime terrorism. Sharing data on temporal patterns, weapon types, and perpetrator groups can enhance global maritime security.

10) Support capacity-building initiatives in vulnerable regions. This includes assisting countries with political instability or governance challenges to improve their ability to counter maritime terrorism.

11) Encourage regional cooperation in addressing maritime security challenges. Understanding regional dynamics and challenges is crucial for effective security measures.

12) The defence industry should continue to innovate in both defensive and offensive capabilities to address evolving terrorist tactics. Developing advanced monitoring and detection systems can play a pivotal role in mitigating the impact of new weaponry.

13) Invest in research and development of countermeasures against potential threats involving aquatic drones or other emerging technologies. Developing technology to counter such threats can enhance maritime security.

14) Civil society organizations should advocate for government policies that prioritize maritime security and counterterrorism efforts. They can also contribute to public education and awareness campaigns.

3.7 Conclusion

This chapter presents a novel contribution to maritime terrorism research, encompassing both qualitative and quantitative dimensions. The study draws upon incidents from the widely regarded GTD database, the primary and publicly accessible repository, covering the past two decades. From an initial pool of over 200 cases, meticulous refinement leaves approximately 160 incidents for in-depth analysis, focusing specifically on terrorist attacks directed at maritime transportation. The investigation, fuelled by both data analysis and an extensive literature review, identifies 12 SRIFs. Four distinct types of terrorist attacks, namely as

assailment, explosion, hijacking, and hostage-taking are chosen as target nodes for the study. To model and understand the complex interplay of these factors, a TAN-based BN model is constructed using the curated dataset, facilitating a nuanced exploration of risk diagnosis and prediction in the realm of maritime terrorism. Delving into the model's analysis, it emerges that six SRIFs, namely year, weapon type, country, perpetrator, ship type and region, exert considerable influence on the selected target nodes. The robustness and validity of the model are thoroughly tested through an array of verification techniques, including comparative, metric, sensitivity, and real-case scenario analyses. The results attest to the model's high level of reliability. Taking the investigation, a step further, the model is subjected to real-world scrutiny by testing it against two recent terrorist attacks not included in the training dataset. The model predicts the attack types with over 90% probability accuracy in both cases, showcasing its applicability to real-world scenarios and its potential as a valuable tool for risk assessment and prediction in maritime security. The study's findings offer valuable insights for individuals and government entities, enhancing understanding of maritime terrorism and potentially strengthening preventive measures and emergency management. Additionally, the research establishes a reliable foundation for collaborative counterterrorism initiatives across various countries and regions.

Chapter 4 : Cybersecurity risk assessment

4.1 Summary

This chapter introduces an innovative approach to maritime cybersecurity risk analysis, developed to bridge existing gaps in this emerging domain. Drawing on a comprehensive dataset of cyber incidents spanning the past two decades, a data-driven Bayesian Network model is constructed to provide a more systematic and quantitative framework for assessing cybersecurity risks within the maritime sector. The chapter begins by outlining the development of a refined dataset that captures key risk factors and attack characteristics, followed by the application of an advanced Tree-Augmented Naïve (TAN) Bayesian structure, building upon the methodological foundation established in Chapter 3.

Through this model, the chapter investigates contemporary trends and evolving patterns in maritime cyber-attacks, identifying critical contributing factors, analysing their causal interdependencies, and estimating the probability of various threat scenarios. Given that disruptions to any component of the maritime transport system, whether vessels, seaports, or associated infrastructures can have far-reaching economic and operational implications, the study emphasizes the urgency of addressing vulnerabilities created by increasing digitalization and technological integration across the sector.

The developed TAN-based DDBN model undergoes rigorous validation through sensitivity and performance analyses to confirm its diagnostic and predictive robustness. The results yield valuable insights into the dynamics of maritime cybersecurity threats, improving prediction accuracy and supporting data-informed decision-making. Ultimately, this chapter provides essential guidance for both industry stakeholders and governmental authorities, offering strategies for optimized resource allocation, proactive risk mitigation, and the formulation of effective preventive measures to enhance the overall cyber-resilience of maritime systems.

4.2 Introduction

Global maritime transport is crucial, accounting for over 80% of global trade in goods (UNCTAD, 2022a). The extensive use of advanced technology and intelligent telecommunication systems in both mobile and fixed maritime components raises significant concerns about the potential impact of cyber-attacks. In the contemporary era, seaports and vessels employ a diverse range of sophisticated technological systems that incorporate electronic software and hardware to improve effectiveness, safety, and overall functionality. The implementation of Automated Terminal Operating Systems (ATOS) for container optimization, Port Security Systems, and Cargo Handling Equipment Automation in seaports, along with Global Positioning Systems (GPS), Automated Identification Systems (AIS), and Electronic Chart Display and Information Systems (ECDIS) on vessels (Weng et al., 2023), raises concerns regarding cybersecurity in the maritime domain. In 2017, Maersk, a leading global shipping company with the largest fleet capacity (comprising 18% of the global fleet capacity), experienced significant financial losses amounting to $300 million due to the most severe cyberattack ever recorded in the maritime industry. The attack involved the NotPetya ransomware, which infiltrated the company's reservation system, resulting in the widespread congestion of 80 ports worldwide. Some of these ports experienced complete disruptions in

loading traffic and container operations. Rotterdam's automated terminal was rendered inactive, and electronic systems in New York and New Jersey froze (Benmalek, 2024). Given the gravity of cyber-attacks and their unique nature, which sets them apart from other security concerns by transcending physical boundaries, hackers have the freedom to target electronic systems worldwide at any given moment.

Recognizing this, there is an essential need to redirect attention from conventional safety and security measures on physical systems toward addressing the risks posed by cyber threats. In 2022, the International Maritime Organization (IMO) took a significant step by revising its guidelines on "Maritime Cyber Risk Management". These updated guidelines offer comprehensive recommendations at a high level, aiming to protect the shipping industry from both existing and evolving cyber threats and vulnerabilities. Notably, the guidelines incorporate functional elements designed to enhance the efficacy of cyber risk management practices in the maritime sector (IMO, 2022). On an individual level, attempts have been made to assess the cybersecurity risks in the maritime sector through both qualitative and quantitative approaches. Oruc et al. (2022) presented a summary of global standards, current bridge test environments, and regulations established by the IMO for evaluating cybersecurity risks in integrated navigation systems. Kessler (2021) offered a technical analysis of Control Area Network (CAN) bus standards and operations within maritime vessels, delving into cybersecurity vulnerabilities that could compromise the confidentiality, integrity, or availability of information in the maritime industry. Schinas and Metzger (2023) conducted a review highlighting policy gaps in the realm of cybersecurity within the maritime domain. In response to these identified gaps, they introduced the concept of "cyber-seaworthiness" as a proposed solution. Kanwal et al. (2022) conducted an evaluation examining the interplay between the cybersecurity performance of ships and six distinct cybersecurity dimensions. These dimensions encompassed aspects such as "regulations," "company procedures," "shipboard system readiness," "training and awareness," "human factor," and "compliance monitoring".

From a quantitative perspective, attempts have been made to apply conventional risk assessment techniques to address cyberthreats. Examples of such efforts include the use of HAZOP (Hazard and Operability), FMEA (Failure Mode and Effect Analysis), FTA (Fault Tree Analysis), ETA (Event Tree Analysis), Bow-tie, attack trees, and risk matrices (Henriques De Gusmão et al., 2018) (Progoulakis et al., 2021) (Yoo and Park, 2021) (Komal, 2023). However, the primary challenge with these approaches lies in the significant uncertainty inherent in data analysis, raising questions about their effectiveness. To address this concern, some researchers have proposed the adoption of advanced methods like BN or a combination of BN with the traditional approaches mentioned earlier. This integration is exemplified in the work of Park et al. (2023), who utilized a combination of FMEA and Rule-based BN (RBN) to assess and prioritize the risk levels associated with various cyber-attacks. Despite some improvement in cybersecurity analysis through these recent methodologies, a drawback is their reliance on subjective data. The collection of data predominantly relies on expert judgment, a practice that invites debate due to inherent biases in expert opinions. Factors such as the number of experts responding to questionnaires and the quality of their responses critically determine the study's reliability. Additionally, the weighting assigned to experts and their opinions is a point of contention. While in safety and security analyses, greater weight is often given to experts with more experience, in the realm of cyberthreats, there is an argument that younger experts, possessing greater familiarity with Information Technology (IT) systems, may offer more

realistic insights (Öğütçü et al., 2016). Basically, the existing maritime cybersecurity analysis methods at large rely on subjective and/or qualitative analysis due to the constraints of data availability. Therefore, in Park's work (Park et al., 2023), the risk parameters are generic at a macro level, such as likelihood and consequence severity that could be evaluated by domain experts. Additionally, a detailed classification of cyber threats across different maritime sectors is lacking. In contrast, in this study, it is for the first time to employ micro-level risk factors (e.g., regions, attack modes, vulnerable targets,) to quantify maritime cybersecurity risk levels. It can therefore better reflect the real-world cyber security threats and evaluate/predict their risk levels, as revealed by the implications of the work.

Taking into account the limitations identified in prior research, this study endeavours to pioneer a novel approach to maritime cybersecurity risk analysis. The proposed method involves harnessing real data encompassing all cyber incidents within the maritime industry over the past two decades. The intention is to employ this comprehensive dataset to train a data-driven BN model, offering a more robust and empirically grounded framework for evaluating cybersecurity risks in the maritime sector. The contributions of this chapter can be summarized as follows:

1) Comprehensive data collection on maritime cybersecurity: An exhaustive collection of recorded cyber-attacks within the maritime industry was conducted, and the data was refined to develop a new dataset that encompasses comprehensive information on the most relevant risk factors.
2) Novel diagnosis analysis: This study introduces a pioneering approach to quantifying maritime cybersecurity risk analysis by utilizing real data spanning two decades to train a data-driven BN model. This enhances the empirical foundation of cybersecurity risk assessment in the maritime sector and marks the first significant improvement in the accuracy of cybersecurity diagnosis analysis.
3) Identification of contemporary patterns: This study contributes to tracking contemporary patterns in maritime cyber-attacks, elucidating key influencing factors such as vulnerable targets, affected countries, high-risk regions, types of cyber-attacks, and their origins.
4) Insights for nuanced understanding: The adopted approach offers valuable insights for a nuanced comprehension of the dynamics surrounding maritime cyber threats, providing a more comprehensive perspective. The results serve as a benchmark for enhancing diagnostic analyses, ultimately leading to improved prediction accuracy.
5) Implications for stakeholders and governmental bodies: The study's implications provide valuable insights for stakeholders and governmental bodies, enriching their understanding of addressing cyber threats in the maritime industry. This includes optimized resource allocation, preventive measures, and mitigation strategies.

The following sections of the chapter are structured as follows: Section 4.3 offers a brief critique of existing literature on maritime cybersecurity and studies related to data-driven BN risk analysis. In Section 4.4, the study delves into the details of the data collection process, methodology, and validation techniques employed for the developed model. Section 4.5 presents the analysis results and engages in discussions regarding the model's outputs. Further discourse on the results and their potential implications, along with considerations for future

research directions, is provided in Section 4.6. The chapter concludes in Section 4.7 by drawing overall insights and summarizing key findings.

4.3 Literature review

4.3.1 Studies on cybersecurity risk assessment

Examining the literature pertaining to cyber-attacks, a significant portion of the published papers originates from the fields of computer security and related disciplines (Diao et al., 2024) (Berghout and Benbouzid, 2022) (D. Tang et al., 2023) (Patriarca et al., 2022). However, when focusing on the maritime field, there is a limited number of identified papers, indicating a substantial gap requiring additional research. Several review papers (Ben Farah et al., 2022) (Tusher et al., 2022) (Ashraf et al., 2022) (Larsen and Lund, 2021) offer a thorough overview of published papers on maritime cybersecurity, with the work by Bolbot et al. (2022) standing out as the most comprehensive among them. To narrow the focus to papers employing a risk assessment methodology, the emphasis will be on studies involving risk identification, evaluation, and analysis.

Additionally, attention will be given to research that develops frameworks and conducts vulnerability analyses within this domain. Several contributions in the realm of cybersecurity studies can be attributed to model-based approaches. Tam and Jones (2019), for instance, introduced a model-based framework named 'MaCRA' (Maritime Cyber Risk Analysis). This framework aims to identify primary risk outcomes, attackers, attack vectors, and systems that would benefit or require additional security. Moreover, it seeks to characterize the severity of maritime cyber risks and, crucially, to present risk data in informative views that aid human decision-making processes. Schauer et al. (2019) introduced a six-stage methodology named 'MITIGATE SCRA', utilizing a graph-based approach to analyse the risk of cyber-attacks within the maritime supply chain. Carreras Guzman et al. (2020) presented a master model diagram that features a multi-layered diagrammatic representation of cyber-physical systems. This model is designed for a comprehensive safety and security risk analysis, showcasing its application in the maritime sector through the analysis of an autonomous surface vehicle. In the realm of quantitative cyber threat risk assessment, notable work includes the following: Park et al. (2023) introduced an innovative hybrid framework, combining FMEA with a rule-based BN approach. This framework was developed to assess the risk levels of various cyber-attacks in maritime operations and rank them accordingly. Quantitative data for this assessment was gathered through a questionnaire and expert judgments, contributing to a robust understanding of cyber threat risks. A similar study in the realm of quantifying cyber threat risks was undertaken by Uflaz et al. (2024), focusing on the assessment of potential cyber-attacks on bridge navigational systems. Their approach involved a combination of Failure Modes, Effects, and Criticality Analysis (FMECA), expert judgment, Dempster-Shafer theory, and a rule-based BN technique. This comprehensive methodology aimed to provide a quantitative evaluation of the risks associated with cyber threats on bridge navigational systems. In terms of the port sector, Gunes et al. (2021) proposed a cyber security risk assessment methodology tailored for seaports. Their approach involved simulating four distinct cyber-attack scenarios within a designated container port. Employing a comprehensive 13-stage framework, they quantified the risk associated with each scenario on a scale ranging from

1 to 10. This systematic assessment provided a nuanced understanding of cyber security risks specific to seaport environments.

4.3.2 Application of BN in maritime risk assessment

Among the array of methodologies discussed for assessing the risks posed by cyber-attacks, BN stands out for its exceptional ability to model and manage uncertainty effectively. When compared to conventional risk assessment approaches such as FTA, FMEA, and risk matrices, BN emerges as superior in its capacity to capture the intricate causal relationships among risk factors. It excels in managing both subjective and objective data concurrently. Moreover, in terms of scalability, recent advancements in computational techniques have empowered BN to handle the construction and analysis of large-scale structures (Cheng et al., 2024; Kong et al., 2024; Sheng et al., 2024). This progress facilitates the modelling of complex systems with myriad interconnected variables. Additionally, in relation to adaptability, BN offers the flexibility to be updated and refined with emerging data or evolving system insights. This feature ensures that risk assessments remain pertinent and up to date over time (Kabir and Papadopoulos, 2019). These inherent characteristics position BN as a promising and effective tool for the analysis of cyber-attacks, enabling comprehensive modelling and the study of their potential consequences. In this context, initiating the deployment of such a methodology begins with the structural learning of the BN. Existing literature indicates that mastering the structure learning of BN can be a formidable task, given the super-exponential multitude of potential graphs and the challenge of accurately diagnosing relationships among various nodes. The integration of expert knowledge has the potential to enhance the learning process, particularly when the number of experts and their level of experience reach a satisfactory threshold. In this regard, leveraging experts' insights into cause-effect relationships can be employed to shape the network's structure. Furthermore, modelling the individual probabilities of experts correctly labelling the inclusion or exclusion of edges can be employed to refine and improve the overall learning algorithm (Amirkhani et al., 2017). Given the wealth of literature on the application of BN in maritime risk, a selection strategy is implemented to offer a manageable yet inclusive set of papers. This strategy involves picking a combination of both highly cited and recently published papers. These chosen papers should not only focus on maritime security but also offer innovative perspectives on the application of BN within this context. Both Bouejla et al. (2014) and Pristrom et al. (2016) utilized expert judgment alongside data from the IMO to establish a BN structure for evaluating the risk of piracy attacks on ships. Jiang and Lu (2020) adopted a hybrid approach, combining statistical data with expert knowledge for BN structure learning, applying this methodology to analyse maritime piracy in Southeast Asia. Hao et al. (2023) introduced a risk analysis and prediction model that explores the internal dynamics of maritime piracy accidents using a combination of the Markov model and BN. Chang et al. (2021) conducted a risk assessment of autonomous ships with a hybrid method combining FMEA and BN. Tunçel et al. (2024) devised an integrated approach incorporating rule-based BN and FMECA under evidential reasoning (ER) to assess the risks associated with anchoring operations on ships.

Although expert judgment is acknowledged as a valuable resource for BN structure learning, especially in scenarios with limited or unavailable data, it is essential to acknowledge the potential presence of uncertainty and biases. When abundant data is accessible, the utilization of machine learning algorithms becomes a precise and efficient alternative for learning the BN

structure. With the latest progress in BN capabilities, integrating machine learning methods into BN can boost their predictive power and enable the management of complex datasets, thereby enhancing the precision of risk assessments. Furthermore, the integration of sophisticated techniques for quantifying and propagating uncertainty within BN has been devised, leading to more resilient and trustworthy risk assessments through the consideration of uncertainty in input variables and model parameters. This approach, referred to as data-driven BN, involves the extraction of causal relationships, dependencies, and interdependencies among risk factors directly from the available data. By leveraging the information contained in the data, this method offers a more objective and empirical way to establish the structure of the BN, particularly in situations where extensive datasets are available. The adoption of a data-driven approach is observable in numerous maritime risk assessment studies. In order to provide a representative array of papers concerning data-driven BN structure learning, a comparable approach is utilized, selecting a mix of both widely referenced and recently published works, all of which are represented in Table 4.1.

Table 4. 1: Summarization of data-driven BN approach in maritime risk analysis

No.	Source	Amount of dataset	Number of nodes	Structure learning technique	Application
1	*(Fan et al., 2020)*	208	25	Tree Augmented Naïve (TAN) Bayes	Human factors in maritime accidents
2	*(Liu et al., 2021)*	414	20	Bayesian searching approach	Maritime major accident records in the Chinese coastal waters
3	*(Liu et al., 2022)*	1880	11	Bayesian searching approach	Port State Control inspection
4	*(Fan et al., 2022)*	61	25	TAN Bayes	Maritime accidents within restricted waters
5	*(Li et al., 2023)*	428	23	TAN Bayes	Global maritime accident
6	*(Zhou et al., 2024)*	402	24	TAN Bayes	Maritime casualty analysis
7	*(Fan and Yang, 2024)*	104	6	LASSO and TAN Bayes	Human fatigue investigation in maritime accidents
8	*(Xu et al., 2024)*	42418	18	Noisy-OR gate and the IF-THEN method	Navigation status control of cargo ships.
9	*(Wang and Yang, 2018)*	350	21	Augmented naive Bayesian Networks	Accident severity in waterborne transportation
10	*(Kamal and Çakır, 2022)*	418	13	TAN Bayes	Marine accidents in Istanbul Strait

4.3.3 Research gaps

With consideration of the conducted literature review, the following research gaps have been revealed:

1) The dominance of conventional risk assessment techniques in cybersecurity: The majority of the existing literature relies on conventional risk assessment techniques (e.g., HAZOP, FMEA, FTA, ETA, Bowtie, attack trees, and risk matrices) to address

cyber threats. However, these methods have been criticized due to the high uncertainty in cybersecurity risk data and the associated challenges in risk inference. There is a need for further research to adapt or improve risk analysis methods to enable them to handle the inherent uncertainty in cybersecurity data.

2) Subjectivity in expert judgment: The reliance on subjective data and expert judgment in most studies introduces potential biases, affecting the reliability of cyber risk assessments. New research should focus on finding ways to minimize these biases and enhance the objectivity of cybersecurity evaluations. It is essential to explore methods of mitigating expert bias in cybersecurity risk assessment.

3) Quality and weighting of expert opinions: Since most current studies rely on subjective data, leading to the ongoing debate about how to weigh expert opinions, particularly when balancing between the insights of experienced and less experienced experts. New research is needed to develop methods for systematically and fairly weighing expert opinions or to create alternative approaches that can effectively balance different types of expertise.

4) Comprehensive classification of cyber threats in different maritime sectors: Many existing studies on maritime cybersecurity risk analysis suffer from a lack of comprehensive classification of cyber threats across various maritime sectors. Some studies focus solely on cyber threats affecting vessels, while others concentrate only on shore-based entities. New research should aim to develop more granular and sector-specific classifications of cyber threats to improve the accuracy and relevance of risk assessments.

5) Real-world cybersecurity threat reflection: Many studies fail to adequately consider real-world cyber incidents within the industry, which can result in unrealistic objectives and less accurate outcomes. To address this gap, incorporating micro-level risk factors and developing an objective database based on historical data could provide a more accurate reflection of real-world threats. Research should further validate this approach by comparing the effectiveness of micro-level versus macro-level risk assessments in predicting and mitigating real-world cyber threats.

This study builds on the existing literature by pioneering the use of data-driven learning in developing a BN model for analysing cyber threats in the maritime sector. However, in contrast to prior research, it introduces a novel approach to analysing the risks associated with maritime cyberattacks by incorporating objective data for the first time. To achieve this goal, two decades' worth of maritime cyber incidents are manually collected, analysed and utilized to construct a BN model driven by machine learning. Additionally, a comprehensive manual examination of each maritime cybersecurity incident across diverse entities, including seaports, shipping companies, offshore installations, vessels, and others, is conducted to establish the inaugural maritime cybersecurity risk database. This study approaches the process from a broad and worldwide viewpoint, emphasizing its theoretical novelty. The research progresses through several phases, including data collection, model development, comparative analysis of models, validation of the model, and the resulting model output. In contrast to the traditional use of BN in risk assessment, this study is among the pioneering ones investigating cyber security risk

assessment, and it additionally proves the effectiveness of the developed model in maritime cybersecurity risk analysis, a less explored but crucial area of growing importance for safety at sea. It newly identifies the risk factors during the model comparison stage, using real-world data. This endeavour marks a substantial leap forward in the discipline, enhancing comprehension of maritime cyber-attacks and refining our understanding of the risk attributes linked to cyber threats within this field.

4.4 Methodology

This study utilizes a data-driven BN methodology to pinpoint the 'Security Risk Influencing Factors' (SRIFs) related to cyber threats in maritime infrastructures such as seaports and vessels. In this regard, a holistic framework encompassing four pivotal stages is developed: data collection and processing, BN model construction, model validation and verification, analysis of model outputs, and extraction of useful information. The ultimate goal is to propose effective guidelines for bolstering maritime security. Figure 4.1 demonstrates the entirety of our proposed methodology.

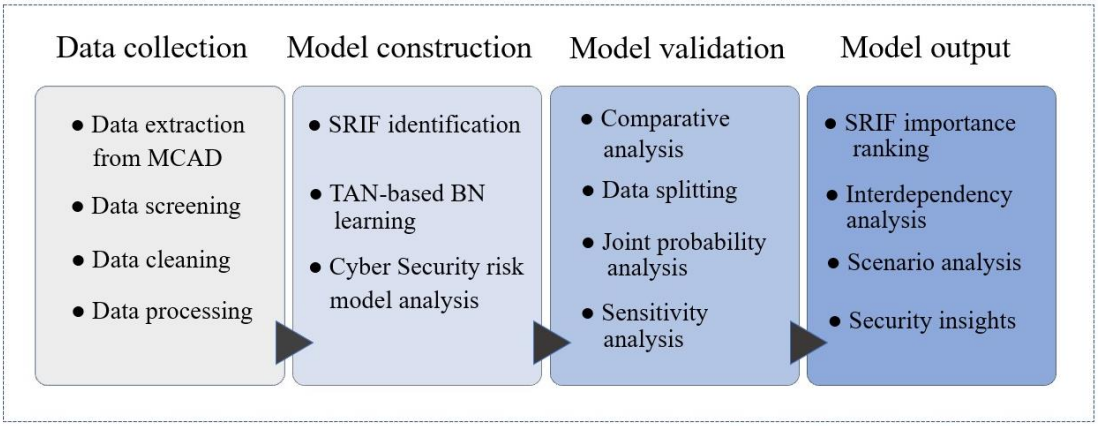

Figure 4. 1: The proposed framework for cybersecurity risk analysis.

4.4.1 Data collection and processing

In the process of gathering information on cyber-attacks targeting maritime infrastructures, the Maritime Cyber Attack Database (MCAD) is employed for its specific focus (MCAD, 2023). Originating from open-source data, the MCAD is the result of collaborative efforts by the Maritime IT Security research group at NHL Stenden University of Applied Sciences in the Netherlands, encompassing details on more than 160 cyber incidents within the maritime sector. This database goes beyond vessel-related events, also documenting incidents affecting seaports and various maritime facilities on a global scale. The timeline for data collection spans from 2001 to 2023, allowing for a comprehensive analysis of maritime cyber threats and the identification of meaningful patterns over an extensive period. Upon thorough examination of the database and consideration of pertinent cases within the realm of maritime cyber-attacks, the decision was made to adopt a comprehensive approach. Given the novelty of the subject and the intricate interplay of cyber-attacks across diverse elements of the maritime industry, including the potential impact on seaports, it was determined that all incidents, irrespective of their specific target (seaports, ships, offshore structures, and related components), would be included for analysis. This inclusive approach ensures a holistic understanding of the various cyber threats within the maritime domain.

Data collection involved manual extraction from the MCAD database, with categorization according to various SRIFs. However, during this process, certain shortcomings were encountered in obtaining precise information regarding the SRIFs. These shortcomings stem from certain gaps in the data, such as missing details about the target characteristics (such as whether it was offshore infrastructure, a port, a shipping company, or a maritime organization), the extent of the consequences (whether the impact of the cyberattack was significant or minimal), the source of the attack (with some cases having unidentified origins in the database), and the geographical region of the incidents. Not all data were available in the database. To address these issues, additional information from news articles and public sources was researched and gathered to create a refined database suitable for model development. Each case was scrutinized individually to extract missing information through resources referenced by MCAD and cross-referencing relevant websites to validate the data in MCAD. For instance, in February 2022, the UK ferry operator Wightlink, based in Portsmouth, was hit by a cyber-attack. The database only mentioned that the back-office IT systems were compromised. Our further investigation revealed it was a phishing attack with a minor impact on the company's functionality. Another example is the June 2021 ransomware attack on the network of the Woods Hole, 'Martha's Vineyard, and Nantucket Steamship Authority in Boston, MA, USA. Initially, the database only mentioned that malware encrypted files, rendering the system inoperable. Additional research uncovered that the attack had a major impact, preventing changes or bookings for reservations, causing ticketing delays, and limiting the availability of credit card systems, necessitating cash transactions. Overall, the refined database underwent rigorous scrutiny and cross-checked with multiple information sources to ensure the reliability of the collected data and address any missing items in the MCAD.

4.4.2 SRIF identification

In this study, the elements influencing the security of maritime infrastructures and vessels are denoted as SRIFs. These factors are identified by examining data from the MCAD, as well as by incorporating information from a literature review to classify and compile relevant indicators. The pertinent literature is chosen by conducting searches with keywords such as "cybersecurity", "cyberattacks," and "cyber threats" on the Web of Science. From numerous identified papers, 10 have been scrutinized for their relevance and content, with the aim of extracting the most significant SRIFs. Table 4.2 presents the selected literature along with their corresponding SRIFs.

Table 4. 2: The sources of SRIFs based on the retrieved results and the comprehensive dataset.

Reference	SRIFs											
	1	2	3	4	5	6	7	8	9	10	11	12
(Uflaz et al., 2024)				*	*	*	*		*	*	*	
(Gunes et al., 2021)			*	*	*	*	*		*	*	*	
(Kavallieratos et al., 2021)					*	*			*	*		
(Bolbot et al., 2020)			*	*	*	*	*	*	*	*	*	
(Kavallieratos et al., 2019)					*	*	*			*	*	
(Yoo and Park, 2021)						*			*	*	*	
(Park et al., 2023)					*					*	*	
(Tam and Jones, 2019)			*	*	*	*	*	*	*	*	*	
(Henriques De Gusmão et al., 2018)					*	*	*		*		*	
MCAD	*	*	*		*	*	*				*	*

Note: 1. Region; 2. Country; 3. Perpetrator; 4. Scenario; 5. Cyber-attack type; 6. Target; 7. Successful attack; 8. Property damage; 9. Prevention ability; 10. Security risk level; 11. Consequence; 12. Temporal trend.

In the context of cyber-attacks, the precise factors that exert a significant influence on the overall risk level are not yet fully understood due to their novel and complex nature. However, a literature review, as outlined in Table 4.2, and available historical data have identified 7 SRIFs for a data-driven BN analysis. These factors encompass cyber threats, target entities (including offshore structures, shipping companies, vessels, etc., not limited to seaports), victim and origin countries, regions, years, and consequences. It is noteworthy that the scope of potential targets extends beyond seaports to include various maritime-related elements. This broader perspective provides a holistic understanding of how cyber-attacks may unfold in the maritime industry. Throughout the selection process of SRIFs, several criteria were considered to ensure the model's accuracy, relevance, and practicality. Here are the key criteria adopted for this study:

1) Literature review: It is evident that SRIFs recognized in the literature as critical to cybersecurity should be prioritized. This process involves examining academic papers, industry reports, and case studies to identify factors with a significant impact on research outcomes. Furthermore, among the identified SRIFs, those empirically validated through previous studies are more likely to have a well-established relationship with the outcomes being modelled. Therefore, we conducted a comprehensive literature review by conducting searches with keywords such as "cybersecurity", "cyberattacks," and "cyber threats" on the Web of Science. From numerous identified results, 10 papers have been scrutinized for their relevance and content to extract the most significant SRIFs. Table 4.2 presents the selected literature along with their corresponding SRIFs.
2) Availability of factors in the database: It is essential to ensure that the selected SRIFs are well-represented in the database with minimal missing data, as factors with significant missing information can result in inaccurate or biased outcomes. Additionally, it is crucial to verify that the data related to these factors is consistently recorded and formatted. Inconsistent data can complicate the modelling process and diminish the reliability of the results. In this context, the SRIFs identified from the literature review were cross-referenced with the existing factors in the MCAD database to ensure a consistent selection process. For instance, factors such as scenario, property damage, prevention ability, and security risk level were identified in the literature review but were missing in the database. Consequently, these factors were excluded from further analysis.
3) Expert judgment and domain knowledge: Experts can offer insights that are not visible in data or literature alone, aiding in capturing the subtle complexities of the domain. In this study, we sought assistance from two experts with substantial knowledge and experience in this domain and requested their approval of the selected SRIFs.
4) Model testing and validation: By creating a preliminary, TAN-based BN with the initially selected SRIFs and testing its performance, the least relevant factors can be identified. By eliminating these irrelevant factors and continuously refining the model through iterative adjustments based on performance metrics and the D-separation technique, the final SRIFs are selected. For example, we initially considered the factor "months of the year" to determine if it contributed to the occurrence of cyber threats.

After running the model and testing this factor's influence on the target node, we found it to be irrelevant and ineffective. Therefore, it was excluded from the study.

For detailed information about the cyber SRIFs, their states, and descriptions, refer to Table 4.3.

Table 4. 3: Cyber SRIFs states and their descriptions

SRIFs	States	Description
Cyber threats	DDOS, Hacking, Jamming, Malware, Phishing, Ransomware, Spoofing	A “DDOS” which stands for Distributed Denial of Service attack, is an intentional effort to disrupt the normal operation of a network, service, or website by inundating it with a surge of internet traffic. “Hacking” serves as a broad term encompassing unauthorized access into computer or network systems, aiming to manipulate information, engage in data theft, or disrupt normal operations. “Jamming” refers to intentional interference with radio and GPS signals, wireless communications, or radar systems, with the goal of disrupting or preventing normal communication. “Malware” involves introducing harmful software to disrupt the functioning of computer systems, networks, or devices, leading to malfunctions or the dissemination of inaccurate data. “Phishing” occurred when victims are deceived into revealing sensitive information through deceptive communication posing as a trustworthy entity. “Ransomware”, evident from its name, is a form of virtual extortion in which malicious software encrypts the victim's system, rendering it inaccessible, and demands payment for the decryption key. “Spoofing” deceives AIS systems with false signals, causing incorrect vessel information, while the system remains operational; distinct from jamming, which disrupts and disables the system.
Target	Offshore structures, Port, Shipping company, Vessel, Other	“Offshore structures” encompass a range of installations and facilities situated in bodies of water, usually distant from the shore. Examples include gas and oil platforms, wind farms, and drilling rigs. “Shipping companies” are responsible for the sea transportation of goods or passengers. They own, operate, and manage vessels, including cargo ships, container ships, tankers, and more, facilitating global maritime trade and transportation. Entities related to maritime activities, including shipbuilding firms, energy distributors, insurance, and brokerage organizations situated on the shore, are categorized under the label "other."
Victim countries	Australia, Belgium, Canada, China, Cyprus, Denmark, Germany, Greece, India, Indonesia, Iran, Israel, Japan, Kuwait,	“Countries” experiencing fewer than three cyber-attacks are collectively categorized under the "other" state. The screening criteria are established at fewer than 3 cyber-attacks to eliminate over 15 countries as new states. This method is adopted to circumvent the subsequent drawbacks: 1) As the quantity of states within a node rises,

	Netherland, Norway, Philippines, Russia, Saudi Arabia, Singapore, South Korea, UK, Ukraine, USA, Other	so does the complexity of BN. 2) A greater volume of data is required to precisely gauge the probabilities linked with each state as the number of states increases. 3) A BN featuring numerous states within a node might become less understandable. This approach is applied to the rest of the nodes as well.
Region	Eastern Asia, Europe, Middle East & North Africa, North America, Other	"Regions" experiencing fewer than three cyber-attacks are collectively categorized under the "other" state. The selection of regions is based on the frequency of cyber-attacks as well as the focus of maritime entities in different areas of the world. For instance, Europe encompasses all territories surrounding the European continent, spanning both Western and Eastern Europe. While, Eastern Asia concentrates solely on this specific part of the continent, encompassing Southeast Asian countries due to the dense concentration of maritime entities in this region. This concept applies similarly to other regions across the globe.
Cyber threat origin	China, Iran, Nigeria, North Korea, Russia, Other, Unknown	It's important to clarify that identifying origin countries in cyber-attacks doesn't necessarily implicate the involvement of their states. The attribution is based on tracking the cyber-attack to a specific location. "Countries" involving fewer than three cyber-attacks are collectively categorized under the "other" state.
Consequence	Major, Minor	Consequences are categorized as "major" if they cause substantial disruption to the targeted entity's operations, resulting in significant physical and financial damage, as well as serious data theft and credential compromise. Conversely, attacks with less severe consequences are attributed to the "minor" category. To clarify this categorization, the NotPetya ransomware attack on Maersk, a major cyber-attack causing a $300 million loss, exemplifies significant consequences. Similarly, the hacking of India's Jawaharlal Nehru Port Container Terminal in February 2022, resulting in a five-day shutdown, underscores "major" repercussions. Conversely, less impactful incidents, either successfully thwarted or quickly recovered from, are labelled as "minor" cyber-attacks *(Benmalek, 2024)*.
Year	2001-2023	-

4.4.3 Data-driven BN structure learning process

BN is an advanced graphical inference technique capable of modelling both subjective and objective data, taking into account the uncertainty associated with them. As a formal probabilistic approach, BN can also depict the causal relationships among random variables by employing conditional probabilities (Yang et al., 2018).

This study aims to construct a BN structure by adopting the data-driven approach. This method seeks to capture various relationships, encompassing dependencies and interdependencies among different identified SRIFs. Based on the discussion of the previous chapter, the same approach has been implemented in this section.

4.5 Results

4.5.1 TAN-based BN modelling construction

Employing the identified SRIFs outlined in Table 4.3 and designating the cyber threats as the target node, the TAN model for maritime cybersecurity is constructed. This modelling process was carried out using Netica software ("Netica (Version 607).," 2019), as illustrated in Figure 4.2. The resulting model adeptly captures and signifies the probabilistic dependencies among various variables, employing a specific structure conducive to streamlined computations. Following the model's establishment, it undergoes a data-driven procedure wherein the diagnostic and prognostic capabilities of the model are activated based on the feeding of prior data, enhancing its practical utility.

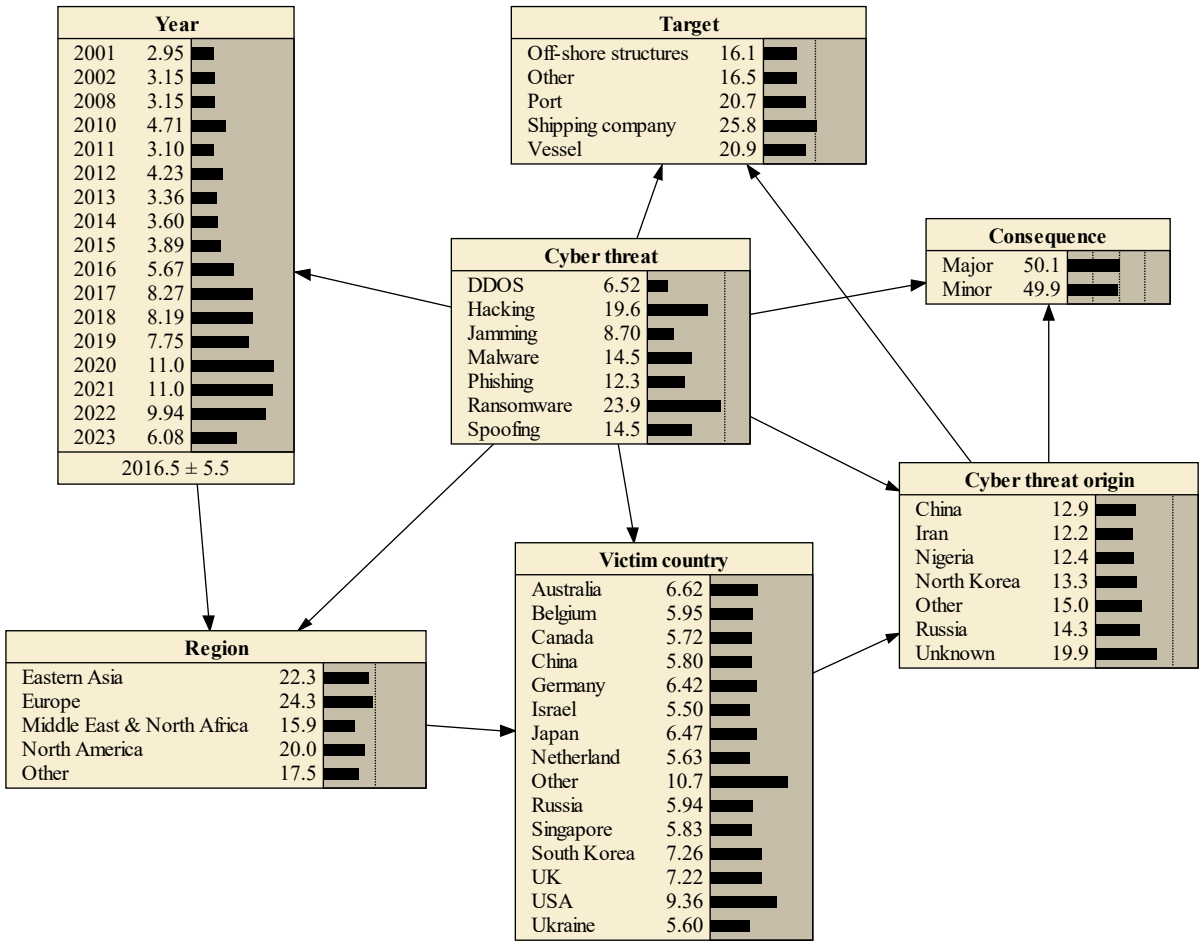

Figure 4. 2: TAN-based BN model of cyber-attacks.

4.5.2 Model validation

Using the concepts and validation methodologies described in section 3.4.4, the constructed BN model for cyber threats undergoes validation to assess its accuracy in both diagnostic and prognostic capabilities. Table 4.4 presents a comparison between the results of statistical analysis and the TAN model, revealing a substantial level of agreement.

Table 4. 4: Comparative analysis of historical and TAN results

Attack type	Historical data (%)	TAN results (%)	Accuracy (%)
DDOS	6.80	6.52	95.8
Hacking	19.1	19.6	97.4
Jamming	8.70	8.70	100
Malware	14.8	14.5	98
Phishing	11.7	12.3	95.1
Ransomware	24.1	23.9	99.2
Spoofing	14.8	14.5	98

The findings indicate that ransomware emerges as the most prevalent form of cyber-attacks in stationary maritime infrastructures, followed by hacking, malware, phishing, and DDOS. It's important to highlight that all the recorded DDOS attacks occurred within seaports. In the case of vessels, the two most frequent cyber-attacks are spoofing and jamming, respectively. Regarding cyber threats against vessels, certain regions worldwide are more susceptible than others. Jamming incidents are frequently observed in Eastern Asia, while spoofing tends to be more prevalent in the seas around Europe and Northern America. In terms of time, the recent years, specifically over the past five years, have witnessed a notable increase in cyber-attacks, reaching a peak in 2020 and 2021. This trend suggests a continuous upward trajectory. These initial findings suggest that BN outperforms statistical analysis. BN demonstrates the ability to identify causal relationships and the interdependence of various variables, showcasing its superiority in this context. Another validation method utilized in this phase is the D-separation technique. D-separation (or Directed Separation) is a key concept in BN modelling, used to determine conditional independence between nodes. It helps in assessing whether two variables are independent given certain evidence, making it essential for reasoning within the network (Yu et al., 2021). After the BN is initially constructed, D-separation is applied to examine correlations between any two nodes in the network. For instance, when the "cyber threat" node is observed, the nodes "Target" and "Region" become independent, meaning they are D-separated and conditionally independent. Conducting similar analyses across other nodes and connections helps to validate the BN structure, ensuring its rationality.

To assess the prognostic capability of the developed model, a data splitting process is employed by reserving 20 percent of the collected data for testing. The model is trained using the remaining 80 percent of the data. The resulting confusion matrix, as depicted in Table 4.5, reveals an overall accuracy exceeding 93 percent, with a perfect predictability rate of 100 percent for the majority of the target states. This indicates a high level of success in the model's ability to make accurate predictions and underscores its reliability for prognostic purposes.

Table 4. 5: Confusion matrix of predicted results.

		Actual							Actual total	Accuracy rate (%)
		DDOS	Hacking	Jamming	Malware	Phishing	Ransomware	Spoofing		
Predicted	DDOS	3	0	0	0	0	0	0	3	100
	Hacking	0	4	0	1	0	1	0	6	66.6
	Jamming	0	0	3	0	0	0	0	3	100
	Malware	0	0	0	3	0	0	1	4	75.0
	Phishing	0	0	0	0	3	0	0	3	100
	Ransomware	0	0	0	0	0	7	0	7	100

	Spoofing	0	0	0	0	0	0	5	5	100
	Total	3	4	3	4	3	8	6	31	93.3

After obtaining the accuracy rate from the confusion matrix, an additional metric is utilized to validate the model's reliability, known as the Kappa coefficient, often referred to as Cohen's Kappa (Cohen, 1960). This statistical measure evaluates the degree of agreement between two raters or observers when categorizing or classifying items. In the context of this study, the aim is to quantify the agreement between predicted and actual results. By applying the Kappa coefficient formula and incorporating relevant values, such as the expected proportion of agreement and the observed proportion of agreement derived from the confusion matrix (representing overall accuracy), the calculated Kappa coefficient is 0.92. The result suggests a remarkable degree of consistency in the model, as per Landis and Koch (1977), where a coefficient exceeding 0.8 is deemed ideal. This underscores a level of agreement that far exceeds what might be expected through random chance.

In line with the information provided in the validation section, Figure 4.3 displays diverse performance metrics for each cyber-attack based on an analysis of the confusion matrix. Notably, the model's precision is remarkably high, reaching 100% for the majority of cyber-attacks and maintaining satisfactory values above 75% for the rest. Concerning Recall, hacking and malware exhibit values of 66.6% and 75%, respectively, while other types of attacks achieve a perfect 100%. The F-measure, a metric that harmonizes precision and recall, surpasses 75% across all categories, with the majority scoring above 90%, indicating a well-balanced assessment of the model's performance. As previously mentioned, a higher specificity contributes to enhanced model robustness. Specifically, DDoS, hacking, jamming, and phishing showcase a specificity of 100%, while malware, ransomware, and spoofing, though around 96%, still indicate substantial robustness. An analysis of these performance metrics highlights the notable reliability and robustness exhibited by the developed model.

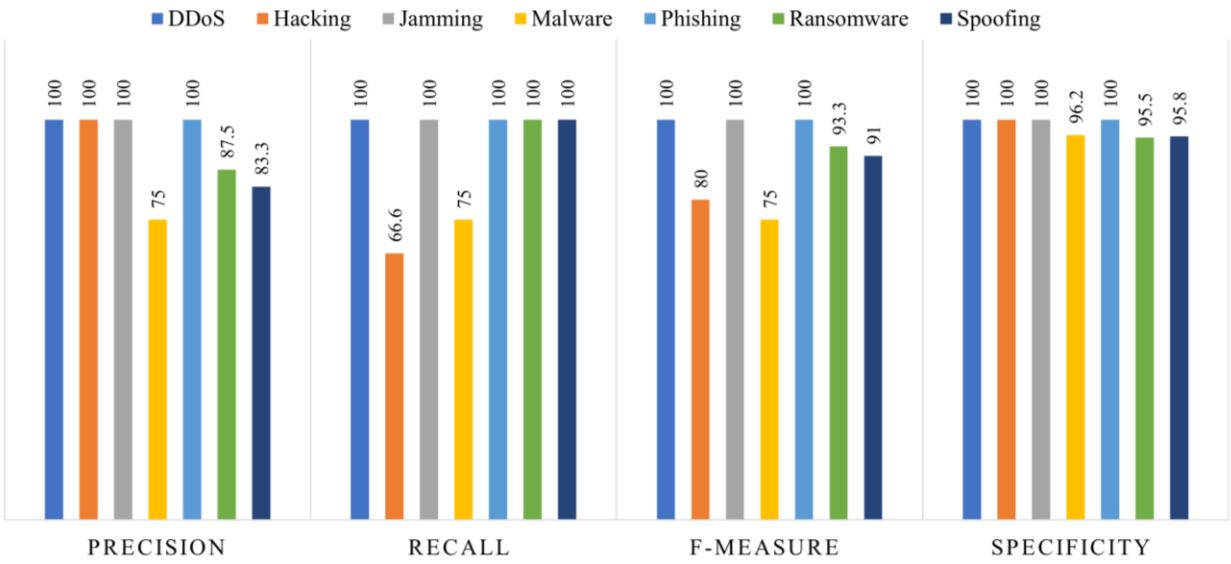

Figure 4. 3: The performance metrics for different cyber-attacks.

During the next phase of the validation process, the strength of the relationship between cyber threats and other SRIFs is assessed by measuring mutual information, as detailed in Table 4.6.

Significantly, the analysis indicates that the factor of "year" emerges as the most impactful, far surpassing the influence of “target” and the “countries falling victim” to cyber threats. This underscores the paramount importance of temporal considerations, the type of targets and the readiness of cyber defence abilities of countries in comprehending and addressing cybersecurity challenges, with a notable distinction in the significance of these factors.

Table 4. 6: Mutual information between cyber threats and other SRIFs.

Node	Mutual information	Percentage (%)	Variance of belief
Cyber threat	2.69722	100	0.7011338
Year	0.24606	9.12	0.0165646
Target	0.06310	2.34	0.0028549
Victim country	0.03683	1.37	0.0016443
Consequence	0.03446	1.28	0.0012589
Region	0.02861	1.06	0.0012553
Cyber threat origin	0.01744	0.646	0.0007828

Based on the details outlined in section 3.4.4, the joint probability of the target node (referred to as cyber threats) and other relevant variables across different nodes is computed and displayed in Table 4.7. Altering the values of various states in nodes induces corresponding changes in the states of the target node. The extent of these variations is contingent upon the significance of the states influencing the target node. To facilitate clarity and highlight the most and least influential factors, bold formatting is applied to the highest and lowest values for both types of terrorist attacks. The joint probability analysis yields valuable insights: concerning targets, seaports are predominantly targeted by DDOS attacks, whereas ransomware incidents are more common in the context of shipping companies. Spoofing, on the other hand, tends to disrupt the normal operation of vessels. From a temporal perspective, the early years saw DDOS as the dominant cyber-attack type on stationary infrastructures like seaports; however, in recent years, ransomware has gained traction among attackers. This trend extends to vessels, which were previously disrupted by jamming but now face spoofing, considered a more sophisticated version of jamming. Spatially, European and North American seaports are more targeted by ransomware, while phishing and malware emerge as typical cyber threats for Asian targets. Further insights on this matter will be expounded upon in section 4.6.

Table 4. 7: The joint probability.

	DDOS	Hacking	Jamming	Malware	Phishing	Ransomware	Spoofing
Target							
Off-shore structure	6.76	20.6	8.74	14.9	14.1	22.3	12.5
Other	6.58	18.0	8.51	**16.3**	13.5	24.9	12.2
Port	**10.5**	**22.6**	8.22	**11.8**	8.68	28.5	9.75
Shipping company	**4.22**	21.0	**5.46**	16.3	**16.4**	**28.7**	**7.84**
Vessel	5.21	**15.2**	**13.3**	13.2	**8.60**	**13.9**	**30.7**
Year							
2001	**17.7**	15.4	10.5	13.6	12.6	16.5	13.6
2002	8.29	28.9	9.87	12.8	11.9	15.5	12.8
2008	8.29	28.9	9.87	12.8	11.9	15.5	12.8
2010	5.54	9.67	6.60	**51.3**	7.93	10.4	8.55
2011	8.43	14.7	10.0	26.0	12.1	15.8	13.0

2012	6.16	21.5	14.7	19.0	17.6	11.5	9.51
2013	15.5	13.6	9.25	24.0	11.1	14.5	12.0
2014	7.24	**37.9**	8.62	11.2	10.4	13.5	11.2
2015	6.70	23.4	7.97	10.3	28.8	12.5	10.3
2016	9.19	16.0	**38.3**	7.09	6.58	8.60	14.2
2017	6.31	33.0	3.75	9.73	**31.6**	**5.90**	9.73
2018	6.37	16.7	15.2	14.8	4.56	17.9	24.6
2019	3.37	**5.87**	4.01	15.6	9.63	25.2	**36.4**
2020	**2.37**	20.7	**2.82**	**3.66**	**3.39**	**48.8**	18.3
2021	2.38	16.6	2.84	25.7	10.2	31.2	11.0
2022	5.25	18.3	6.25	4.05	18.8	39.3	8.10
2023	12.9	22.5	5.11	6.62	6.14	40.2	**6.62**
Victim country							
Australia	5.93	23.3	7.52	11.4	10.1	30.2	11.5
Belgium	6.60	16.3	8.37	15.2	11.3	26.7	15.5
Canada	**9.64**	20.3	8.69	13.2	11.7	23.1	13.3
China	6.77	16.7	8.58	13.0	11.6	18.8	**24.5**
Germany	6.11	21.3	7.75	11.8	12.6	28.6	11.9
Israel	8.57	21.0	10.8	13.7	12.2	19.8	13.8
Japan	6.06	**24.0**	7.68	20.2	10.4	19.9	11.7
Netherland	8.39	17.2	8.84	13.4	11.9	23.8	16.4
Other	**3.67**	**16.1**	7.36	17.6	**16.8**	28.3	**10.2**
Russia	6.61	16.3	8.38	15.3	11.3	18.4	23.8
Singapore	6.73	20.0	8.53	13.0	16.6	22.1	13.0
South Korea	5.41	18.7	**18.5**	**20.5**	11.3	**15.0**	10.5
UK	6.54	21.7	6.89	10.5	15.1	22.0	17.3
Ukraine	7.01	17.3	8.88	18.8	12.0	19.5	16.5
USA	6.74	22.8	**5.32**	**9.58**	**8.51**	**34.0**	13.1
Cyber threat origin							
China	6.68	19.6	8.55	16.5	14.4	19.8	14.4
Iran	**7.54**	19.3	9.02	14.1	12.3	22.5	15.2
Nigeria	6.96	17.9	8.90	13.9	**17.7**	20.6	13.5
North Korea	6.47	18.9	**13.3**	**16.9**	11.3	**19.2**	13.9
Other	6.15	21.2	7.36	14.0	10.8	28.1	12.4
Russia	6.87	**15.5**	7.69	14.6	**10.5**	24.3	**20.7**
Unknown	**5.58**	**22.9**	**7.10**	**12.5**	10.8	**29.3**	**11.9**
Consequences							
Major	**5.03**	**20.4**	**9.11**	**16.4**	**12.7**	**28.6**	**7.84**
Minor	**8.02**	**18.7**	**8.28**	**12.6**	**11.9**	**19.2**	**21.2**
Region							
Eastern Asia	**5.18**	18.4	**11.9**	**20.6**	**14.0**	**15.1**	14.8
Europe	5.58	**16.4**	**6.70**	11.7	12.6	**29.6**	**17.5**
Middle east & North Africa	**7.99**	21.3	10.6	16.3	13.1	17.6	13.1
North America	7.93	21.3	6.82	**11.2**	**9.95**	28.9	13.9
Other	6.60	**21.8**	7.82	12.8	11.8	27.2	**11.9**

Taking into account the noteworthy findings highlighted in bold from the joint probability analysis, the TRI for all SRIFs is computed using the procedure outlined in section 3.4.4, and the outcomes are presented in Table 4.8. The results underscore that the factor "year" emerges

as the most influential, significantly impacting the target node. In comparison to other SRIFs, "year" obtains the highest TRI value by a substantial margin for all types of cyber-attacks. Following, the victim country stands out as the second most important variable, with "target" trailing closely. The remaining SRIFs can be ranked in the following order: region, cyber threat origin, and, finally, consequence. These findings shed light on the relative importance of these factors in assessing cyber threats in the context of the maritime industry.

Table 4. 8: TRI of SRIF for different cyber threats.

	DDOS	Hacking	Jamming	Malware	Phishing	Ransomware	Spoofing	Average
Year	7.67	16.02	17.74	23.82	14.11	21.45	14.89	**16.53**
Victim country	2.99	3.95	6.59	5.46	4.15	9.50	7.15	**5.68**
Target	3.14	3.70	3.92	2.25	3.90	7.40	11.43	**5.11**
Region	1.41	2.70	2.60	4.70	2.03	7.25	2.80	**3.36**
Cyber threat origin	0.98	3.70	3.10	2.20	3.60	5.05	4.40	**3.29**
Consequence	1.50	0.85	0.42	1.90	0.40	4.70	6.70	**2.35**

In the final stage of the validation process, the developed BN model undergoes sensitivity testing. Following the ranking obtained through mutual information, each variable is systematically adjusted, starting from the least important to the most crucial, with a 3 percent incremental change, and the resulting impact on the target node states is observed. Figure 4.4 illustrates the gradual increase in the elements of the bar chart for all types of cyber threats, clearly indicating that the model responds to the changes in a discernible manner. The term “reference” denotes the original value of each target node state prior to conducting the sensitivity analysis. As shown, for each state (e.g., spoofing, ransomware), the baseline values are lower than the corresponding perturbed values. This gradual increase is consistent with Principle 2 of the sensitivity analysis. This sensitivity testing further validates the robustness and adaptability of the BN model in capturing the dynamics of the interrelated variables and their influence on the target states.

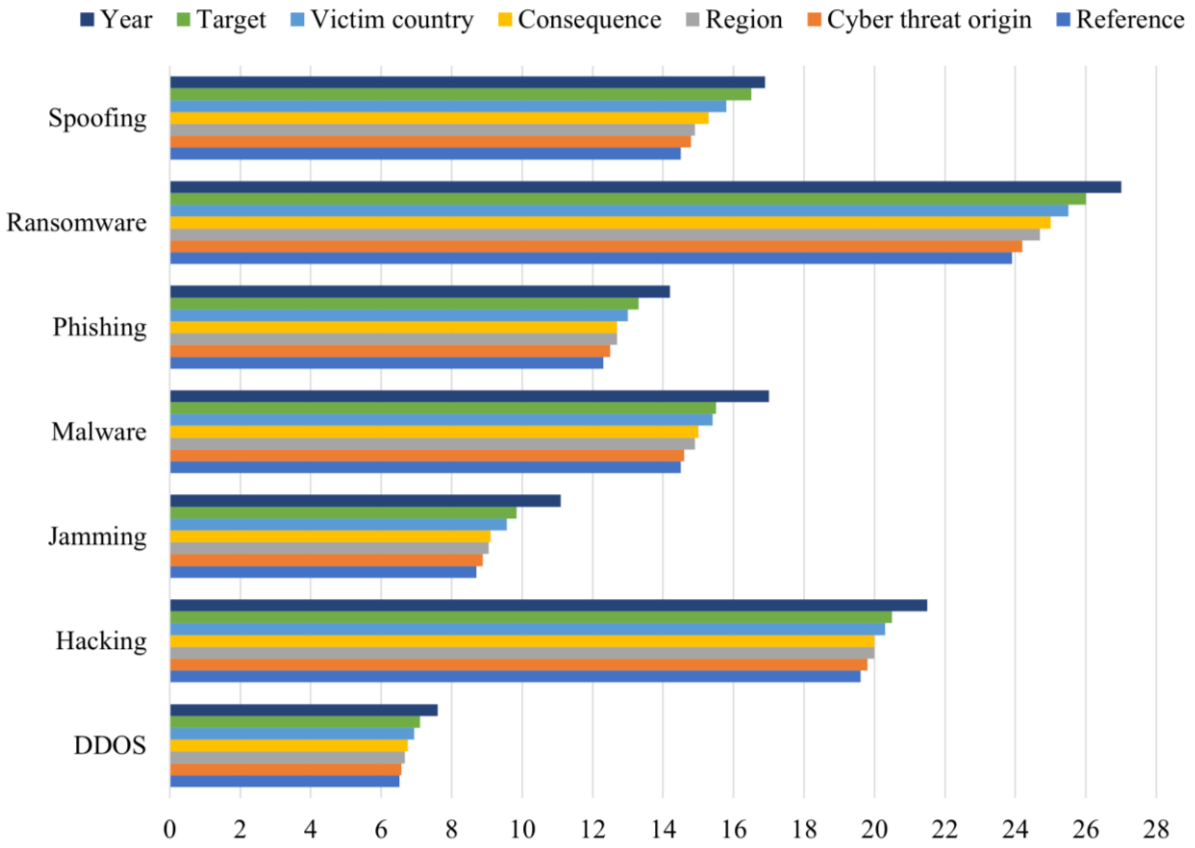

Figure 4. 4: Sensitivity analysis of BN model.

4.6 Discussions, implications, and future research directions

4.6.1 Discussions

4.6.1.1 Different types of cyber-attacks

Examining the compiled database obtained from MCAD and utilizing the BN model built from this information, seven distinct cyber threats were discerned within the maritime sector. These include DDOS, hacking, jamming, malware, phishing, ransomware, and spoofing. Notably, ransomware stands out as the most prevalent threat, accounting for nearly 25% of all documented incidents, followed by hacking, which comprises almost one-fifth of the total attacks. Through the utilization of the model and scenario analysis, valuable information and insights are acquired. For instance, by elevating the probability of ransomware to 100%, an effort is made to discern the primary contributing factors influencing the selected state of the target node. Illustrated in Figure 4.5, the probabilities associated with various states of other SRIFs undergo changes, signalling specific insights. Concerning the target, ransomware exhibits a preference for targeting shipping companies and seaports. This preference can be rationalized by the fact that ransomware attackers commonly demand cryptocurrency payments to restore access to compromised systems, compelling companies and seaports to potentially pay the ransom to mitigate downtime and operational disruptions. In terms of time, an examination of the past four years reveals a notable surge in ransomware incidents, with the peak occurring in 2020. Analysing the geographical distribution of these attacks, Europe emerges as the primary target, closely followed by North America. Among the specific nations

affected, the United States, Australia, and Germany stand out as the top three victim countries experiencing ransomware incidents. Notably, a significant majority of these cyber-attacks fall into the category of major incidents, underscoring the severity of their consequences. This temporal and geographical analysis highlights the alarming trend of ransomware activity over the specified period and emphasizes the global impact of these malicious incidents.

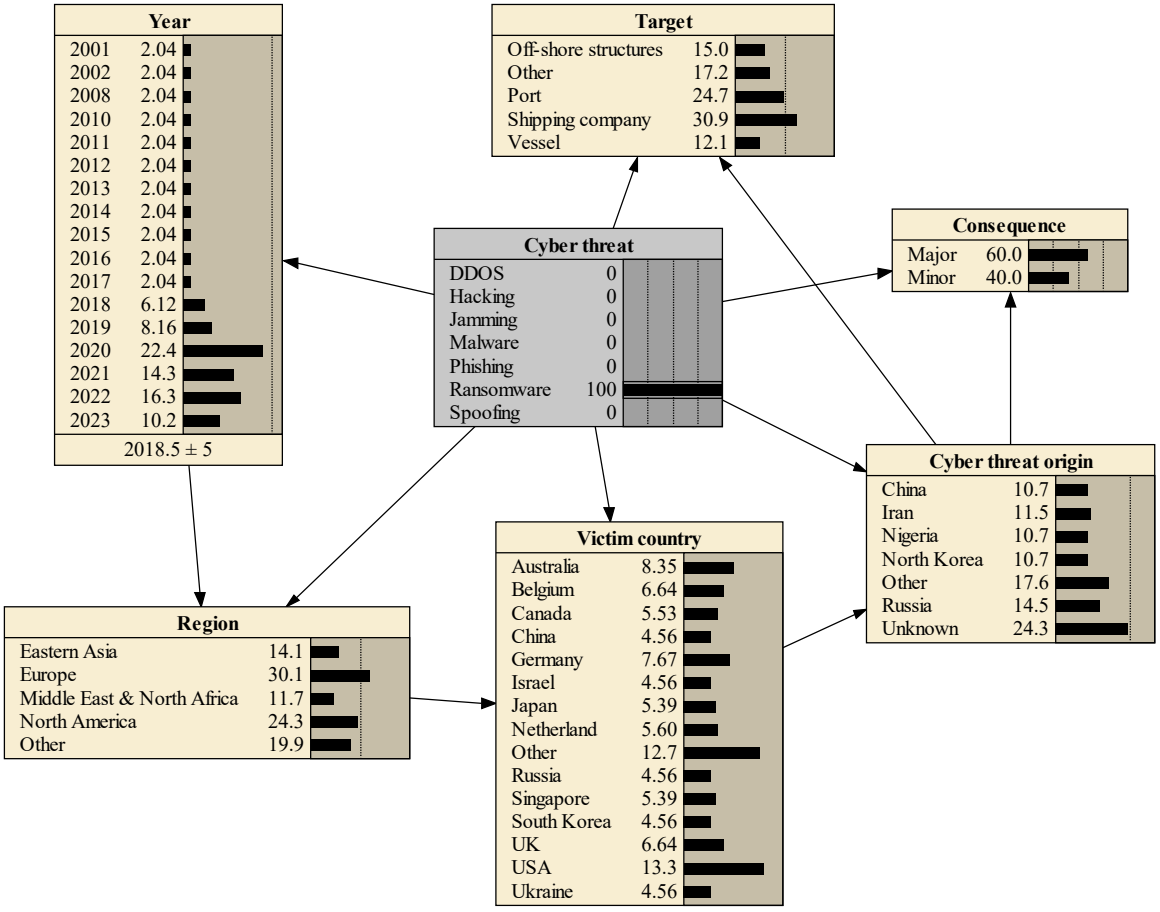

Figure 4. 5: Ransomware cyber-attack scenario.

Applying a methodology similar to the one employed for ransomware, valuable insights can be derived concerning other cyber threats. Particularly noteworthy are DDoS attacks, renowned for their disruptive impact, all meticulously documented within the realm of seaports, causing disruptions to their regular operations. Figure 4.6 represents the corresponding values for different SRIFs when the DDoS cyber-attack is set as 100 percent. Notably, the majority of these attacks have been directed at U.S. seaports, with a discernible origin traced back to Russia. Examining the timeline, a significant surge in DDoS attacks has been observed in 2023, underscoring the critical nature of the situation during this period.

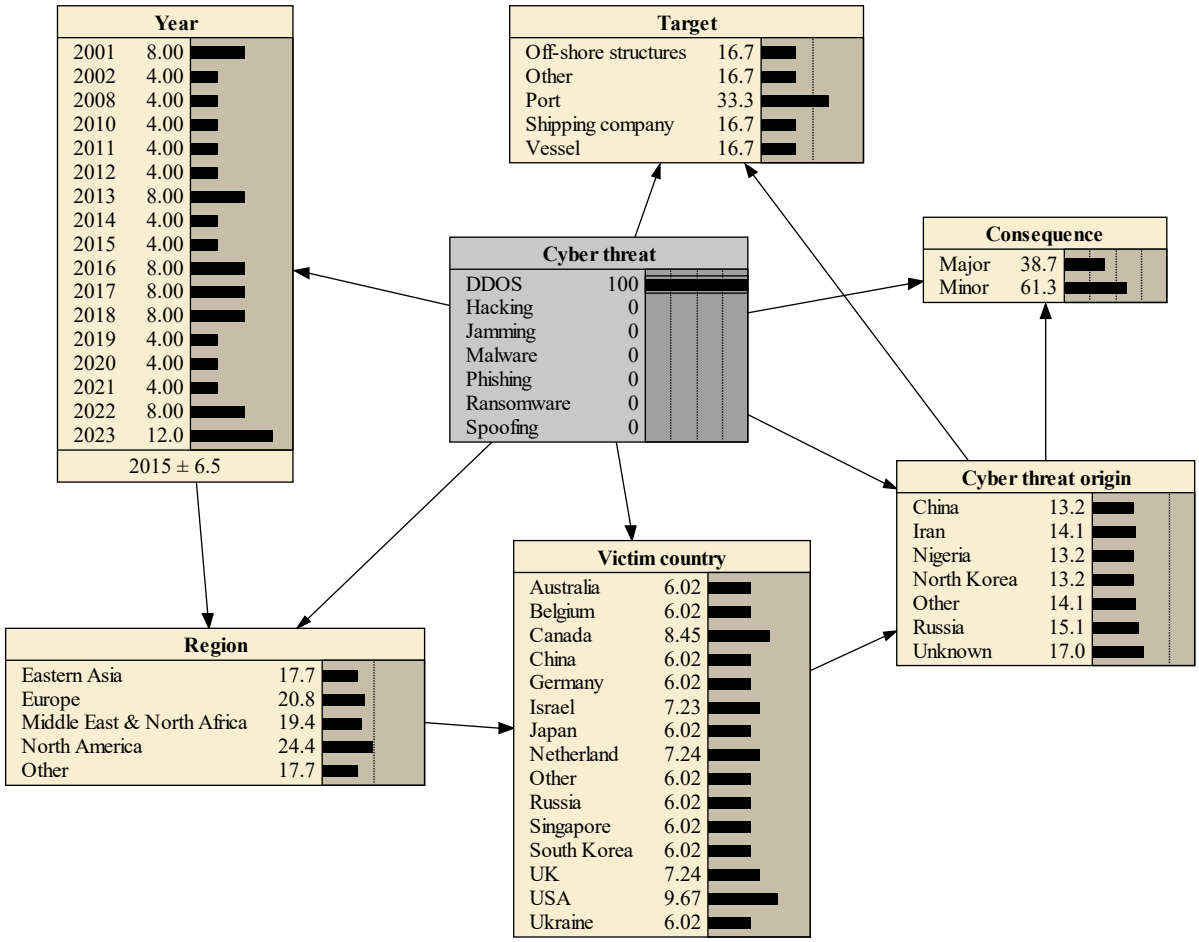

Figure 4. 6: DDoS cyber-attack scenario.

The patterns observed in hacking, malware, and phishing incidents exhibit striking similarities concerning their targets and consequences. However, when viewed through a temporal lens, hacking records appear to be distributed relatively evenly over the past five years. In contrast, malware incidents reached their peak in 2019, and phishing incidents were most pronounced in 2017. In terms of spatial distribution, Eastern Asia emerges as a focal point for malware and phishing activities, collectively accounting for one-third and one-fourth of all incidents worldwide, respectively. This geographical concentration underscores the significance of Eastern Asia in the prevalence of these cyber threats on a global scale.

When considering cyber-attacks such as jamming and spoofing that specifically target vessels, two prominent countries, namely North Korea and Russia, have been identified as leading actors in deploying these tactics against maritime targets. The prevalence of jamming incidents has notably affected the majority of South Korean vessels, consequently establishing Eastern Asia as the region with the highest frequency of jamming events from a geographical standpoint. Spoofing, characterized as a more sophisticated form of jamming, has witnessed prevalent usage, particularly in European seas, over the past five years. Russia, in particular, is acknowledged as a trailblazer in employing spoofing attacks against vessels in these maritime regions.

4.6.1.2 Top cyber SRIFs

Taking into account the findings presented in Table 4.8, the top cyber SRIFs, ranked according to their TRI values, are identified as the year, victim country, and target. Identifying the "year" as the foremost influential factor in cyber SRIFs highlights the importance of considering the temporal dimension when assessing cyber threat trends in the maritime domain. Over the last five years, nearly 60% of recorded cyber-attacks have exhibited a significant surge, peaking in 2020 and 2021. This pattern indicates a consistent upward trend. In contrast, attacks from the years preceding 2016 contribute only 15% to the overall recorded incidents. Given this pattern, the primary explanation that arises is the technological advancement, the increasing digitization of systems, and the substantial reliance of the maritime sector on network-based communications and applications. The evolution in technology broadens the potential targets and expands the attack surface for cybercriminals to take advantage of vulnerabilities. Emerging digital systems may not possess sufficient cybersecurity protections when compared to traditional analogue or manual operations. Another factor to consider is the evolving tactics, techniques, and procedures employed by cyber-attackers over time. They continually refine their approaches to circumvent security measures, with methods becoming more sophisticated as defences strengthen. Additionally, there is an increased collaboration among cybercriminals, who have established their own networks to exchange information, knowledge, and experience, facilitating the execution of cyberattacks. Furthermore, the accessibility and ease of use of hacking tools online have reduced the resources required for cyberattacks, enabling even less skilled attackers to target maritime infrastructure. From a different perspective, the response time of regulations and the industry lags behind the pace of evolving cyber threats. The emergence of new cyber threats often precedes the establishment of new regulations or industry best practices to address them, providing attackers with a window of opportunity. To further analyse the dependence of specific years and types of cyberattacks, Figure 4.7 illustrates the distribution of various cyberattacks in the maritime industry from 2016 to 2023. The evolving trend in maritime cyber threats is evident, with different attack types peaking at different times. Significant increases in specific attack types underscore the dynamic nature of these threats and highlight the need for adaptive and robust cybersecurity measures in the maritime industry.
In 2016, jamming attacks reached an extremely high percentage, nearly 70%, significantly higher than any other type of attack that year. This suggests a specific vulnerability or focus on jamming attacks in the maritime sector during this period. Conversely, the more sophisticated version of jamming, known as spoofing, shows an increasing trend in subsequent years, reaching its peak in 2021. In 2017, phishing incidents saw a substantial increase, accounting for nearly 50% of the reported cases. This highlights a shift or escalation in targeting individuals within the maritime industry during this year. However, the number of phishing incidents began to decrease in the following years, which can be attributed to improved cybersecurity training and increased awareness of these types of threats among individuals in the industry. As seen over the past few years, ransomware attacks have gained popularity among cyber attackers, spiking dramatically in 2020 and accounting for almost 60% of all cyber incidents. Despite moderate fluctuations, ransomware has continued to be the most frequent cyber threat up to the present. This marks ransomware as the dominant threat in the maritime sector, likely reflecting broader global trends in cybercrime where ransomware has become increasingly prevalent. For the other types of cyber threats, the trend has followed an oscillating pattern over the years, indicating a consistent underlying threat. Overall, scrutinizing the temporal dimension of cyber threats highlights the importance of historical

data in understanding and predicting future threats. This emphasizes the necessity of continuous monitoring and regular updates to cybersecurity strategies to effectively address the most pressing vulnerabilities. Furthermore, "year" has been an important influential factor in other maritime security studies such as maritime terrorism risk analysis (Mohsendokht et al., 2024) and cargo theft from freight supply chains (Liang et al., 2022).

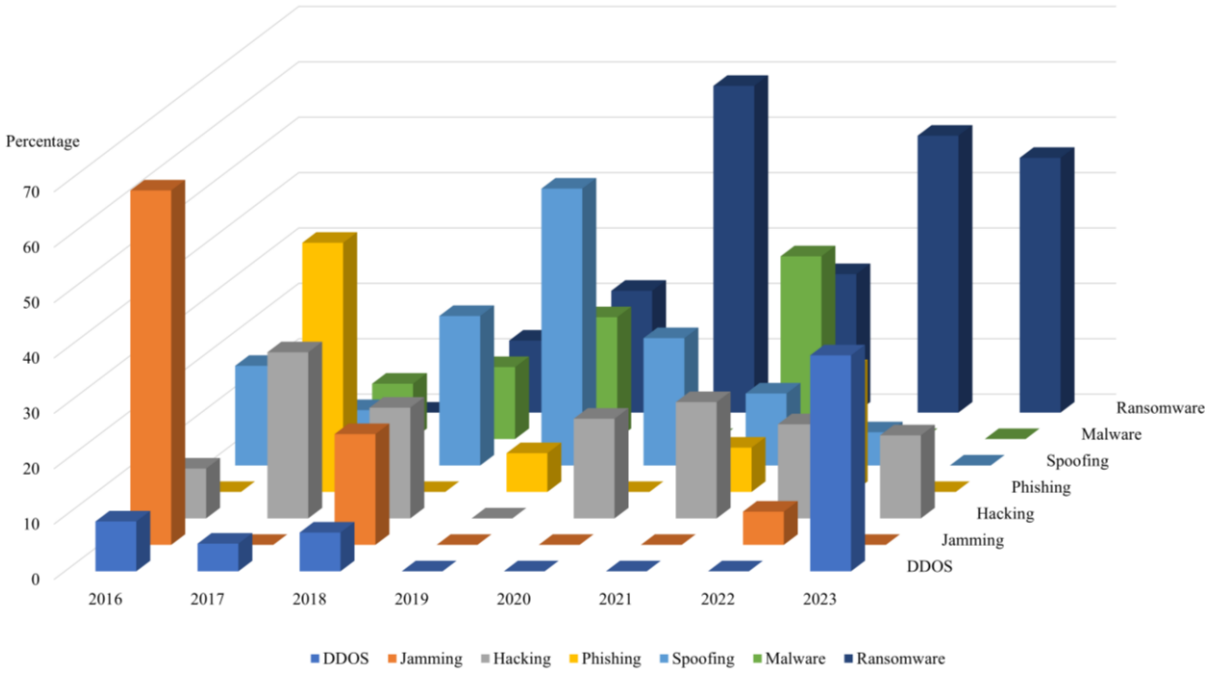

Figure 4. 7: The distribution of cyberattacks over the past 8 years.

The recognition of “country” as the second most significant SRIF underscores the crucial role of national and governmental readiness in dealing with cyber-attacks. Unlike physical terrorist attacks, which are often prevalent in developing countries or regions facing political or economic instability, cyber-attacks are predominantly observed in developed nations, with the USA having the highest number of recorded incidents. This observation can be understood from different angles. Firstly, it relates to the widespread use of advanced, high-tech digital systems across various sectors of the maritime industry, such as seaports, shipping companies, offshore structures, and transportation vessels. These technological advancements are typically more prevalent in developed countries, rendering them more susceptible to cyber-attacks. Secondly, the nature of cyber-attacks is characterized by the absence of geographical constraints. This means that an attacker from any part of the world can pose a threat to the infrastructure of a victim country, regardless of the distance between them. Thirdly, when considering ransomware as the most prevalent form of cyber-attacks, the wealth of developed countries renders them attractive targets for such incidents, serving as a means of fundraising for cybercriminals. The financial resources and economic strength of these developed nations make them tempting targets for malicious actors seeking monetary gains through cyber extortion. This highlights the need for advanced preparedness measures at a national and governmental level to address cyber threats effectively.

The third cyber SRIF is linked to the nature of the target. Through the data-driven approach, five distinct maritime targets have been identified as susceptible to cyber-attacks, including

ports, shipping companies, vessels, offshore structures and others. Among these, shipping companies, encompassing various businesses involved in the global supply chain, emerge as the primary focus of cyber threats, followed by ports as the main hub for maritime transportation. This heightened susceptibility can be attributed to several key factors. Firstly, these entities are pivotal strategic assets that hold a central role in the global supply chain, rendering them attractive targets for cyber attackers aiming to disrupt international trade and commerce. Secondly, the complex operations within shipping companies and ports, involving a multitude of stakeholders, diverse cargo types, and complex logistics, create an environment with increased opportunities for cyber vulnerabilities. Additionally, the extensive scale of operations in shipping and port activities contributes to a broader attack surface, making them more vulnerable to cyber threats compared to smaller maritime structures. Furthermore, the nature of sensitive information handled by shipping companies and ports, encompassing details about cargo, routes, and logistics, adds to their attractiveness as targets. This valuable data can be exploited by cyber attackers for financial gain, operational disruption, or ransom demands, a trend substantiated by the prevalence of frequent ransomware cyber-attacks in this sector. This emphasizes the urgent need for stakeholders, governments, and decision-makers to redirect their focus towards the vulnerable sectors of the maritime industry and allocate sufficient resources to fortify them against potential cyber-attacks. It is imperative to implement proactive measures and robust cybersecurity strategies to safeguard the critical functions of shipping companies and ports, thereby ensuring the resilience and security of the global supply chain.

4.6.1.3 Comparative examination of research findings

In this section, a succinct comparison between the current research outcomes and those of various relevant studies in the domain is conducted. The aim is to underscore the commonalities, distinctions, and comprehensiveness of each study, thereby accentuating the significance of our work. For this purpose, seven recent journal papers centred on cybersecurity risk assessment are selected. These papers have developed quantitative frameworks that yield comparable result categories. The categories encompass various aspects, including distinct cyber-attack types, data classifications, diverse types of SRIFs, targets, application domains, prioritization of cybersecurity factors, analysis of SRIF interdependencies, and implications within the domain, as delineated in Table 4.9. As evident, the present study offers a more comprehensive perspective on the aforementioned categories, providing a more realistic depiction of results attributed to its reliance on objective data for analysis.

Table 4. 9: Research findings and outcomes comparison.

Literature	*(Gunes et al., 2021)*	*(Uflaz et al., 2024)*	*(Tam and Jones, 2019)*	*(Park et al., 2023)*	*(Svilicic et al., 2019)*	*(Yoo and Park, 2021)*	*(Schauer et al., 2019)*	Current study
Cyber-attacks	B, D	A, B, C, D, G	A, B, C, G	A, B, D, E,	NP	NP	A, B, E, F	A-G
Type of data	Subjective	Subjective	Subjective	Subjective	Subjective	Subjective	Subjective	Objective
SRIF	4, 5, 6, 9, 10, 11	4, 5, 6, 9, 11	3, 4, 5, 6, 7, 9, 11	5, 9, 10, 11	4, 5, 6, 9, 10, 11	4, 6, 10, 11	3, 4, 5, 6, 7, 9, 10, 11	1-9
Target	SP	VS	VS	GN	VS	VS	GN	SP, SC, VS, OS,

								ED, SB, MO
Domain	Specific	General	General	General	Specific	General	General	Global
Importance ranking	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Interdependency analysis	No	No	No	No	No	No	No	Yes
Implications	Technical	Technical	Technical	Technical, organizational	Technical	Technical, organizational	Technical, organizational	Technical, organizational
Cyber-attacks: (A: DDOS; B: Hacking; C: Jamming; D: Malware; E: Phishing; F: Ransomware; G: Spoofing; NP: No particular attack)								
Target: (SP: Seaport; SC: Shipping company; VS: vessel; OS: Off-shore structures; ED: Energy distributers; SB: Shipbuilding firms; MO: Managerial organization; GN: General)								
SRIF: (1. Region; 2. Country; 3. Perpetrator; 4. Scenario; 5. Cyber-attack type; 6. Target; 7. Successful attack; 8. Temporal trend; 9. Consequence; 10. Prevention ability; 11. Security risk level								
Domain: (Specific: Focusing on a case study; General: No particular case study; Global: applicable in a global scale)								

4.6.2 Implications

The implications derived from the study's findings are discussed across technical and organizational perspectives.

From a technical standpoint, considering the widespread occurrence of ransomware, it is crucial for maritime stakeholders, particularly shipping companies and seaports, to prioritize robust cybersecurity measures to safeguard against ransomware attacks. To achieve this, effective measures include implementing routine backups, utilizing network segmentation, ensuring offline storage, and providing employee training. In the context of DDoS attacks, investments in scalable infrastructure, anomaly detection systems, and collaboration with internet service providers can help mitigate their impact (De Neira et al., 2023). Generally, maintaining up-to-date software and deploying real-time threat monitoring systems utilizing AI for detecting unusual network activities, indicative of a cyber-attack, enables prompt action and enhances the defensive capabilities of the target (Caprolu et al., 2020) (Boudehenn et al., 2021) (Laso et al., 2022) (Freire et al., 2022). In dealing with cyber threats such as hacking, phishing, and malware, mitigating risks involves conducting regular security audits and employing robust security measures like strong passwords and multi-factor authentication. It is essential for shipping companies and ports to stay vigilant by keeping anti-virus software up-to-date and offering training on identifying phishing attempts. Additionally, implementing mechanisms such as email filtering and validation can enhance the ability to identify and block phishing attempts (BIMCO, 2018). To safeguard against the risks of jamming and spoofing, vessels should adopt precautionary measures, including the formulation of contingency communication plans and adherence to best practices concerning navigational systems. Specifically, it is advisable to incorporate GPS signal authentication mechanisms to counteract potential jamming and spoofing attacks. Additionally, enhancing the security of vessel communication systems can be achieved through the implementation of advanced encryption protocols. To proactively address cyber threats, vessels are encouraged to deploy intrusion detection systems that can identify and respond to potential security breaches (Kessler et al., 2018) (Struck and Stoppe, 2021).

From an organizational standpoint, it is worth considering some useful insights drawn from this study. Examining the experiences of comparable industries, adopting and integrating a comprehensive cybersecurity framework tailored to maritime operations, such as the C2M2

and CSF frameworks (Gourisetti et al., 2020), which encompass identification, protection, detection, response, and recovery, appears advantageous. Given the prevalence of diverse cyber threats across various regions, sharing threat intelligence and implementing region-specific cybersecurity measures help enhance the overall resilience of the maritime industry (Meland et al., 2021). Collaborating with cybersecurity experts to develop and implement comprehensive cybersecurity policies and incident response plans is also advisable. Additionally, recognizing the geopolitical implications of cyber threats and advocating for international cooperation to strengthen global cybersecurity resilience is essential. Within this framework, fostering international collaboration, sharing information, and conducting joint exercises to address the transnational nature of cyber threats in the maritime domain can be effectively achieved. It is clear that there are still lessons to be gleaned from each incident. Given the limited history of maritime cyber threats and the tendency of some sectors to avoid reporting cyber-attacks to preserve their image and reputation, establishing clear and accessible channels for reporting cyber incidents is crucial to cultivate a culture of transparency and prompt response. This necessitates bolstering international partnerships to exchange intelligence on threats and cooperate on strategies to mitigate cyber threats (Al Ali et al., 2021). In pursuit of this goal, backing cybersecurity education at the national level to improve the overall security stance of the maritime sector, and offering regular cybersecurity training for all personnel, along with ensuring employees are proficient in identifying signs of attacks, must all be enacted from an organizational standpoint (Ahvenjärvi et al., 2019).

Looking at the various technical and organizational measures outlined above, it is clear that successfully tackling cyber threats in the maritime sector necessitates a comprehensive approach covering both technological and institutional angles. A multifaceted cybersecurity strategy that integrates robust technical safeguards along with organizational policies and procedures is vital for building a resilient defence system capable of withstanding the complex and rapidly advancing cyber threat landscape. No single solution can fully address the issue, but rather a combination of technical defences and organizational processes working in tandem will be key to effectively counteracting cyberattacks targeting the maritime industry.

In summary, the current study pioneered the use of micro-level risk factors to quantify maritime cybersecurity risk levels, accurately reflecting real-world threats. By employing a data-driven analysis, it captured intricate dependencies and enabled quantitative analysis, enhancing statistical inference and model validation. The adaptable model, validated through various techniques, demonstrated efficacy and offered valuable insights, making it highly applicable in predicting and mitigating cybersecurity risks.

4.7 Conclusion

This study introduces an innovative approach to assessing cybersecurity risks in maritime infrastructures, including offshore structures, seaports, shipping companies, and vessels. By conducting a thorough literature review and utilizing real data, based on the open-source MCAD database, which documents incidents of cyber threats in the maritime domain, the key SRIFs are identified, and a distinct data-driven BN model is constructed. The model assists in successfully analysing the potential cybersecurity risks posed to different sectors of the maritime industry. The validation of the developed model involves employing a diverse set of techniques, including comparative, data splitting, metric and sensitivity analyses. The

outcomes of these analyses affirm the model's strong robustness and reliability. In the examination of the cybersecurity model, ransomware emerges as the most prevalent form of cyber-attacks in stationary maritime infrastructures, followed by hacking, malware, phishing, and DDOS. For vessels, the predominant cyber threats consist of spoofing and jamming, in that order. Moreover, it becomes evident that three significant SRIFs, specifically year, country, and target exert substantial influence on the target node. Based on the results, it can be concluded that developed nations, while potentially spared from physical terrorist attacks, face cybersecurity threats that jeopardize their maritime infrastructures, especially shipping companies and seaports. The findings of the study provide valuable insights for stakeholders and government entities, contributing to a better comprehension of cybersecurity issues concerning various elements of the maritime industry. This knowledge has the potential to fortify preventive measures and improve emergency management strategies. Furthermore, the study highlights the necessity for additional exploration within maritime cybersecurity, outlining potential avenues for future research and indicating the limitations within existing studies. However, it is to be noted that the current study's limitation lies in its reliance on a relatively modest list of the recorded maritime cyber incidents in the most comprehensive database in the field so far, which might not encompass all possible attack scenarios. To enhance the recognition and management of cyber threats in this sector, it is crucial to keep updating the database and consider integrating expert judgment, data-driven analysis, and insights from other relevant fields in future.

Chapter 5 : Systemic risk analysis based on Safety-II concept

5.1 Summary

This chapter presents a comprehensive and integrated framework for systemic risk analysis in seaports, developed under the Safety-II paradigm. Recognizing that safety constitutes a fundamental dimension of resilience, the chapter redefines safety not merely as the absence of failures but as the system's ability to function effectively under varying conditions. This shift toward a resilience-oriented understanding of safety enables the analysis of how normal performance variability can both sustain and challenge the overall functioning of maritime systems.

The proposed framework combines the Functional Resonance Analysis Method (FRAM) with Bayesian Networks, supported by a suite of advanced analytical tools, including Monte Carlo simulation, probabilistic and statistical modelling, evidential reasoning, Dempster-Shafer theory, and the CREAM methodology. This hybrid integration bridges the qualitative strengths of FRAM with the quantitative rigor of Bayesian inference. The approach allows for the assessment of technological, human, and organizational elements both individually and in interaction, tracing upstream–downstream dependencies and emergent systemic effects within complex seaport operations.

Through this framework, performance variabilities are quantified and propagated across interconnected functions, enabling both retrospective (diagnostic) and prospective (predictive) risk analyses. The model facilitates risk-based decision-making by identifying critical functions, prioritizing interventions, and supporting the design of targeted mitigation measures. Demonstrated through a case study encompassing key operational activities from berth assignment and mooring to container unloading on the yard side, the framework proves effective in addressing the intricate, nonlinear, and interdependent nature of seaport systems.

Ultimately, this chapter extends the Safety-II concept into a quantifiable, resilience-based methodology, offering a unified perspective that strengthens the understanding of systemic safety, enhances risk quantification, and supports the development of adaptive and proactive management strategies for complex maritime infrastructures such as seaports.

5.2 Introduction

Complex Socio-Technical Systems (CSTS) are defined by tightly interconnected structures, unpredictable workflows, non-linear operations, and intricate interactions among their elements. These systems encompass the interplay of human, technological, and environmental factors within an organizational context *(Baxter and Sommerville, 2011; Bayramova et al., 2023; Jensen and Aven, 2018)*. Traditional risk analysis methods, including fault tree analysis, event tree analysis, and probabilistic safety assessment, are primarily grounded in the Safety-I paradigm. This approach operates on several foundational assumptions: systems can be decomposed into simpler components; their functioning is categorized as either successful or failed; risk analysis depends on predefined cause-and-effect relationships; and event sequences are assumed to be linear. While this methodology proved effective for purely technological systems and was widely applied in critical industries such as chemical, nuclear, and aviation during the 20th century, its limitations became apparent when dealing with CSTS *(Aven, 2022)*.

Safety-I philosophy, rooted in traditional thinking, struggles to accommodate the dynamic, nonlinear, and emergent nature of modern systems, making its continued application in the 21st century increasingly questionable *(Hollnagel et al., 2015)*. To address these limitations, a new paradigm known as Safety-II has emerged. Rather than focusing solely on the prevention of failures, Safety-II emphasizes ensuring that "as many things as possible go right." This approach adopts a proactive stance, recognizing the adaptability of human operators and underscoring the importance of monitoring everyday performance variability as a means of sustaining system safety.

Over the past decade, this paradigm has sparked extensive discussion among researchers, who have both supported and critiqued its underlying philosophy, a detailed exploration of which lies beyond the scope of this study *(Aven, 2022; Cooper, 2022; Hollnagel, 2018; Martinetti et al., 2019; Provan et al., 2020)*. However, the research trend indicates that Safety-II concept has gained significant traction, with scholars from various disciplines incorporating it into their studies. Applications span diverse fields, including maritime operations *(Adhita et al., 2023; Qiao et al., 2021; Wahl et al., 2020)*, energy systems *(Riemersma et al., 2024)*, aviation *(Yang et al., 2017)*, chemical industry *(Yu et al., 2020)*, construction *(Martinetti et al., 2019; Martins et al., 2022)*, transportation *(Papadimitriou et al., 2022; Wang et al., 2020)*, and nuclear power plants *(Ham and Park, 2020; Park et al., 2018)*.

A common critique of these studies is the lack of a systematic approach to enhancing safety performance while integrating both qualitative and quantitative methods. Nonetheless, efforts have been made to introduce techniques for systemic risk analysis, including the Function Analysis System Technique (FAST) *(Bytheway, 2007)*, the Structured Analysis and Design Technique (SADT) *(Ahmed et al., 2014)*, the Systematic Human Error Reduction and Prediction Approach (SHERPA) *(Stanton, 2004)*, the Accident Causation Analysis and Taxonomy (ACAT) *(Li et al., 2017)*, the Systems Theoretic Accident Model and Processes (STAMP) *(Ceylan et al., 2021)*, and the FRAM.

Among these techniques, FRAM has gained significant popularity for systemic risk analysis in CSTS due to several compelling advantages. Unlike traditional methods, FRAM avoids decomposing systems into individual components and operates independently of cause-effect analysis, aligning seamlessly with the principles of Safety-II paradigm. Furthermore, it identifies the various elements of a CSTS (Human, technological, and organizational factors) and addresses each individually while accounting for their interactions and interdependencies. Additionally, FRAM enables detailed monitoring and analysis of the performance variability of each function, its influence on downstream functions, and its overall impact on the entire system.

Despite its many advantages, the FRAM remains primarily a qualitative approach, lacking the capability to provide quantitative measurements for interpreting performance variability. This limitation is widely recognized as a significant drawback. To address this issue, researchers have investigated various approaches to enhance FRAM by incorporating standardized and quantitative techniques. One of the earliest efforts in this direction was undertaken by *Rosa et al. (2015)*, who combined FRAM with the Analytical Hierarchy Process (AHP) to generate numerical rankings. *Patriarca et al. (2017)* introduced an innovative semi-quantitative FRAM-based approach by integrating it with Monte Carlo simulations (MSC), enabling the representation of performance variability as discrete probability distributions. The integration of fuzzy logic theory with FRAM has also been proposed in multiple studies, offering another pathway to quantification *(Hirose and Sawaragi, 2020, 2019; Slim and Nadeau, 2020)*. In their

work, *Lee and Chung (2018)* developed a method to quantify Human-System Interaction (HSI) variability and assess criticality using a semi-quantitative FRAM process.

More advanced techniques have emerged in recent years, including the integration of machine learning and data-driven approaches with FRAM, which have been applied across various domains. BNs have also been explored as a powerful probabilistic tool for quantifying FRAM. For instance, *Zarei et al. (2022)* developed a causation model based on FRAM, which they incorporated into a dynamic BN to analyse internal and external performance variability, referred to as uncoupled variability, within the petrochemical industry. In maritime operations, *Guo et al. (2023)* proposed a similar approach, further enhanced by embedding a Markov model to analyse the evolution of collision risk during ship pilotage. These advancements demonstrate the growing efforts to integrate qualitative and quantitative analyses in FRAM applications.

Previous studies have primarily focused on addressing the quantitative limitations of the FRAM by integrating it with BN. In these studies, FRAM is often utilized as a tool for identifying Risk Influential Factors (RIFs). However, these approaches exhibit certain limitations. Some studies prioritize the interactions between functions while overlooking the internal and external variabilities within individual functions. Conversely, others emphasize internal and external variabilities but neglect how functions interact dynamically within a system. To the best of the authors' knowledge, no comprehensive framework has been developed that systematically addresses these limitations while providing a holistic mechanism to track performance variability both within and across functions in the FRAM context.

This chapter aims to address these gaps by proposing an integrated framework for systemic risk analysis within the context of CSTS, aligning with the principles of Safety-II concept. The novel methodology integrates FRAM and BN with advanced analytical tools, including MSC, canonical probabilistic methods, statistical and mathematical modelling, evidential reasoning, Dempster-Shafer theory, criticality matrix, and the CREAM methodology. The key contributions of this study can be summarized as follows:

1) Individual analysis of CSTS elements: Each element of the CSTS, namely as technological, human, and organizational functions is independently analysed to assess their internal and external performance variabilities. These variabilities account for factors such as operational uncertainties, environmental conditions, and human performance fluctuations.

2) Interaction between functions: The interactions among related functions are systematically examined to identify and track their upstream-downstream performance variability. This includes assessing their potential impacts, including negative, damping, or even positive on the entire system. Such an analysis helps to highlight critical dependencies and emergent behaviours within the system.

3) Retrospective and prospective risk analysis: The proposed framework enables both retrospective and prospective evaluations of the performance variability. This dual perspective equips decision-makers with actionable insights to address risks effectively.

4) Support for risk-based decision-making: By quantifying and visualizing variabilities across the CSTS, the framework empowers decision-makers to prioritize interventions and implement targeted measures to manage identified risks.

The remainder of this chapter is structured as follows: Section 5.3 presents a detailed discussion of the adopted methodology, with an in-depth explanation of the various techniques employed. Section 5.4 demonstrates the application of the proposed methodology to seaport operations, including a discussion of the results and their interpretation. Finally, Section 5.5 summarizes the key insights derived from this study and concludes the chapter.

5.3 Methodology

This section proposes a novel systemic risk analysis methodology based on a hybrid approach combining FRAM and BN, representing three key elements of CSTS: technological, human, and organizational functions. FRAM is utilized to describe the complex interrelationships among various functions, while BN enables the quantitative analysis of this complexity. Figure 5.1 demonstrates the overall framework of the proposed methodology in four consecutive phases.

- Phase 1: Based on Hierarchical Task Analysis (HTA) and the principles of FRAM, the functions, associated variabilities, and couplings between functions are identified, leading to the construction of the final FRAM model.
- Phase 2: Each function is represented as either a technological, human, or organizational function. The internal variability within each function is modelled using a BN, in which the interrelationships among its internal contributing factors are defined both qualitatively and quantitatively.
- Phase 3: The conditional probability tables for the BN nodes are generated through a novel systematic approach that captures the quantitative relationships between parent and child nodes.
- Phase 4: The FRAM, serving as the primary model, is integrated with BN as a tool to represent variabilities, enabling the monitoring of interactions between functions and the detection of resonance among them.

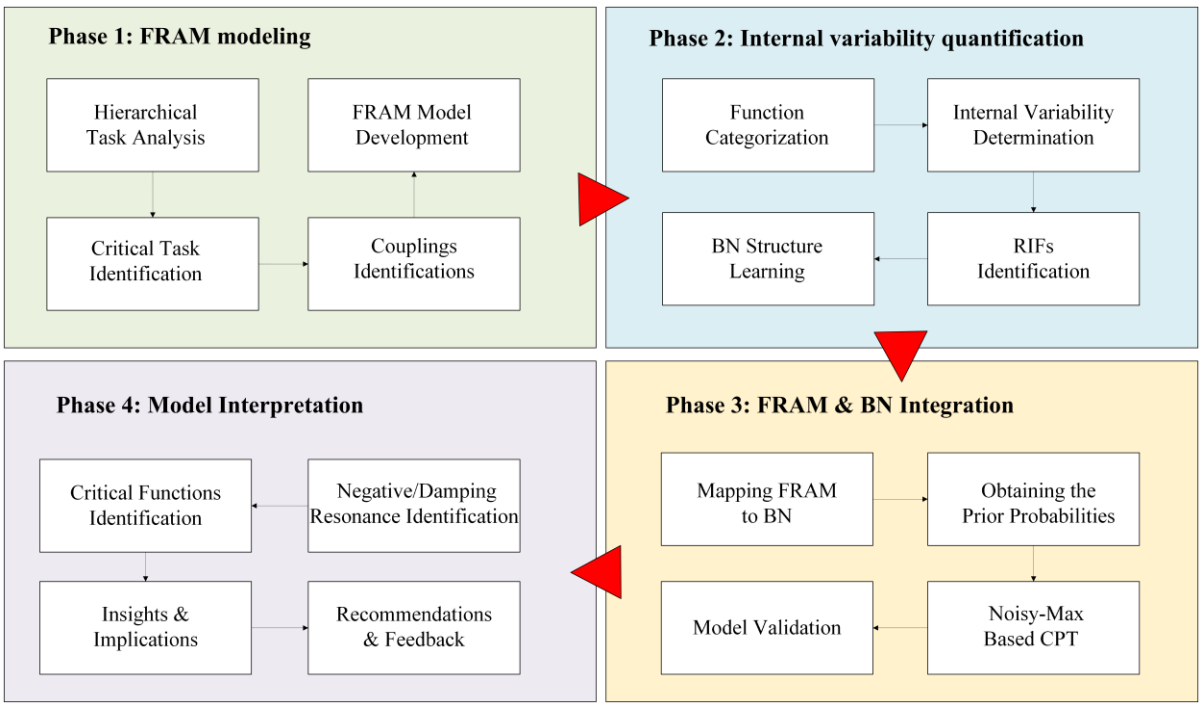

Figure 5. 1: The overall framework of the proposed methodology.

5.3.1 FRAM modelling

In the first phase, an HTA is developed to better understand the activities within the process under study and to provide a general overview of its tasks. The hierarchical structure of HTA enables detailed analysis of specific tasks and helps clarify the relationships among them. HTA has been extensively described in prior research *(Salmon et al., 2010; Stanton, 2006)*. Once the HTA is developed, key functions are identified and selected for further analysis through FRAM modelling. FRAM is employed to qualitatively analyse the effective operation of CSTS. The four main principles of FRAM can be summarized as follows *(Erik, 2017)*: First, the nature of success and failure is equivalent; in other words, everyday work variability determines whether outcomes are positive or negative. Second, individuals and organizations must make ongoing, often approximate, adjustments to adapt to changing conditions. Third, both positive and negative outcomes of a CSTS emerge from interactions among multiple system functions rather than from individual components alone, meaning outcomes cannot be traced directly to isolated causes. Fourth, functional resonance refers to the amplification of normal function variability due to unexpected interactions. It emphasizes the importance of identifying areas where such resonances may occur, as they can lead to significant system-wide consequences.

Following these principles, the FRAM model can be constructed using the steps outlined below:

1) Identification of functions: The results from the HTA inform the FRAM construction. Activities that significantly contribute to the overall process are identified as candidate functions.

2) Definition of aspects: Each function is characterized by six aspects: input, output, resource, pre-condition, control, and time.

3) Determination of couplings: By understanding the flow of information or resources within the system, links between different aspects of various functions are identified, allowing for visualization of interdependencies among functions.

4) Identification of variabilities: Function variability refers to deviations in a function's output caused by factors from internal, external, or upstream functions.

Once the FRAM structure is constructed, each function can be characterized by potential performance variabilities. In FRAM modelling, three types of variability are considered: (1) Internal variability: which originates from factors within the function itself, such as staff training levels and equipment maintenance schedules; (2) External variability: which is driven by external factors like weather conditions, geopolitical events, market demands, and security issues; (3) Upstream Variability Index (UVI), which captures the effects of interdependencies with upstream functions that affect downstream functions, such as the impact of container unloading efficiency and speed on the subsequent transport accuracy and timing to yard storage in a seaport. In this study, the first two variabilities are referred to as Self-contained Variability Index (SVI), which pertains to performance fluctuations caused by internal and external factors that do not arise from interactions between system functions.

These variabilities, interpreted as abnormal daily fluctuations, manifest in different ways, known as phenotypes, according to Erik (2017). Phenotypes may include aspects such as

timing, precision, speed, distance, force, duration, and direction. Depending on the nature of the analysis, a suitable combination of these phenotypes is chosen for FRAM analysis. In this study, timing and precision are selected to represent the performance variability of the functions. Timing represents the punctuality of activities being conducted. The output of a function may occur too early, on time, late, or in the worst case, missed, meaning it arrives too late to be useful for its intended purpose or is not produced at all (Kaya et al., 2021). Regarding precision, an output can be accurate, satisfactory, inaccurate, or, in the worst case, faulty. From a systemic perspective, performance variability arises from local adjustments made to meet performance demands and ensure the functioning of a CSTS. To conduct a meaningful analysis, it is essential to evaluate the potential variability of each function. Therefore, a unified representation of performance variability is needed, enabling an aggregated view across different types of functions. To this end, integrating these two phenotypes not only provides a unified language for describing performance variability among functions but also facilitates the interpretation of interactions between these functions. Table 5.1 presents the results of this integration using four qualitative scales: stable (ST), low variable (LV), moderately variable (MV), and highly variable (HV).

Table 5. 1: Unification of performance variability based on time and precision phenotypes.

		Time			
		Early	Timely	Delayed	Missed
Precision	Accurate	ST	ST	LV	HV
	Satisfactory	LV	LV	MV	HV
	Inaccurate	MV	MV	HV	HV
	Faulty	HV	HV	HV	HV

In this context, "ST" performance is achieved when activities are both timely and accurate, indicating no variability and reliable outcomes. It is the only case where "work as imagined" corresponds exactly to "work as done". "LV" describes situations where performance may show slight deviations but remains satisfactory, being either timely or accurate. "MV" occurs when inaccuracies or delays begin to affect performance, though it remains functional. "HV" represents significant deviation, with outputs frequently delayed, missed, or faulty, leading to unreliability and potential system disruption.

5.3.2 BN modelling

For a quantitative analysis of FRAM, using BN to represent qualitative performance variability scales in a numerical form is highly effective. This approach offers two primary advantages. First, since performance variability has four defined states, BN can seamlessly manage these multi-state conditions, accommodating the complexity introduced by numerous interacting functions within a system. Second, performance variability can be expressed as probability percentages, a task well-suited to BN's strength in handling probabilistic analysis and uncertainty. Thus, integrating BN with FRAM enables a robust approach to systemic risk analysis in CSTS, leveraging probabilistic reasoning to capture the nuanced variability and interdependencies inherent in these environments. To begin, it is essential to differentiate functions based on their inherent characteristics, categorizing them into three primary types: technological functions, human functions, and organizational functions. Each category represents a distinct aspect of the system with unique dependencies, behaviours, and potential risks. Separate BN models will be developed for each of these categories to capture the specific

interactions, uncertainties, and causal relationships within each function type, a concept referred to as SVI.

5.3.2.1 Organizational function

Organizational factors play a crucial role in system safety, either enhancing or impairing the safety performance of a CSTS. Within an organization, numerous interactions occur among various components, including staff, operators, management, structure, and culture, among others (Li et al., 2012; Pence and Mohaghegh, 2020). To explicitly account for the impact of organizational factors on system performance variability and to capture the collective nature of its constituent elements, it is essential to consider all relevant aspects across multiple dimensions. These dimensions include social factors (e.g., safety culture, level of training), structural factors (e.g., authority gradients), resources (e.g., financial), management (e.g., leadership quality), and even external factors (e.g., geopolitical influences). Furthermore, the interactions among these dimensions must also be thoroughly examined (Mohaghegh et al., 2009). Table 5.2 outlines the contributing factors of organizational functions, along with their sub-factors and corresponding descriptions, within the context of BN development. In this respect, efforts are made to define the states of each node to ensure an appropriate depth of causality in the model, while accounting for the objectives of systemic risk analysis and the multidimensional nature of organizational factors.

Table 5. 2: The identified contributing factors to the performance variability of organizational functions.

Categories	Nodes	States	Descriptions
External factors	Regulation and enforcement	Strict, moderate, lax	Refers to the laws, regulations, standards, and oversight mechanisms established by governmental or regulatory bodies that an organization is required to follow. Stricter rules generally lead to improved organizational performance in the relevant functions.
	Market conditions	Favourable, unfavourable	Refers to the various economic factors and dynamics that impact the supply and demand for goods and services within a specific market. Unfavourable market conditions can significantly influence an organization's operational decisions, strategic planning, and overall performance.
	External stakeholder relationships	Strong, average, weak	A strong relationship with external stakeholders can enhance organizational performance by fostering trust, facilitating resource access, and enabling smoother collaboration. Conversely, a weak relationship may lead to communication gaps, reduced support, and potential conflicts, leading to an increased performance variability.
	Geopolitical factors	Stable, tense	Intense geopolitical factors, such as international conflicts, trade policies, tariffs, and economic sanctions, can negatively impact organizational performance, as managing these external pressures requires complex and challenging decision-making. In stable conditions, however, the organization is relieved from such difficulties.
	Environmental factors	Favourable, unfavourable	Environmental factors, such as climate change and natural disasters, can disrupt operations, increase costs, and require investment in sustainable practices. Failure to respond, adapt, and recover effectively from these factors can damage the organization's reputation, hinder compliance, and negatively impact overall performance.
	Security factors	Secure, insecure	Security factors, including data breaches, cyber threats, and physical security risks, can compromise sensitive

			information, disrupt business continuity, and increase organizational performance variability.
Organizational Structure	Span of control	Wide, balanced, narrow	Refers to the horizontal aspect of management, i.e., how many employees are directly under the supervision of a single manager. A wider span of control means fewer managers are needed, leading to a flatter organizational structure. A narrower span of control requires more managers, leading to a taller structure. A balanced span of control indicates the appropriate number of managers.
	Communication paths	Adequate, inadequate	Communication paths refer to the adequacy and quality of communication between different levels of an organization. When communication is sufficient and effective, the organization's performance variability becomes more stable.
	Authority gradient	Steep, balanced, shallow	An authority gradient describes the hierarchy of power within an organization, influencing how freely subordinates can challenge superiors. A steep gradient discourages lower-ranking individuals from speaking up, while a balanced gradient promotes open dialogue across levels. Conversely, a shallow gradient can lead to a chaotic environment.
Organizational resources	Equipment resources	Adequate, inadequate	An adequate amount of equipment resources is essential for stable organizational performance.
	Human resources	Adequate, inadequate	An adequate number of personnel is essential for stable organizational performance.
	Financial resources	Adequate, inadequate	An adequate number of financial resources is essential for stable organizational performance.
	Information resources	Adequate, inadequate	An adequate amount of information resources is essential for stable organizational performance.
	Time resources	Adequate, inadequate	An adequate amount of time resources is critical for meeting deadlines, maintaining productivity, and ensuring efficient workflow.
Organizational management	Resource management	Efficient, moderately efficient, inefficient	Refers to the organized efforts and procedures an organization implements to allocate existing resources effectively and efficiently.
	Leadership quality	Strong, moderate, weak	Refers to the effectiveness and characteristics of leaders within an organization. Strong and high-quality leadership is crucial for setting the direction, inspiring employees, and ensuring the achievement of organizational goals.
	Communication effectiveness	Adequate, inadequate	Refers to the quality of communication within an organization and its impact on achieving stable performance. It encompasses the clarity, accuracy, and timeliness of information shared among team members. Clear communication promotes collaboration, minimizes misunderstandings, and aligns everyone with the organization's objectives, ultimately ensuring consistent performance.
	Rules & regulations implementation	Compliant, partially compliant, incompliant	Refers to the effectiveness with which an organization enforces and adheres to internal policies, standards, and external regulations governing its operations. Greater compliance with these rules and regulations leads to more stable organizational performance variability.
	Emergency management	Strong, moderate, weak	Refers to the organized efforts and procedures that an organization establishes strategies to handle emergencies by planning ahead, managing responses, and facilitating recovery efforts, including natural disasters, technological incidents, security threats, and other unexpected events that may disrupt normal operations. The stronger the emergency management, the more stable the organization's performance variability.

Organizational culture	Education/training	Adequate, inadequate	An adequate level of education and training among personnel contributes to a vibrant organizational culture.
	Information sharing	Adequate, inadequate	Refers to the process of exchanging relevant information, including data, knowledge, insights, and updates among individuals, teams, departments, or organizations. Adequate level of information sharing is crucial for overall organizational efficiency.
	Safety culture	Rich, moderate, poor	Refers to shared mindset, outlook, and priorities of employees concerning safety practices and standards within an organization. It encompasses how safety is prioritized, communicated, and practiced at all levels, from management to front-line workers. A rich safety culture fosters a proactive approach to managing risks.
	Organizational cohesion	High, moderate, low	It reflects how well employees work together toward common goals, the strength of relationships within the organization, and the overall sense of belonging and loyalty that employees feel. An organization with high level of cohesion typically experiences higher levels of productivity, and performance stability.
	Employee inclusivity	Inclusive, moderately inclusive, exclusive	Encompasses initiatives aimed at fostering an inclusive and supportive workplace where every employee feels respected, appreciated, and encouraged to actively participate. A high level of inclusivity within an organization fosters a rich organizational culture.

5.3.2.2 Technological function

Technological functions are primarily driven by machinery, equipment, or software and represent automated processes or technical operations within CSTS. These functions rely on the technical features of the system to perform specific tasks. Technological functions are typically characterized by precision, consistency, and a predictable range of variability, usually governed by design specifications, technical capabilities, or programmed protocols. To determine the SVI of this function, the contributing factors to its performance variability must first be identified. Performance variability states, designated as the child node of the BN, include ST, LV, MV, and HV. The parent nodes, representing primary influences on performance variability, can be categorized into three main groups: safety-oriented factors, material integrity factors, and operational context factors. Safety-oriented factors encompass the protocols, practices, and resources dedicated to ensuring operational safety, reliability, and performance stability. These factors reflect the effectiveness of safety management within the system and play a crucial role in building resilience to variability and failure. Key contributors include maintenance activities, inspection policies, and reliability indices. Material integrity factors represent the physical condition and degradation of materials over time, accounting for natural wear, corrosion, and age-related issues. Material integrity is essential in determining a system's ability to withstand ongoing use and environmental exposure. Key factors include equipment aging, structural degradation, wear and tear, and corrosion. Operational conditions are another key factor influencing the performance variability of technological functions. These include external conditions, such as environmental factors, that impact system operation. Stable environments offer predictability, while harsh conditions such as extreme temperatures or high humidity pose challenges that can compromise equipment functionality and increase variability. Table 5.3 presents the nodes, their respective states, and detailed descriptions.

Table 5. 3: The identified contributing factors to the performance variability of technological functions.

Categories	Nodes	States	Descriptions
Safety-oriented factors	Maintenance strategy	Preventive-oriented, balanced, corrective-oriented	A preventive-oriented maintenance strategy emphasizes proactive measures to prevent potential failures, significantly boosting reliability but at a higher cost. In contrast, a corrective-oriented strategy addresses failures only after they occur. A balanced strategy combines both approaches, optimizing reliability while distributing the budget more evenly.
	Maintenance quality	Optimal, acceptable, poor	Maintenance quality evaluates the thoroughness and technical precision of maintenance tasks. optimal maintenance quality reflects skilled execution, accuracy, attention to detail, and adherence to best practices and standards, while poor quality indicates a lack of these attributes.
	Inspection practice	Intensive, moderate, sporadic	Sporadic or inadequate inspections raise the risk of undetected degradation, whereas an intensive inspection regimen enhances the detection of potential degradation.
	Maintenance effectiveness	High, moderate, low	Maintenance effectiveness refers to how successful maintenance activities prevent or mitigate failures and ensure the reliable operation of system components. It encompasses the impact of maintenance strategies, inspection frequency, and the quality of maintenance activities on equipment performance.
	Reliability	High, moderate, low	Reliability indicates the system's likelihood to perform its function without failure, under a specified condition, and over a specified period of time.
	Redundancy	Adequate, inadequate	Redundancy adds a layer of resilience; adequate redundancy reduces the likelihood of high variability in performance.
	MTTR	Short, long	Mean Time To Repair affects downtime; longer repair times increase the risk of performance interruptions.
	Availability	High, moderate, low	Availability measures how often the system can perform its intended function, impacted by reliability, redundancy, and MTTR.
Material integrity factors	Equipment aging	New, old	Equipment aging is the gradual decline in performance and reliability due to the natural lifecycle of components. With older equipment, it is more likely to exhibit variability in performance due to accumulated wear, reduced flexibility, and potentially outdated technology.
	Structural degradation	Low, moderate, high	Structural degradation captures the overall deterioration of components or subsystems due to a combination of internal stresses, environmental conditions, and aging. High levels of structural degradation pose significant risks to the system, leading to more frequent breakdowns, reduced load-bearing capacities, and increased variability in performance.
	Wear and tear condition	Minimal, moderate, severe	Mechanical wear and tear describe the progressive degradation of parts caused by continuous usage and friction over time. it affects performance and longevity, with severe wear leading to higher failure rates.
	Corrosion	Low, moderate, high	Corrosion impacts the integrity of materials, particularly metals and surfaces exposed to harsh environments. High corrosion rates significantly compromise structural strength, increase the likelihood of unexpected failures, and lead to reduced performance reliability.
Operational context factors	Environmental conditions	Stable, variable, harsh	A stable environment features predictable and consistent conditions, with minimal fluctuations in factors like temperature, humidity, and air quality. In contrast, a harsh environment is marked by extreme or persistent stressors such as high temperatures, corrosive substances, heavy vibrations, high humidity, or dust. A variable environment exhibits moderate fluctuations in external conditions.

5.3.2.3 Human function

Human functions, within the framework of Safety-II concept, play a pivotal role as they offer the most flexibility to adapt to variability and mitigate its adverse effects on the overall system. Consequently, modelling human performance becomes a crucial component of systemic risk analysis in a CSTS. Numerous Human Reliability Analysis (HRA) methods have been developed in the literature to address this challenge (Patriarca et al., 2020). Among these, the Cognitive Reliability and Error Analysis Method (CREAM) stands out as the most suitable for this study due to the following reasons:

I. Systemic perspective: CREAM is aligned with modern systemic approaches, such as Safety-II concept, by examining both successful and erroneous human actions, rather than focusing solely on failures.
II. Versatility and applicability**:** CREAM is adaptable across various industries and contexts. It evaluates the interactions between human, technological, and organizational factors, making it an ideal tool for analysing CSTS.
III. Context-sensitive analysis**:** The methodology integrates the impact of context on human performance using Common Performance Conditions (CPCs), enabling a detailed and situational understanding of reliability.
IV. Focus on cognitive processes**:** Unlike traditional HRA methods that emphasize physical tasks, CREAM prioritizes cognitive functions such as decision-making and problem-solving, which are crucial in today's complex systems.
V. Output compatibility with performance variability**:** CREAM's output, represented by Contextual Control Modes (CCMs), aligns seamlessly with the four types of performance variability outlined in this study: ST, LV, MV, and HV.

Building on the aforementioned reasons and drawing inspiration from the work of Yang et al. (2013), this study applies a modified CREAM methodology to assess the SVI of human functions. The methodology involves several key steps:

Step 1: Define CPCs and variables: Identify and describe CPCs, their associated variables, and their effects on human performance.
Step 2: Model CPC-CCM relationships: Establish rules to model the relationships between CPCs and CCMs.
Step 3: Assign belief degrees: Allocate belief degrees to the CCMs based on the influence of CPCs.
Step 4: Develop the BN: Construct a BN model to incorporate dependencies and facilitate analysis.
Step 5: BN inference process and validation: Update and compute the posterior probabilities of target variables within the network and perform validation to ensure the accuracy and reliability of the developed methodology.

In the first step, various CPCs are described, along with their potential states and how they influence human performance reliability. The original CPCs are divided into nine categories *(Hollnagel, 1998)*. In this study, a minor modification is introduced which replaces the "time of day" CPC with "circadian rhythm and stress." This change highlights the significant impact that sleep deprivation or misalignment with natural circadian cycles can have on performance. Unlike the "time of day" classification, which is based on fixed time intervals like day and

night, the circadian rhythm considers biological phases that influence cognitive performance and alertness. This approach provides a more accurate reflection of how these factors affect human performance reliability. Table 5.4 presents the CPCs along with the associated details.

Table 5. 4: CPCs description, their states, and effects.

CPC	CPC states	Effects
1) Training and competence (TAC)	Inadequate ($S_{1,1}$)	Negative
	Adequate with limited experience ($S_{1,2}$)	Neutral
	Adequate with high experience ($S_{1,3}$)	Positive
2) Human-machine interface and operational support (HMI)	Inappropriate ($S_{2,1}$)	Negative
	Tolerable ($S_{2,2}$)	Neutral
	Adequate ($S_{2,3}$)	Neutral
	Supportive ($S_{2,4}$)	Positive
3) Availability of procedures and plans (APP)	Inappropriate ($S_{3,1}$)	Negative
	Acceptable ($S_{3,2}$)	Neutral
	Appropriate ($S_{3,3}$)	Positive
4) Conditions of working (COW)	Incompatible ($S_{4,1}$)	Negative
	Compatible ($S_{4,2}$)	Neutral
	Advantageous ($S_{4,3}$)	Positive
5) Number of goals and conflict resolution (NGC)	More than actual capacity ($S_{5,1}$)	Negative
	Matching current capacity ($S_{5,2}$)	Neutral
	Fewer than actual capacity ($S_{5,3}$)	Positive
6) Available time and time pressure (ATT)	Continuously inadequate ($S_{6,1}$)	Negative
	Temporarily inadequate ($S_{6,2}$)	Neutral
	Adequate ($S_{6,3}$)	Positive
7) Circadian rhythm and stress (CRS)	High ($S_{7,1}$)	Negative
	Moderate ($S_{7,2}$)	Neutral
	Low ($S_{7,3}$)	Positive
8) Team collaboration quality (TCQ)	Deficient ($S_{8,1}$)	Negative
	Inefficient ($S_{8,2}$)	Neutral
	Efficient ($S_{8,3}$)	Neutral
	Very efficient ($S_{8,4}$)	Positive
9) Quality and support of the organization (QSO)	Deficient ($S_{9,1}$)	Negative
	Inefficient ($S_{9,2}$)	Negative
	Efficient ($S_{9,3}$)	Neutral
	Very efficient ($S_{9,4}$)	Positive

In step 2, the relationships between CPCs and CCMs are established by defining specific rules. These rules determine how various combinations of CPCs, along with their corresponding effects, influence the assigned values of the CCMs. The CCM, which represents the context of human cognition and action, is characterized by four distinct states: “strategic,” “tactical,” “opportunistic,” and “scrambled.” These relationships are formulated as if-then rules, where the "if" component specifies different CPC combinations and their effects, and the "then" component maps these combinations to the appropriate CCM characteristics.

As an example,

R_1: IF $S_{1,1}$ AND $S_{2,1}$ AND $S_{3,1}$ AND $S_{4,1}$ AND $S_{5,1}$ AND $S_{6,1}$ AND $S_{7,1}$ AND $S_{8,1}$ AND $S_{9,1}$ THEN $\{(\beta_1,CCM_1), (\beta_2,CCM_2), (\beta_3,CCM_3), (\beta_4,CCM_4)\}$

This can be interpreted as follows:

Rule 1: If all contributing factors, namely "Training and competence," "Human-machine interface and operational support," "Availability of procedures and plans," "Conditions of working,", "Number of goals and conflict resolution," , "Available time and time pressure," , "Circadian rhythm and stress," , "Team collaboration quality," and "Quality and support of the organization" are rated negative, THEN the human performance can be attributed to a distribution over four CCM states with their proportional belief degrees (β).

In step 3, belief degrees are assigned to the consequences, or the "THEN" components of the rules, to account for uncertainty and ensure that minor variations in the "IF" components are accurately reflected in the "THEN" outcomes. To achieve this, a systematic approach is employed to determine the belief degrees by leveraging the basic control mode diagram of CREAM and a weighting system. The AHP is used to calculate the relative weights of all CPCs based on their importance. Subsequently, the conditional belief degrees, denoted as β^+ and β^-, are derived using the diagram shown in Figure 5.2. These degrees correspond to the positive or negative effects of various CPC states *(Konstandinidou et al., 2006)*.

To clarify the approach, let's consider an illustrative example. In rule number k, out of the nine CPCs, four have positive effects, three have negative effects, and two have neutral effects. Referring to the vertical axis of the diagram, which corresponds to the value four, and analysing the portions of the slots representing different CCMs, it is evident that there is one block for "strategic", five blocks for "tactical", and none for the other CCMs. Based on this, β^+ is estimated as:

$$\beta^+ = \{(0.17,CCM_1), (0.73,CCM_2), (0, CCM_3), (0,CCM_4)\}$$

Similarly, using the horizontal axis of the diagram and identifying the value three, two blocks are observed for "opportunistic", five blocks for "tactical", and none for the other CCMs. Consequently, β^- is calculated as:

$$\beta^- = \{(0,CCM_1), (0.71,CCM_2), (0.29, CCM_3), (0,CCM_4)\}$$

It should be emphasized that the "neutral" effect does not contribute to the integrated result, as it has already been accounted for in the uncertainty, and its belief degree is therefore excluded from the process.

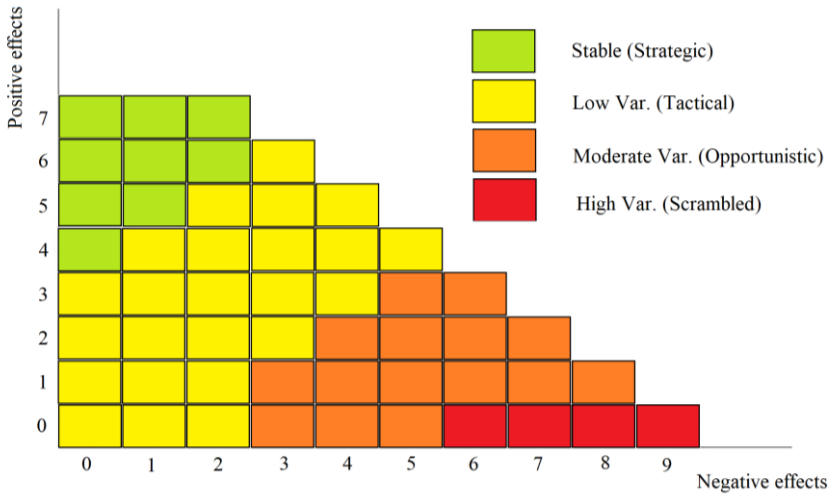

Figure 5. 2: Basic Diagram of CREAM for different CCMs.

Once the positive and negative belief degrees are determined, and the weights derived using the AHP approach are incorporated, evidential reasoning is employed to synthesize this information (Jian-Bo Yang and Dong-Ling Xu, 2002). This process delivers the final combined belief degree for each CCM.

Step 4 involves constructing a BN to model the dependencies between CPCs. While CPCs share similarities with Performance Shaping Factors (PSFs) in other HRA methods, they are not the same. Their interdependencies are based on their influence on human performance reliability. Furthermore, CPCs may be calibrated based on the states of other CPCs. For instance, if a CPC initially exhibits a neutral effect but depends on other CPCs, its primary effect may shift toward either a positive or negative influence depending on the states of the CPCs it relies on. Table 5.5 illustrates the dependencies among various CPCs. The CPCs listed in the left-hand column are influenced by those defined in the top row. For instance, examining the third column reveals that "COW," "NGC," and "ATT" depend on "HMI." This implies that if the human-machine interface and operational support improve, working conditions and the availability of time are expected to improve, as indicated by the letter "P," representing a positive influence. Conversely, the number of goals and conflict resolution tasks required of the operator are expected to decrease, as denoted by the letter "N," signifying a negative influence. The remaining cells in the table, marked with "-," indicate no dependencies between the respective CPCs.

Table 5. 5: Dependencies among CPCs.

	TAC	HMI	APP	COW	NGC	ATT	CRS	TCQ	QSO
TAC	-	-	-	-	-	-	-	-	P
HMI	-	-	-	-	-	-	-	-	P
APP	-	-	-	-	-	-	-	-	P
COW	P	P	-	-	-	P	P	-	P
NGC	-	N	N	N	-	-	-	-	-
ATT	-	P	P	P	N	-	P	P	-
CRS	-	-	-	-	-	-	-	-	-
TCQ	P	-	-	-	-	-	-	-	P
QSO	-	-	-	-	-	-	-	-	-

Considering these dependencies and the dynamic adjustability of CPCs based on the status of other related CPCs, a BN is well-suited for modelling these variabilities and interactive relationships. In this framework, the child node of the BN represents CCMs, which include the four defined states: strategic, tactical, opportunistic, and scrambled. These states align closely with the four performance variability levels commonly applied in both technological and organizational functions: ST, LV, MV, and HV, respectively. The parent nodes, representing the CPCs with their multiple states, are outlined in Table 5.4. To account for the dependencies shown in Table 5.5, four additional nodes, referred to as calibrated nodes, were introduced. These nodes capture the interactive relationships among CPCs and reflect their updated status based on changes in related CPCs. The four calibrated nodes are labelled as "calibrated COW", "calibrated TCQ", "calibrated NGC", and "calibrated ATT".

In the final step, the BN inference and validation process is carried out. This process includes determining the posterior probabilities of the target variables in the network and verifying the outcomes to confirm the precision and dependability of the suggested approach. First, observations are analysed to derive the prior probabilities for each CPC in terms of numerical variables that correspond to CPC states and their effects. Next, during the inference process, belief degrees are converted into rules, which serve as the conditional probabilities for the constructed BN. Using these transformed rules and the prior probabilities, the marginal probabilities of the leaf node states are then computed accordingly.

5.3.3 Establishment of conditional probability tables

CPTs represent the quantitative relationships between parent and child nodes. These tables can be derived through several methods, including empirical data collection, statistical analysis, expert judgment and elicitation, machine learning, data-driven techniques, simulations, and simplified models such as Noisy-OR (Mkrtchyan et al., 2016). The choice of approach depends on data availability and the specific context. In a BN, as the number of states for both parent and child nodes increase, the size of the CPT for a child node expands exponentially with respect to the number of parent nodes and their states. Let N represent the number of parent nodes, each with S possible states. The total number of unique combinations of parent states is therefore S^N. Let C be the number of states for the child node. For each unique combination of parent states, a probability distribution over the C states of the child node is required. Consequently, the total number of entries needed in the CPT is given by: $S^N \times C$. For example, if there are 5 parent nodes, each with 4 states, connected to a child node with 3 states, then the CPT would require $4^5 \times 3 = 3072$ entries to capture all possible combinations. This exponential increase highlights why CPTs can quickly grow unwieldy and computationally intensive as the number of parents and their respective states increase.

This study presents a novel technique that leverages both empirical data and expert elicitation, accounting for data uncertainty. This approach is particularly useful when empirical data is limited, and the CPT complexity makes it challenging for experts to provide accurate judgments. To address this, an algorithm is designed to populate the CPT while reducing the burden of knowledge acquisition. The process consists of five main steps:

1) Identify extremes: obtain the CPT values for the two most extreme states of the parent nodes, either through expert elicitation or empirical data.

2) Establish a scoring system: assign scores to represent different states of each parent node.

3) Develop interpolation methods: create mathematical relationships to interpolate values between the extreme cases.

4) Incorporate uncertainty: use MSC to account for uncertainty.

5) Expert verification: verify the results with experts to ensure accuracy.

In the first step, the combination of the two most extreme states of the parent nodes is used to assign values in the CPT rows. These values can be derived either from expert elicitation or empirical data. Once these values are determined, these two rows serve as anchor points, with the values in other rows falling between them. In the second step, a scoring system is established to rank combinations of various parent states, enabling the algorithm to interpolate CPT values smoothly and systematically. Each parent state is assigned a score based on its relative significance, and the cumulative score of each state combination guides the expected values for that specific row of the CPT. This system allows flexibility, as scores can be adjusted to reflect the influence or priority of certain states over others. The more critical a state is deemed, the higher the score it is assigned, allowing the model to better capture nuanced variations in the likelihoods across different state combinations.

In the next step, mathematical relationships are formulated to enable effective interpolation across different rows in the CPT. These relationships leverage the states of the child node and the corresponding scores assigned to each CPT row. Since smooth transitions between the extreme rows are desired, a linear interpolation approach is used, allowing values to change gradually across the CPT.

Rows are ranked based on their scores and segmented into specific ranges that align with the child node's states. For instance, if the child node states are High, Moderate, and Low, and the combination scores fall between 10 and 3, the following score ranges might be assigned: High (scores 10 to 8), Moderate (scores 7 to 5), and Low (scores 4 to 3).

A distinct formula is developed for each area to capture the mode of each state. This approach ensures that values do not drift toward specific child node states, resulting in realistic values for each row. For the “high area”, the mode is calculated using:

$$\hat{X}_H = min(H) + D \times (max(H) - min(H)) \tag{5.1}$$

where $\hat{X}_H$ is the mode value of the high state for the child node. Min(H) denotes the minimum observed value of the high state across the entire CPT. Max(H) indicates maximum observed value of the high state across the CPT. D is decay factor, which smooths the transition, calculated as:

$$D = \frac{Com(S) - min\ (S)}{max(S) - min\ (S)} \tag{5.2}$$

where,

Com(S): Sum of scores in a specific CPT row.

Max(S): Maximum possible score in the CPT.

Min(S): Minimum possible score in the CPT.

For the "low area", the mode is computed as:

$$\hat{X}_L = max(L) - D \times (max(L) - min(L)) \tag{5.3}$$

where,

$\hat{X}_L$: Mode value of the Low state for the child node.

Min(L): Minimum value of the Low state in the CPT.

Max(L): Maximum value of the Low state in the CPT.

And finally, for the moderate state, a balanced relationship between the high and low modes is used, with an adjustable boosting factor (K) to fine-tune the mode:

$$\hat{X}_M = K \times \frac{(\hat{X}_L + \hat{X}_H)}{2} \tag{5.4}$$

Where,

$\hat{X}_M$: Mode value of the Moderate state for the child node.

K: Boosting factor, which can be determined by experts, and is generally between 1.5 and 1.7, depending on the importance and nature of the states.

This structured approach ensures that the CPT values transition smoothly across different combinations, while allowing expert-adjusted flexibility based on the distinct roles of each state.

In the fourth step, to account for uncertainty in the initial values and capture a range of possible outcomes where inputs exhibit variability, MSC is recommended. This method addresses input variability by running numerous trials with diverse possible values, yielding a distribution of potential outcomes rather than a single expected result. This distribution provides insights into best-case, worst-case, and most likely scenarios. Consequently, the preliminary CPT values are represented using suitable probability distributions, such as uniform, normal, lognormal, Weibull, or triangular, depending on the nature of each variable (Rausand et al., 2020). For instance, a uniform distribution may be chosen if there is no strong prior belief about intermediate behaviour, whereas a normal distribution may be appropriate if intermediate values are likely to cluster around a central point. Other distributions are similarly selected based on the specific characteristics of each variable.

At the end, once final values are derived from numerous MSC trials, the appropriate values are selected and integrated into the CPT. At this stage, it is essential to confirm that each row of the CPT sums to one, ensuring probabilistic consistency. Additionally, expert review serves as the final verification step to confirm that the resulting values are realistic and, if needed, to adjust them for greater accuracy. This approach is designed to alleviate the burden on experts,

especially in cases where empirical data is limited and CPTs are too complex to construct based solely on expert judgment.

5.3.4 Prior probabilities extraction

Due to the complexity of CSTS and the diverse nature of their elements, various data sources with different origins are required to inform the developed models. For technical functions, several data types are particularly useful. Measurements from equipment sensors, operational conditions, and processes provide valuable empirical data. Operational logs detailing equipment performance and failures are essential, as are records of preventive and corrective maintenance activities, which help evaluate maintenance effectiveness. Additionally, manufacturer specifications, including reliability data such as Mean Time to Failure (MTTF), Mean Time to Repair (MTTR), and other relevant metrics, are integral to reliability assessment.

When it comes to organizational functions, obtaining realistic data can be challenging. Managers are often reluctant to critique their management practices, organizational structure, or operational efficiency due to concerns about reputation and prestige (Liu, 2021; LÜScher and Lewis, 2008). Nevertheless, valuable information can still be gathered through sources such as compliance and incident data from internal audits, human resource databases (e.g., staff turnover rates, training schedules, and role-specific data), and regulatory databases containing compliance records or industry-level performance benchmarks. Additionally, input from independent expert elicitation is a valuable resource in this context.

Assessing human performance variability requires the use of expert judgment, as databases in this area are often insufficient to meet expectations. However, the inherent subjectivity of expert judgment is frequently criticized due to potential uncertainties and gaps in knowledge. It is unreasonable to expect experts to provide precise outputs based solely on their experience, especially when different experts may offer divergent views on the same task. To address this limitation, the Dempster-Shafer evidence theory (DSET) is employed for several purposes:

a) Systematically combining diverse expert opinions to produce a unified final judgment.
b) Accounting for both epistemic and aleatory uncertainties, thanks to its unique features, such as representing and propagating degrees of belief.
c) Providing a structured framework for reasoning under uncertainty, allowing for the integration of incomplete or conflicting evidence.

This approach enhances the reliability of expert-based assessments by managing variability and uncertainty in a more systematic and robust manner.

DSET is frequently characterized as an advanced form of probability theory or an expanded interpretation of Bayesian inference. It has been widely used to extract subjective expert judgments and resolve disparities between differing viewpoints to produce an aggregated output. In this context, DSET is referred to as a theory of evidence because it focuses on the weight of evidence. Before combining information, the foundational principles of DSET must be introduced. A comprehensive explanation of DSET can be found in the literature *(Gros, 1997; Y. Tang et al., 2023)*; however, a brief introduction is provided here:

Consider a set of n mutually exclusive and exhaustive propositions, referred to in this context as the BN states, $\Omega=\{X_0, X_1,\ldots, X_n\}$. This set Ω is called the frame of discernment.

The power set, denoted 2^{Ω}, includes all possible subsets of Ω, including the empty set (∅) and Ω itself. For a frame $\Omega=\{X_0, X_1\}$, the power set is: $2^{\Omega}=\{\emptyset,\{X_0\},\{X_1\},\{X_0,X_1\}\}$. In general, for n elements in Ω, 2^n subsets are formed.

DSET comprises three vital functions: the Basic Probability Assignment (BPA), the Belief Function (BEL), and Plausibility Function (PL). BPA, denoted as m(A), assigns a mass of probability to a subset A of the frame of discernment Ω, where A∈Ω.

The following rules are applied: The mass of the empty set is always zero: m(∅)=0 and the sum of all masses over 2^{Ω} is 1, which is illustrated as $\sum_{A\in\Omega} m(A) = 1$. A is referred to as a focal element if m(A)>0 and m(A) represents the extent to which the evidence supports the proposition A.

Continuing, the BEL serves as the lower bound of the probability interval, while the PL acts as the upper bound. They are defined as follows:

$$BEL\ (X) = \sum_{P\subseteq X} \prod_{1\leq i\leq n} m_i(P_i) \tag{5.5}$$

$$PL(X) = 1 - BEL(\bar{X}) \tag{5.6}$$

where P is the proper subset of the set of interest (X), and $\bar{X}$ signifies the complement of X, indicating that the belief is governed by the principle that the total basic probability BPA must equal 1.

When multiple pieces of evidence from different sources are presented, the fusion of beliefs is determined by the combination rule of DSET as follows:

$$m(A) = m_1(A)\oplus m_2(A)\ldots m_n(A) = \frac{\sum_{B\cap C\cap\ldots Z=A} m_1(B)m_2(C)\ldots m_n(Z)}{1-K} \tag{5.7}$$

when A≠Ø, m(Ø)=0,

and where,

$$K = \sum_{B\cap C\cap\ldots Z=\emptyset} m_1(B)m_2(C)\ldots m_n(Z) \tag{5.8}$$

K represents the level of conflict between the pieces of evidence, with K=0 indicating no conflict and K=1 signifying complete contradiction between the evidence.

5.3.5 FRAM and BN integration

Once the FRAM model is developed and the internal variabilities across all function categories are obtained, the next step is to map the FRAM model into a BN to conduct a quantitative analysis of system performance variability. As previously discussed, various types of

variabilities are integral to an FRAM model, including SVI and UVI. Aggregating these variabilities across different functions is essential to gain a comprehensive understanding of performance variability within a CSTS. This aggregation represents the unified interactions between functions that are interconnected in a sequential manner within the FRAM model.

The process begins by converting various aspects of a function into discrete probability distributions, categorized into states such as ST, LV, MV, and HV. This approach enhances the representation of functional variability and serves as a common framework, simplifying the interpretation of interactions between functions (Patriarca et al., 2017). Furthermore, the internal variability identified for each function can be regarded as an additional dimension, reflecting the influence of the operational environment and current performance conditions during the function's execution (Slim and Nadeau, 2020). The mapping process begins with the output from background functions, establishing the initial performance variability distribution for downstream functions. This variability can be determined either through empirical data, if available, or expert elicitation when data is limited. To represent this as discrete probability distributions, the frequency of event occurrences may be used when empirical data is applied. For each function, all available and defined aspects are set as parent nodes in the BN model, with the output serving as the child node. This configuration enables a quantitative calculation of the interactions among different aspects of each function, resulting in an integrated performance variability distribution with consistent state definitions. Figure 5.3 demonstrates a simplified mechanism for mapping the FRAM model onto a BN, providing clearer insight into the process.

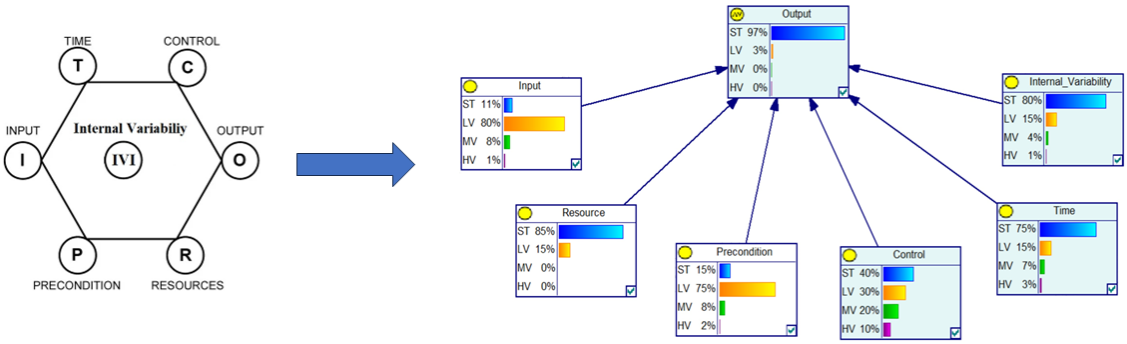

Figure 5. 3: The simplified process of mapping FRAM into a BN model.

A key advantage of BN is its flexibility in integrating a variety of nodes with multiple states, accommodating both discrete and continuous forms. Given this flexibility and recognizing performance variability across four distinct states defined by a discrete probability distribution, as well as the independence of different functional aspects and their separate impacts on the output, the CPT can be calculated using canonical probabilistic models like noisy OR, noisy MAX, noisy MIN, noisy AND, and noisy Adder gates (Diez and Druzdzel, 2006). This formulation assumes conditional independence among the contributing functional aspects, meaning that each parent factor influences the output independently of the others, with their combined effect determining the resulting state. The Noisy-OR model, introduced by Pearl (1988), initially addressed probabilistic dependencies among binary variables. Henrion (1989) extended this concept, adapting the model to include binary leaky Noisy-OR gates, which

account for additional uncertainty in influence pathways. Further developments came when Díez (1993) and Srinivas (1993) independently proposed generalizations of the model to accommodate multi-valued variables, leading to the creation of multi-valued Noisy-OR gates. These foundational works eventually paved the way for the Noisy-MAX model, which expanded the framework to capture more complex probabilistic relationships across diverse variable states. In this study, the complexity of the problem, characterized by multi-state parent nodes, a multi-state child node, and the independent influence of each parent on the child makes the Noisy-MAX technique particularly suitable. This approach not only streamlines the construction of the CPT but also effectively captures the non-linear relationships between parent and child nodes, enabling a more accurate representation of these dependencies.

5.3.5.1 Noisy-MAX structure-based BN modelling

Using the Noisy-MAX technique, the conditional probability between a child node C and its parent node R can be represented by incorporating a set of n auxiliary variables $\{A_1,\ldots,A_n\}$(Diez and Druzdzel, 2006). As illustrated in Figure 5.4, this formulation allows the conditional probability to be expressed as:

$$P(C/R) = \sum_{A} P(C/A).P(A/R) \tag{5.9}$$

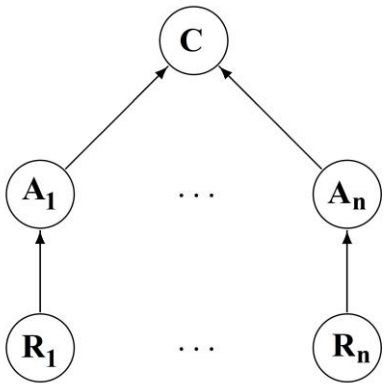

Figure 5. 4: Simplified BN structure for noisy-MAX model derivation.

Note that the variables A_i are purely auxiliary elements used to facilitate equation derivation and are not part of the actual model. Given the graph in Figure 5.4, there are no interactions between the causal mechanisms through which R_i influences the value of C. In the graph, this property is represented by the absence of connections $R_i \rightarrow A_j$ and $A_i \rightarrow A_j$ for all $i \neq j$, indicating that:

$$P(A/R) = \prod_{i} P(A_i/R_i) \tag{5.10}$$

With this, combined with Equations 9 and 10, results in:

$$P(C/R) = \sum_{A/f(A)=C} \prod_{i} P(A_i/R_i) \tag{5.11}$$

In this context, each A_i signifies the contribution of R_i to the value of C. The combined outcome generated by each R_i is represented as $C=f_{MAX(A)}$. Consequently, C and A_i variables must operate within the same domain. Each A_i reflects the impact of R_i elevating C to a particular level, and the actual value of C is determined as the maximum among the A_i values.

Now, to establish the CPT for the Noisy-MAX model, we must calculate P(C=c|A) for every possible value c and each configuration of R. This is achieved by applying Equation 5.11 and recognizing that $f_{MAX(A)}=\max(A_1,\ldots,A_n)$. This function implies that $f_{MAX(A)}\leq y$, if and only if $A_i \leq C$ for each i. Therefore, we have:

$$P(C \leq c \Big/ R) = \sum_{A/f_{MAX(A)} \leq c} \prod_{i} P(A_i/R_i) = \sum_{A_1 \leq c} \ldots \sum_{A_n \leq c} \prod_{i} P(A_i/R_i) = \prod_{i} \left(\sum_{A_i \leq c} P(A_i/R_i) \right) \tag{5.12}$$

With consideration of accumulative parameters, the values of the CPT can be obtained as follows:

$$P(c/R) = \begin{cases} P(C \leq c/R) - P(C \leq c-1/R) & for\ c \neq c_{min} \\ P(C \leq c/R) & for\ c = c_{min} \end{cases} \tag{5.13}$$

After calculating the CPTs for all BNs related to each function, using prior probabilities derived from either empirical data or expert input, the complete set of BN models is analysed to generate the final output for the last function. This analysis enables us to assess the performance variability of each function independently, as well as to evaluate its impact on downstream functions.

5.3.5.2 FRAM interpretation process

The ultimate goal of FRAM modelling is to understand how disruptions or variations in upstream functions influence the performance variability of connected functions. In essence, it examines how resonance, whether positive or negative, affects the variability in performance across downstream functions. This approach provides a detailed view of how any disruption in a CSTS can propagate, helping us understand how changes in one part of the system influence the entire system's behaviour. To this end, a 2-D criticality matrix is proposed to support the decision-making process (Kaya et al., 2021; Patriarca et al., 2018; Zarei et al., 2022). The matrix dimensions represent probability and consequence. For the probability dimension, the mean value of performance variability serves as a numerical representation of the average variability a function experiences. This considers the likelihood of being in one of four states: HV, MV, LV, or ST, multiplied by the assigned scores of 4, 3, 2, and 1, respectively. These scores reflect the significance of each state in terms of safety impact. HV is given the highest score (4) to represent substantial disruption; MV receives a moderate score (3) for moderate variability; while LV and ST are assigned lower scores (2 and 1) to indicate minimal variability or stability. For the consequence dimension, three categories are defined: critical (indicating severe consequences), moderate (manageable consequences requiring attention), and minor

(minimal or tolerable consequences). Functions are classified into these categories based on their significance to both safety and operational performance. The magnitude of consequences is highly dependent on the specific domain under study and the function's role in the system's operation and safety. This classification can be determined using expert judgment or established criteria. Figure 5.5 illustrates the proposed criticality matrix, which categorizes functions into three levels of criticality based on their variability and consequence severity.

Variability level	**Severity level**		
	Minor	Moderate	Critical
HV	B	C	C
MV	B	B	C
LV	A	B	B
ST	A	A	B

Figure 5. 5: The proposed criticality matrix.

Level C, located in the top-right quadrant, represents high variability and critical consequences. Functions in this category are prime candidates for triggering negative resonance, as their high variability combined with critical consequences makes them likely to interact unpredictably with downstream functions, potentially amplifying risks across the system. Level B, which includes functions with moderate variability, highlights that these functions can also contribute to negative resonance. This occurs particularly when their variability interacts with other moderately variable or interconnected functions, creating conditions where risks propagate through the system. Such interactions are especially critical when these functions are linked to others with similar variability characteristics. Level A encompasses functions that are relatively stable or exhibit low variability. These functions can play a stabilizing role within the system and be strategically leveraged to design interventions that dampen variability and mitigate risks. By strengthening the interactions of these stable functions, they can counteract the effects of high variability in connected functions. This criticality matrix provides a systematic tool to prioritize functions for intervention based on their role in system dynamics. It facilitates the detection and mitigation of resonances in the FRAM model by anticipating how function interactions might lead to either risk amplification (negative resonance) or system stabilization (damping resonance).

5.3.6 The model validation

Model validation is an essential component of any methodological approach, ensuring that developed models are reliable, robust, and sensible. It also builds confidence in the accuracy of the findings and results. In this study, various techniques and numerous models have been employed to address the complexity of CSTS, making comprehensive benchmarking challenging. To address this, we adopted a modular approach using a range of techniques, allowing us to validate and benchmark different models independently. Validation of the HTA and FRAM components, as qualitative analysis methods, primarily depends on the knowledge and proficiency of the analysts conducting the evaluation. Additionally, the results and findings from these models are compared and benchmarked against outcomes from similar studies.

For validating the developed BN models, sensitivity analysis, regarded as one of the most practical validation methods, is applied. This analysis involves two approaches. The first

approach confirms the model's robustness by verifying that small adjustments in the prior probabilities of parent nodes reliably affect the probabilities of child nodes. This principle-based sensitivity analysis ensures that the model responds predictably to changes in inputs, enhancing its reliability and accuracy. To achieve this, the analysis follows these principles (Jones et al., 2010):

- Principle 1: A small change in the prior probabilities of parent node states should correspond to a proportional increase or decrease in the posterior probability distribution of the child node.

- Principle 2: The total impact of variations in evidence probabilities should be at least as strong as the impact of variations in any subset of the evidence.

In the second approach, the analysis focuses on how changes in probability parameters influence the BN's output. This is done by calculating the derivatives of the posterior probability distributions, which helps reveal the sensitivity of the model's target nodes (such as performance variability) to adjustments in various numerical parameters. This derivative-based analysis measures the rate at which each target node's probability shifts in response to small modifications in the prior probabilities of parent nodes. By examining these derivatives, the parameters that most strongly influence the network's outcomes can be identified. When certain variables show high sensitivity to parameter changes, it indicates that the model depends significantly on those specific inputs. Recognizing these key parameters allows for prioritizing data that may require more precise estimates or rigorous validation, as they play a crucial role in determining the model's predictions.

5.4 Results and discussion

Seaports are widely regarded as a CSTS that are highly interconnected and interdependent, making them vulnerable to a diverse range of risks. Given that reliable and efficient seaport operations are essential for the maritime transportation sector, any disruptions or fluctuations in their performance can significantly impact national safety, security, economic stability, and public health (Mohsendokht et al., 2025). This underscores the critical need for focused attention from risk analysts to develop robust approaches to address these challenges. This section applies the proposed methodology to a typical seaport, illustrating both its practicality and potential impact.

5.4.1 HTA and FRAM development

To identify the key functions for FRAM development, an initial HTA is conducted to represent the workflow of activities typically performed in a seaport. The hierarchical structure of the HTA provides a comprehensive understanding of the workflow and facilitates a detailed analysis of specific tasks along with their prerequisite requirements. It is important to note that seaport operations involve a vast array of tasks and the collaboration of numerous teams and crews (Carlo et al., 2015; Haas, 2016). To maintain simplicity and align with the scope of a research study, a streamlined version of the HTA focusing on the most critical activities is produced. The HTA was developed by synthesizing insights from an extensive review of the seaport operations literature, the collective research contributions of the author team, and subsequent verification and approval by a panel of experts whose profiles are provided in the

Appendix, Table Ap. 2. It is worth noting that the scope of activities considered in this study is limited to those occurring between the quay side and the yard site within the seaport. Figure 5.6 presents this simplified HTA, which serves as the foundation for the FRAM model.

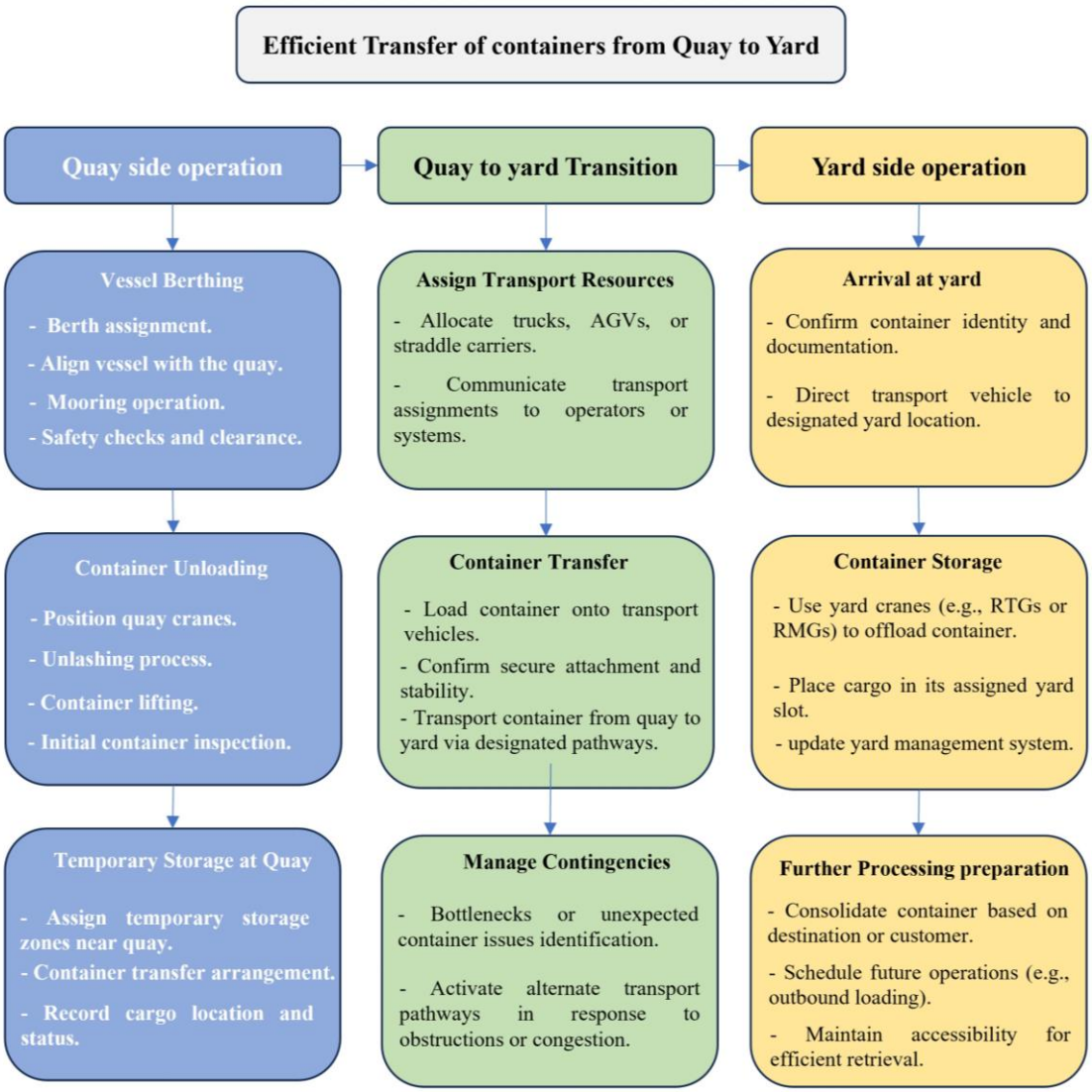

Figure 5. 6: HTA for seaport activities.

Based on the HTA results, nine foreground functions, referred to as main functions, and four background functions have been selected for the FRAM development. The background functions define the boundaries of the analysis, providing fixed outputs that feed into and support the operation of the main functions. It is important to note that the characterization and selection of functions to define the analysis context are flexible. Functions can be adjusted, updated, or revised in response to new insights, changing analytical contexts, or varying objectives of the analysis. Subsequently, the influential relationships between the functions are determined based on the defined aspects of each function. Table 5.6 outlines the functions, their characteristics, and the connections between them, while Table 5.7 details the various aspects of each function. It is not mandatory to define and provide all aspects for every function; instead, this depends on the function's nature, the analysis objectives, and the potential relationships between upstream and downstream functions. Finally, all the identified functions

and their interconnections are synthesized and visualized using the FRAM Model Visualization (FMV) tool (Hollnagel et al., 2023), as shown in Figure 5.7.

Table 5. 6: Function description, characterization, and links.

Function	Description	Type	Links
F1	Berth assignment and confirmation	Organizational	F1(O)→F2(I)
F2	Initial Safety and Security Checks	Human	F2(O)→F3(I)
F3	Unlashing of Containers	Human	F3(O)→F4(I)
F4	Cargo Unloading Preparation	Organizational	F4(O)→F5(I), F6(I)
F5	Quay crane operation	Technological	F5(O)→F7(I)
F6	Quay crane operator	Human	F6(O)→F5(C)
F7	Cargo Transport to Yard Storage	Technological	F7(O)→F8(I), F9(I)
F8	Yard crane operator	Human	F8(O)→F9(C)
F9	Yard crane operation	Technological	-
BG1	Vessel securely moored	Background function	BG1(O)→F2(P)
BG2	Port operations management	Background function	BG2(O)→F1(C), F2(C), F3(C), F7(C), F8(C), F9(C)
BG3	Berth assignment information	Background function	BG3(O)→F1(I)
BG4	Resource management	Background function	BG4(O)→ F1(R), F2(R), F3(R), F4(R), F5(R), F6(R), F7(R), F8(R), F9(R)

Table 5. 7: Functions aspects descriptions.

Function	Output	Input	Pre-condition	Control	Resource
F1	Confirmation of berth assignment	Berth assignment information	-	Port authority protocols	Communication systems, Port staff
F2	Safety and security status report	Confirmation of berth assignment	Vessel securely moored	Port security regulations	Safety and security equipment, Personnel (security officers)
F3	Unlashed containers ready for unloading	Safety and security status report	-	Unlashing protocols, Supervisor instructions	Unlashing tools, Personnel (dock workers)
F4	Instructions for crane operators, Updated cargo status	Unlashed containers	-	Port operations management, Communication from the vessel	Communication systems
F5	Cargo unloaded to dock	Updated cargo status	-	Crane operator's commands, Crane control system	Crane and fuel/power supply, Operator
F6	Crane operator's commands	Instructions for crane operators	-	-	Communication systems
F7	Cargo delivered to yard storage	Cargo unloaded to dock	-	AGV control management system	Transport vehicles (e.g., AGVs, trucks),

					Drivers and handlers
F8	Crane operator's commands	Cargo delivered to yard storage	Clear storage allocation instructions, Safety checks completed	-	Communication systems
F9	Cargo properly placed in designated storage areas	Cargo delivered to yard storage	-	Yard management system, Operator commands,	Crane and fuel/power supply, Operator

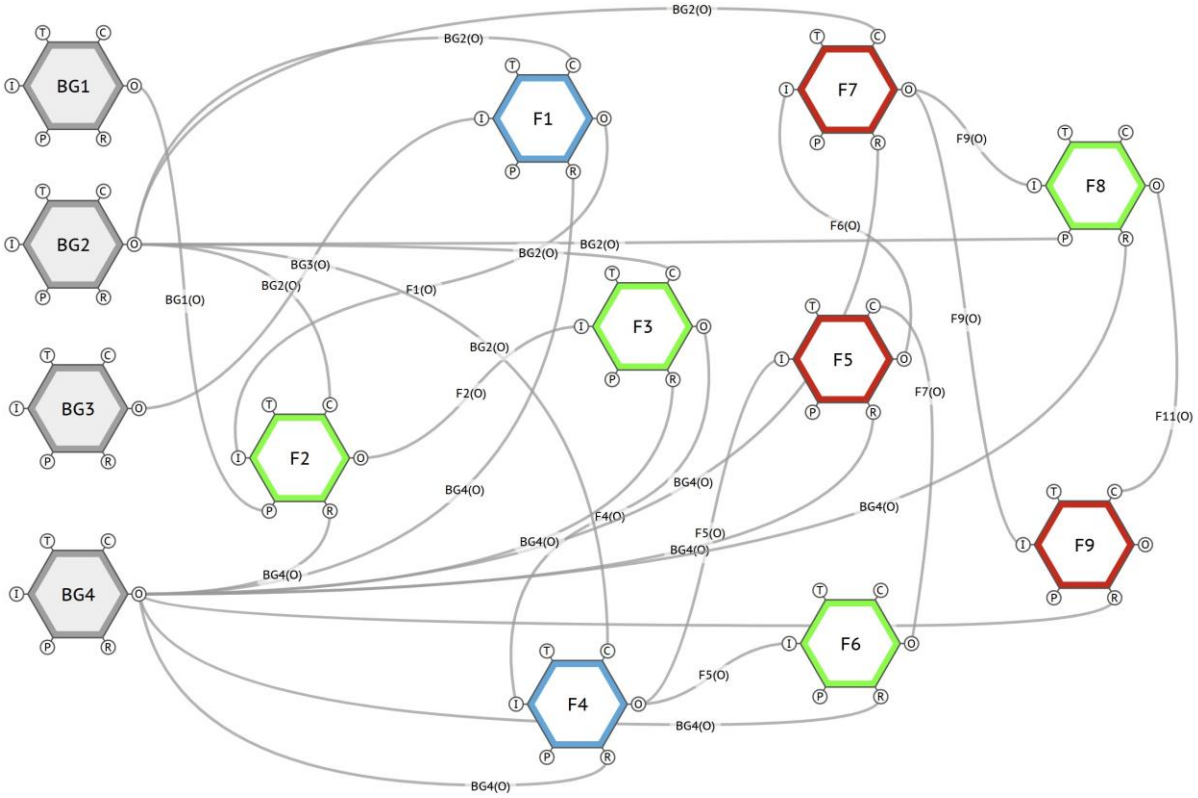

Figure 5. 7: The FRAM model of typical activities conducted in a seaport.

5.4.2 SVI assessment for key functions

5.4.2.1 Organizational functions

In the context of seaport organizational functions, numerous entities are involved, with complex interactions among their components. To assess the performance of their internal variability, a BN for the organizational function is constructed, following the information and framework described in Section 5.3.2.1. As shown in Figure 5.8, the performance variability of an organizational function is influenced by five intermediate nodes: organizational culture, organizational management, organizational resources, organizational structure, and external factors. Each of these intermediate nodes is determined by their respective parent nodes. Achieving a stable condition with a high probability requires all intermediate nodes to be in their most favourable states. This includes having a highly efficient organizational structure, sufficient and well-allocated resources, optimal organizational management practices, a rich and supportive organizational culture, and minimal impact from external factors. On the other

hand, highly variable organizational performance arises when the intermediate nodes are in their least favourable states. For instance, inefficient structure, inadequate resources, poor management, a weak organizational culture, and significant external pressures collectively lead to increased variability in performance. This relationship underscores the importance of maintaining favourable conditions across all intermediate nodes to ensure organizational stability.

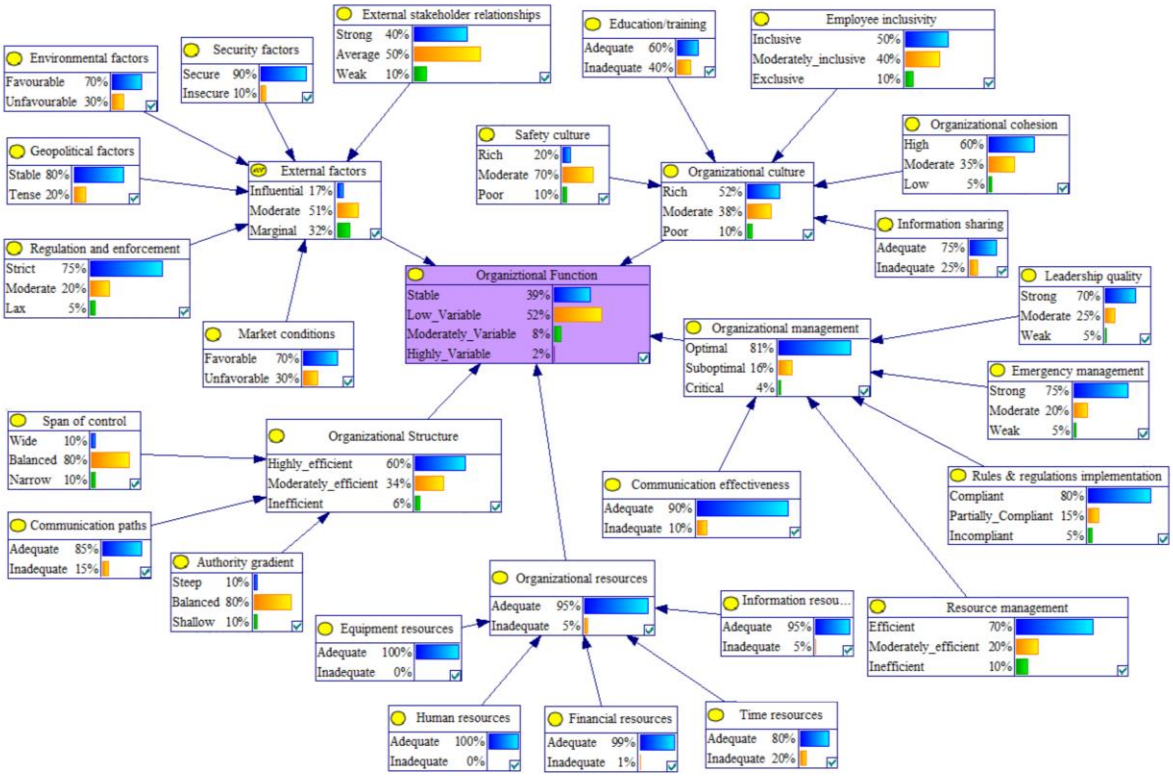

Figure 5. 8: The BN model for SVI assessment of organizational functions.

The first step in the developed BN assessment involves determining the CPT for each intermediate node and the child node. To illustrate the practical development of a CPT, the intermediate node "Organizational Culture" is used as an example. As outlined in Section 5.3.3, all possible combinations of the parent nodes' states are generated and compiled in Table 5.8. Based on the state values, a numerical score is assigned to each state. In this example, the states "Adequate" and "Inadequate" for both parent nodes, "Education/Training" and "Information Sharing," are assigned scores of 3 and 1, respectively. Similarly, for the "Safety Culture" node, the states "Rich," "Moderate," and "Poor" are scored as 3, 2, and 1, respectively. For the "Cohesion" node, scores are assigned as 3 for "High," 2 for "Moderate," and 1 for "Low." Finally, the "Inclusivity" node assigns 3 to "Inclusive," 2 to "Moderate," and 1 to "Exclusive." The seventh column of Table 5.8 sums these scores for each row, with the maximum and minimum total scores being 15 and 5, respectively. Next, the extreme cases (the first and last rows of the CPT table) are assigned corresponding probabilities. In the first row, where all parent states are at their most favourable levels, the child node ("Rich" state) is assigned the highest probability. To account for uncertainty and avoid overconfidence, a 1% probability is attributed to the "Moderate" state. A similar approach is applied to the last row, where all parent states are in their least favourable conditions, leading to a high probability for the "Poor" state in the child node. For the rows between these extremes, interpolation is used to estimate probabilities. The scores are divided into three categories: $12 \leq Rich \leq 15$, $9 \leq Moderate \leq 11$, and

5≤Poor≤8, with the corresponding equations, developed in Section 5.3.3, applied to each category. For instance, in the second row, the probability for the "Rich" state is calculated as follows:

$$D = \frac{Com(S) - min\ (S)}{max(S) - min\ (S)} = \frac{14 - 5}{15 - 5} = 0.9 \tag{5.14}$$

And,

$$\hat{X}_H = min(H) + D \times (max(H) - min(H)) = 0.01 + 0.9 \times (0.99 - 0.01) = 0.89 \tag{5.15}$$

After determining the value for the "Rich" state, the probabilities for the other states in the same row are calculated by subtracting the assigned value for "Rich" from 1 and applying a decay factor. This approach yields probabilities of 0.09 for the "Moderate" state and 0.02 for the "Poor" state. The same method is applied to the remaining rows, taking into account each row's score and the corresponding formula. In the final stage, the calculated values are treated as raw data and assigned appropriate probability distributions for MSC. This step introduces uncertainty into the data, enabling more realistic value generation. For the organizational factors in this example, all values are assigned a normal distribution *(DARMAWAN, 2024)*. Using XLRisk, an Excel add-in, MSCs are conducted by performing 100,000 iterations to refine and finalize the CPT values, as presented in Table 5.8.

Table 5. 8: The CPT development for organizational culture node.

#	Education /Training	Information sharing	Safety culture	Organizational cohesion	Employee inclusivity	Score	Organizational culture		
							Rich	Moderate	Poor
1	Adequate	Adequate	Rich	High	Inclusive	15	**0.99**	**0.01**	**0**
2	Adequate	Adequate	Rich	High	Moderately inclusive	14	0.91	0.07	0.02
…	…	…	…	…	…	…	…	…	…
24	Adequate	Adequate	Poor	Moderate	Exclusive	10	0.10	0.77	0.13
…	…	…	…	…	…	…	…	…	…
107	Inadequate	Inadequate	Poor	Low	Moderately inclusive	6	0.02	0.07	0.91
108	Inadequate	Inadequate	Poor	Low	Exclusive	5	**0.00**	**0.01**	**0.99**

This procedure is similarly applied to all other nodes to determine their respective CPTs. However, it is worth highlighting that the CPT for the "External Factors" node is derived using the Noisy-MAX technique. This approach is particularly suitable due to the nature of the relationships between the parent nodes and the child node. Specifically, the parent nodes influencing the "External Factors" node are independent of one another, meaning their effects on the child node are not interdependent but rather separate and distinct. To this end, the Noisy-MAX model is employed because it allows for the representation of such independent causal relationships in a probabilistic framework. By accounting for the individual contributions of each parent node, this technique provides a more accurate and computationally efficient method for modelling the probabilities of the child node's states. This approach ensures that the CPT reflects the distinct and non-overlapping influence of the parent nodes, aligning with the real-world characteristics of external factors that independently affect organizational performance.

5.4.2.2 Technological functions

In a seaport, various types of machinery, equipment, and their components contribute to the activities of technological functions. To evaluate their internal variability performance, the corresponding BN for each technological function is developed based on the information and structures outlined in Section 5.3.2.2. Due to space constraints, only the BN for quay cranes is presented in Figure 5.9 to demonstrate the applicability of the proposed methodology. Quay cranes are widely regarded as the most important, valuable, costly, and complex components in a seaport. A seaport without them is often considered paralyzed, as they serve as the critical link between sea and land operations.

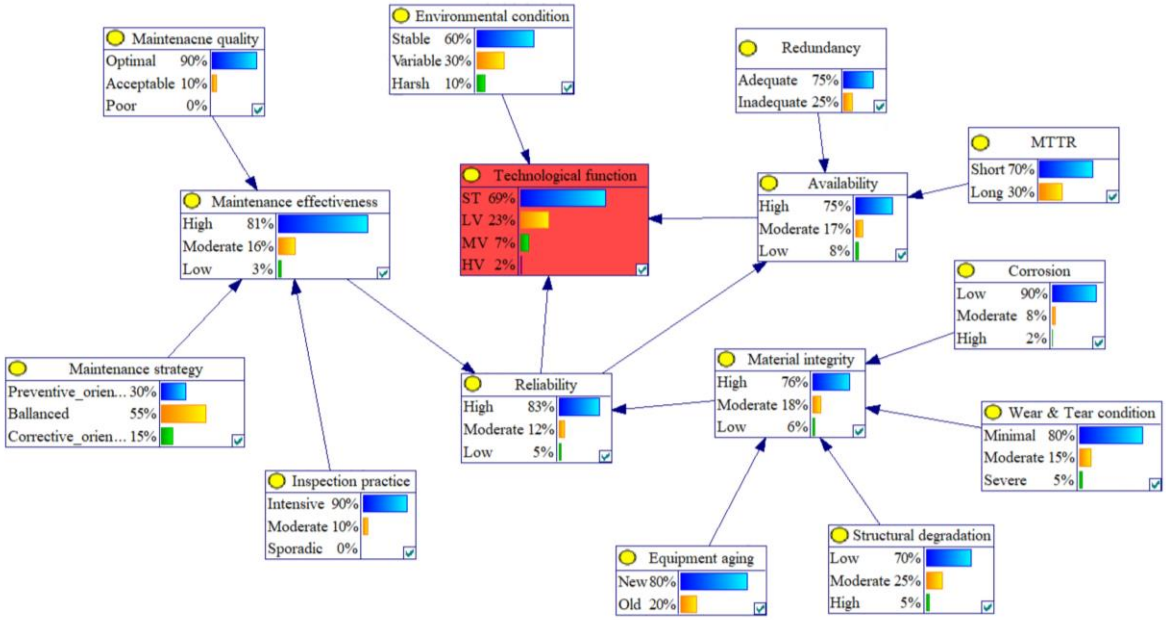

Figure 5. 9: The BN model for SVI assessment of technological functions.

In the developed BN, maintenance effectiveness and material integrity are identified as the two key factors directly influencing equipment reliability. Greater levels of material integrity and maintenance effectiveness correspond to higher reliability. It is noteworthy that the operation of complex systems such as quay cranes often involves dynamic processes that impact their structure and the reliability of their components over time. Given the critical importance of ensuring both safety and operational effectiveness, a shift from a two-state to a multistate approach in reliability analysis is warranted. This approach enables a more precise evaluation of their reliability and operational performance. It also helps identify critical reliability thresholds, where exceeding these limits may fail to ensure the required level of operational effectiveness (Kołowrocki and Soszyńska-Budny, 2011). Therefore, the reliability is categorized into three states: high, moderate, and low, defined according to the specific characteristics of the component in question. For quay cranes, high reliability corresponds to a reliability level between 95% and 100%, moderate reliability falls between 85% and 95%, and low reliability is defined as below 85% (Deng, 2000; Jo and Kim, 2019). Availability is determined by three key factors: reliability, MTTR, and redundancy. Higher reliability and redundancy contribute to increased availability, while a shorter MTTR enhances availability by reducing equipment downtime. Technological performance variability depends on three

factors: reliability, availability, and environmental conditions. The SVI is likely to remain stable with high probability if environmental conditions are stable and both reliability and availability are high. Other SVI states are assigned proportional values based on the probabilities of their parent states.

To calculate the quantitative values for SVI states, the process begins with determining the CPT for each intermediate nodes and the child node. For technological factors, the values for the two extreme cases in each row of the CPT are derived based on the historical data available from the seaport, as outlined in Section 5.3.3. Using Equations 1 to 4 and the scoring system, the initial CPT values are calculated. In the subsequent step, appropriate probability distributions are assigned to each value. MSCs are then performed using XLRisk software to refine and finalize the CPT values. To illustrate the applicability of the methodology, prior probabilities were derived from historical records of the seaport under study, representing its current status. As depicted in Figure 5.9, the stable state of the technological function is assigned a probability of 68.8%, while the remaining probabilities are distributed as follows: 22.7% for the LV state, 6.7% for the MV state, and 1.8% for the HV state. These values reflect the system's realistic behaviour, highlighting the influence of various factors that create discrepancies between "work as imagined" and "work as done."

5.4.2.3 Human function

To determine the SVI for human functions, the modified CREAM methodology outlined in Section 5.3.2.3 is employed. The process begins with developing the BN structure by identifying the main CPCs, their interdependencies, and incorporating calibrated CPCs. The leaf node in the network is represented as the CCM, which reflects human action status. The four well-known modes (strategic, tactical, opportunistic, and scrambled) are interpreted as ST, LV, MV, and HV, respectively. Figure 5.10 illustrates the resulting BN for human functions.

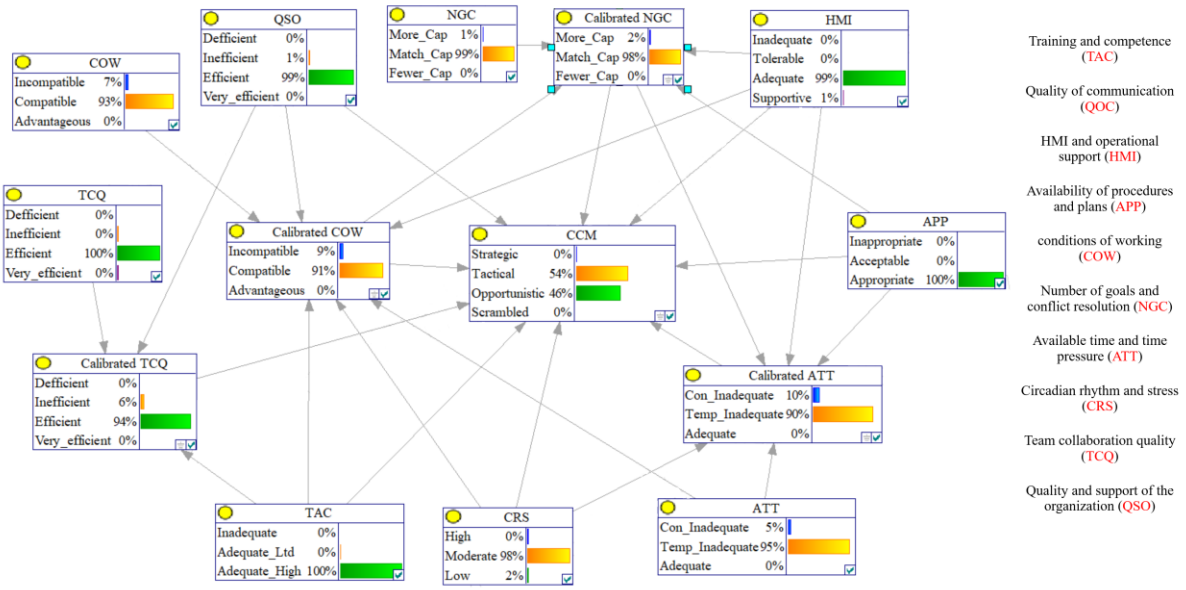

Figure 5. 10: The BN model for SVI assessment of quay crane operator.

Next, the rules governing the BN are organized using a belief structure that accounts for all possible combinations of CPC states. These rules form the CPT for the developed BN. It is

important to note that not all CPCs exert equal influence on human performance variability. Consequently, the Analytic Hierarchy Process (AHP) is employed to derive differentiated weights for each CPC, as it enables the systematic translation of expert judgments into quantitative importance weights while preserving their relative influence. This ensures that CPCs with greater impact on task performance are assigned higher weights, preventing equal-weight assumptions that would otherwise misrepresent their contribution to human performance variability in seaport operations (Yang et al., 2013). Table 5.9 presents a pairwise comparison matrix showing the weights for all nine CPCs. The consistency ratio, calculated as 6.7E-3, confirms that the derived weights are logically consistent and represent a well-justified hierarchy of importance.

Table 5. 9: Deriving CPC weights using AHP method.

CPC	TAC	HMI	APP	COW	NGC	ATT	CRS	TCQ	QSO	Weight
TAC	1.00	5.00	2.00	4.00	1.50	1.50	5.00	5.00	5.00	0.25
HMI	0.20	1.00	0.33	1.00	0.25	0.25	1.00	1.00	1.00	0.05
APP	0.50	3.00	1.00	2.00	0.67	0.67	3.00	3.00	3.00	0.13
COW	0.25	1.00	0.50	1.00	0.33	0.33	0.50	1.50	1.50	0.06
NGC	4.00	4.00	1.50	3.00	1.00	1.00	4.00	4.00	4.00	0.18
ATT	0.67	4.00	1.50	3.00	1.00	1.00	4.00	4.00	4.00	0.18
CRS	0.20	1.00	0.33	2.00	0.25	0.25	1.00	1.00	1.00	0.05
TCQ	0.20	1.00	0.33	0.67	0.25	0.25	1.00	1.00	1.00	0.05
QSO	0.20	1.00	0.33	0.67	0.25	0.25	1.00	1.00	1.00	0.05

5.4.3 Criticality matrix development

Once the performance variability for each function is quantified, the next step is to identify critical functions and evaluate the system's overall weaknesses from a systemic perspective. To achieve this, the UVI values are assigned appropriate scores, as outlined in Section 5.3.5.3, to derive a unique representative value for each function. This process involves calculating the mean, standard deviation, and the lower and upper bounds of the variability.

To represent the variability probabilistically, it is assumed that these aggregate scores follow a normal distribution. This assumption is common in probabilistic modelling, as the normal distribution effectively captures central tendencies (mean) and variability (standard deviation) (Mitrani, 2008). Table 5.10 provides the representative output values for each function, reflecting the variability and its implications for the system. It is to be noted that the lower and upper bounds are determined at a 95% confidence level through MSCs, utilizing 100,000 iterations for precision.

Table 5. 10: The functions representative output values for resonance analysis.

Function	Mean value	Standard deviation	Lower bound	Upper bound	Severity level
F1	1.930	0.570	0.812	3.048	Moderate
F2	1.930	0.515	0.921	2.939	Critical
F3	2.100	0.520	1.082	3.118	Moderate
F4	2.030	0.538	0.976	3.084	Moderate
F5	2.140	0.601	0.963	3.317	Critical
F6	2.300	0.574	1.174	3.426	Critical
F7	1.940	0.562	0.838	3.042	Moderate
F8	2.050	0.517	1.036	3.064	Moderate
F9	1.880	0.520	0.861	2.899	Moderate
BG1	1.935	0.644	0.673	3.197	Critical

BG2	1.970	0.513	0.965	2.975	Critical
BG3	1.614	0.565	0.507	2.721	Moderate
BG4	2.308	0.779	0.781	3.835	Critical

To assess the magnitude of variability in critical functions, their severity levels are also determined. However, accurately quantifying the magnitude of variability and its impact in terms of severity requires an independent study, as this step is crucial for understanding the consequential effects of disruptions in various elements of a CSTS. Given the scope of this study, we have relied on expert judgment to classify each function into three categories of severity: minor, moderate, and critical, as presented in Table 5.10.

Figure 5.11 illustrates the criticality matrix, which maps functions to their appropriate positions within the matrix. In this framework, the vertical axis reflects performance variability, with evenly distributed boundaries defined by the nature of each function in the seaport context. The proposed matrix offers flexibility for adaptation based on user-specific requirements, enabling its application to diverse systems of interest.

Variability level	**Severity level**		
	Minor	Moderate	Critical
HV ($X \geq 3.5$)			
MV ($2.5 \leq X < 3.5$)			
LV ($1.5 \leq X < 2.5$)		F_1, F_3, F_4, F_7, F_8, F_9, BG_3	F_2, F_5, F_6, F_7, BG_1, BG_2, BG_4
ST ($X < 1.5$)			

Figure 5. 11: The criticality matrix for identifying critical functions in resonance analysis.

The criticality analysis reveals that all functions fall into level B, indicating minor levels of variability. While these variabilities are relatively low, they still have the potential to contribute to negative resonance, especially when interacting with moderately variable or interconnected functions. Such interactions can propagate risks throughout the system.

According to Safety-II principle, variability at level B can be viewed as an asset, as it arises from the adaptive adjustments necessary for everyday operations. However, the criticality matrix utilizes mean values derived from variability distributions to categorize variability into three levels. To incorporate uncertainty into risk-based decision-making, the upper and lower bounds of variability scores can provide a more nuanced understanding of the confidence in the mean score's placement within the matrix. For instance, if the upper bound is considered and indicates higher criticality, it could flag functions for further investigation even when the mean suggests a lower criticality level. Using this approach, functions such as F_2, F_5, F_6, F_7, BG_1, BG_2, and BG_4 would move to level C when the upper bounds are applied. This shift indicates that these functions exceed acceptable thresholds and signal a need for immediate attention to mitigate the risk of negative resonance.

All in all, this approach rigorously prioritizes functions of safety measures, emphasizing the need to reduce variability in their outputs. Addressing these criticalities pre-emptively can prevent negative resonance and ensure system stability, particularly in downstream processes.

5.4.4 Model validation process

As outlined in Section 5.3.6, multiple approaches are employed to validate the proposed model and its findings. For the HTA and FRAM, the validation process involved consultation with three experts, each possessing at least 15 years of experience in seaport operations. These experts, with minor revisions, confirmed that the activities represented in the HTA and subsequently modelled in the FRAM, along with their structures and interconnections, accurately reflect the most significant and realistic activities observed in practice. Additionally, the results were partially benchmarked against other studies (Cho et al., 2018; Darbra and Casal, 2004; John et al., 2014a; Majumdar et al., 2022; Mitra et al., 2024; Yin et al., 2024). However, identifying and aligning with similar studies for comparison proved challenging due to the limited availability of directly comparable research and the complexity of matching findings.

In addition to the previously mentioned methods, sensitivity analysis was performed to validate the BN models. This process involved two sequential steps. First, the developed BNs for SVI evaluation were analysed as a partial validation of the overall model. Second, the FRAM-based BN models, which map the relationships between functions, were validated through sensitivity analysis. Using GeNIe software, a derivative-based sensitivity analysis was conducted, allowing the quantification of how changes in the BN's parameters influence the target nodes by calculating their derivatives. In this approach, the software uses mathematical and numerical techniques to compute the derivative of the posterior probability distribution of each target node with respect to each parameter. For instance, if P(C/A) represents the probability of a child node C given a parent node A, the derivative value is obtained as $\frac{\partial P(C)}{\partial P(A)}$, which quantifies how P(C) changes when P(A) is adjusted. Larger derivatives signify that even minor changes in a parameter have a substantial impact on the target node. By comparing derivatives across various parameters, the most influential ones can be identified.

As shown in Table 5.11, the three highest derivatives were selected along with their associated nodes as examples. It is important to note that these selections are based on the ST state of the target node. In other words, by setting the target node's state to ST, the most sensitive parameters were identified. Additionally, the range of changes in the ST state of the target node is presented, highlighting the interval of varying values. For instance, within the technological function, setting environmental conditions to stable, MTTR to short, and ensuring an adequate level of redundancy is expected to contribute to the stability of performance variability. The interval values are centered around the original ST state values of the target node, fulfilling Principle 1 of sensitivity analysis.

To address Principle 2, the top three nodes, along with their relevant states, were subjected to a 10% increase in their values to observe the combined effect on the target node. For human functions, since the initial values for these three top nodes were at their maximum (100%), a 10% decrease was applied instead.

The results indicate that the posterior probabilities of the target node for technological, organizational, and F_2 functions shifted favourably toward the ST state, resulting in a corresponding reduction in performance variability as the ST values increased. In contrast, for human functions, the posterior probabilities leaned toward greater performance variability, with an increase in the MV values. This demonstrates that the collective impact of changes in

the selected nodes on the target node's probabilities is consistently more significant than the impact of individual changes in each node, thereby validating Principle 2.

Table 5. 11: The sensitivity analysis results.

Function	Node	State	Interval	Derivative	Prior prob.	Posterior prob.	Performance variability
Organizational	Authority gradient	Balanced	[0.258-0.419]	0.160	ST=0.38 LV=0.52 MV=0.08 HV=0.02	ST=0.43 LV=0.49 MV=0.07 HV=0.01	PV_1=1.74 PV_2=1.66 ΔP=-5%
	Span of control	Balanced	[0.258-0.419]	0.160			
	Communication effectiveness	Adequate	[0.255-0.410]	0.155			
Technological	Environmental condition	Stable	[0.483-0.820]	0.337	ST=0.69 LV=0.23 MV=0.07 HV=0.01	ST=0.75 LV=0.20 MV=0.05 HV=0.00	PV_1=1.39 PV_2=1.30 ΔP=-7%
	MTTR	Short	[0.582-0.729]	0.148			
	Redundancy	Adequate	[0.575-0.722]	0.146			
Human	QSO	$S_{9,4}$	[0.353-0.540]	0.192	ST=0.00 LV=0.54 MV=0.46 HV=0.00	ST=0.00 LV=0.45 MV=0.55 HV=0.00	PV_1=2.46 PV_2=2.55 ΔP=+4%
	APP	$S_{3,3}$	[0.378-0.540]	0.181			
	TAC	$S_{1,3}$	[0.404-0.540]	0.167			
F_2	Internal	ST	[0.165-0.173]	0.174	ST=0.17 LV=0.73 MV=0.10 HV=0.00	ST=0.22 LV=0.70 MV=0.08 HV=0.00	PV_1=1.93 PV_2=1.86 ΔP=-4%
	BG_1	ST	[0.164-0.172]	0.173			
	F_1	ST	[0.162-0.171]	0.172			

5.5 Conclusion

In this chapter, a novel systemic risk analysis approach is designed to capture the dynamic interactions among the various elements of a seaport. Performance variability is acknowledged as a distinctive framework for expressing and understanding the interdependencies between diverse functions. The FRAM serves as the foundational component of the approach, enabling the visualization of real-world relationships between activities, referred to as functions, within a seaport context. To enhance FRAM's capability for quantitative analysis, it is integrated with BN, allowing consideration of both internal and external factors that may influence individual functions. The proposed methodology builds upon the principles of Safety-II concept, emphasizing a functional safety perspective. The outcomes of the study and the application of the framework provide deeper insights into system dynamics and offer more practical, versatile strategies for improving overall system safety.

Given the results, insights, and implications, this study makes several significant contributions, as follows:

1) Independent analysis of CSTS elements**:** Technological, human, and organizational functions within the CSTS are analysed individually to evaluate their internal and external performance variabilities, considering factors such as operational uncertainties, environmental conditions, and human performance fluctuations.

2) Function interactions: Interactions between functions are systematically analysed to track upstream-downstream performance variability, assessing their impacts, whether negative, dampening, or positive, on the overall system. This approach highlights critical dependencies and emergent behaviours.

3) Comprehensive risk analysis: The framework supports both retrospective and prospective evaluations of performance variability, providing actionable insights for addressing risks effectively.

4) Enhanced decision-making: By quantifying and visualizing performance variabilities, the framework enables risk-based decision-making, helping prioritize interventions and implement targeted risk management measures.

This integrated approach offers a robust foundation for understanding and mitigating systemic risks in CSTS environments.

While the proposed approach offers a promising method for systemic risk analysis in CSTS, it has certain limitations and areas for improvement. Firstly, the FRAM model in this study was developed using expert knowledge and focused only on key functions. As system complexity increases, the number of functions and their interdependencies can grow rapidly, making manual modelling through expert input increasingly difficult. In the future, integrating machine learning techniques, such as those based on HTA could help automatically identify functions and their interactions, improving scalability and modelling efficiency.

Secondly, limited availability of data, especially for human and organizational functions, means that the model currently relies heavily on expert judgment. While expert input is valuable, it can introduce subjectivity and inconsistency. To overcome this, future work should focus on building a platform for systematically recording daily performance data. This would enable continuous tracking of both normal and abnormal operations, reduce dependence on subjective input, and support the development of more robust, data-driven models.

Chapter 6 : Risk-informed resilience assessment

6.1 Summary

This chapter develops a simulation-based resilience analysis framework designed to quantify both the physical and economic impacts of natural hazards on seaport operations. Positioned within a broader risk-informed perspective, the framework integrates multiple disruption types, such as natural hazards, cyber incidents, security breaches, and operational accidents with a particular emphasis on climate-induced risks. By linking hazard exposure, asset vulnerability, and functional recovery, the framework advances current research toward a more holistic and measurable understanding of seaport resilience.

Seaports, as the operational core of global maritime transportation, are inherently vulnerable to environmental extremes due to their coastal locations. Among these, cyclones represent one of the most severe threats, capable of causing substantial physical damage and prolonged operational downtime. Climate change further amplifies this challenge, intensifying both the frequency and magnitude of such events. Despite these escalating risks, few existing approaches quantitatively capture the probabilistic nature of cyclone hazards alongside their functional and economic consequences.

Addressing this gap, the chapter introduces a comprehensive risk-based simulation framework that: (i) models cyclone occurrence probabilistically, (ii) applies fragility curves to estimate functional degradation and loss of capacity, and (iii) monetizes both direct physical damages and indirect economic losses arising from downtime during maintenance and repair. The framework is demonstrated through a detailed case study of Terminal 7 at the Port of Kaohsiung in southwestern Taiwan, employing historical cyclone records, terminal data, and operational parameters to simulate throughput loss across different cyclone intensities.

The simulation results provide valuable insights into the port's absorptive, adaptive, and restorative capacities, revealing its ability to withstand, adapt to, and recover from disruptions. The findings enable the identification of critical vulnerabilities and the formulation of targeted adaptation and restoration strategies. By integrating empirical data with advanced simulation and resilience-based principles, the framework offers a robust decision-support tool for port authorities and policymakers, promoting proactive risk management and long-term sustainability of maritime infrastructure.

6.2 Introduction

It is quite evident that the continuous operation of seaports, as the heart of maritime transportation, is absolutely essential. Any failure or disruption at a seaport has the potential to significantly hinder the global and domestic flow of goods, severely affecting supply chains and the economy at large. As such, any disturbance in their operations can lead to substantial economic consequences, not just for the port itself, but for the broader economy, including industries dependent on timely and efficient transportation services.

Due to their coastal locations, seaports are highly vulnerable to a wide variety of natural and man-made catastrophes. These hazards range from seismic events and typhoons to rising sea levels, flooding, and storm surges, all of which can disrupt port activities in unpredictable ways.

When a seaport is affected by one of these catastrophes, its superstructures, systems, sub-systems, equipment, and relevant components, such as berths, quay walls, quay cranes, trucks, yard cranes, automated guided vehicles (AGVs), electrical substations, and others can suffer significant physical damage. This damage not only leads to immediate operational delays but often results in long-term financial losses due to extensive repair and recovery efforts.

The recovery process can be particularly lengthy and resource-intensive, requiring not only substantial time and manpower but also significant financial investments to restore the port's operations to pre-disaster levels. In some extreme cases, a seaport may never return to its full capacity, even after years of recovery, leading to long-lasting disruptions to regional and global supply chains.

Several real-world examples of catastrophic disruptions to seaport operations illustrate the gravity of such events:

- Kobe Earthquake (1995): The Great Hanshin-Awaji Earthquake that struck Japan in January 1995 severely damaged the Port of Kobe, one of the largest ports in Japan. The quake caused widespread infrastructure collapse, including the destruction of quay walls, cranes, and other vital port facilities. Despite extensive recovery efforts, the port was unable to resume its previous level of capacity for many years. Direct physical damage was estimated to be around $5.5 billion, and the overall economic loss, considering trade disruptions and lost productivity, was estimated to exceed $6 billion (Yamamura, 2016). The port's inability to recover to pre-disaster capacity had long-lasting effects on Japan's regional and global trade.

- 2004 Indian Ocean Tsunami: The massive tsunami that followed the earthquake off the coast of Sumatra in December 2004 caused catastrophic damage to several coastal regions, including the Port of Banda Aceh in Indonesia. The port was completely destroyed and was closed for several months. The economic loss caused by the disruption of operations and the costs of rebuilding were estimated to exceed $1 billion, impacting both the local economy and international trade routes (Athukorala and Resosudarmo, 2005). The Port of Banda Aceh remained a key logistical hub for relief efforts in the aftermath of the disaster, but its recovery process was slow, and the economic loss was felt for years.

- Hurricane Katrina (2005): When Hurricane Katrina struck the Gulf Coast of the United States in August 2005, it wreaked havoc on the Port of New Orleans, one of the largest and most vital ports in the U.S. The port's infrastructure, including cranes, warehouses, and berths, was severely damaged. Direct damages were estimated to be around $1 billion, while the total economic loss due to operational disruptions and the port's inability to function at full capacity was estimated to exceed $3 billion (Deryugina et al., 2018). The hurricane's impact demonstrated the vulnerability of ports to extreme weather events and highlighted the importance of resilience measures.

These examples underscore the far-reaching economic impacts that natural hazards can have on seaport operations. In addition to the direct costs of infrastructure repair and recovery, the economic losses extend to disruptions in global trade, delays in the delivery of goods, increased shipping costs, and long-term reputational damage to affected ports.

Given the increasing frequency and intensity of natural hazards, largely driven by climate change, assessing the resilience of ports to these events has become an urgent task. However, this process is complex and challenging for several reasons:

1) Uncertainty in predicting hazards and impacts: accurately predicting natural hazards such as storms, flooding, or earthquakes, as well as their potential impacts on seaport infrastructure, remains a major challenge. The unpredictability of such events, combined with the long-term nature of climate change, makes it difficult to anticipate the full extent of their consequences.

2) Confidentiality of port operations: port operators often face concerns regarding the confidentiality of their operational data. The competitive nature of the maritime industry means that sensitive information about port capacities, vulnerabilities, and risk mitigation strategies is often not publicly disclosed. This lack of transparency complicates efforts to assess resilience across different ports and share best practices.

3) Scarcity of publicly available data: another significant challenge is the limited availability of historical data on past hazards that have affected ports. Much of this information is not publicly available due to privacy concerns, security issues, or proprietary data restrictions. This data scarcity makes it difficult to build comprehensive models of seaport resilience.

Despite these challenges, recent research efforts have advanced the use of simulation-based techniques to assess seaport resilience. Simulation models are particularly useful for predicting the impacts of natural hazards and estimating both direct and indirect losses due to disruptions. By simulating seaport operations under different hazard scenarios, these models can help identify vulnerabilities and design more resilient systems.

As previously discussed, simulation techniques have proven to be among the most reliable methods for seaport resilience studies. However, the application of these techniques to assess the full scope of resilience assessment and the economic loss from natural hazards remains underdeveloped. Two notable efforts in this direction include:

- Na and Shinozuka (2009): Developed a computerized simulation model using ARENA software to estimate seismic losses for seaport transportation systems. By incorporating fragility curves for port facility components, the model was able to simulate the impact of an earthquake on port operations, providing valuable insights into potential operational disruptions and economic losses.

- Cao et al. (2017): Designed a similar simulation framework using ARENA to analyse the economic losses due to typhoon hazards at Shenzhen Port. Their model accounted for the direct damage to infrastructure as well as the economic consequences of operational delays and lost productivity, illustrating the usefulness of simulation in disaster preparedness and resilience planning.

The objective of this chapter is to extend the current body of knowledge by developing a simulation-based resilience analysis framework that not only focuses on estimating the direct and indirect physical damage caused by natural hazards but also considers the economic losses

that result from such catastrophic events. This novel framework will fill the research gap identified earlier by providing a risk-informed resilience analysis that incorporates a broader set of disruptions, including natural hazards, cyber-attacks, security breaches, and accidents. However, given the urgent need to address the impacts of climate change, the focus of this framework will primarily be on natural hazards to demonstrate its applicability and effectiveness.

The proposed framework will help port authorities and stakeholders better understand the potential risks to their operations, evaluate their capacity to withstand these risks, and design more effective strategies for adapting to and recovering from such events. By incorporating realistic data, advanced simulation techniques, and a holistic view of resilience, this framework offers a powerful tool for improving the long-term sustainability and reliability of seaports in the face of increasing climate-related hazards.

6.3 Methodology

This section presents a novel risk-informed resilience analysis methodology, grounded in simulation techniques, which accounts for various dimensions of functionality loss and economic loss. Figure 6.1 illustrates the overall framework of the proposed methodology, structured into five consecutive phases:

- Phase 1: Hazard identification

The process begins with identifying the most critical natural hazards relevant to the seaport context. This involves assessing the frequency and intensity of each hazard and developing a port-specific hazard database.

- Phase 2: Functionality loss estimation

Functionality loss is assessed through a multi-step process involving hazard intensity analysis, derivation of fragility curves, and estimation of the probability of different damage states.

- Phase 3: Economic loss estimation

This phase addresses the multiple dimensions of economic loss. Mathematical formulations are developed for each type of economic impact, and total potential loss is calculated based on the severity and probability of the identified damage states.

- Phase 4: Simulation model development

The logical structure of the simulation model is established, and input data is collected from real-world port operations. Model validation is performed, and various disruption scenarios are simulated to capture a range of possible outcomes and responses.

- Phase 5: Throughput loss estimation

Outputs from the previous phases are integrated into the simulation-based model, while implementing the novel resilience strategies. This platform evaluates the current level of

resilience and identifies optimal resilience strategies to enhance system performance. Final recommendations are derived from the insights gained through this comprehensive analysis.

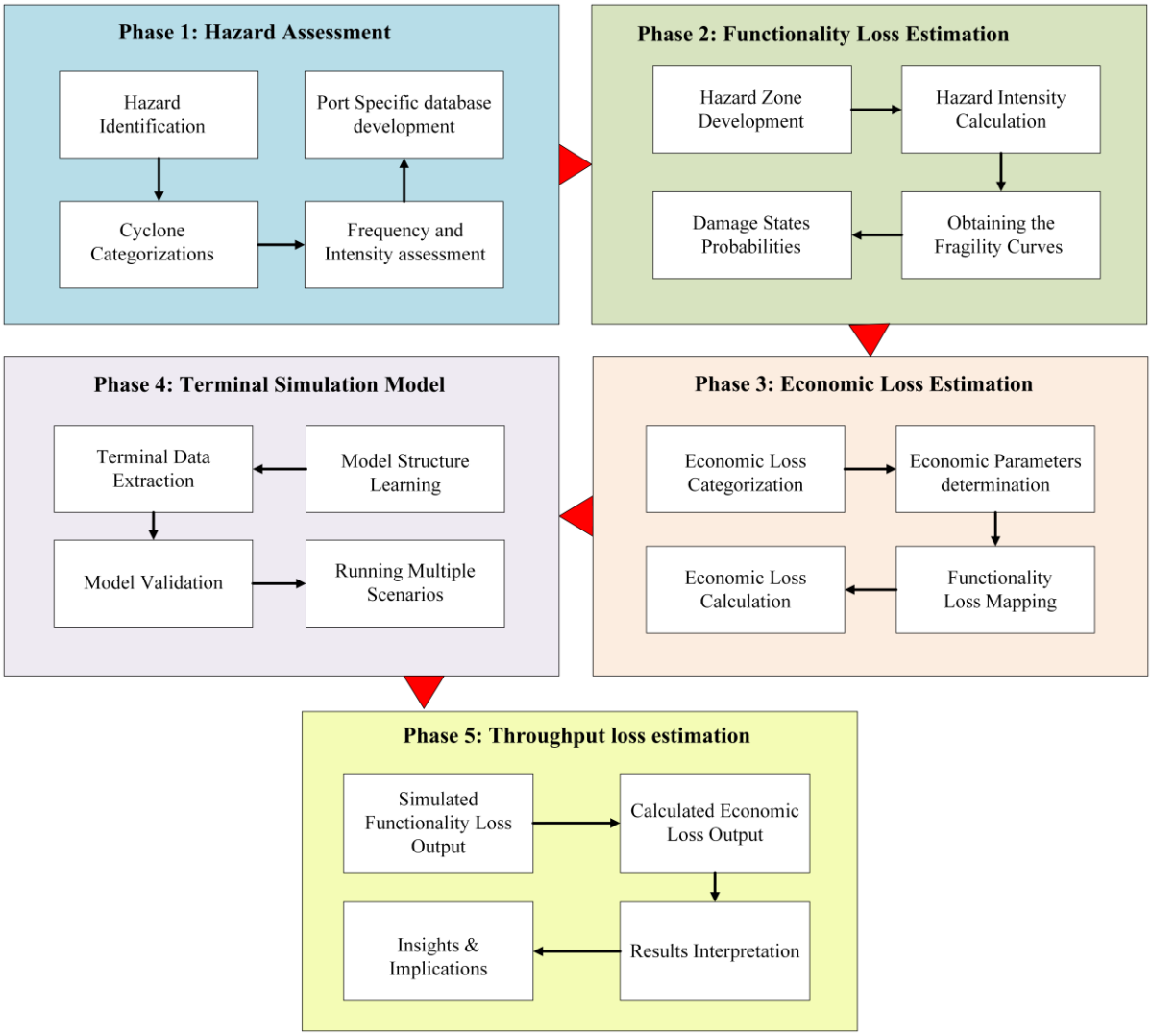

Figure 6. 1: The overall framework of the methodology.

6.3.1 Hazard categorization

In the initial step of the resilience analysis, it is essential to identify the hazards that need to be addressed. Since this study focuses on natural hazards, all relevant types should be categorized and ranked based on both their frequency and potential consequences. Table 6.1 presents a list of natural hazards that disrupt seaports, supported by global evidence on their occurrence rates and severity. To enhance clarity, selected historical events are also included, along with their estimated impacts on seaport operations.

Table 6. 1: Global overview of natural hazards disrupting seaport operations.

Hazard type	Description	Frequency	Downtime	Real case	Reference
Pluvial flooding	Intense rainfall causing surface water to inundate port	84 % of the world's major ports are exposed.	Less than 3 days	UK 2013–14 floods damaged port assets £1.8	*(Prieto et al., 2024)*

	areas, disrupting operations and damaging infrastructure.			m (Port of Hull)	
Fluvial flooding	River overflow inundating port facilities, halting cargo movement and causing structural and navigational hazards	80 % of ports exposed	days-weeks	Mississippi 2011: > US$0.3 bn to Gulf ports	*(Merz et al., 2010)*
Cyclones	Hurricanes or typhoons combining high winds, storm surge, and waves, severely damaging port infrastructure and operations	Leading hazard at 25 % of ports; seasonal clustering	days-weeks	Hurricane Ike 2008: ≈ US$2.4 bn to Texas ports	*(Pan, 2015; Verschuur et al., 2023)*
Sea rise	Elevated sea levels from storms overtopping defences, flooding docks, quays, and storage areas.	Dominant hazard for 24 % of ports (exposure higher in NW Europe, East Asia)	hours-days	UK east-coast surge 1953, King's Lynn 1953 (> US$1 bn equiv.)	*(Verschuur et al., 2023)*
Extreme maritime conditions	Non-storm high waves, winds, or extreme temperatures forcing temporary port closures due to safety risks.	Operational thresholds exceeded 40 % of ports each year	hours-days; cause > 40 % of short closures	Port Elizabeth, SA: recurrent wave-height shutting the port for 12–24 hours on ~40% of days per year	*(Izaguirre et al., 2021)*
Earthquakes & liquefaction	Seismic shaking and soil failure collapsing quay walls and piers, causing prolonged port downtime.	Leading hazard for 11 % of ports (hot-spots Chile, Japan, Med.)	Weeks-months (infrastructure rebuild)	Kobe 1995: ~ US$3–4 bn port damage	*(Iai, 2019; Na and Shinozuka, 2009)*
Tsunamis	Sudden, powerful sea waves inundating ports, destroying equipment, docks, and infrastructure with catastrophic impact.	Rare (decadal)	Weeks-months	Tōhoku 2011: US$12 bn port damage; ~ US$3.4 bn trade loss per day	*(Chua et al., 2024)*

Volcanic ash / eruptions	Ash falls and pyroclastic debris contaminating waterways, clogging machinery, and halting port operations.	Localised; < 1 % of ports near active centres	Hours-weeks (ash clean-up)	Tonga 2022 ash closed Nuku'alofa port forcing a 72-hour shutdown	*(Miller et al., 2016)*

As shown in Table 6.1, seaports are exposed to a range of natural hazards that differ in both frequency and severity. Although pluvial and fluvial floods affect the greatest number of facilities, the tropical cyclones, despite impacting fewer ports, account for roughly one-third of all port-specific risk and routinely force week-long closures (Verschuur et al., 2023). This combination of substantial economic losses and extended operational downtime makes cyclones one of the most dangerous threats to seaports in vulnerable regions. For this reason, our study focuses on characterizing the various types of tropical cyclones and assessing their potential impacts on port infrastructure and operations. It is noted that the term cyclone is used as a generic designation for tropical cyclones, encompassing regionally specific terms such as hurricanes (Atlantic and Northeast Pacific) and typhoons (Northwest Pacific).

This study adopts the Japan Meteorological Agency (JMA) intensity classification (https://www.data.jma.go.jp/multi/cyclone/cyclone_caplink.html?lang=en&utm) as Taiwan's Central Weather Administration (CWA) scheme is comparatively broad (Central Weather Administration (CWA) Taiwan., 2015). Both JMA and CWA use 10-minute sustained wind speeds in line with WMO practice, so our choice preserves consistency with Western North Pacific records and with local warning standards while providing finer analytical resolution. These thresholds also follow the WMO Typhoon Committee's wind-bracket definitions, as documented in the CWA RDC28 Typhoon Database web tool (TDB, 2024). The resulting six-tier classification is as follows: Tropical Depression (TD), Tropical Storm (TS), Severe Tropical Storm (STS), Typhoon (TY), Very Strong Typhoon (VST), and Violent Typhoon (VTY). Figure 6.2 shows the classifications along with their characteristics.

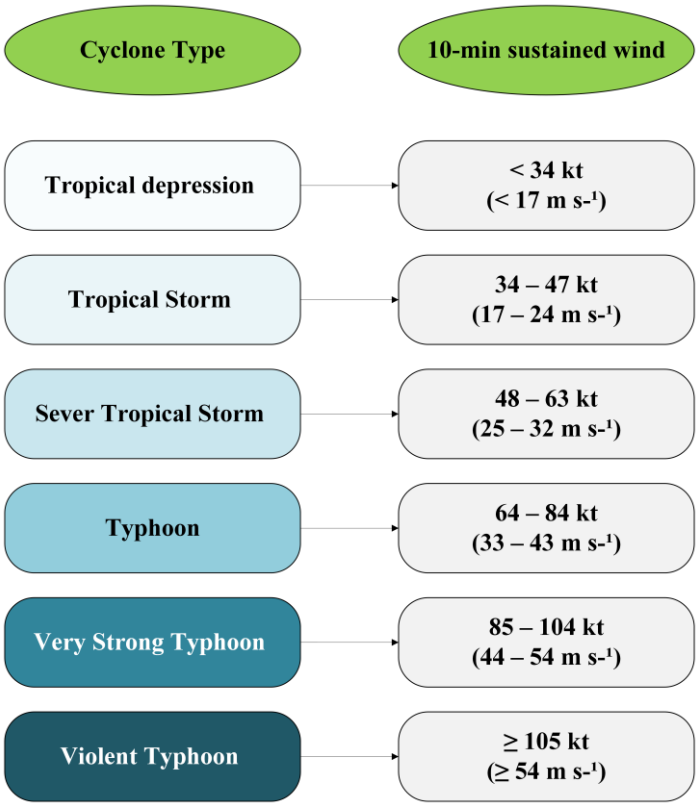

Figure 6. 2: Cyclone categories.

Lower categories denote systems with organized convection but limited potential for severe structural damage, whereas STSs begin to pose noteworthy wind risks to port infrastructure. Once winds reach Typhoon strength, significant harm to quay structures, cranes, and moored vessels becomes likely. The subdivision into very strong, and violent Typhoons reflects progressively extreme wind forces that can devastate terminal buildings, container stacks, and access roads, leading to extended closures and costly repairs (Lin et al., 2022). This gradation not only facilitates consistent historical analysis across basins but also underpins early-warning systems and resilience planning for vulnerable seaports.

6.3.2 Functionality loss estimation

Functionality loss due to natural hazards represents a complex and multifaceted challenge affecting the operational continuity and overall resilience of seaports. Effectively assessing this loss demands a comprehensive understanding of various critical factors, including the intensity and scale of the hazard events, such as cyclones, their proximity and trajectory relative to the seaport, and both direct and indirect consequences resulting from such disruptions. It is also crucial to clearly differentiate between various phases of disruption, encompassing immediate impacts, prolonged downtime, and the subsequent recovery processes. Furthermore, it is vital to acknowledge the interdependencies that exist within individual port systems (e.g., quay cranes, yard operations, cargo handling equipment) and between external infrastructure and services (e.g., transportation networks, utilities, and logistical supply chains).

To accurately estimate functionality loss, a structured and systematic approach is indispensable. Drawing upon methodologies such as HAZUS (FEMA, 2024a), as well as insights from other

relevant studies across diverse sectors (Di Ludovico et al., 2022; Koks et al., 2015; Tanoue et al., 2020), functionality loss can typically be delineated into direct and indirect categories, specifically focusing on physical and economic losses. Direct physical losses involve immediate damage to port infrastructure and critical equipment (such as berths, cranes, and storage facilities), while indirect physical losses capture subsequent impairments or reduced capacities resulting from initial disruptions and cascading failures. Direct economic losses are generally quantified as revenue reductions and operational expenditures related to damage recovery, whereas indirect economic losses consider broader financial implications, including lost business opportunities, market share reductions, increased insurance premiums, and costs associated with logistical rerouting.

Beyond these quantifiable physical and economic dimensions, additional impacts such as social disruption, environmental harm, and compromised security conditions should ideally also be integrated into comprehensive resilience assessments. Nevertheless, within the specific context of immediate hazard-induced disruptions, direct and indirect physical and economic losses constitute the most transparent, measurable, and critical categories to inform initial emergency responses and long-term resilience strategies.

6.3.2.1 Physical loss estimation

Accurate estimation of functionality loss in seaports exposed to tropical cyclones requires categorizing impacts by geospatial zones defined by strike distance. Each zone corresponds to characteristic hazard profiles, ranging from the eyewall's maximum winds and storm surge, through gale-force wind fields and rainband effects, to peripheral swell and residual surge, each driving distinct failure modes in port infrastructure and operations (Emanuel, 2006, 2005; Huang et al., 2024; Jian et al., 2019; Schott et al., 2019).

Cyclone impact zones were stratified into two principal distance classes, direct strike (0-200 km) and vicinity strike (>200-400 km), to reflect distinct hazard regimes observed in previous studies (Cao and Lam, 2018; Lu et al., 2022; Zong and Chen, 1999). The direct strike region encompasses the most intense meteorological features, including the eyewall, radius of maximum wind (RMW < 50 km), secondary eyewalls, inner rainbands, and the principal gale field. These features exhibit steep radial gradients in wind speed and precipitation, which are typically concentrated within 200 km of the cyclone centre. This distance is consistent with the operational warning systems, and hazard classification schemes that define significant impact zones within 125-232 km of the storm track (Chavas and Emanuel, 2010). Accordingly, the 0-200 km range was discretized into four 50 km intervals (0-50, 50-100, 100-150, and 150-200 km) to resolve rapid spatial gradients and transitions across the storm core and inner wind field.

Beyond 200 km, cyclone hazards become increasingly dependent on storm size rather than inner-core dynamics. This vicinity strike zone is characterized by flatter radial gradients and greater influence from the outer wind field. Hazards in this region, particularly storm surge and wave impacts, scale with storm size and expand more gradually with distance. Therefore, the region beyond 200 km was divided into broader 100 km intervals (200-300 and 300-400 km) to capture variability in storm size while avoiding unnecessary segmentation where gradients diminish. The outer cutoff at 400 km was selected based on evidence from satellite-based

climatology (e.g., QuikSCAT, infrared imagery) indicating that the majority of structural variability and hazard significance is contained within this range, while gradients beyond 400 km are weak and largely negligible (Knaff et al., 2007).

Table 6.2 summarizes commonly adopted distance bands, their operational significance, and rationale behind them.

Table 6. 2: Cyclone strike distance categorization.

Ring (km)	Zone Name	Physical / Impact Rationale
0-50	Direct Inner Core (Eyewall & RMW Domain)	Encompasses typical RMW range (often <50 km) concentrating peak tangential winds, tightest pressure gradient, highest structural load and surge driver; RMW retrieval / structural evolution studies show large variability but clustering within tens of km, warranting finest resolution here.
50-100	Outer Eyewall / Inner Rainband Periphery	Captures secondary eyewall formation zone and intense inner rainbands where winds remain well above gale force and rainfall maxima persist; wind radii prediction and rainfall composites show robust wind & rain field to ≥100 km.
100-150	Inner Gale Field Transition (A)	First sub-region of broad 100-200 km gale/rainband zone; distinguishes ports just outside inner eyewall influence but still under high mean rain rates and rising probability of sustained gale (R34 frequently spans well beyond 150 km) allowing finer calibration of operational thresholds.
150-200	Inner Gale Field Transition (B)	Upper portion of direct gale domain approaching typical mean R34 extent; rainfall composites and wind radii continue to show significant wind/precipitation anomalies here, justifying separation from 100-150 km for risk gradients and response staging.
200-300	Transitional Outer Core / Size-Sensitive Zone (1)	Beyond most RMW and much of inner rainband forcing; hazard dominated by variability in storm size (R34 tail) and evolving outer wind strength; size metrics and growth ("fullness") studies show continued structural adjustments, and surge potential still size-sensitive here.
300-400	Outer Wind Envelope / Large-Storm Impact Zone	Captures large / very large cyclones' extended gale field and outer closed isobar influence where size (not core intensity) drives residual wind seas, swell and longer surge setup.

Having categorized cyclones by intensity and distance, the next step is to determine the frequency of each cyclone type within the defined ring zones. This can be approached in two ways: Closest Approach (CA), Encountered View (EW).

In the CA method, for every storm recorded within a 400 km radius of the port, the time of minimum geodesic distance (its closest point of approach) is identified. The storm is then assigned to a single category and ring based on the reported sustained wind at that time. CA produces a clean, one-storm-one-cell exposure matrix, making results directly comparable to previous studies (Flynn, 2023).

In the EW method, all storm fixes within 400 km window are considered, and the highest intensity category reached within that range is identified. Among the times corresponding to that highest category, the smallest ring is selected for classification. EW captures the storms whose peak intensity occurs before or after the closest pass and ties classification to the peak hazard state experienced in proximity. This mirrors established exposure datasets that categorize events by the peak sustained wind experienced at a site rather than solely by the distance at closest approach (FEMA, 2018; Geiger et al., 2018).

In this study, both approaches are applied to develop a port-specific cyclone database for multiple purposes, including documenting past cyclone events within 400 km of the port, their frequencies, strike distances, and intensities. The distance from each cyclone fix to the seaport is calculated using the Vincenty formula, which determines geodesic distances on an ellipsoidal model of the Earth (Thomas and Featherstone, 2005). This method offers greater accuracy than spherical models, such as the haversine formula, as it accounts for the Earth's flattening and is widely used in geodesy.

Regarding the hazard zones defined above, it is important to note that the distance between the cyclone's eyewall and the port is not a reliable indicator for categorizing cyclone intensity. Instead, the wind speed experienced at the port should serve as the primary criterion for classifying cyclone types. This approach ensures that the classification reflects the actual conditions encountered at the seaport, rather than the cyclone's peak intensity over the ocean.

To implement this, we calculate the wind speed at the port and use these values to categorize the cyclones accordingly. The following steps outline the methodology:

a) Cyclone track and wind data

   For each recorded cyclone, the centre position (at 6-hour intervals) and the official peak 10-minute mean wind speed (denoted as Vmax) are extracted.

b) Distance to the seaport

   The distance from each cyclone fix to the seaport is computed using the Vincenty formula (Thomas and Featherstone, 2005), which calculates geodesic distances on an ellipsoidal model of the Earth. This method is more accurate than spherical models, as it accounts for the Earth's flattening and is commonly used in geodesy.

c) Radius of maximum wind (RMW)
   Since most storms lack an observed RMW, it is estimated using the climatological power-law–exponential relation of (Trabing et al., 2024), which links RMW to storm intensity and latitude, as follows:

$$RMW = \alpha {V_{Max}}^{\beta} e^{\gamma * LAT} \quad (6.1)$$

   Where V_{MAX} is the maximum intensity in units of m/s, LAT is the latitude in degrees, and the coefficients are $\alpha = 671.3$, $\beta = -0.9516$, and $\gamma = 0.0242$.

d) The Holland parametric wind-field.

In the next step, the symmetric Holland vortex model is applied to calculate the gradient wind at any given radius r, corresponding to the port location (Holland, 1980). This provides an estimate of the highest 10-minute mean wind speed that could have been experienced at the seaport during the cyclone's passage.

$$V_P(r) = K_m V_g(r) = k_m \sqrt{\frac{B\Delta P}{\rho}\left(\frac{R_m}{r}\right)^B e^{-\left(\frac{R_m}{r}\right)^B} + \frac{(f_r)^2}{4}} - \frac{f_r}{2} \tag{6.2}$$

where,
$V_P(r)$: the estimated wind speed at port,
$V_g(r)$: the gradient-level tangential wind at radius r from the cyclone centre,
k_m: 10-min reduction factor at 10m height,
B: Holland shape parameter (dimensionless), typically between 1-2,
ΔP: the sea-level pressure deficit,
ρ: air density,
R_m: radius of maximum wind (m),
f_r: Coriolis parameter.

Once the cyclones are categorized based on the wind speed experienced at the seaport, it becomes possible to estimate their impact on the port's functionality. To do this, we adopt the damage classification framework from HAZUS and relevant references (DNV GL, 2018; FEMA, 2020; USACE, 2019), which divides port damage into four discrete damage states, ranging from DS1 to DS4.

To quantify cyclone-induced losses at a typical terminal, the four-state HAZUS damage taxonomy is adopted, which ranges from DS1 (Slight damage) to DS4 (near-complete failure). DS1, or cosmetic damage, involves non-load-bearing elements such as cladding, signage, LED mast lights, CCTV housings, fender facings, paint, cable trays, being dented, shattered, or scoured by debris. Such superficial defects have no effect on throughput and can be repaired in parallel with more serious work.

When a cyclone pushes the facility into DS2, the structures themselves remain sound, but functionality is interrupted. Typical triggers include a tripped 11-kV substation, flooded fibre-optic rings, de-calibrated automated stacking cranes, or misaligned gate traffic-control masts. Throughput is curtailed until systems are reset or minor components replaced, usually a matter of hours to days.

DS3 marks the threshold of localised structural failure: a quay crane boom may collapse onto a vessel while the tower and sill beam survive; a rubber-tyred gantry's sheave housing may tear away; or a warehouse roof truss may partially uplift. The affected berth or yard is closed, and neighbouring assets operate under caution, with repairs typically stretching into weeks.

Finally, DS4 denotes major structural failure or near-total loss. Core load-carrying elements such as wharf decks, piles, or bollards suffer full-depth cracking, displacement, or pull-out, which sometimes cause tearing crane rails and slabs in the process. Progressive collapse of warehouse frames is possible. The berth is out of service for months, often requiring redesign before reconstruction.

By coupling each damage state with clear operational consequences and indicative repair horizons, this approach provides a consistent basis for developing fragility curves, estimating downtime, and prioritising resilience investments at cyclone-exposed ports.

Prior to assigning damage states to individual port assets, it is essential to identify those whose failure would critically impair port functionality. Drawing on the Critical Path Method (CPM), a scheduling technique long employed in construction and recently recommended by the U.S. National Institute of Standards and Technology (NIST) for disaster-recovery modelling (Lavelle et al., 2020), an analogous concept is adopted for seaport operations. Here, the critical path denotes the sequence of repair and restoration activities that constrains the earliest time at which a port can resume operations, given limited labour, and the technical precedence of tasks. Any delay along this chain postpones the port's overall reopening. Table 6.3 summarises the critical-path components developed from historical post-cyclone recovery records and the relevant literature.

Table 6. 3: Critical path items in a typical seaport.

Items	Descriptions	References
Navigation channels	Hydro surveys and debris clearance are prerequisites for reopening to vessel traffic; these activities control the initial restart.	*(Touzinsky et al., 2018)*
Quay/berth sub-structure (quay wall, relieving platform, rails)	A berth must be structurally sound and level before cranes can run or a vessel can moor. PIANC's *Seismic Design Guidelines for Port Structures* and ASCE/COPRI 61-14 both treat pile or gravity-wall failure as a "functional collapse" mode for the terminal.	*(Association, 2002; Engineers, 2014)*
Quay cranes	They are the only means to transfer containers between ship and shore; downtime directly halts throughput. Recent reliability studies rank quay cranes as the highest-critical asset class in container terminals.	*(Đelović, 2024; Rosca et al., 2025)*
High-voltage power supply (11-33 kV ring, main sub-station)	Modern quay cranes and many berth services are 100 % electric. Loss of the ring or primary sub-station disables every crane simultaneously. Both the FEMA and HAZUS hurricane manual and multi-hazard risk assessments for ports flag electric power as a dominant single-point vulnerability.	*(FEMA, 2024a; Verschuur et al., 2023)*
Terminal backbone IT / SCADA node	After Sandy, submerged control rooms and servers kept otherwise undamaged terminals closed for weeks; the USCG Hurricane-Sandy after-action report lists TOS servers and fibre switches with the same priority as cranes and fuel jetties.	*(Sturgis et al., 2014)*

To estimate the probability of physical damage and potential downtime of seaport equipment caused by different types of cyclones, fragility curves are developed. A fragility curve addresses the following question:

"Given that the port is impacted by a wind speed of V_{kt}, what is the probability that a structure reaches or exceeds a specific damage state (DS)?"

In line with performance-based engineering practice and hurricane vulnerability studies, the port-asset fragility curve is modelled as a lognormal exceedance function (Du and Hajjar, 2024; Li and Ellingwood, 2006). Specifically, for damage state k,

$$F_{q,k}(v) = P[DS \geq k | V_{10} = v] = \Phi\left(\frac{ln\, v - ln\, \theta_{q,k}}{\beta_{q,k}}\right) \tag{6.3}$$

where,

$F_{q,k}(v)$: the fragility curve for critical item q in the damage state k,

$\theta_{q,k}$: the median resistance-wind at which there is a 50 % chance of reaching DS ≥ k,

V_{10}: the 10-minute sustained wind at the quay,

$\beta_{q,k}$: the log-dispersion.

The lognormal form is standard as wind demand and capacity uncertainties are multiplicative and strictly positive, and it is the default in FEMA fragility development guidance (FEMA, 2020).

Having derived the fragility curves, the probability that each critical item q will fall into a given damage state k can be expressed as a Monte Carlo expectation, as follows:

$$P_{q,k}(S) = E\left[F_{q,k}(v)/S\right] \tag{6.4}$$

$$S = (Ring\ zone\ [r_{min}, r_{max}], JMA\ class\ C) \tag{6.5}$$

Here, S represents the cyclone type within the predefined ring zones boundary.

The expected downtime associated with each damage state is normally presented as a baseline MTTR. This baseline reflects standard operating conditions, assuming:

- Normal availability of spare parts,
- One heavy-lift contractor on call,
- No pre-arranged mutual-aid cranes, and
- Repairs conducted during regular weekday working hours.

This scenario aligns with what USACE (USACE, 2019) define as a “Tier-2, standard-practice” port. Deviations from this baseline, whether due to better preparedness or more constrained conditions, will generally cause downtime to scale almost linearly.

For DS1, which typically reflects minor or cosmetic damage, it is assumed that repairs occur concurrently with the port’s normal operational recovery. As such, berth availability is not affected. The FEMA Maritime Addendum supports this assumption by assigning a downtime of maximum “one day” for DS1, indicating that service resumes as soon as the wind hazard has passed, with no additional repair time required.

Recovery durations are provided as realistic ranges, reflecting the inherent uncertainty due to varying parameters such as event intensity, cascading effects, preparedness, budget constraints, and severity of damage consequences. Rather than exact values, ranges offer a better practical understanding of potential downtime.

These ranges are supported by an extensive collection of sources, including industry case studies, historical event analyses, OEM (Original Equipment Manufacturer) documentation, insurer claims databases, and peer-reviewed academic research. The lower bounds reflect the fastest credible recoveries observed historically, supported by OEM emergency-service guarantees. For example, ZPMC (Zhenhua Port Machinery Company), the OEM for quay cranes, guarantees rapid technician deployment within 24 hours and critical spare parts within 72 hours through its Global Remote Monitoring Centre (https://www.zpmc.com/products/integrated-service). Similarly, the Port of New Orleans managed to restore full crane functionality within three days following Hurricane Gustav (FreightWaves/AP, 2008), and DOE/EPRI reports (https://www.energy.gov/ceser/articles/hurricanes-nate-maria-irma-and-harvey-situation-reports) from Hurricanes Sandy and Harvey confirm that critical electrical infrastructure, such as 11 kV breaker racks, could be re-energised within approximately five days when prefab skids were readily available.

The upper bounds capture the longest credible recovery durations documented in practical scenarios and case studies. Insurer databases, such as TT Club & ICHCA's Windstorm database (TT CLUB, 2009), indicate structural crane repairs commonly extend from 8-14 weeks in worst-case scenarios. Additionally, comprehensive global analyses study (Verschuur et al., 2020) identify a 95-percentile mixed-asset disruption period of around 22 days. Extreme scenarios, like the UNCTAD-documented Gulfport berth reconstruction following Hurricane Katrina, set benchmarks with berth-span replacements ranging from four to six months (UNCTAD, 2022b).

It's crucial to note that different damage states (DS2, DS3, and DS4) involve separate teams and equipment (electrical, structural, and heavy-lift specialists), allowing parallel rather than cumulative recovery efforts. Thus, the provided ranges apply per unit, reflecting practical recovery operations rather than aggregated downtime.

6.3.2.2 Economic loss estimation

Economic loss estimation in seaports exposed to tropical cyclones is a critical process that requires categorizing various cost types and understanding their specific nature. When a seaport is affected by a cyclone, economic losses can generally be classified into three main categories:

1) Direct damage costs: These refer to the physical damage sustained by port equipment, infrastructure, and components.

2) Downtime costs: These represent the economic impact of throughput loss due to service interruption or reduced operational capacity.

3) Repair and recovery costs: These include expenses associated with restoring damaged assets and resuming normal operations.

Each of these cost components should be incorporated into a comprehensive economic loss model, with their respective contributions accurately formulated to estimate total losses.

Direct damage cost: Direct damage costs can be estimated by assessing the probability of different damage states for each scenario and applying the corresponding loss ratios for those states, as follows:

$$PL_c = \sum_{i=1}^{n} Q_i \, C_i \bar{d}_i \tag{6.6}$$

$$\bar{d}_i = \sum_{k=2}^{4} P_i^{DS_k} \; LR_i^{DS_k} \tag{6.7}$$

$$LR_i^{DS_k} = \frac{Replacement\ cost\ of\ asset\ i|DS_k}{Full\ replacement\ cost\ of\ asset\ i} \tag{6.8}$$

Where,

PL_c: direct physical damage cost.

Q_i: quantity of asset i (e.g. quay cranes, berths equipment, power system equipment).

C_i: Replacement or major-repair cost per unit of asset i.

$\bar{d}_i$: the expected damage ratio for asset i.

$P_i^{DS_k}$: the probability of damage state k for asset i.

$LR_i^{DS_k}$: the mean loss ratio of asset i associated with damage state k.

It is noted that the loss ratio for each specific component is typically derived from empirical claims data, engineering quantity take-offs, and published default values.

Downtime cost: Downtime costs in seaports affected by tropical cyclones can be broadly categorized into two components: throughput loss, and the gale-force-induced operational stoppages. Throughput loss refers to the revenue shortfall resulting from a reduction in cargo handling capacity following a cyclone event. This loss represents the gap between the terminal's expected operational throughput under normal conditions and the reduced capacity during and after the disruption. The period required to restore operations to pre-event levels contributes directly to this economic loss.

Gale-force stoppages occur when port operations are suspended due to high wind speeds, typically exceeding 35 knots, in compliance with safety regulations. During this time, all container-handling activities are stopped, leading to a complete halt in throughput. Although this stoppage is temporary and safety-driven, the associated downtime could result in considerable economic implications due to idle resources and delayed cargo processing.

The total downtime cost can be calculated as follows:

$$DL_c = T_c + G_c \tag{6.9}$$

$$T_c = (T^{intact} - T^{disrupted}) \times \rho \tag{6.10}$$

$$G_c = \frac{Hr_{gale}}{24} \times T_{daily}^{intact} \times \rho \tag{6.11}$$

where,

DL_c: the total downtime cost.

T_c: the throughput revenue loss.

T^{intact}: the intact throughput (TEU).

$T^{disrupted}$: the throughput after disruption (TEU).

ρ: handling tariff or margin per TEU.

G_c: Gale-force compulsory stop cost.

Hr_{gale}: Hours of sustained wind ≥ 35 kt at the quay.

Repair and recovery cost: Recovery costs are a crucial component of overall operational expenses following disruptions, particularly in seaport operations. These costs not only include direct repair expenditures but also affect other cost categories, creating a ripple effect throughout the system. The faster the recovery process is initiated, the higher the immediate costs can be. Expedited repairs often require additional resources, such as overtime labour, air-freighted spare parts, and the use of dual shifts to ensure that operations resume as quickly as possible. While these measures increase recovery expenses, they can help mitigate longer-term costs associated with extended downtime.

Faster recovery can reduce overall downtime, which in turn minimizes revenue loss costs. This means that while immediate recovery efforts may appear costly, the long-term financial impact could be lower due to the quicker return to full operational capacity (Toğan and Eirgash, 2019). The balance between rapid recovery and cost efficiency is, therefore, a critical consideration for seaports.

Seaports differ significantly in their recovery capabilities, which are influenced by various factors such as logistical infrastructure, available investments, operational policies, and past experiences with disruptions. Some ports may have robust contingency plans, advanced equipment, and highly trained personnel, allowing for faster recovery. In contrast, other ports may have more limited resources, which could lengthen the recovery process and increase associated costs.

Thus, it is important to consider all relevant factors, such as the port's logistical capabilities, financial resources, and operational strategies, when developing an accurate estimation of recovery costs. A comprehensive understanding of these factors will allow for more effective planning and cost management during the recovery phase.

In the recovery cost modelling process, costs are classified into two categories: time-sensitive and non-time-sensitive. Direct damage costs apply uniformly to equipment and items requiring replacement. However, accelerable blocks, which are time-sensitive, include:

1) Crew and logistics labour (overtime, extra shifts),
2) Mobilization/demobilization and site setup (barges, temporary workshops, cranes),
3) Expedited parts and freight premiums (air freight, customs, courier),
4) Equipment rental and standby (mobile cranes, generators, IT trailers).

Time is critical for these items; delays or accelerated processes directly impact expenditure. The following formula outlines the developed approach for estimating recovery costs in seaport contexts:

$$RC(t) = PL_c + \sum_{i,k} \sum_{j \in J} B_{i,k}^{(j)} F_{i,k}^{(j)}(\alpha_{i,k}) \tag{6.12}$$

$$F_{i,k}^{(j)}(a_{i,k}) = 1 + \alpha_{i,k}^{(j)} (\gamma_{i,k}^{b_{i,k}^{(j)}} - 1) \tag{6.13}$$

$$\gamma_{i,k}^{(j)} = \frac{T_{i,k}^{base}}{T_{i,k}^{acc}} \tag{6.14}$$

$$B_{i,k}^{(j)} = \begin{cases} \left(n_{i,k}^{int} w^{int} + n_{i,k}^{ext} w^{ext}\right) T_{i,k}^{base} & (j = 1) \\ M_{i,k}^{mob} & (j = 2) \\ E_{i,k}^{exp} & (j = 3) \\ R_{i,k}^{rent} . T_{i,k}^{base} & (j = 4) \end{cases} \tag{6.15}$$

where,

$RC(t)$: the recovery cost,

PL_c: Components replacement cost,

$B_{i,k}^{(j)}$: Baseline costs for accelerable blocks of class i in state k,

$F_{i,k}^{(j)}(\alpha_{i,k})$: Time-compression premium,

$\gamma_{i,k}^{(j)}$: Recovery duration ratio,

$a_{i,k}^{(j)}$: First-increment mark-up coefficient,

$b_{i,k}^{(j)}$: Convexity (escalation) exponent,

$n_{i,k}^{int}$, w^{int}: In-house crew size and daily wage,

$n_{i,k}^{ext}$, w^{ext}: External crew size and daily wage,

T_{ik}^{base}: The baseline repair duration for component class i, DS_k (day).

$T_{i,k}^{acc}$: The accelerated recovery duration for component class i, DS_k (day),

$M_{i,k}^{mob}$: One-time mobilization/demobilization cost at normal speed,

$E_{i,k}^{exp}$: Baseline expediting/freight cost,

$R_{i,k}^{rent}$: Daily rental rate of external equipment.

The parameter $\alpha_{i,k}^{(j)}$ represents the proportional cost premium incurred when the initial reduction in repair time occurs (i.e., when $\frac{T_{i,k}^{base}}{T_{i,k}^{acc}}$ is just above 1). It accounts for additional expenses such as overtime pay, night-shift differentials, expedited freight for spare parts, and standby-crew retainers. The parameter $b_{i,k}^{(j)}$ indicates how rapidly the cost slope steepens as repair time decreases. In other words, it governs the rate at which costs escalate as the repair process approaches its crash limit. If b=1, the relationship between time and cost follows a linear trajectory. However, if b>1, the curve becomes convex, meaning that each additional day of effort to reduce repair time incurs exponentially higher costs compared to the previous day. Together, these two parameters ($\alpha_{i,k}^{(j)}$, $b_{i,k}^{(j)}$) make the recovery cost model fully time-sensitive, transparent, and aligned with the time-cost trade-off objectives (Błaszczyk and Nowak, 2009).

6.3.3 Resilience strategies implementation

As previously discussed, the resilience strategies implemented in a seaport can be classified into three primary categories: absorptive, adaptive, and restorative. These capacities, along with their associated strategies, contribute to enhancing the resilience, depending on their effectiveness and the level of investment dedicated to them. For instance, a seaport that benefits from redundant systems and has invested in the robustness of its superstructures is likely to exhibit greater resistance and performance during the initial stages of a hazard event, resulting in reduced functionality loss.

A notable example of enhancing quay crane robustness against earthquakes and cyclones is the installation of ductile link tie-down systems. A ductile link is a small, purpose-designed steel “fuse” integrated into each crane tie-down. By yielding in a controlled manner, it equalizes uplift forces, dissipates energy, and prevents the domino-style collapses observed during past cyclones. Both field experience and analytical studies confirm that this is among the most cost-effective upgrades available to improve quay crane resilience in the face of increasing wind intensities driven by climate change (McCarthy et al., 2009). For instance, during Typhoon Maemi in 2003, six quay cranes collapsed in Busan after a single overloaded tie-down failed. Since the first installations in 2004, over 150 cranes equipped with ductile links have withstood eight Category 4-5 storms without a single reported collapse (Lee, 2019).

In addition, effective adaptability and recovery strategies help minimize the downtime of port systems and further contribute to improving the overall resilience of the port. Naturally, each

of these strategies requires financial investment, and the associated costs must be taken into consideration.

To quantitatively represent the impact of these capacities on the damage states of equipment resulting from hazards, a Recovery Capacity Factor (RCF) is defined as follows:

$$RCF = \frac{Industry-standard\ MTTR}{Port-specific\ MTTR} \qquad (6.16)$$

Here, the industry-standard Mean Time to Repair (MTTR) is presented as a baseline value, reflecting the expected downtime for each damage state. This baseline aligns with what PIANC and USACE define as a "Tier-2, standard-practice" port. The Port-specific MTTR denotes the level of performance that the port under study can realistically achieve, given its resilience measures and strategies. An RCF greater than 1 indicates that the port can recover more rapidly than an average port, whereas an RCF less than 1 implies slower recovery.

With this in mind, the grading rubric is adapted from (PIANC WG-174, 2022), which is based on the community resilience scale originally proposed by (Bruneau et al., 2003). The rubric consists of numerical scores (ranging from 1 to 5) assigned across four key resilience dimensions: robustness, redundancy, resourcefulness, and rapidity. As presented in Table 6.4, each score reflects the level of preparedness and strength of a seaport in each respective dimension.

Table 6. 4: The grading system for different resilience measures in seaports.

Score (per dimension)	**Qualitative meaning**	**Observable yardstick** *(PIANC WG-174, 2022)*
1	Minimal capability	Only statutory standards met; no formal contingency plan.
2	Basic	Contingency plan exists but no drills; limited spares; single-shift response.
3	Standard	Annual drills; basic mutual-aid MoU; 2-shift repairs possible.
4	High	Spare crane-boom on site; dual 11 kV feeder; 24 h repair roster; remote monitoring.
5	World-class	Redundant berth, mobile crane fleet, on-site parts depot, 72 h guaranteed OEM intervention, AI-enabled predictive maintenance, Redundant power micro-grid.

Based on Table 6.4 and the guidelines provided in (PIANC WG-174, 2022), each resilience score is associated with an expected repair-time multiplier. For instance, a score of 3 corresponds to "standard practice" (multiplier = 1.0), whereas a score of 4 or 5 yields a reduced multiplier, depending on the severity of the damage. These scores can be determined through various assessment methods, including site walk-throughs, document reviews, and stakeholder interviews.

To support the scoring process, evaluators may consider example questions such as: "Do we have a spare quay crane boom?", "Is there a dual fibre loop in place?", or "Is a 24-hour maintenance roster maintained?" These inquiries help assess the level of preparedness and inform the assignment of resilience scores. Table Ap.3 presents established resilience measures

applicable to various critical items, categorized according to the three resilience capacities and aligned with either high or world-class performance levels.

By applying this approach and assigning scores to the four identified resilience dimensions, different RCF values can be determined, based on the capability band assigned to a port. These RCF values are then used to derive a port-specific MTTR. This adjusted MTTR inherently reflects the influence of resilience strategies on damage severity, system downtime, and other hazard-related impacts. Table 6.5 presents the various capability bands to which a port may be assigned.

Table 6. 5: The indicative capability band for seaports.

Total score (Sum of the four 1-5 grades)	**PIANC capability qualitative band**
4-8	Low
9-12	Standard
13-16	High
17-20	World-class

It is important to note that minor or cosmetic damage is assumed to be addressed concurrently with the routine recovery of normal operations. As such, this level of damage does not significantly affect the overall availability or functionality of the port. Consequently, RCFs have been assigned only to DS2, DS3, and DS4, where the extent of damage is more substantial and has a measurable impact on system performance and downtime.

6.3.4 Seaport simulation model

6.3.4.1 Structure learning of the model

Terminal operations, particularly at container terminals, are characterized by tightly interconnected infrastructures, non-linear dynamics, and complex workflows involving continuous interactions between human operators, technological systems, and organizational processes.

From a structural perspective, a container terminal can typically be divided into three main sections: the quay side, yard side, and land side. Each section encompasses specific types of equipment and facilities that support the handling, movement, and storage of containers.

- Quay Side: This area facilitates ship-to-shore operations. Key equipment includes:
    - Quay cranes (ship-to-shore cranes)
    - Berths and fenders
    - Mooring facilities
    - Buffer platforms
    - Terminal trucks (prime movers)

    - AGVs (Automated Guided Vehicles)
    - Straddle carriers (sometimes used at the quay for short transfers)
    - Supporting ICT systems (e.g., vessel traffic systems, terminal operating systems)
- Yard Side: The yard serves as a temporary storage area for containers between ship and gate or rail. It typically includes:
    - Rubber-Tyred Gantry (RTG) cranes or Rail-Mounted Gantry (RMG) cranes
    - Reach stackers and forklifts
    - Straddle carriers (if used for stacking)
    - Container stacks and designated yard blocks
    - Reefer points (for refrigerated containers)
    - Yard tractors and trailers
    - Yard management systems
- Land Side: This area manages intermodal transfer of containers to and from the terminal via road and rail. It includes:
    - Truck gates and gatehouses
    - Weighbridges and inspection booths
    - OCR (Optical Character Recognition) scanners
    - Rail terminals and transfer cranes
    - External truck parking and staging areas
    - Customs inspection zones
    - Security checkpoints and smart access control systems

Figure 6.3 illustrates a simplified layout of a typical container terminal, structured around these three core zones. The port boundary in this configuration extends from the navigable waterways to the inland intermodal connection points, encompassing all superstructures involved in the loading, unloading, transfer, and temporary storage of goods.

Figure 6. 3: A typical container terminal configuration.

Although all three terminal sections, namely quay side, yard side, and land side are essential for the smooth functioning of container terminal operations, evidence from accident reports, scholarly literature, and the inherent nature of terminal workflows indicates that the quay side, particularly berthing operations such as loading and unloading, represents the most critical segment (Darbra and Casal, 2004; Geerlings et al., 2017; Kim and Park, 2004; Kizilay and Eliiyi, 2021; Majumdar et al., 2022; Sunaryo and Hamka, 2017). This is primarily due to its role as the interface between the maritime and landside domains, where complex coordination is required between large ocean-going vessels, quay cranes, and terminal transport systems. The sheer scale of the vessels involved, combined with the high density of operational activities and time sensitivity of port calls, further amplifies the operational and safety-critical nature of this zone.

Accordingly, this study concentrates on the quay side, with a particular emphasis on berthing and cargo-handling operations. Based on this focus, the simulation model developed in this study is specifically designed to capture the dynamics, constraints, and interdependencies characteristic of this vital terminal section.

The first step in simulation modelling is the selection of an appropriate modelling method, which serves as the foundational framework used to represent a container terminal within a computational environment. This method can be understood as a modelling language or a set of “rules” that guide how the elements, processes, and interactions of the actual system are abstracted and implemented in the model.

Three principal simulation methods are widely used: System Dynamics (SD), Discrete Event Simulation (DES), and Agent-Based Modelling (ABM). Each method operates at a different level of abstraction and is suitable for specific types of problems (Grigoryev, 2015):

- System Dynamics is suited for highly aggregated, strategic-level modelling and is often applied to systems characterized by feedback loops and accumulations over time (e.g., policy analysis or long-term planning).

- Agent-based modelling supports a broad range of abstraction levels and is typically used when individual behaviours and interactions of autonomous agents (e.g., vehicles, companies, or workers) must be modelled explicitly.

- Discrete event simulation, by contrast, is most appropriate for systems where operations unfold as a sequence of discrete events over time, and where individual entities (e.g., containers, trucks, cranes) interact with resources, queues, and processes.

Given the operational and process-driven nature of container terminal activities, DES is the most suitable method for this study. DES requires the modeler to conceptualize the system as a set of interrelated processes and events (Karnon et al., 2012; Robinson, 2005), such as the arrival of a vessel, the unloading of containers by quay cranes, the transport of containers by AGVs or trucks, and the storage and retrieval operations within the yard. These processes are characterized by:

- The competition for limited resources (e.g., cranes, yard space, trucks),

- Queuing behaviour (e.g., waiting for a crane or gate access),

- Delays and service times (e.g., loading and unloading durations),

- Sequential and branching operations (e.g., routing containers to different yard blocks based on availability).

The typical performance metrics generated from a DES model align closely with the key performance indicators in terminal operations, such as:

- Resource utilization (e.g., crane and yard equipment usage rates),

- Throughput (e.g., number of containers processed),

- Turnaround times (e.g., for vessels, trucks, or containers),

- Queue lengths and waiting times (e.g., at gates, cranes, or yard areas),

- Identification of system bottlenecks.

Therefore, DES provides a realistic and structured approach to modelling the complexity of container terminal operations, where events occur at discrete points in time, and resource allocation and process flow are central to overall system performance. This makes DES an ideal choice for developing a detailed, process-oriented simulation model of container terminal behaviour, which is the focus of this study.

To ensure the model is developed appropriately, a systematic and structured approach is adopted. This includes clearly identifying the input data, defining model assumptions, mapping the interactions between simulation entities, and determining the expected outputs. Figure 6.4 presents the flowchart of quayside operations, highlighting each critical entity involved in the simulation as part of the modelled system.

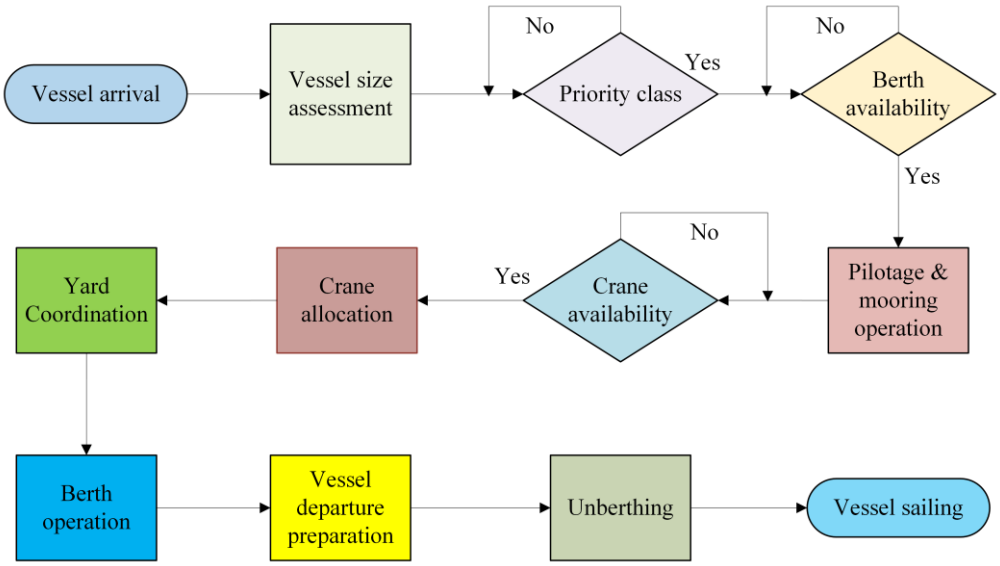

Figure 6. 4: Illustrative flowchart of quayside processes in a standard container terminal.

As shown in the figure, the arrival of vessels marks the starting point of the simulation, while vessel departure (sailing) represents the end point. Upon arrival, a vessel enters a queue of waiting ships. In real-world container terminals, vessel arrivals generally follow predefined schedules set by shipping lines and terminal operators. These schedules are relatively fixed and available in advance, making it possible to extract this data and feed it directly into the simulation model. This approach enhances realism and robustness, providing a more accurate representation of actual terminal operations than using arbitrary or fixed statistical distributions. However, it is important to note that terminals do not always follow a strict First-Come-First-Served (FCFS) policy for berth allocation. In practice, berthing decisions are influenced by a variety of operational factors, including service agreements, contractual obligations, vessel size and priority, and strategic scheduling. Incorporating these elements into the simulation allows for a more nuanced and realistic model, where different vessel types or service tiers may experience varying waiting times and resource access, better reflecting the complexities of real-world quayside operations.

The next step involves vessel size classification, where vessels are categorized based on key characteristics such as TEU capacity, length overall, draft, and other relevant operational parameters. This classification is critical for ensuring accurate modelling of berth assignment and crane allocation in the quayside operation simulation. Using TEU capacity as a standard metric enables the model to realistically reflect the differences in space and equipment requirements associated with various vessel classes, thereby enhancing the precision and reliability of the simulation results. Table 6.6 provides a standardized classification of container ships, organized by capacity and key operational characteristics (Rodrigue, 2024; UNCTAD, 2010).

Table 6. 6: Ship size classification.

Size Category	TEU Capacity (approx.)	Description	Real-world Examples

Feeder	< 1,000	Small ships operating on short-haul routes, typically connecting regional or smaller ports to mainline hubs.	MV Conmar Gulf (712 TEU)
Feedermax	1000-3000	Larger regional ships feeding from or to major ports, often used in intra-Asia routes.	MV Lantau Bridge (2702 TEU)
Panamax	3000-5100	Ships designed to fit the original Panama Canal locks, with specific beam and draft restrictions.	MV Sealand Washington (4246 TEU)
Post-Panamax	5100-10000	Too large for original Panama locks but commonly used in mainline services on key global trade routes.	COSCO Glory (8200 TEU)
New Panamax	10000-14500	Sized to fit through the expanded Panama Canal (post-2016), enabling higher volume transits.	MV MSC Cordoba (13000 TEU)
Ultra Large Container Vessel (ULCV)	>14500	Ultra Large Container Vessels are the largest ships, operating mainly on Asia-Europe routes.	HMM Algeciras (23964 TEU)

Once vessel sizing is finalized, the model proceeds to evaluate berth availability based on the vessel's length, draft, and the capacity and specifications of available berths, alongside predefined priority rules. When a suitable berth becomes available that matches the vessel's profile, it is allocated accordingly. This assignment process includes safety, and compatibility checks to ensure the selected berth can safely accommodate the vessel's dimensions and requirements.

Following berth allocation, the vessel undergoes pilotage and mooring, a critical stage during which a certified port pilot assists in safely navigating the ship to the designated berth. Once the vessel reaches the berth, mooring lines are secured, ensuring that the ship is safely and securely berthed. The duration of this stage can vary depending on factors such as vessel size, port layout, tidal conditions, and prevailing weather, particularly wind speed and direction.

After successful berthing, the next step is the allocation of quay cranes. If cranes are not immediately available, the vessel remains idle at the berth, contributing to quay crane idle time. Once assigned, the number of cranes allocated depends on several factors, including the vessel's classification, the number of containers to be handled, berth length, available crane fleet, and any contractual service level agreements. While initial assignments may follow standard guidelines (e.g., one crane per 50-55 meters of vessel length to avoid crane interference), actual deployment decisions often reflect operational constraints and dynamic terminal conditions. For instance, a 400-meter Ultra Large Container Vessel (ULCV) may typically receive 6-8 quay cranes, consistent with upper-quartile practices in major hub ports.

Once quay cranes are operational, the container exchange process begins. The duration of this operation depends on several key variables:

- The number of cranes assigned,
- Crane productivity rates, typically ranging from 30 to 45 container moves per hour,
- The total number of containers to be loaded and unloaded,

- The availability of horizontal transport, such as terminal trucks or AGVs,
- Yard capacity and the level of yard congestion.

Following the completion of loading and unloading activities, the vessel must be prepared for departure. This involves documentation checks, port authority clearance, disconnection of quay cranes, and, if required, the engagement of tugboats for safe manoeuvring. The unberthing process, including administrative and operational clearance, represents an additional source of delay and is not instantaneous.

Finally, the vessel departs the port, and the berth and quay cranes are released and returned to the pool of available resources, ready to be allocated to the next arriving vessel in the simulation process.

This sequence of events constitutes the overall logical framework of the quayside simulation in a seaport, capturing the essential processes, resource dependencies, and operational dynamics involved in vessel handling. To capture operational inefficiencies and enhance model realism, the simulation incorporates three primary types of delays that significantly affect overall port throughput and vessel turnaround time, both key outputs of the model, as shown in Table 6.7. These delays are treated as influencing variables and are systematically monitored and measured throughout the simulation period to assess their impact on terminal performance.

Table 6. 7: Types of Delays in Simulation Logic.

Berthing Idle Time (t_{db})	Definition	The delay between the time a ship arrives at the port and the time it is assigned to a berth.
	Calculation	Berthing Idle Time = Time of Berthing - Time of Arrival
	Cause	Caused by berth unavailability due to congestion or priority rules.
Crane Allocation Idle Time (t_{dc})	Definition	The delay between the time a ship is berthed, and the time loading/unloading begins.
	Calculation	Crane Allocation Idle Time = Start Time of Operation - Time of Berthing
	Cause	Occurs when cranes are unavailable or occupied with other operations.
Unberthing and Clearance Time (t_{du})	Definition	The time between the end of the loading/unloading process and the ship's actual departure.
	Calculation	Unberthing Delay = Time of Departure - End of Berth Operation
	Cause	Caused by administrative, operational, or physical delays in releasing the ship.

6.3.4.2 The validation procedures of the simulation model

A multi-faceted validation approach is adopted to ensure the reliability and robustness of the developed simulation model representing a typical container terminal. The following validation strategies are applied:

1) Face validation: The model structure, flow logic, and operational assumptions are reviewed by academic and industry experts with experience in maritime logistics and port operations. Their feedback confirms that the simulation flow,

including vessel arrival, berth allocation, crane operations, and container throughput processing reflect realistic port dynamics.

2) Literature-based parameter validation: Input parameters such as vessel inter-arrival times, quay crane efficiency, berth utilization, and vessel turnaround times are compared with the existing literature and port studies. The resulting outputs, such as average berth occupancy and crane usage rates, should be consistent with reported benchmarks for medium-to-large container ports.
3) Comparison with actual terminal records: To ensure the accuracy and reliability of the simulation model, its output, specifically, the predicted throughput (e.g., container movements, vessel handling times, and cargo processing rates) is rigorously compared against historical terminal operation records.
4) Sensitivity analysis: Key operational parameters (e.g., crane downtime, number of available berths, different idle times) are systematically varied to assess model responsiveness. Results should represent plausible system behaviour, such as proportional changes in throughput and recovery time, thereby confirming the model's internal consistency.

6.4 Case study

Kaohsiung Port, the largest seaport in Taiwan and a major transshipment hub in East Asia, plays a critical role in regional trade. Terminal 7, one of its most modern and busiest terminals, handles significant container volumes and features advanced infrastructure. This terminal is Taiwan’s first fully automated container terminal. Developed collaboratively by Evergreen Marine Corp. and Taiwan International Ports Corporation (TIPC), it features state-of-the-art automation technologies, including remote-controlled gantry cranes, unmanned rail-mounted gantry cranes (URMGCs), and integrated AI-driven systems. This terminal represents a significant advancement in Taiwan's maritime infrastructure, aligning with global trends toward smart port development. Its strategic location and high exposure to typhoons make it an ideal case for simulating cyclone impacts and assessing resilience in a real-world, high-risk operational environment. Table 6.8 presents technical details of Terminal 7 at Kaohsiung Port.

Table 6. 8: Technical information about Terminal 7 at Kaohsiung port (Port Technology International, 2024).

Entity	Description
Terminal 7	Geographical Area: Located in Kaohsiung, Taiwan: Latitude: 22.560112° N Longitude: 120.331185° E Total Area: Approximately 149 hectares.
Throughput	Annual: Current capacity of 4.5 million TEUs, with planned enhancements to reach 6.5 million TEUs. Monthly: Approximately with the capacity of 375,000 TEUs. Daily: Approximately with the capacity of 12,300 TEUs.
Berths	Number of Berths: 5 deep-water berths. Berth Capacity: Capable of accommodating up to four 24,000 TEU ultra-large container ships and two feeder vessels simultaneously. Draft: 18 meters. Length: Total quay length of 2,415 meters.
Quay crane	Automated: 19 out of 24 quay gantry cranes are remote-controlled. Speed: Each crane can handle 30-45 moves per hour.

	Capacity: Each crane can handle 25 rows of containers on deck; 16 cranes are 55.5 meters high.
AGVS or trucks	Number: No public information is specified. Estimated to be around 100-120 for this size of terminal. Capacity: Designed to handle standard container sizes efficiently. Reserve: Information not specified.
Yard crane	Number: 60 Automated Rail-Mounted Gantry Cranes. Capacity: Each crane has a lift capacity of 40 tons.
Electrical station	Equipped with a dedicated substation supporting full electrification of terminal operations, ensuring a peak power demand of approximately 10 megawatts.
IT services	Utilizes Evergreen's intelligent terminal operating system (EMCTOS), integrating 5G communication systems, optical fibre connectivity, Internet of Things (IoT) networks, Optical Character Recognition (OCR) technology, and real-time power consumption monitoring to enhance operational efficiency
Gates	Number: 24 smart gates. Capacity: Each gate is designed for automated processing to facilitate swift truck ingress and egress.

6.4.1 Data collection of terminal operations

Operational data were collected from Terminal 7 records covering the period from 1 August 2024 to 31 July 2025 (Shipmentlink, 2025). The dataset includes key information such as vessel name, arrival time, berthing time, and departure time. The collected data were systematically processed to classify vessels by size and estimate the number of containers to be loaded and unloaded. As shown in Figure 6.5, more than 2010 vessels visited the terminal during the study period, with the majority classified as feedermax vessels.

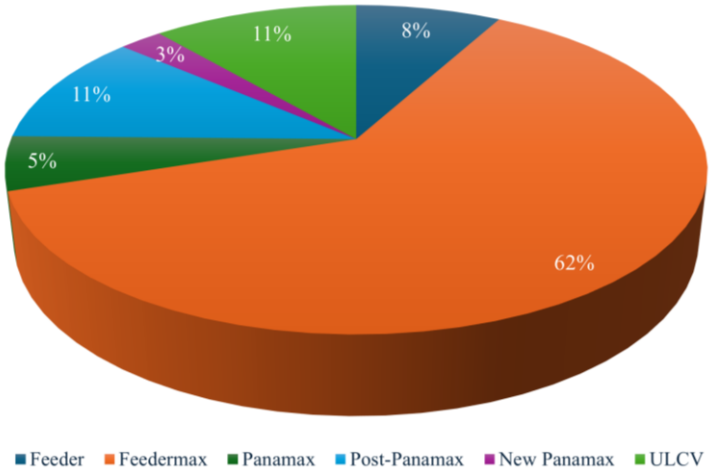

Figure 6. 5: Percentage of different vessel types visiting Terminal 7 of Kaohsiung port.

For each vessel category, key operational time components were analysed in detail: berthing time (which includes the time required for pilotage and mooring), operation time (the duration needed for loading and unloading containers), departure time (the time allocated for vessel preparation before leaving the terminal) and finally the turnaround time (the time between the vessel arrival and departure). Table 6.9 presents the statistical distribution summary derived from the collected data for various types of vessels that called at Terminal 7.

Probability distributions were fitted to each category based on observed patterns, enabling a more accurate characterization of their time behaviour. To obtain these statistical distributions, first, extreme observations were removed because vessel-time data occasionally include key-entry errors or very rare events that distort goodness-of-fit tests. Each dataset was trimmed with Tukey's rule as follows (Hoaglin et al., 2000):

$$Q_1 - 1.5d \leq x \leq Q_3 + 1.5d \tag{6.17}$$

where Q_1 and Q_3 are the first and third quartiles and $d=Q_3-Q_1$. The resulting samples retained more than 90% of the original records, so the fitted models still describe typical behaviour while allowing the most extreme outliers to be treated separately.

The cleaned data were then fitted to several standard duration distributions (normal, log-normal, gamma and Weibull-minimum). Parameters were estimated by maximum likelihood technique. To choose the best model, the Akaike Information Criterion (AIC) was computed (Guthery et al., 2003),

$$AIC = 2K - 2LnL \tag{6.18}$$

with k the number of parameters and L the maximised likelihood. The distribution with the lowest AIC minimises expected Kullback-Leibler information loss while discouraging over-parameterisation (Cover and Thomas, 2005).

Finally, goodness-of-fit was assessed with the Kolmogorov–Smirnov test (D'Agostino, 1986), in which:

a) $p>0.05$: no evidence against the model, so it is accepted.

b) $0.01<p\leq0.050$: borderline; useful but heavy tails or multimodality may remain.

c) $p\leq0.01$: poor fit; mixture or non-parametric alternatives should be considered.

Once the tests were conducted, only models with $p>0.05$ were retained as the final distributions.

This information provides valuable insights into the operational profile of the terminal, specifically, the types of vessels it accommodates, their arrival frequency, and the time they typically spend at berth. Such insights are instrumental for strategic planning, capacity management, and the development of realistic simulation models that reflect the actual conditions and operational demands faced by the terminal.

Table 6. 9: Statistical distribution for different types of vessels.

Vessel type	Berthing time (hr.)	Crane allocation time (hr.)	Operation time (hr.)	Departure time (hr.)	Turnaround time (hr.)
Feeder	Inverse-Gaussian (μ=2.74, Scale=1.214)+0.4	Weibull (k=1.92, λ=1.104)+0.35	Weibull (k=2.036, λ=17.094)+1.95	Gamma (k=2.288, θ=0.369)+0.3	Gamma (k=4.289, θ=5.445)

Feedermax	Inverse-Gaussian (μ=5.239, Scale=1.159)+0.5	Weibull (k=2.881, λ=1.332)+0.4	Gamma (k=4.282, θ=4.622)+2.0	Lognormal (μ=-0.127, σ=0.573)+0.2	Inverse-Gaussian (μ=0.26, Scale=115.987)+2
Panamax	Inverse-Gaussian (μ=2.082, Scale=1.445)+0.4	Lognormal (μ=0.101, σ=0.376)+0.45	Inverse-Gaussian (μ=0.126, Scale=155.932)	Lognormal (μ=0.108, σ=0.364)	Inverse-Gaussian (μ=0.124, Scale=210.64)
Post-Panamax	Inverse-Gaussian (μ=5.651, Scale=1.298)+0.55	Weibull (k=2.405, λ=1.25)+0.4	Gamma (k=7.052, θ=2.991)	Lognormal (μ=-0.05, σ=0.529)+0.25	Inverse-Gaussian (μ=0. 202, Scale=161.357)
New Panamax	Inverse-Gaussian (μ=6.877, Scale=1.438)+0.6	Inverse-Gaussian (μ=0.047, Scale=31.244)	Weibull (k=2.996, λ=43.597)	Gamma (k=15.905, θ=0.095)	Inverse-Gaussian (μ=0. 228, Scale=240.341)
ULCV	Inverse-Gaussian (μ=4.765, Scale=1.177)+0.5	Gamma (k=9.614, θ=0.164)	Gamma (k=4.657, θ=6.846)	Lognormal (μ=0.313, σ=0.331)	Inverse-Gaussian (μ=0. 229, Scale=182.853)

Based on the precise scheduling information, the collected operational data were compiled into a structured Excel file. This dataset includes detailed time stamps for vessel arrivals, berthing, and departures, which are essential for accurately modelling terminal activity. The organized data file was then integrated into the simulation model to replicate real-world conditions and assess the performance of quayside operations under actual scheduling scenarios.

6.4.2 Simulation model for terminal 7 of Kaohsiung port

Kaohsiung's brand-new Terminal 7 design is to keep four ultra-large 24000 TEU vessels alongside while still leaving room for two feeders, an arrangement made possible by splitting the central berth into sub-positions 3A and 3B. In fact, the first construction phase opened with Berths S5, S4 and S3B already in service, while Berths S1, S2 and the companion S3A came on-line in the second phase. To capture that physical layout, the AnyLogic DES model begins with the Excel-driven Source block that reads the real vessel schedule. Each spreadsheet row spawns a Ship agent carrying its call-size, class (Feeder through ULCV) and the time of its arrival. Because the spreadsheet preserves exact data, the model can be validated directly against terminal logs later.

Newly created ships flow into an anchorage modelled by a "Wait block" whose release condition is the Boolean function "isBerthAvailable()". "Wait" was chosen instead of a simple Queue because it can listen for a logical expression and wake all waiting entities the moment any berth becomes available.

Routing is handled by a five-exit "SelectOutput". The block evaluates berths in priority order, but contains a short Java snippet that treats Berth 3 as two 285-m "slots":

```
if (berth3_freeSlots == 2 && shipType == FEEDER) exit(3);   // pair of feeders
else if (berth3_freeSlots == 2 && shipType != FEEDER) {     // big ship
    berth3_freeSlots = 0;
    exit(3);
}
```

All other berths have a single slot, so one line of code keeps the special quay logic transparent and centralised.

Once a ship reaches its dedicated lane, the first task is to reserve the berth. A “Seize block” linked to a Berth X resource pool does just that; Berths 1, 2, 4 and 5 have capacity 1, while Berth 3 has capacity 2 to reflect 3A/3B. The Seize is immediately followed by a “MoveTo” so the agent can animate its own pilotage run. The block's speed parameter is derived from “agent.sailingSpeed”, and a brief mooring delay is added. The timing distribution assigned to each agent varies depending on the vessel type.

The model then simulates the loading and unloading process. A second “Seize block” taps a common resource pool of 24 STS units. The quantity expression “agent.nQCrequested” allows different vessels to request an appropriate number of cranes, as defined by a predefined distribution. On average, feeder and feedermax vessels normally request two cranes (with a maximum of three), Panamax vessels four, post-Panamax five, New Panamax six, and ULCVs up to eight., while the “Unit Seizure Time” field adds the travel and positioning delay as the crane drives from its parking spot to the ship. Quayside work itself happens inside a “Delay block” whose duration is computed as follows:

$$Delay\ time\ (Hour) = \frac{Container\ quantity}{number\ of\ cranes \times crane\ efficiency\ (MPH)} \tag{6.19}$$

where, Crane efficiency refers to the number of containers a crane can process per hour (moves per hour).

When loading and unloading finish, a “Release” returns the cranes, and the ship enters a brief customs/clearance “Delay”. At its end, a final “Release” frees the berth resource and flips the Boolean that will unblock the next waiting arrival. The agent then leaves through a “Sink” block.

Throughout the simulation, each resource pool, such as berths and cranes, maintains its own utilization statistics, while the timing blocks generate datasets that record ship turnaround times, berth throughput, and crane occupancy histories. While Figure 6.6 presents a schematic of the simulated Terminal 7 in the AnyLogic environment, Table 6.10 summarizes the key information for each simulation stage, providing justification for the selection of each block based on the corresponding phase of real terminal operations.

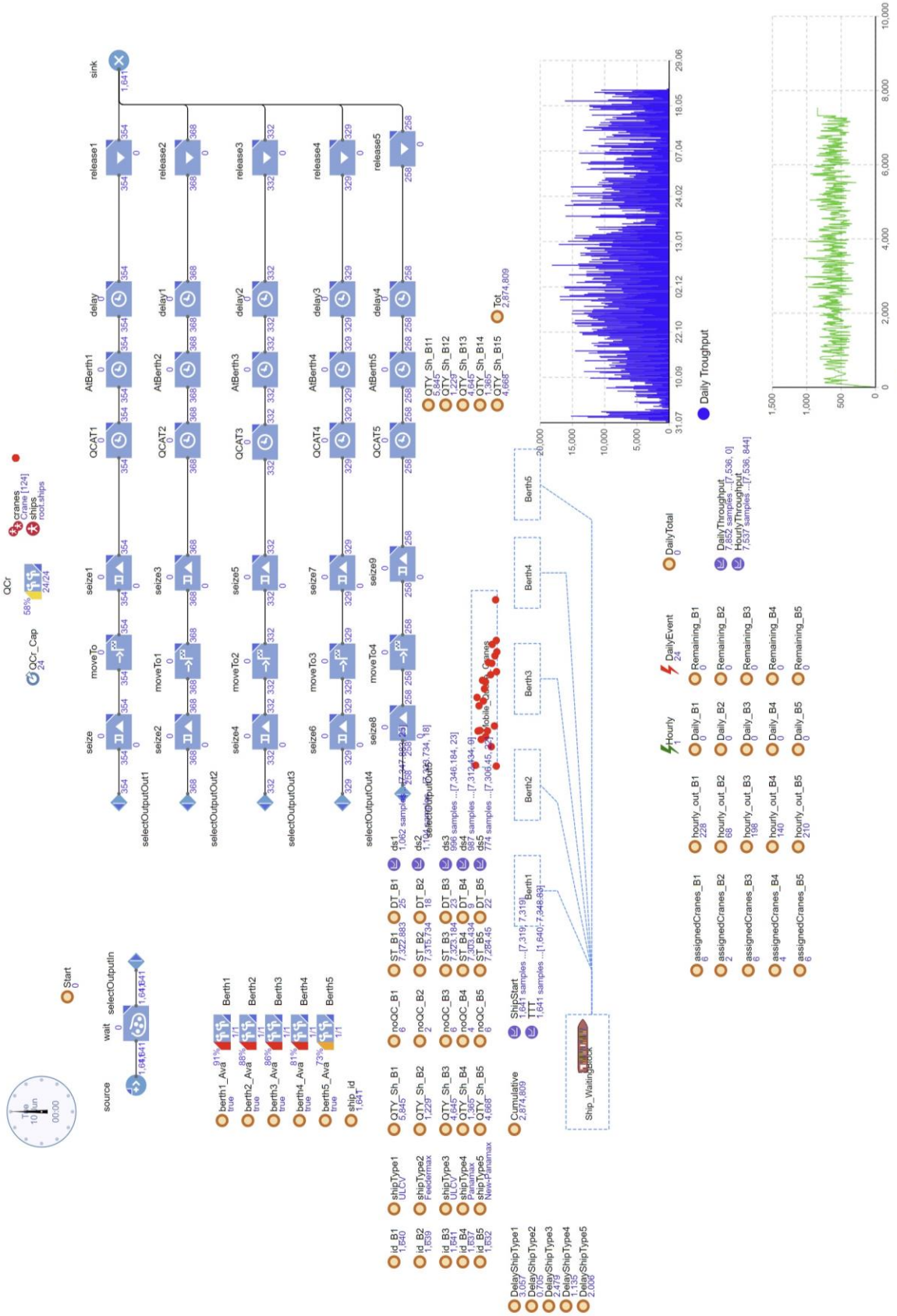

Figure 6. 6: Schematic configuration of DES blocks for the simulation of Terminal 7 in the AnyLogic environment.

Table 6. 10: The walk-through of the discrete-event model for Kaohsiung port's Terminal 7.

	Real-world concept	AnyLogic implementation	Notes
Data input & entity creation	Scheduled ship calls drawn from an Excel timetable that lists arrival time, service window, call size, number of containers, and ship class (Feeder → ULCV).	"*Source block*". "Arrivals defined by: Excel" is ticked, and the table is read with readTable("ShipSchedule.xlsx"). Each row becomes an agent of vessel type.	Vessel has attributes: "cat" representing vessel type, arrival_time, and "qty" representing the number of containers to be processed. These are populated in the on exit code of Source.
Berth occupation & pilotage / mooring time	Reserve the berth so nothing else can tie up there.	"*Seize block*". The block is linked to a resource pool called Berth1 (or 2, 3, 4, 5). Pool capacity=1 except Berth3.capacity = 2, matching the physical 3A + 3B layout.	The Quantity field is: shipType==FEEDER ? 1 : (berthId==3 ? 2 : 1) which forces bigger ships to grab both 3A & 3B at once.
	Pilotage, tug assist and mooring–the time from the breakwater to all fast.	"*MoveTo block*". Although a simple Delay could do, "*MoveTo*" lets the model animate the ship sailing down the channel and let speed vary by type.	Destination: point node at the berth's centre line
Crane assignment & cargo operation	Allocate quay cranes from the source pool of 24, based on vessel type.	Second *"Seize block"* in the lane. Connected to resource pool Quay_Cranes (capacity = 24). Quantity = agent.nQCrequested. Unit Seizure Time = distribution for cranes travelling from park + positioning on rails.	This models competition between berths for the same crane fleet, a major driver of berth productivity.
	Actual loading / discharging time.	*"Delay block".* Delay time = agent.qtycontainers / (agent.nQCrequested * craneEfficiency) so the block duration is endogenous, recalculated per vessel.	The crane efficiency is interpreted as move per hour, in which is sth between 30-40 MPH.
	Cranes leave the ship	*"Release block"* tied to Quay_Cranes.	Once the cranes are released, they join the resource pool for other missions.
Clearance, unmooring & departure	Customs clearance, documentation, tug fastening and departure.	Another "*Delay block"* with a triangular distribution (0.5 h, 1 h, 1.5 h) (example).	*Short stochastic delay reflects port variability.*
	Berth becomes available again.	Final *"Release block"* attached to the berth resource pool.	On exit action flips the Boolean berthX_Av = true, which in turn wakes the Wait block at the head of the line.
	The vessel departs simulation.	*"Sink block".* The vessels vanish at this point.	-

6.4.3 Tropical cyclones data collection and processing

In this study, the International Best Track Archive for Climate Stewardship (IBTrACS) database was used alongside the Typhoon Database Web Tool provided by the Central Weather Administration (CWA) of Taiwan (https://rdc28.cwa.gov.tw/TDB/public/typhoon_list) to identify and extract all tropical cyclones that have affected Kaohsiung Port over the past 30 years. IBTrACS, maintained by National Oceanic and Atmospheric Administration (NOAA), serves as a globally recognized repository that consolidates best-track data from multiple meteorological agencies, providing detailed records such as storm centre positions, wind speeds, and central pressures at six-hour intervals (Kenneth et al., 2019).

The selected 30-year timeframe (1995-2024) was chosen to enable a comprehensive and long-term assessment of historical cyclone activity, thereby facilitating a clearer understanding of the potential frequency and impact of such events in the future.

To conduct this analysis, the IBTrACS dataset covering the Western North Pacific region was downloaded for the period between 1995 and 2024. For each recorded cyclone, the centre position (at six-hour intervals) and the official peak 10-minute mean wind speed (Vmax) were extracted.

As described in previous sections, the wind speeds experienced at Kaohsiung Port were estimated using a multi-step approach. First, the Vincenty formula was applied to calculate the distance between the Kaohsiung Lighthouse and the eye of each cyclone.

Results indicate that 182 cyclones, irrespective of intensity or ring zone, passed within 400 km of Kaohsiung Port. Occurrence is strongly seasonal, peaking in July-August due to Kaohsiung's proximity to the highly active mid-summer Luzon Strait storm corridor, then declining in September as many tracks recurve northward and move away from Taiwan (Xue et al., 2023). The filtered cyclones, from both temporal and spatial perspectives, were derived using the CA and EW approaches and are illustrated in Figures 6.7 and 6.8. Among storms with wind assignment at their CA approach ring, Typhoon-class cases account for 34.5% overall. At very close range (≤100 km) that share drops to 16.7%; whereas within 0-200 km it rises to 29.2%. In practice, direct eyewall-strength conditions at the port are uncommon, suggesting that most close CA events are TD, TS, and STS at the port. Under the EW approach, high-end exposure in the Typhoon-class is most common in the 150-300 km belt. Even when the closest pass is not near the port, the outer wind field can still drive gales, and operational slowdowns. EW approach is therefore the appropriate lens for ring-based triggers (e.g., crane derating, berth limits) tied to distance thresholds.

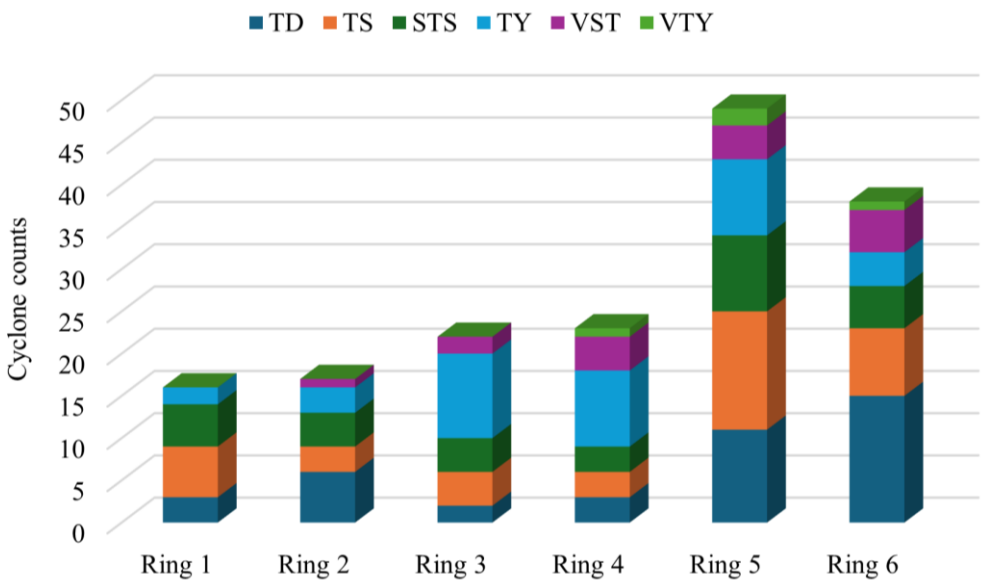

Figure 6. 7: The recorded cyclones in different distance rings based on CA approach.

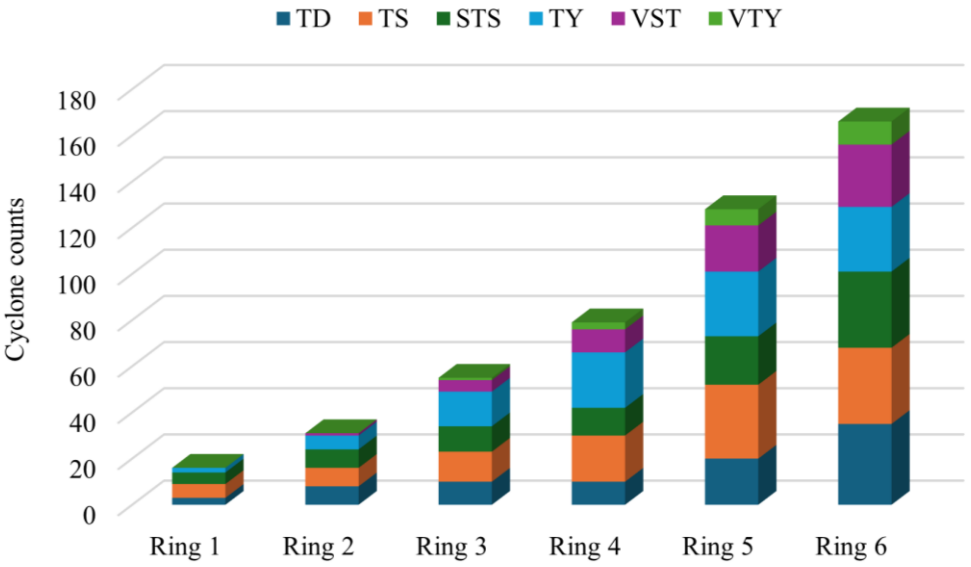

Figure 6. 8: The recorded cyclones in different distance rings based on EW approach.

The statistical analysis of cyclones affecting Kaohsiung Port from 1995 to 2024 reveals several important trends and insights as follows:

1) Seasonality and peak activity:
   The monthly distribution of cyclone occurrences highlights a strong seasonal pattern, with July and August accounting for the majority of events. This is primarily due to Kaohsiung's proximity to the Luzon Strait storm corridor, which is most active during the mid-summer months. Activity begins to taper off in September as many cyclone tracks begin to recurve northward, moving away from Taiwan. This seasonal

concentration indicates that port authorities should expect the highest operational risk and plan resource allocation accordingly during these peak months.

2) Intensity distribution and operational implications:
While less than 70% of cyclone encounters at the quay were categorized as TDs with wind speeds below 34 knots, the small subset of Typhoon-class events (64-83 kt) had a disproportionately large impact. The Typhoon-class encounters, accounting for just 35% of total events, are strongly correlated with berth closures and operational disruptions. Thus, although high-intensity storms are less frequent, they pose the most significant threat to terminal functionality and must be central to resilience planning and design-basis load assessments.

3) Interannual variability and climate signals:
The annual frequency of cyclones ranged from 3 to 13 events per year, with a coefficient of variation of approximately 0.32, indicating moderate interannual variability. Years with exceptionally high activity (e.g., 1997–1998, 2015–2016) coincide with El Niño events, a warm phase of the El Niño–Southern Oscillation (ENSO) characterized by anomalous sea surface warming in the equatorial Pacific that alters atmospheric circulation and storm tracks, shifting them westward. In contrast, La Niña years, representing the cold ENSO phase, such as 2010, are associated with reduced cyclone activity in the region. These patterns suggest that regional climate oscillations should be incorporated into long-term planning and probabilistic risk assessments for the port.

4) Spatial proximity and risk zones:
Spatial analysis of cyclone tracks shows that only 8% of all events penetrated the 0-50 km radius around Kaohsiung Port, representing direct hits with the highest potential for damage. In contrast, about 60% of cyclones remained within the 101-300 km range, aligning with the Luzon Strait “super-highway” where most storms pass without making direct landfall near the port. This spatial signal is vital for refining emergency preparedness strategies and determining when precautionary shutdowns may be warranted based on predicted storm proximity.

5) Gale force shutdown:
Kaohsiung Port’s Typhoon Command Centre (KPTCC) applies two wind thresholds, defined in terms of Beaufort scale gale forces, to determine when container terminal operations must be reduced or suspended. These operational requirements are specified in the Port of Kaohsiung Typhoon Evacuation Regulations, which apply to all classes of vessels. Table 6.11 outlines the two gale force thresholds along with their corresponding set-point criteria. It is important to note that the KPTCC permits terminals to resume operations, and reopens port entrances, only after on-site wind conditions have decreased to below Beaufort Force 5, and post-typhoon inspections of the quay, navigation channels, and aids to navigation have been successfully completed. Given these strict reactivation criteria, the duration distribution of each cyclone category near the port was analysed.

Table 6. 11: Gale force shutdown criteria at Kaohsiung port.

Trigger	wind speed	Actions taken in the container terminals
Gale force 5	34 Kt	• KPTCCL closes Harbor Entrances 1 & 2, halting all new vessel movements. • Ship-to-shore crane work and container loading/unloading are suspended for safety.

		• Preparations for typhoon mode begin; pilots and tugs stand down; port users alerted.
Gale force 7	55 Kt	• Full "gale-force shutdown": the KPTCC orders a blanket suspension of all sea- and land-side activity inside port limits, including yard, gate and rail operations. • Work at leased container wharves may continue only if the individual operator judges conditions safe and the KPTCC agrees. •Anchored or buoy-moored ships must clear out; larger container vessels already alongside are told to sail if time permits; emergency crews only remain on the quays

6) Top high-impact cyclones documented at Kaohsiung port

To validate the frequency and severity of significant cyclone events, Table 6.12 presents the most intense and high-impact cyclones recorded at Kaohsiung Port, along with the corresponding wind speeds measured by the port's monitoring systems. As the most recent example, Typhoon Krathon can be represented in the severe disruption it caused at Kaohsiung Port's Terminal 7. Between October 1 and 3, 2024, Krathon forced the terminal to suspend operations, no vessels docked for three days, as gale-force winds and storm warnings mounted. Krathon made landfall on October 3 with gusts up to Force 17 (Beaufort wind-force scale), scattering empty containers and inflicting minor deck and pavement damage, which required mobile cranes and inspection crews to clear debris and assess quay infrastructure. Although no gantry cranes or rail-mounted cranes suffered structural failure, potential saltwater intrusion in control cabins and corroded electrical panels demanded thorough testing. After safety checks and cleanup, the terminal resumed normal operations on October 4.

Table 6. 12: Record of the Most Intense and High-Risk Cyclones at Kaohsiung (1995-2024).

Year	Name	Distance (Km)	Wind at quay (Kt)	Class at port
1995	Kent	18	78	Typhoon
1996	GLORIA	16.2	78.2	Typhoon
2011	NANMADOL	29.2	67.1	Typhoon
2016	MERANTI	20.6	109.9	Violent Typhoon
2023	HAIKUI	20.6	78.7	Typhoon
2024	KRATHON	10.4	112.6	Violent Typhoon

6.5 Results and discussions

6.5.1 Simulation model under normal operation

Based on real data collected from Terminal 7 and their integration into the simulation model developed in Section 6.4, the output results were obtained and are presented in Table 6.13. The model was initially run under normal operational conditions using the actual data from terminal operations. As shown, the simulated throughput closely matches the actual throughput of Terminal 7, with a minor deviation of 0.1%, which falls within an excellent margin of error. Additionally, the number of vessels that visited the terminal during the study period (from 1 August 2024 to 31 May 2025) perfectly aligns with the number recorded in the operational logs, further confirming the reliability of the input data and model behaviour. Moreover, the average turnaround duration for all types of vessels visiting the terminal is comparable, with only a small, acceptable difference when compared to the average of the actual records.

Table 6. 13: Model validation through comparison.

Items	Actual data	Simulation data	Accuracy rate (%)
Container throughput (TEU)	3651186	3647709	99.9
Number of vessels	2014	2010	99.8
Average turnaround (Hour)	27.3	26.2	95.9

To verify and validate the model more thoroughly, the multi-faceted validation approach introduced in Section 6.3.4.2 was applied. The results are detailed as follows:

Firstly, as part of the face validation technique, the simulation model was presented to five experts with over 15 years of experience in seaport operations (Table Ap. 2 in the Appendix). All the experts unanimously confirmed the logical accuracy of the model from vessel arrival through to departure. Minor adjustments were suggested regarding berthing idle time and berth allocation rules, which were subsequently implemented in the model. Additionally, the logic for crane allocation, including the flexibility to share cranes between neighbouring berths was reviewed and enhanced based on experts' feedback. These refinements were incorporated into the final version of the model to ensure a more accurate representation of real-world operations.

From a literature perspective, the most critical parameters used in the developed simulation model were cross-checked against corresponding values reported in the literature for similar ports. As shown in Table 6.14, these parameters are consistent with values commonly found in previous studies, reinforcing the credibility and reliability of the inputs used in the model. This consistency indicates that the parameter selection is well-founded and that the model reflects realistic port operations. Consequently, the outputs generated by the simulation can be considered valid and aligned with established benchmarks in the field.

Table 6. 14: Parameter validation through literature review.

Parameter	Simulated model	Literature range	References
Vessel inter-arrival time (h)	4-8	3-10	*(Kuo et al., 2006; Lai and Shih, 1992)*
Average berth utilization (%)	77	60-85	*(Notteboom et al., 2021)*
Average Vessel turnaround time (h)	25.7	20-35	*(Notteboom et al., 2021)*
Quay crane productivity (MPH)	30-40	25-45	*(Achterkamp, 2019)*
Average daily throughput (TEU)	8500	7000-12000	*(Choi et al., 2022)*
Average pilotage and mooring duration (h)	1.8	0.5-2	*(Abou Kasm et al., 2021; Wu et al., 2020)*
Average crane allocation duration (h)	1.6	0.5-2	*(Al-Dhaheri et al., 2016; Bierwirth and Meisel, 2010)*
Average clearance and departure process duration (h)	1.5	1-3	*(International Taskforce, 2019)*

Finally, the last validation technique applied was sensitivity analysis. The three most critical variables in the simulation model were selected for this purpose. As shown in Table 6.15, two different values, one below and one above the baseline, were chosen for each selected variable. The model was then run separately for each scenario to observe its response to changes in

individual parameter values. It should be noted that the analysis period covers only a month of the whole collected data, allowing the model flexibility to account for fluctuations in logistics and throughput levels.

The results of these simulations are presented in Figures 6.9, 6.10, and 6.11. It is evident that the model exhibits proportional behaviour in terms of quay crane utilization rate, level of throughput, and the number of vessels it processes. As the values of the critical variables increase or decrease, these variables' levels correspondingly rise or fall. This response confirms the logical consistency and robustness of the model, demonstrating that it reacts appropriately to changes in key operational inputs.

Table 6. 15: Sensitivity analysis logic.

#	Sensitivity Scenario (SS)	Low	Base	High
SS1	Number of quay cranes	19	24	29
SS2	Quay crane efficiency (MPH)	25-35	30-40	35-45
SS3	Number of berths	4	5	6

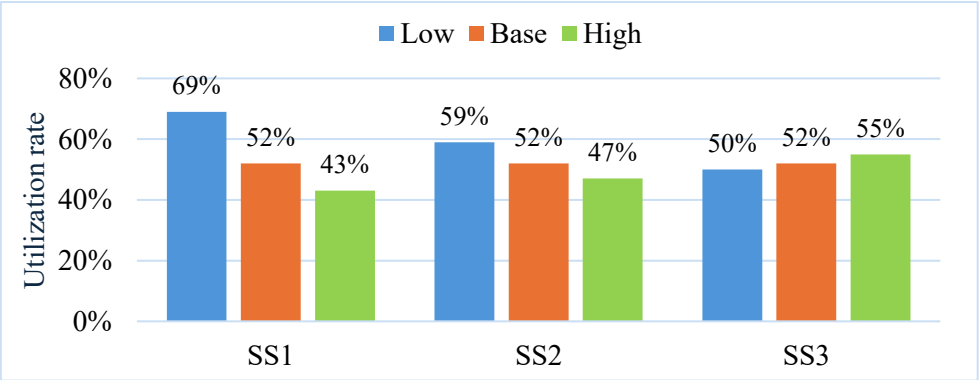

Figure 6. 9: Sensitivity analysis based on crane utilization rate.

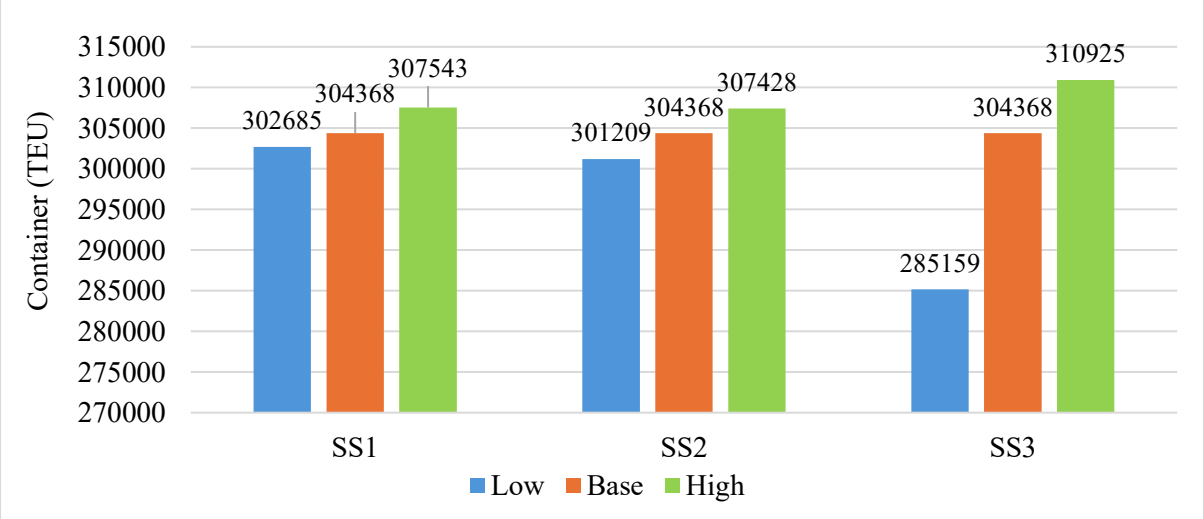

Figure 6. 10: Sensitivity analysis based on terminal throughput.

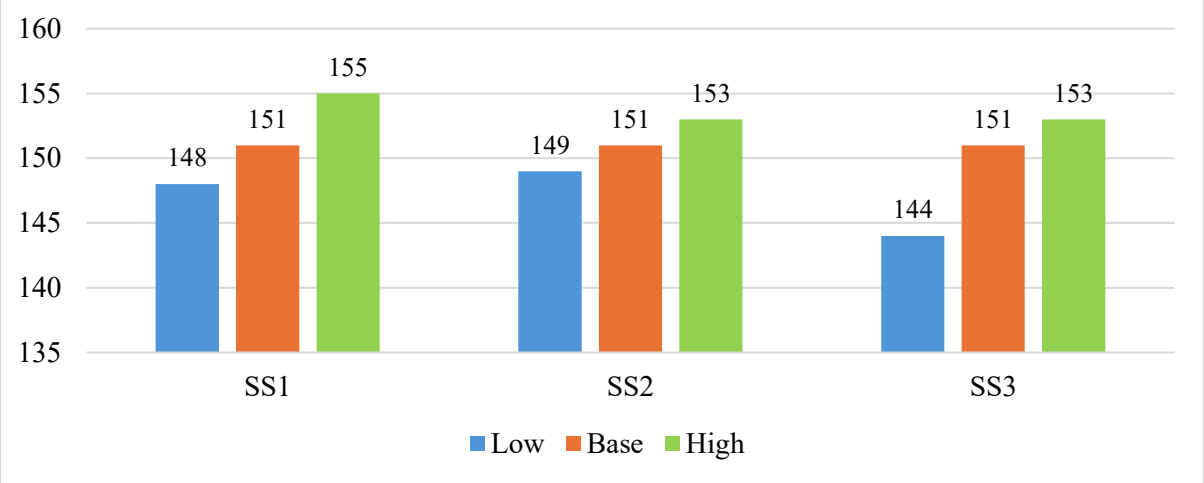

Figure 6. 11: Sensitivity analysis based on the number of vessels.

6.5.2 Estimation of Physical Damage Probability

To estimate the probability of cyclone-induced damage states, fragility curves are developed. Quay cranes are pivotal to terminal operations and particularly susceptible to high winds due to their height, structural complexity, and exposed components. Accordingly, parameter values for the lognormal fragility functions were derived from published technical documents and relevant case studies. Table 6.16 summarises the adopted values and their justifications, and Figure 6.12 presents the resulting fragility curves for all quay-crane damage states.

Table 6. 16: The quay crane fragility parameters.

Damage state	θ (m/s)	β	Objective basis	Reference
DS1	25	0.30	Minor, non-structural effects are expected a bit above the operational stop. The "gale" begins 17-19 m/s, where slight non-structural damage first appears; choosing 25 m/s centers DS1 above the near-gale band (no throughput impact).	*(Bhimani and Soderberg, 2006; European Committee for Standardization (CEN), 2014; Han and Han, 2011; Hoite et al., 2018; Kang and Lee, 2008; Kim et al., 2004; Konecranes, 2024, 2021; Lee and Kang, 2008; Liebherr Container Cranes, 2025; McCarthy et al., 2009; PEMA, 2019; Wu et al., 2022)*
DS2	30	0.30	Operational cut-off for quay cranes handling is consistently ~18-22 m/s mean; PEMA recommends 18-19 m/s and OEMs list 20 m/s "in-service" wind. DS2 Makes moderate physical damage clearly higher than DS1 and comfortably below stowed design winds, hence the median is set at 30 m/s quite above the tight 18-20 m/s band.	
DS3	50	0.30	OEM out-of-service/stowed design winds bracket 42-60 m/s (e.g., Liebherr at 42m/s, and Konecranes at 60m/s). Case histories (e.g., Typhoon Maemi crane failures) also occur in	

			this band. Picking 50 m/s places the median slightly above the lower OEM design value to represent the onset of localised structural failures across different designs/sites.	
DS4	60	0.30	DS4 is Governed by tie-down exceedance. Liftech recommends rare-event criteria: 7% in 50 yr for cranes, 3% in 50 yr for tie-downs. Taiwan typhoon extremes for 10-min means span 48-76 m/s across RP bands, and OEM lists 60 m/s stowed. Setting θ=60 m/s centers DS4 within the credible collapse/overturning range.	

As shown in Figure 6.12, all curves exhibit the characteristic sigmoidal form of cumulative distribution functions, which indicate near-zero probabilities at low wind speeds, a rapid transition zone, and saturation near unity. DS1 displays a relatively broad transition, reflecting failure of minor attachments and cladding over a range of winds. DS2 also follows a similar trend, consistent with a procedure-driven operational shutdown; once winds approach the in-service limit, exceedance probability increases rapidly. DS3 initiates at substantially higher winds, consistent with the onset of damage to stowed cranes near or above the lower bound of out-of-service design winds, particularly under adverse configurations. DS4 is the rarest port shutdown state, triggered when extreme winds exceed the tie-down capacity of cranes. Although a tail event, its risk remains material for cyclone-exposed ports.

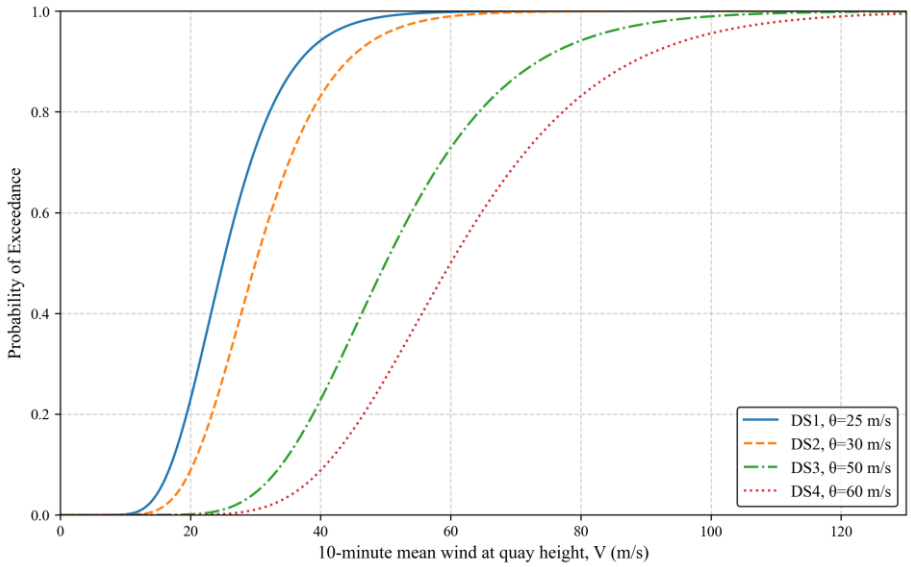

Figure 6. 12: The developed fragility curves for quay cranes.

To characterise fragility-parameter uncertainty and assess model robustness, a sensitivity analysis was performed. The perturbations were applied to the lognormal fragility parameters for each damage state, and the results are shown in Figures 6-13, 6.14, 6.15, 6.16.

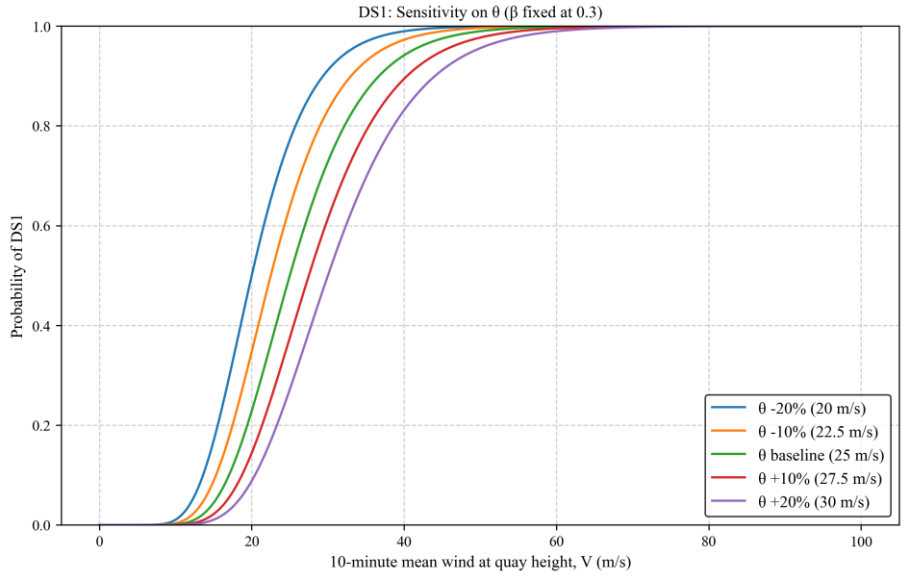

Figure 6. 13: Sensitivity analysis of DS1 with respect to θ.

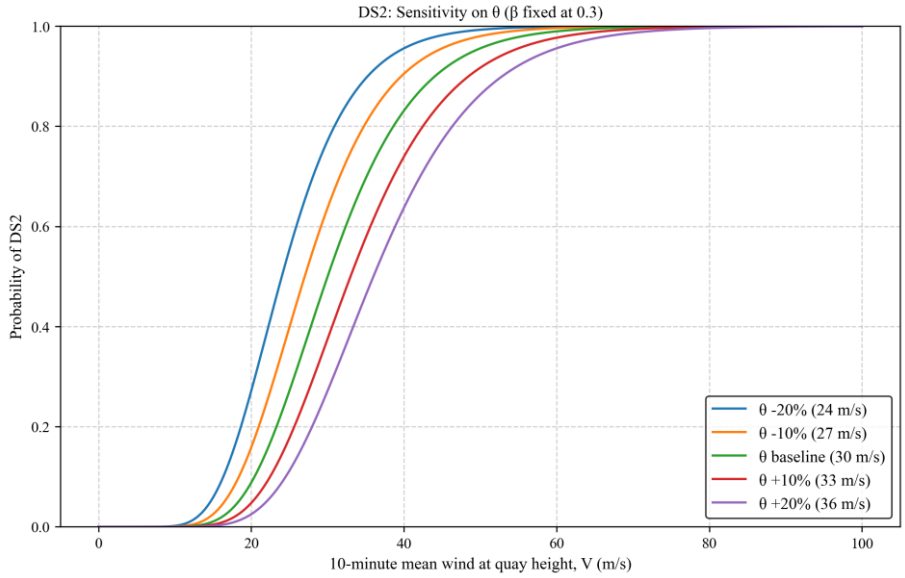

Figure 6. 14: Sensitivity analysis of DS2 with respect to θ.

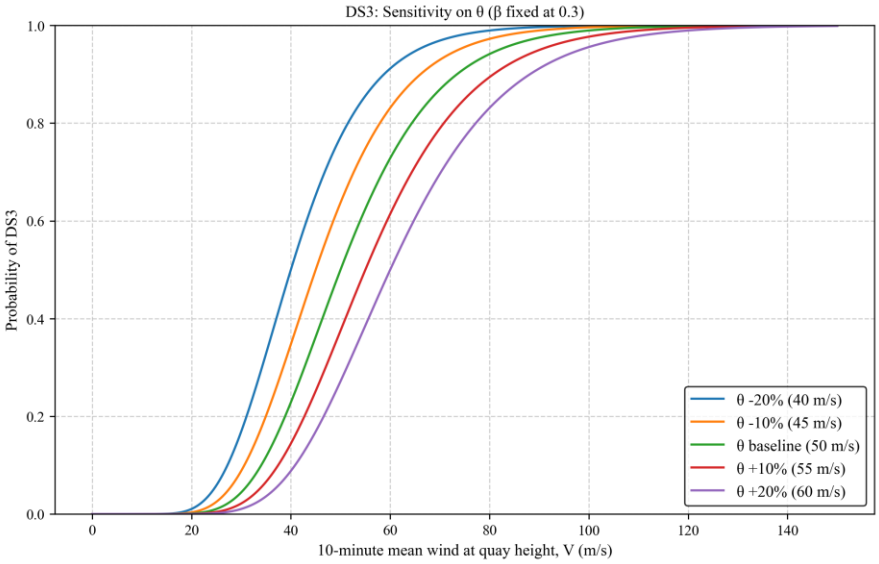

Figure 6. 15: Sensitivity analysis of DS3 with respect to θ.

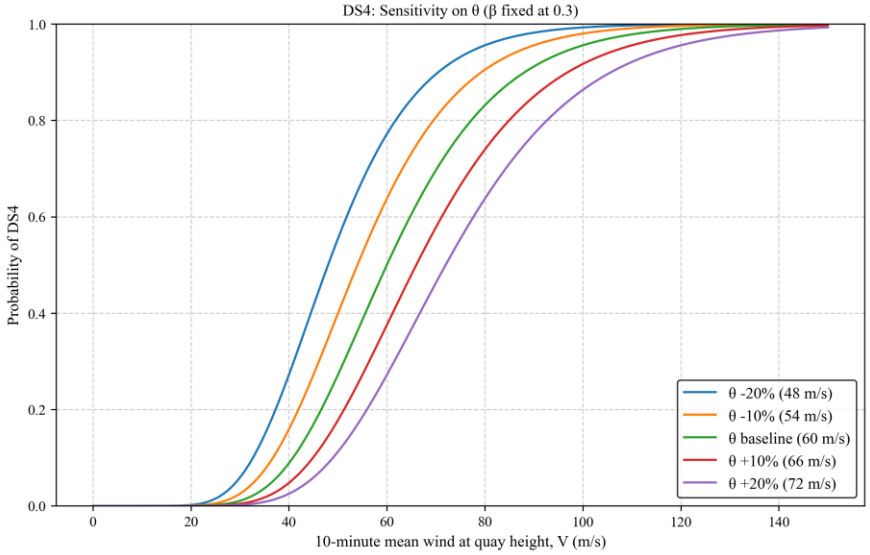

Figure 6. 16: Sensitivity analysis of DS4 with respect to θ.

Varying the median θ translates each curve horizontally without changing its shape. By construction, a 10% increase in θ shifts the 50% exceedance wind towards the higher speeds. This behaviour is evident in Figures 6.17, 6.18, 6.19, 6.20, where each damage state's baseline is bracketed by the ±10% θ curves.

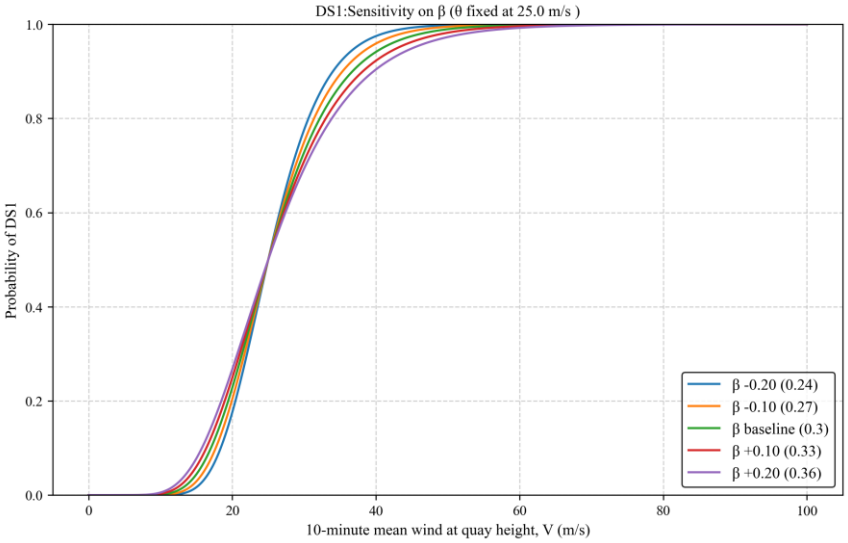

Figure 6. 17: Sensitivity analysis of DS1 with respect to β.

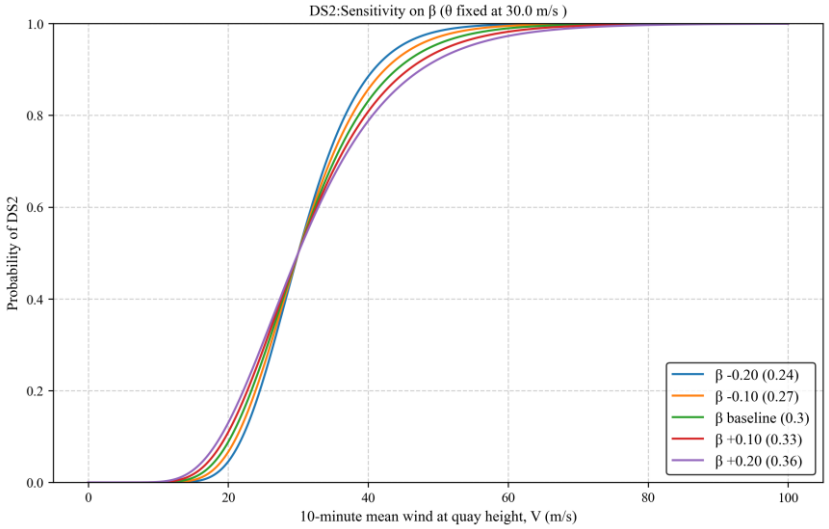

Figure 6. 18: Sensitivity analysis of DS2 with respect to β.

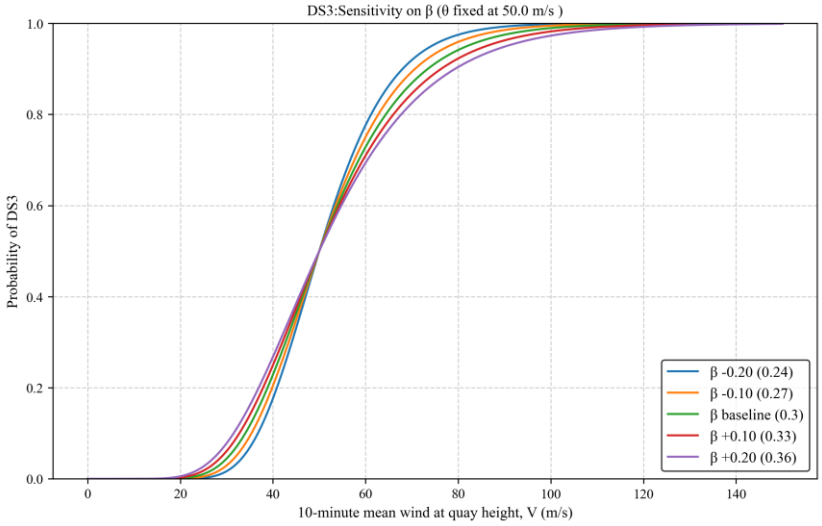

Figure 6. 19: Sensitivity analysis of DS3 with respect to β.

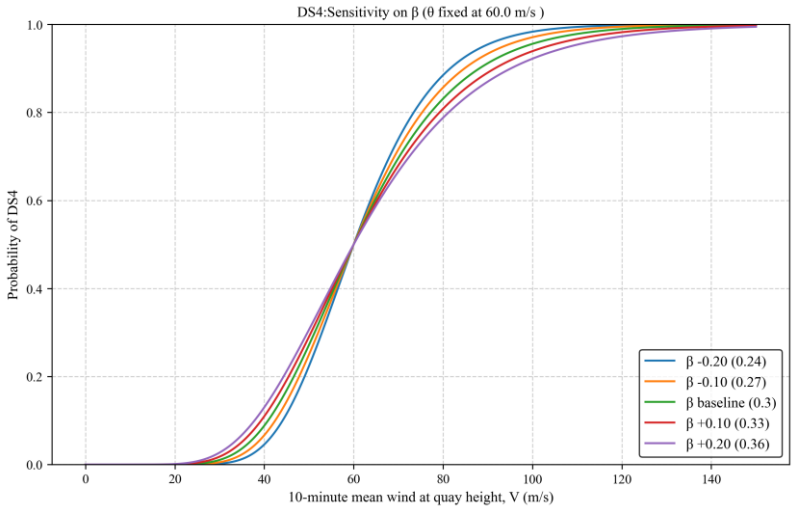

Figure 6. 20: Sensitivity analysis of DS4 with respect to β.

Varying the dispersion β affects only the transition width, in a way that larger β flattens the curve, smaller β steepens it. Quantitatively, the 10-90% transition ratio equals exp(2.563 β). Thus, as an example, DS4 (β=0.25) spans nearly 1.9 times the wind speed between the 10% and 90% exceedance points, whereas DS4 (β=0.30) spans approximately 2.2 times the wind speed.

Within the Kaohsiung wind range, the higher damage states (DS3-DS4) are more sensitive to both parameter types than lower damage states, because DS1-DS2 are essentially saturated (exceedance≈1.0) at V_{10}≈50 m/s, so local parameter variations have minimal effect.

Having derived the fragility curves, and the samples of wind speed at the port site, the probabilities for each damage state are then extracted. To account for the combinatory effect of all damage states and the uncertainty in the calculations, the obtained probabilities were incorporated into a Monte Carlo event model. In each trial, the vector (N_2, N_3, N_4) was drawn from a multinomial distribution with the equivalent parameters (P_2, P_3, P_4). Finally, running

10,000 Monte Carlo trials produced an empirical probability distribution, with the 5th, mean, and 95th percentiles. This procedure was applied to each of the remaining scenarios, yielding the corresponding values. Figure 6.21 illustrates the probabilistic damage profile of quay cranes exposed to six cyclone intensity classes, across five concentric ring-zones (R1-R5) measured outward from the quay. For every class the green solid curve depicts the mean damage probability, bounded by the 5th-percentile (blue dash) and 95th-percentile (red dash) envelopes, conveying modelling uncertainty. Within each class the curves peak at R1 and decay monotonically toward R5, confirming that equipment nearer the storm's core is more vulnerable. As intensity increases, the crest in each ring zone rises sharply: the mean probability at R1 grows from roughly 15 % for a TS to about 90 % for a VTY, while even outer-ring exposure under a violent typhoon rivals inner-ring losses for weaker storms. The worst-case scenario is a violent typhoon striking ring-zone 1 with maximum damage probability.

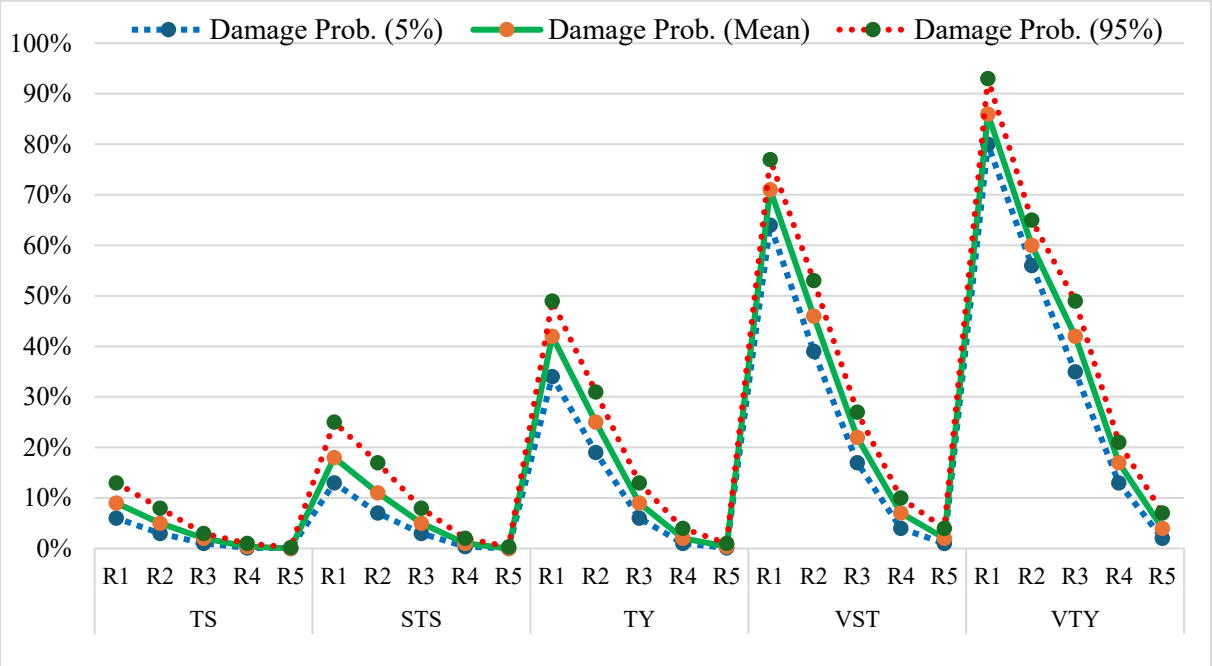

Figure 6. 21: The damage probability for different cyclone scenarios.

Figure 6.22 highlights a clear relationship between cyclone intensity, spatial exposure, and damage likelihood, offering a robust representation of hazard impact escalation across zones and damage levels. The bar chart illustrates the probability distribution of three damage states, DS2 (moderate damage), DS3 (extensive damage), and DS4 (complete damage), across varying intensities of cyclones, ranging from tropical storms to violent typhoons, and different ring zones (R1 to R5), which represent proximity to the cyclone's centre.

Across all cyclone categories and ring zones, the probability of experiencing DS2 consistently surpasses that of more severe damage states, followed by DS3 and then DS4. This hierarchy aligns with expectations, as higher damage states naturally occur less frequently. The chart also clearly demonstrates a proportional increase in damage probabilities with increasing cyclone severity. For instance, in the innermost ring R1, violent typhoons exhibit the highest DS2 probabilities, reaching up to around 80%, while DS3 and DS4 also show noticeable increases compared to weaker cyclones. Moreover, this trend is spatially coherent: inner rings (R1-R3),

being closer to the cyclone's core, exhibit significantly higher damage probabilities than outer zones (R4-R5), especially under stronger cyclone categories.

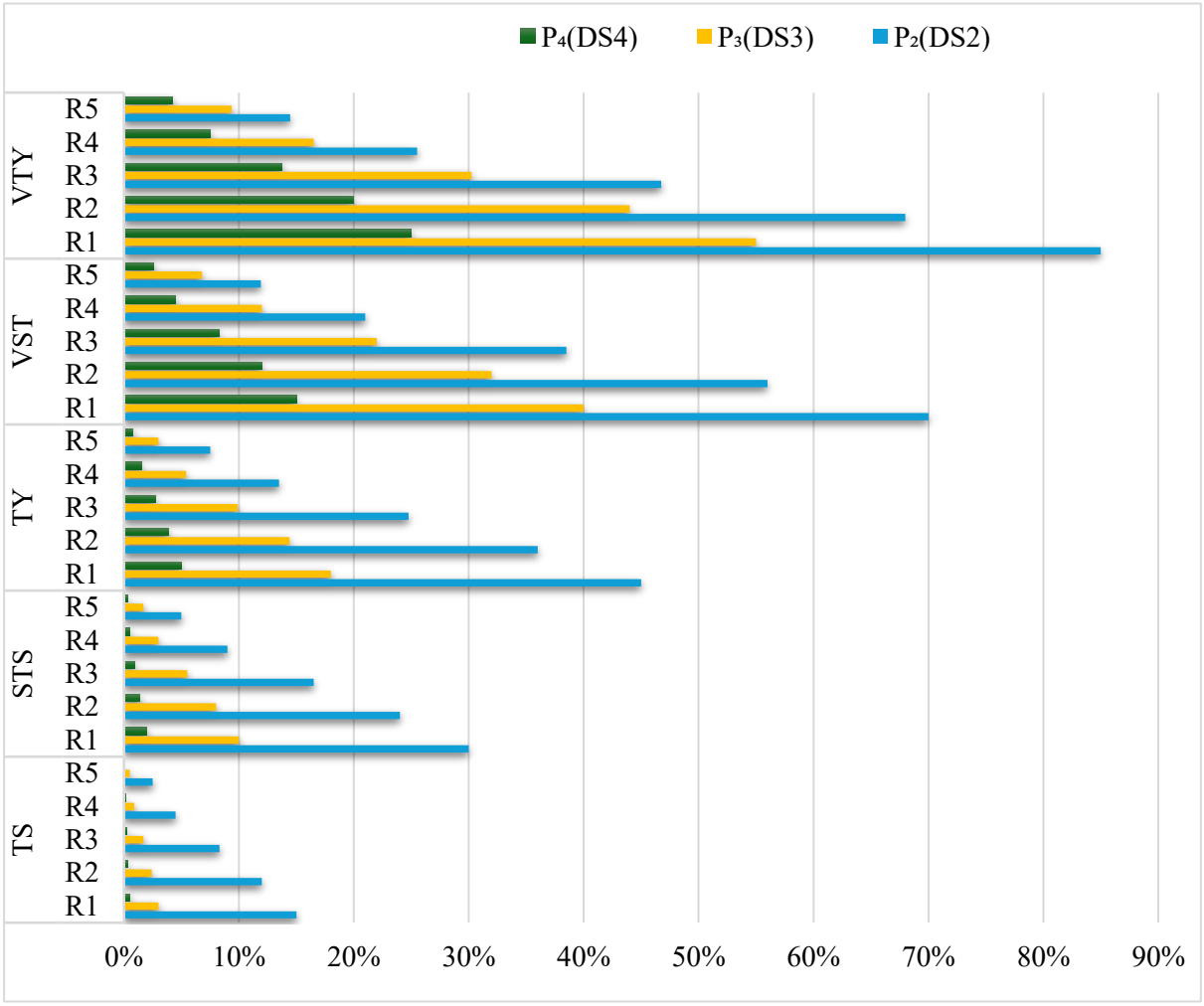

Figure 6. 22: Damage state probabilities across cyclone intensities and ring zones.

The expected downtime for each damage state is expressed as a baseline mean time to recovery (MTTR). This baseline represents standard operating conditions: normal spare-parts availability; at least one heavy-lift contractor on call; no prearranged mutual-aid cranes; and repairs performed during regular weekday working hours. This scenario aligns with what USACE (USACE, 2019) define as a “Tier-2, standard-practice” port. Deviations from this baseline, whether due to better preparedness or more constrained conditions, will generally cause downtime to scale down and up, respectively.

Recovery durations are usually provided as realistic ranges, reflecting the inherent uncertainty due to varying parameters such as event intensity, cascading effects, preparedness, budget constraints, and severity of damage consequences. Rather than exact values, ranges offer a better practical understanding of potential downtime. For this reason, the restoration curves were developed using the HAZUS restoration functions for port system components, modelled as normal distributions (FEMA, 2024b). The means and standard deviations of these functions as well as the discretized restoration probabilities are provided in Table 6.17, and Figure 6.23 presents the corresponding restoration curves for all damage states.

Table 6. 17: Quay crane restoration curve parameters (FEMA, 2024b).

Damage state	Distribution parameters		Discretized recovery probability (%)					
	Mean (days)	Std (days)	1 day	3 days	10 days	30 days	60 days	90 days
DS1	0.4	0.35	96	100	100	100	100	100
DS2	6	6	20	31	75	100	100	100
DS3	30	30	17	18	25	50	84	100
DS4	75	55	9	10	12	21	39	62

As shown in Figure 6.23, the HAZUS-based restoration curves convert uncertainty into time-bound probabilities of recovery. These curves are modelled as cumulative distribution functions, using the specified means and dispersions to yield percentile restoration dates. For quay cranes, a unit in DS2 has a 75% probability of being restored within 10 days, reflecting primarily repairable mechanical/electrical faults and limited structural remediation. DS3 requires more extensive interventions, including component replacement, alignment, and testing, so the probability of recovery reaches 84% only by about two months. DS4 represents toppling or near-total structural failure; recovery is dominated by procurement and installation of a replacement crane, permitting, and specialised contractor availability. The whole process may even exceed a year.

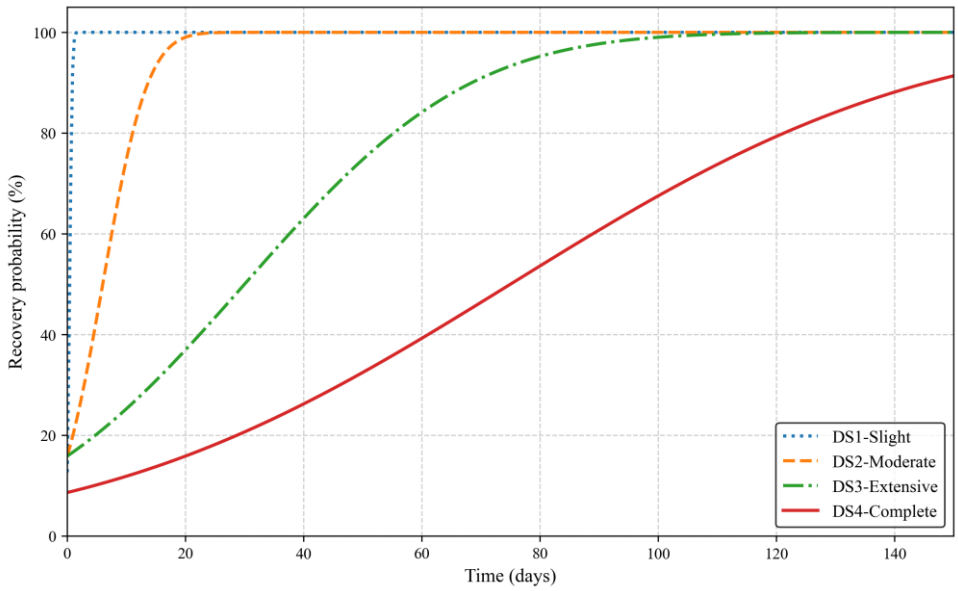

Figure 6. 23: The quay crane restoration curve.

It is to be noted that under a cyclone-wind-only scope and the quayside of the terminal, the only critical-path asset for which four structural damage states can be credibly defined and parameterised is the quay cranes. For the other items on the critical path, either hydrodynamic actions (surge, waves, currents, inundation) dominate physical damage, or the governing mechanism is administrative closure rather than structural failure. As a result, a wind-damage fragility curve development for those assets would therefore be physically misleading. Accordingly, we model each non-quay crane item as a functional node driven by a wind-triggered unavailability event and a restoration-time distribution followed by (FEMA, 2024a; PIANC, 2020).

6.5.3 Estimation of throughput and economic losses

This section presents the results of throughput loss and its corresponding economic impact across various cyclone categories, evaluated within five defined concentric impact zones (rings). Building on the damage state probabilities derived in the previous section, the quantities of critical path infrastructure components, such as quay cranes, berth equipment, power systems, and IT systems, are estimated for each damage state. These estimates serve as key inputs for the simulation model used to assess potential throughput disruptions.

Once these damage state probabilities are integrated into the simulation, the model calculates both the absolute throughput loss and the loss ratio (i.e., the ratio of lost throughput to the pre-disruption or intact throughput) for each scenario. These results are summarized in Table 6.18.

It is important to note that the recovery process in all simulations is based on a baseline recovery policy, commonly referred to as the standard RCF, which represents typical or average post-disaster recovery conditions.

Table 6. 18: Estimated throughput loss for various cyclone classes at different strike distances (RCF=Standard).

Cyclone class	Output	Strike Distance					
		Ring 1	Ring 2	Ring 3	Ring 4	Ring 5	Ring 6
TS	Processed TEU	3635746	3639253	3643173	3647709	3647709	3647709
	Loss ratio	0.33%	0.23%	0.12%	0	0	0
	Rerouted vessels	6	4	2	0	0	0
STS	Processed TEU	3624712	3633960	3640823	3646539	3647639	3647709
	Loss ratio	0.63%	0.38%	0.19%	0.03%	0	0
	Rerouted vessels	12	5	3	1	0	0
TY	Processed TEU	3581303	3615454	3638650	3644229	3647337	3647709
	Loss ratio	1.82%	0.88%	0.25%	0.10%	0	0
	Rerouted vessels	32	14	5	2	0	0
VST	Processed TEU	3517662	3555321	3592254	3632604	3641829	3647709
	Loss ratio	3.57%	2.53%	1.52%	0.41%	0.16%	0
	Rerouted vessels	68	41	25	7	3	0
VTY	Processed TEU	3421385	3484402	3551222	3593077	3625281	3643791
	Loss ratio	6.21%	4.48%	2.65%	1.50%	0.62%	0.11%
	Rerouted vessels	117	75	41	23	8	3

The results represented in Figures 6. 24, and 6. 25, reveal a consistent and intuitive relationship: as the strike distance decreases (i.e., from Ring 6 toward Ring 1), the throughput loss increases across all cyclone classes. This pattern is clearest in the case of Ring 1, which consistently results in the highest container throughput loss, both in absolute terms (TEUs) and as a

percentage of annual throughput. The severity of the cyclone intensifies this impact, further amplifying the losses in shorter strike distances.

In the worst-case scenario, corresponding to a VTY impacting within Ring 1, the terminal experiences a throughput loss of 226324 TEUs, which accounts for 6.21% of the terminal's annual capacity. This is the highest loss figure across the dataset, highlighting the catastrophic operational consequences of close-range, high-intensity cyclone strikes. In comparison, a VTY at Ring 5 results in a loss of only 22428 TEUs (0.62%), indicating a nearly tenfold reduction in losses when the storm strike distance increases from Ring 1 to Ring 5.

A similar trend is observed in the VST and TY categories, where Ring 1 losses are 130047 TEUs (3.57%) and 66406 TEUs (1.82%), respectively. In contrast, for TS and STS, the overall impact is relatively modest, with the highest losses (Ring 1) being 11963 TEUs (0.33%) and 22997 TEUs (0.63%), respectively. This shows that not only distance but also storm intensity significantly governs the extent of disruption.

Notably, the data also suggest that beyond Ring 3, throughput loss drops sharply, especially in weaker storm categories, becoming almost negligible in Ring 5 (the farthest zone). In TS and STS cases, loss ratios in Rings 4, 5, and 6 are effectively zero. Even in the most severe VTY events, the throughput loss in Rings 5 and 6 is significantly lower than in inner rings, suggesting the outer reach of tropical cyclone impacts, while not zero, is much less disruptive to port operations.

In the simulation, a 36-hour waiting time threshold was also applied to manage congestion by rerouting vessels that would otherwise face excessive delays. Figure 6.26 shows the estimated number of rerouted vessels per cyclone scenario and strike distance. As expected, the number of rerouted vessels increases with storm severity and proximity. In the VTY scenario, 117 vessels were rerouted within ring zone 1, where disruption was most severe. This number decreased to 75 and 41 vessels in rings 2 and 3, respectively, reflecting the reduced impact further from the storm centre. A similar pattern is observed across other cyclone categories, with fewer reroutes in outer rings. This indicates that the rerouting mechanism effectively mitigates congestion while aligning vessel diversion rates with the scale of throughput loss and storm intensity across varying strike distances.

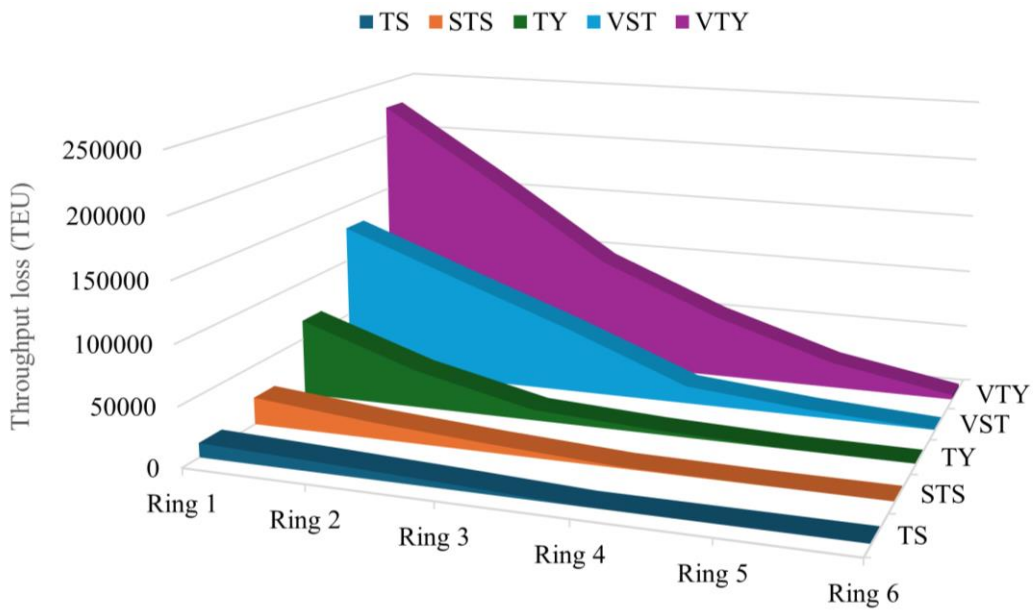

Figure 6. 24: The throughput loss due to cyclone intensities at varying strike distances (TEU).

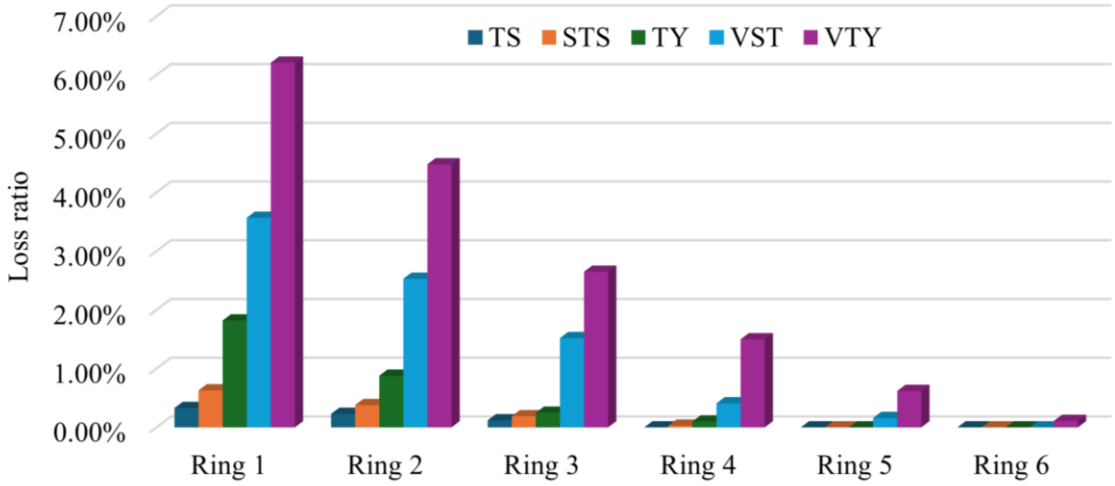

Figure 6. 25: The loss ratio of annual throughput across different cyclone intensities and six strike distances.

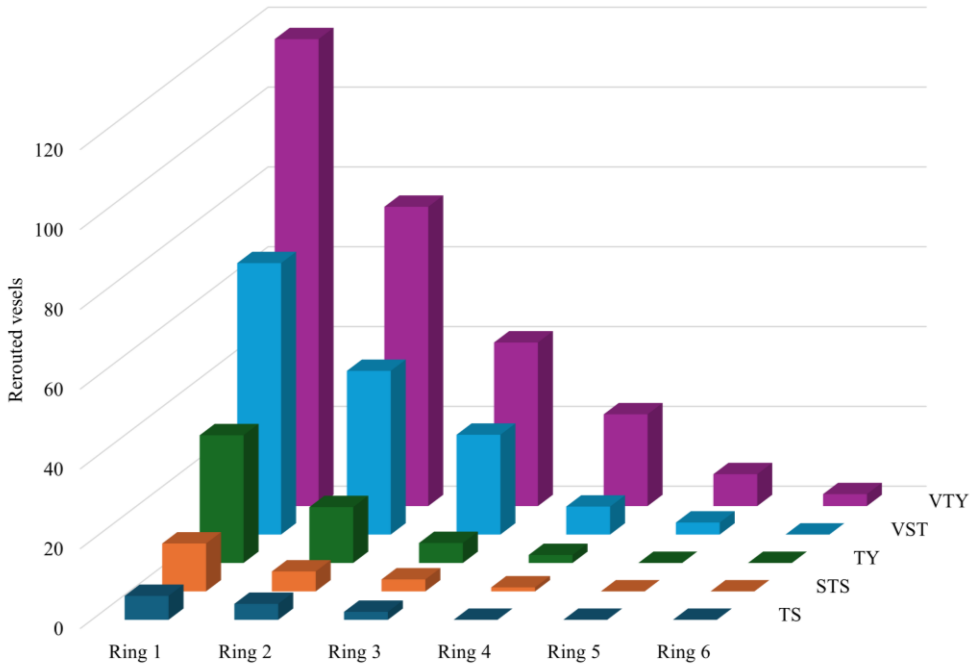

Figure 6. 26: Estimated number of rerouted vessels per cyclone scenario and strike distance.

The economic loss estimation across different disruption scenarios requires well-founded values for the parameters used in the equations developed in Section 6.3.2.2. To this end, a comprehensive data collection effort was undertaken to obtain parameter values from the most recent and publicly available sources. These values were derived from official tariff schedules, government press releases, supplier contracts, and up-to-date market indices.

Specifically, container-handling margins rates was sourced from the 2024 upper limits of rates and charges document published by Taiwan International Ports Corporation (https://kh.twport.com.tw). Replacement cost figures for quay cranes, and other critical path items were extracted from Evergreen Marine Corporation's Terminal 7 procurement disclosures and corroborated by international contract data. In instances where data sources provided a range of values, the mid-point of 2025 market prices were applied as a reasonable estimate. Tables 6.19 and 6.20 summarize the sample parameter values used in the analysis.

To ensure transparency and illustrate the traceability of the selected values, a few key examples are outlined below:

- Quay crane costs: Conventional quay crane prices were obtained from recent European port procurement records, such as the Peel Ports Liverpool tender, which priced operator-cab-equipped units at approximately USD 12 million (source: theloadstar.com).

- Handling tariff per TEU: The handling tariff per TEU covers stevedoring and crane usage, paid by the shipping line to the terminal operator. The rate is USD 190 for a 20-foot container and USD 220 for a 40-foot container. On a per-TEU basis, the average estimated cost is approximately USD 200 (Source: https://kh.twport.com.tw/fapi/AttFile?id=3850&l=2&type=AttFile).

It is important to emphasize that the primary objective of this study is to demonstrate the applicability of the proposed methodology rather than to produce precise monetary estimations. As such, the use of publicly available and approximated data is appropriate. More accurate estimations would require access to detailed, proprietary, or confidential information, which lies beyond the scope of this research.

Table 6. 19: The estimated asset values in the quay side of Terminal 7 in Kaohsiung port.

Component	Number	Price/unit ($\times 10^6$ *USD*)	Total price ($\times 10^6$ *USD*)	Representative sources
Remote-operated quay cranes	19	15	285	*https://pk.craneyt.com/knowledge/rtg-vs-sts-cranes/*
Cabin-operated quay cranes	5	12	60	*https://pk.craneyt.com/knowledge/rtg-vs-sts-cranes/*
Quay fenders & bollards (5 berths)	-	1	5	*https://www.nwseaportalliance.com/about-us/do-business-us/contracting/procurements/pct-fender-system-replacement-project-2023?utm_source*
Shore-power sub-stations & switchgear	-	3	3	*https://www.hitachienergy.com/*
5 G / fibre backbone, RMS & data centre	-	15	15	*https://www.globaltimes.cn/page/202210/1277443.shtml?utm_source*

Table 6. 20: Recovery and downtime cost parameter values.

Parameter	Value	Notes	Representative sources
Handling tariff	200 USD/TEU	Midpoint derived from CMA CGM Kaohsiung THC.	https://www.cma-cgm.com/assets/public/documents/TAIWAN%20-%20LOCAL%20SCES%2011-06-2025_0.pdf
First-increment mark-up (α)	0.15	Assumption to be calibrated with the quality/speed of recovery process.	*https://doi.org/10.3390/su15065578*
Convexity exponent (β)	1.8	Assumption to be calibrated with the quality/spe	https://doi.org/10.3390/su15065578

		ed of recovery process.	
Mobilization/demobilization allowance (M)	5-7% of accelerated block costs	Extracted from USACE cost-estimating guidance & MOB/DEMOB payment practices	https://www.swg.usace.army.mil/Portals/26/docs/Planning/Public%20Notices-Civil%20Works/GIWW%20BRFG-CRL%20Final%20FIFR-EIS/Eng%20App%20-%20-App%2010%20-%20COST%20ESTIMATE%20%28signed%29_1.pdf?ver=2019-06-24-071630-927&utm_source
Maintenance tech wages	120 USD/day	Fluctuates based on contractor method statements.	https://www.salaryexpert.com/salary/job/general-maintenance-worker/taiwan?utm_source
External equipment rental	5k-12k USD/day	Heavy mobile crane daily rental	*https://www.bigge.com/crane-rental/rental-rates/?utm_source*

Figures 6.27 to 6.31 depict estimated economic losses resulting from cyclone events of varying intensities striking within five concentric ring zones. These economic losses are categorized into direct damage costs, downtime costs, and recovery costs, with specific clarifications provided.

In Figure 6.27, illustrating a violent typhoon event, it is evident that ring zone 1 experiences the maximum economic loss, with direct damage reaching approximately $77 million, downtime costs at around $45 million, and recovery (repair and maintenance) costs close to $15 million. Direct damage includes equipment purchases required to restore port functionalities, while the recovery cost specifically accounts for repair and maintenance activities, explicitly excluding equipment purchases. Therefore, the combined direct damage and recovery costs provide a comprehensive view of the total recovery expenses, totalling around $92 million for the most severe scenario.

Figures 6.28 through 6.31 progressively represent less severe cyclone events, including very strong typhoon, typhoon, severe tropical storm, and tropical storm, respectively. For instance, in Figure 6.28 (VST), direct damage in ring zone 1 reduces significantly to approximately $58 million, with downtime costs decreasing to about $30 million and repair costs around $12 million. By comparison, Figure 6.31 (tropical storm) indicates even more modest economic losses in ring zone 1, with direct damage at approximately $6 million, downtime around $2 million, and minimal repair costs.

In these less intense events, particularly those impacting the outer ring zones, both disrupted periods and recovery durations become noticeably less significant. For example, outer rings in tropical storm scenarios (Figure 6.31) exhibit direct damages below $1 million, underscoring substantially lower operational impacts compared to the innermost ring and higher intensity events.

A noteworthy aspect across all scenarios is the operational strategy implemented post-event. After the gale force period concludes and undamaged equipment is assessed, recovery processes begin concurrently with container operations using remaining intact berths and cranes. To mitigate the reduction in container throughput capacity, productivity and utilization rates of available cranes and berths are increased, compensating for the diminished operational capability due to damage.

Comparatively, these figures clearly demonstrate that economic losses significantly escalate with cyclone intensity and proximity to the central ring, with a pronounced peak for violent typhoon conditions within the innermost ring. The distinction in cost categories provides clarity on the nature of incurred expenses, highlighting the gravity of cyclones impact on the terminal operations.

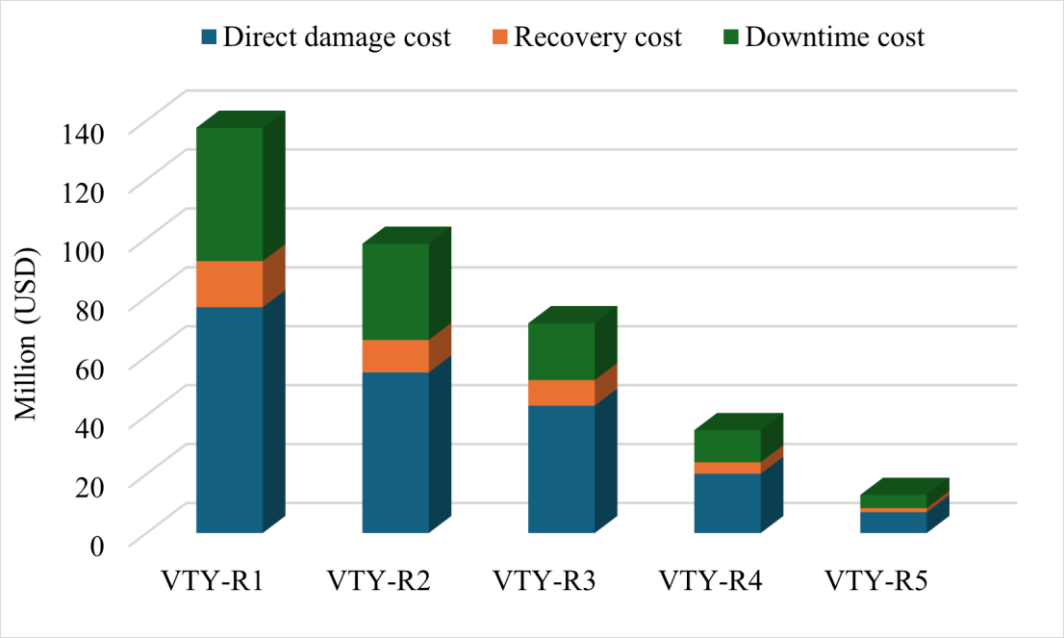

Figure 6. 27: Estimated economic losses for the violent typhoon strike within five concentric ring zones.

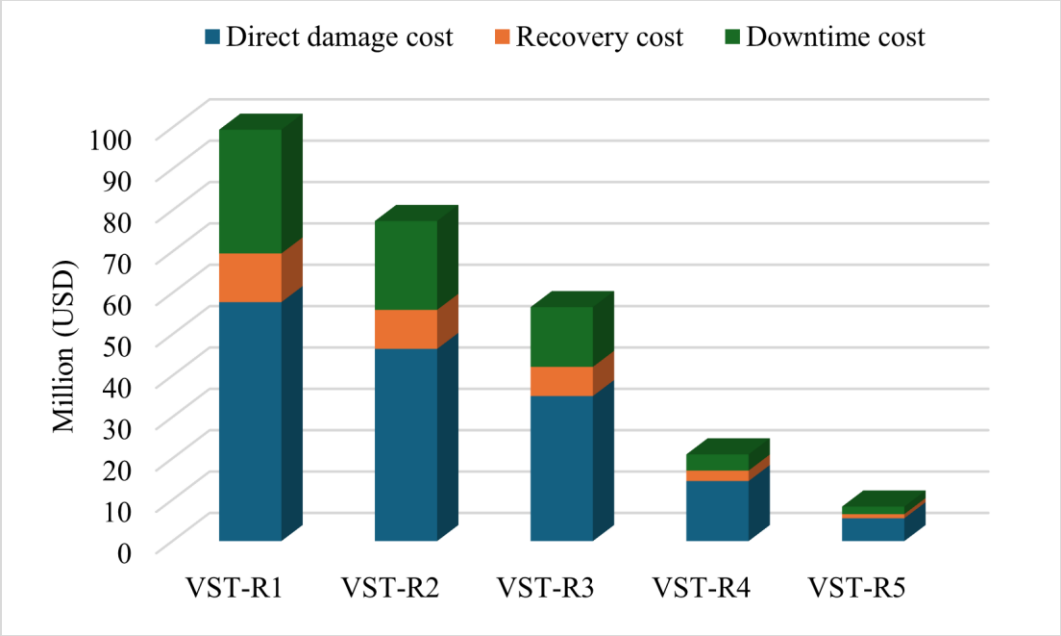

Figure 6. 28: Estimated economic losses for the very strong typhoon strike within five concentric ring zones.

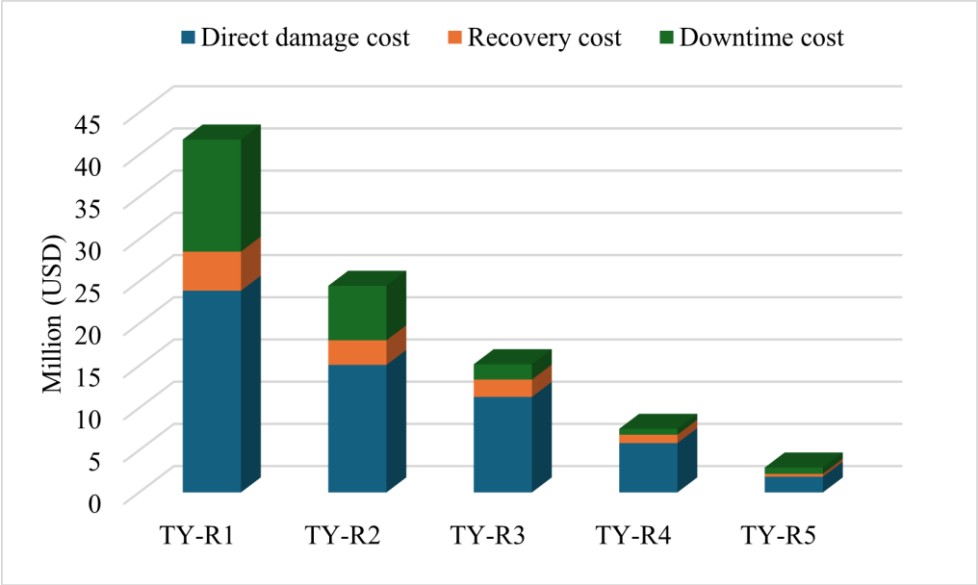

Figure 6. 29: Estimated economic losses for the typhoon strike within five concentric ring zones.

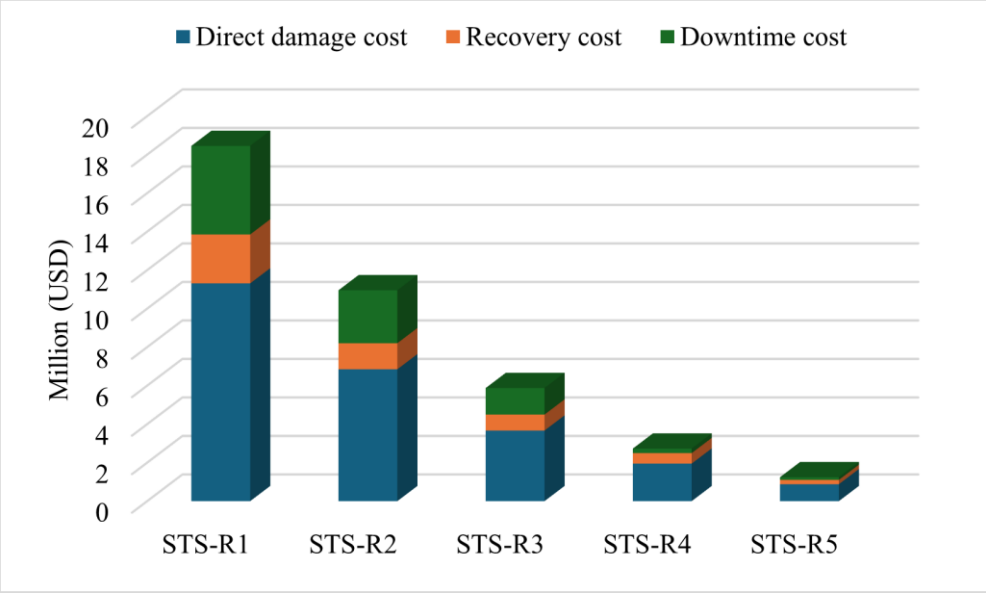

Figure 6. 30: Estimated economic losses for the sever tropical storm strike within five concentric ring zones.

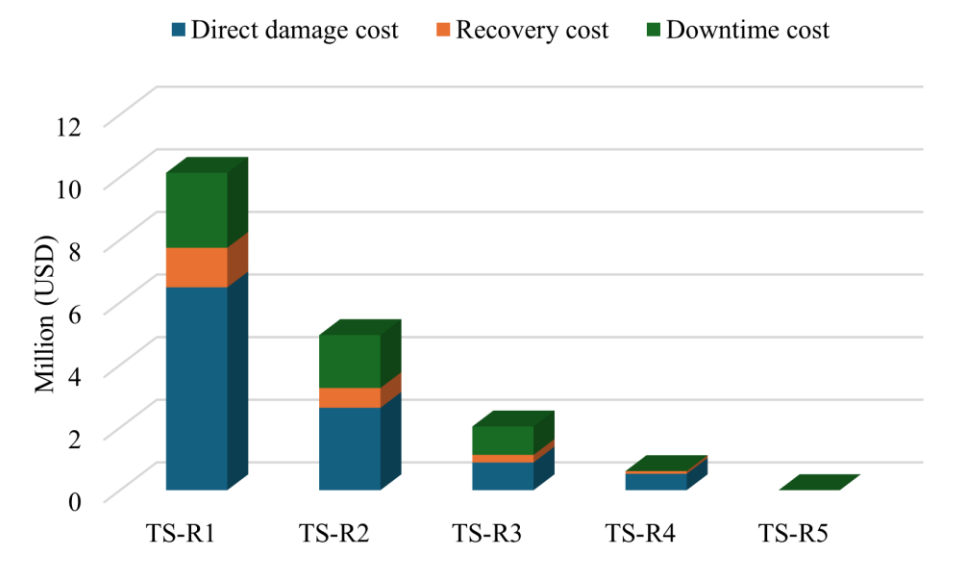

Figure 6. 31: Estimated economic losses for the tropical storm strike within five concentric ring zones.

6.5.4 Terminal resilience assessment against cyclones

According to Section 6.3.3 and the PIANC capability bands, the figures for Ring 1 show a consistent gradient in which the high and world-class resilience regimes experience markedly lower throughput loss than the standard and low regimes. This separation is most pronounced for the very severe cyclone categories (VTY, VST), where the stronger regimes avoid the largest drops in service and keep the loss ratio distinctly lower. In contrast, at weaker intensities (TY, STS, ST), the curves converge and the differences among regimes become relatively small because severe damage states are infrequent and any reductions in service are short-lived. The same ordering appears in the throughput loss ratio, confirming that the pattern is not an artefact of absolute scale but holds when losses are measured relative to baseline capacity. The number

of rerouted vessels follows the throughput signal. Fewer diversions are recorded for the high and world-class regimes, while the low regime shows the greatest tendency to divert traffic under stronger cyclones.

Read together, Figures 6.32-6.34 indicate that the combination of absorptive, adaptive, and restorative measures yields the clearest gains at the top end of the hazard spectrum; by preserving more operating capacity during events and recovering faster immediately after, stronger regimes reduce both the magnitude of the initial throughput shock and the operational need to reroute vessels. In milder events, the visual separation among regimes should not be over-interpreted; it reflects small absolute differences where all regimes maintain most of their capacity. Overall, the figures support the conclusion that resilience investments primarily pay off in the tail of cyclone intensity, while producing modest, incremental improvements under routine or moderate conditions in Ring 1. Tables Ap.4-Ap.6 in the Appendix report throughput loss, loss ratios, and numbers of rerouted vessels for the remaining rings across all PIANC resilience bands.

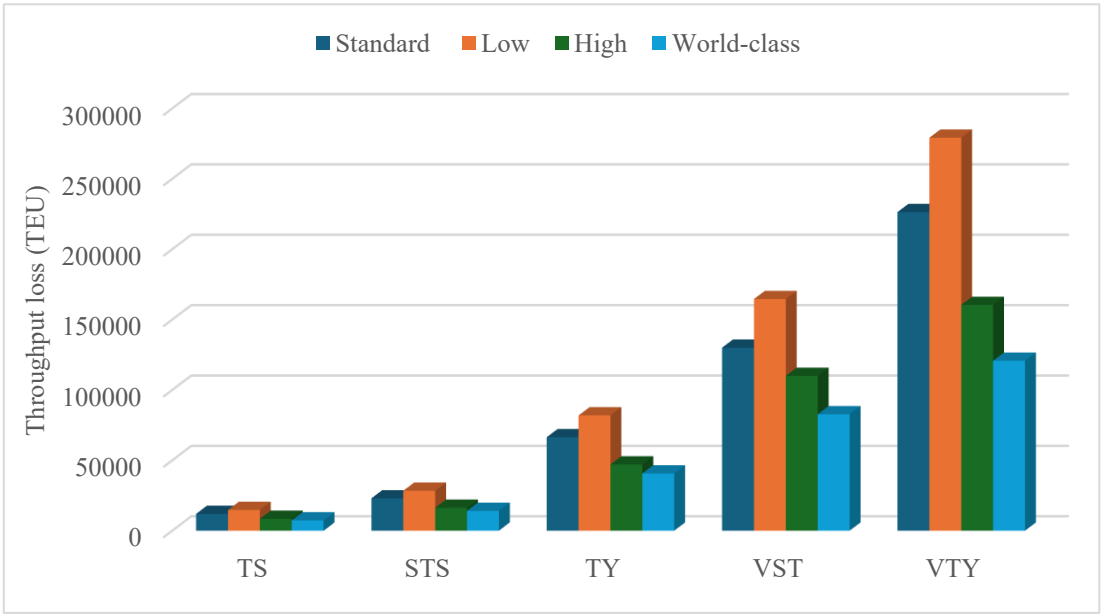

Figure 6. 32: The throughput loss under various resilience regimes due to different cyclone intensities at ring zone 1.

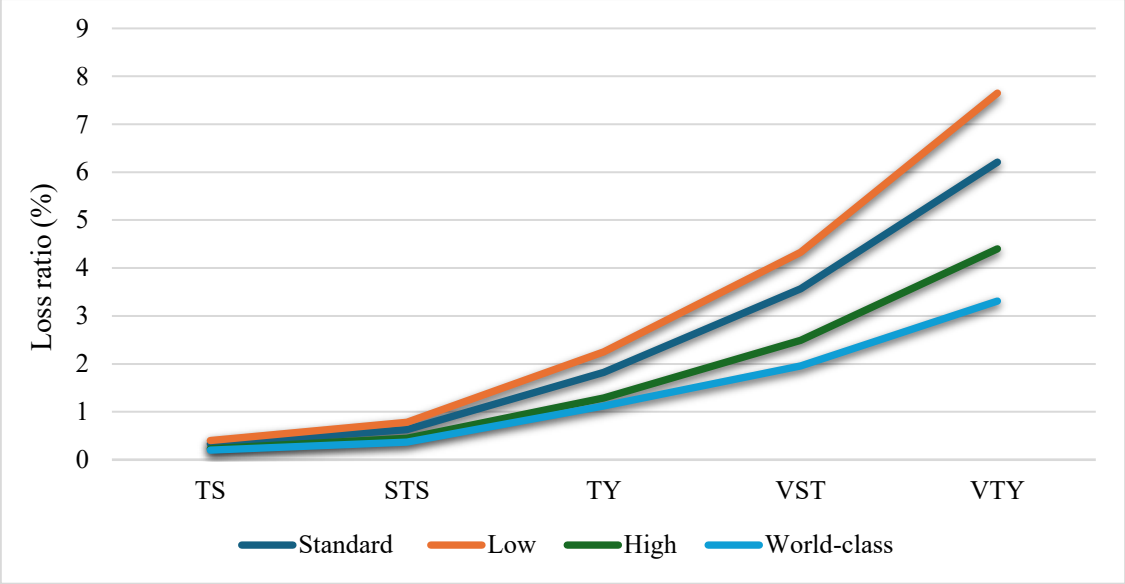

Figure 6. 33: The throughput loss ratio under various resilience regimes due to different cyclone intensities at ring zone 1.

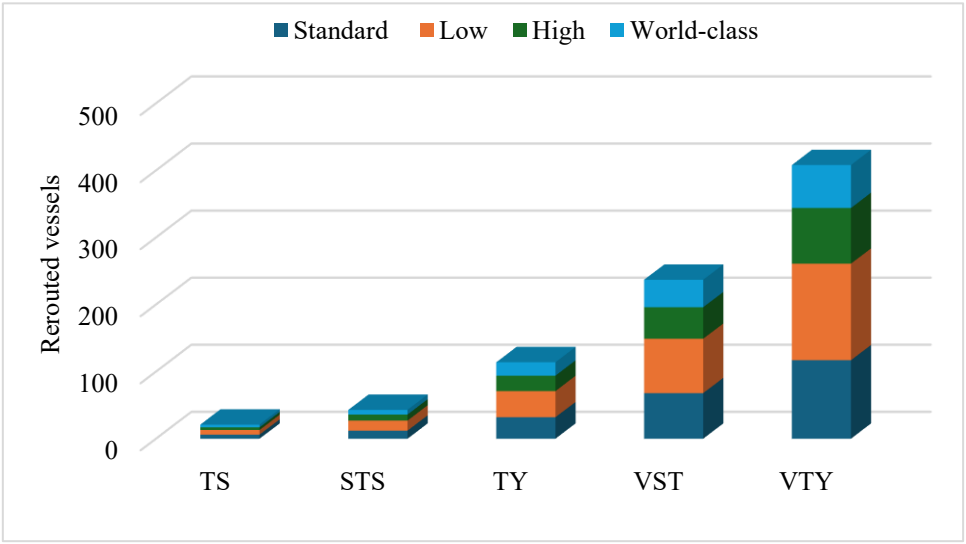

Figure 6. 34: The number of rerouted vessels under various resilience regimes due to different cyclone intensities at ring zone 1.

The cost results mirror the throughput patterns. Across VTY, VST, TY, STS, and ST, total losses, comprising direct damage, recovery/repair, and downtime, decline monotonically as resilience improves from standard to world-class. The widest cost spread appears in the very severe categories, consistent with the larger throughput protection seen in Figures 6.32-6.34; fewer transitions to severe damage states translate into lower direct damage and smaller repair scopes, while quicker recovery shortens the duration of reduced operations that drives downtime costs. In moderate categories, the differences among regimes narrow because damage is less frequent and recovery periods are shorter for all cases; nevertheless, the high and world-class portfolios still maintain an advantage that accumulates over the event window. The alignment between lower rerouting in Figure 6.34 and lower totals in Figures 6.35-6.39 is also notable; avoiding diversions helps contain secondary scheduling and handling disruptions

that would otherwise add to downtime-related costs. Taken together, the cost figures reinforce the interpretation that the primary economic benefit of stronger resilience lies in preventing the most consequential loss scenarios and truncating the period of impaired capacity during severe cyclones, while in milder events the benefit appears as consistent but smaller reductions across all three cost components.

It is methodologically appropriate to exclude the low-resilience capability band from the cost model for Terminal 7 at Kaohsiung Port. As documented earlier, the Recovery Capacity Factor (RCF) framework links resilience capability to repair-time multipliers that adjust MTTR by capability band; ports scoring higher on the rubric recover faster (RCF > 1), while low-capability facilities recover more slowly (RCF < 1). The rubric, adapted from PIANC WG-174 and operationalised across robustness, redundancy, resourcefulness, and rapidity, assigns 1-5 scores per dimension (Table 6.4), which aggregate to capability bands (Table 6.5). The "Low" band corresponds to a total score of 4-8 and represents minimal preparedness (e.g., only statutory compliance, no drills, limited spares). Such conditions do not characterise Terminal 7, which is Taiwan's first automated terminal and operates with advanced technologies and resilience practices consistent with the "High" to "World-class" yardsticks (e.g., remote monitoring, spare/backup capacities, rapid intervention arrangements) enumerated in the rubric. Including the Low band would therefore inject unrealistic repair multipliers and overstate downtime-driven costs for DS2-DS4, contrary to the RCF logic used to derive port-specific MTTRs. Accordingly, the Low band is excluded from the analysis, and costs are computed using capability-appropriate bands only. Moreover, sensitivity tests confirm that introducing Low-band multipliers materially inflates downtime costs relative to observed capability, without improving model fidelity to Terminal 7's resilience profile.

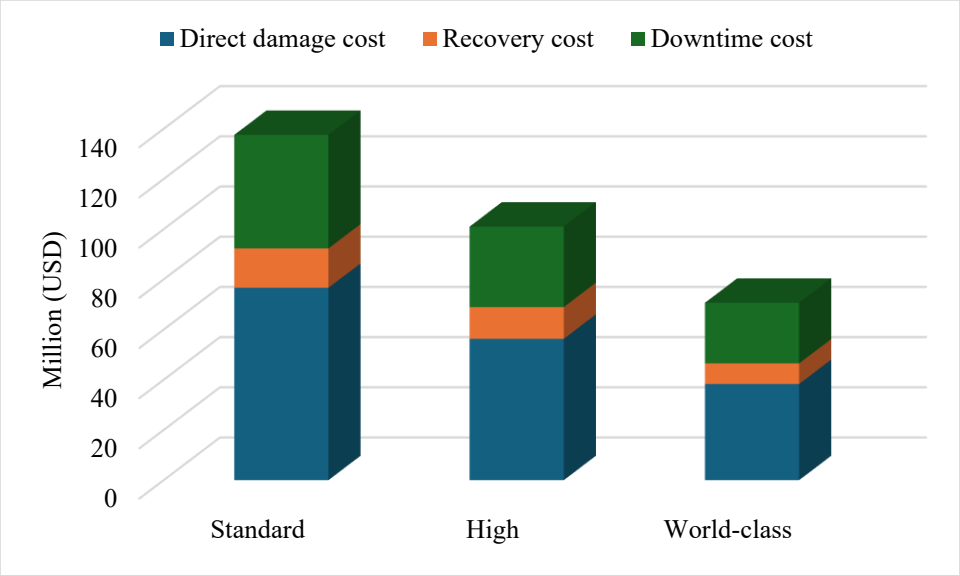

Figure 6. 35: Estimated economic losses for the VTY-Ring 1 under different resilience regimes.

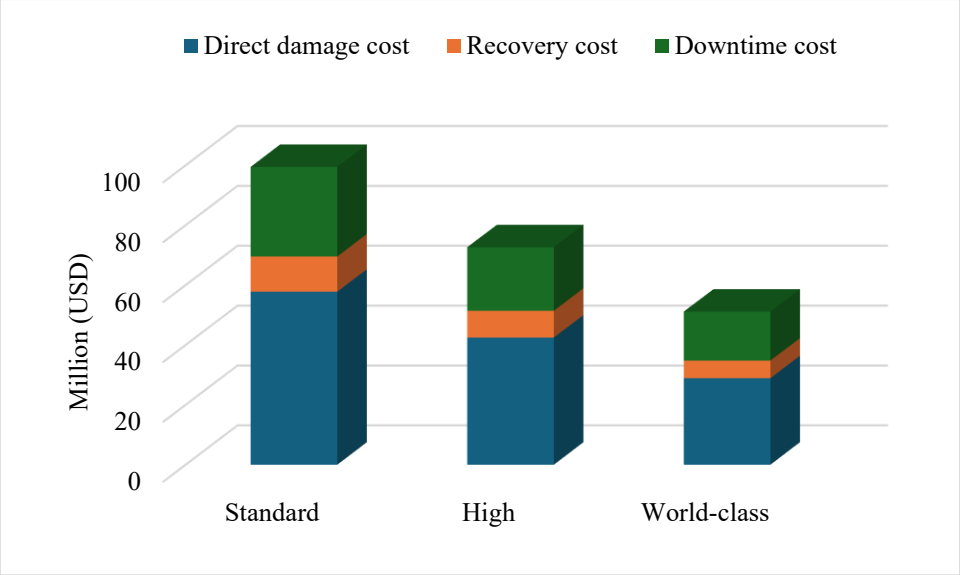

Figure 6. 36: Estimated economic losses for the VST-Ring 1 under different resilience regimes.

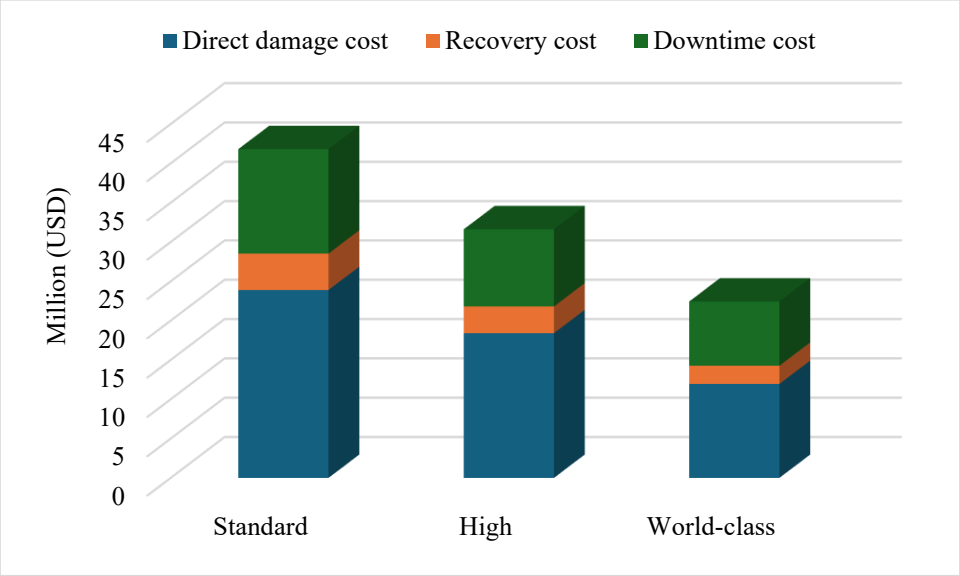

Figure 6. 37: Estimated economic losses for the TY-Ring 1 under different resilience regimes.

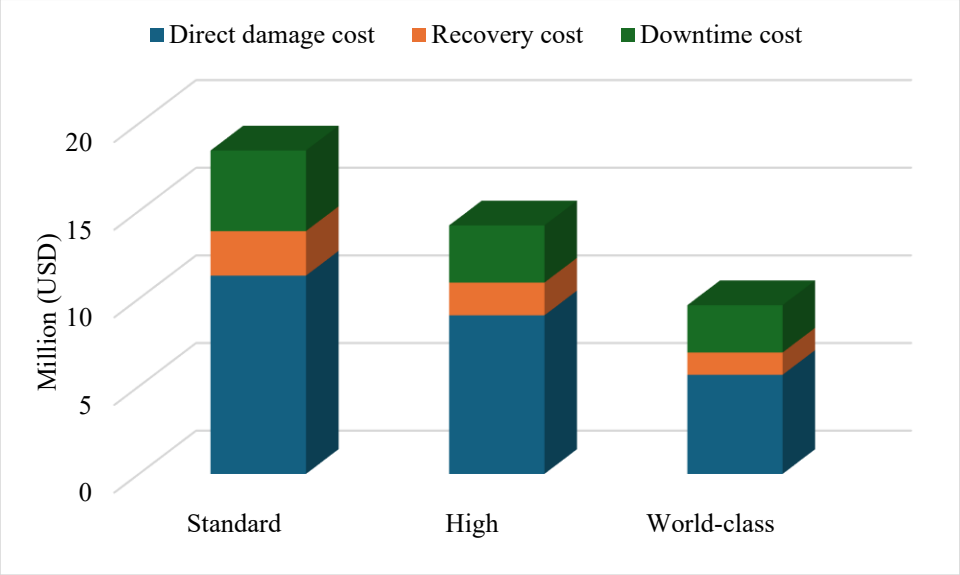

Figure 6. 38: Estimated economic losses for the STS-Ring 1 under different resilience regimes.

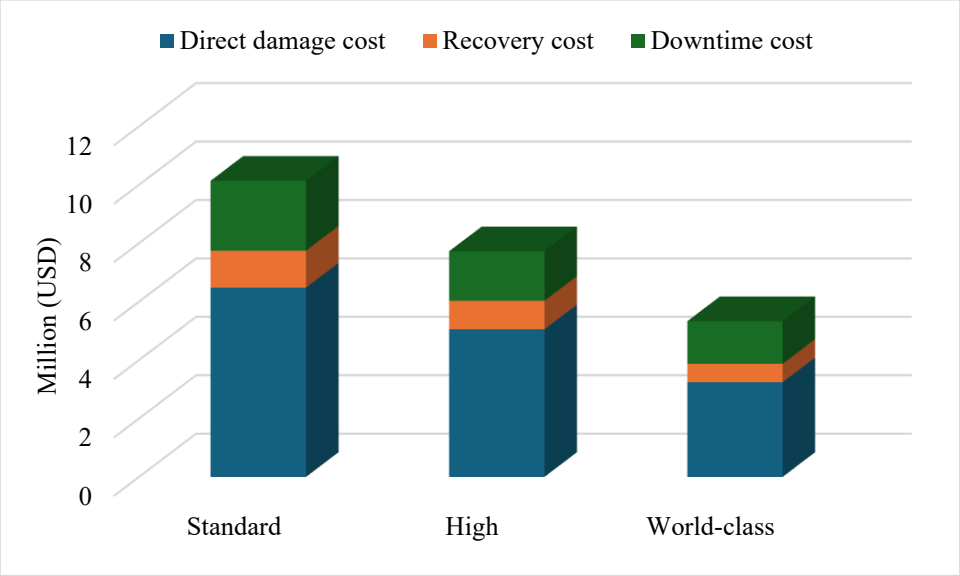

Figure 6. 39: Estimated economic losses for the ST-Ring 1 under different resilience regimes.

6.6 Conclusion

In this chapter, a risk-based simulation framework is developed and applied to Terminal 7 of the Port of Kaohsiung to assess cyclone impacts on port functionality and to estimate associated economic losses. The framework draws on operational records and detailed equipment specifications to parameterize the model and incorporates three decades of cyclone observations affecting the terminal's region to generate objective, data-driven inputs. Cyclones are first classified by type, with occurrence frequencies and intensity distributions estimated. A discrete-event simulation model in AnyLogic then quantifies functionality loss (e.g., throughput degradation and downtime). For each scenario, direct and indirect economic impacts are evaluated using developed mathematical cost models.

The obtained results indicate the following key findings: (1) the total frequency of cyclones within 400 km of Kaohsiung Port, irrespective of type, is about 6.07 per year, with typhoon-class events accounting for 34.5%; (2) in the worst-case scenario, a violent typhoon within 50 km of the terminal, throughput loss exceeds 6% of annual volume, equating to nearly USD 45 million; (3) throughput losses diminish with lower cyclone intensity and greater distance; (4) losses are most pronounced within the first three ring zones, beyond which the impact on terminal functionality drops sharply; (5) for typhoon-class events in the near ring zones, direct physical damage costs typically exceed downtime costs; and (6) advanced resilience measures, such as boom anti-collision sensors and ductile tie-down links, can avert substantial damage and business disruption during cyclone events.

The contributions of this chapter are fivefold: it advances current knowledge on the impact of cyclones on port functionality and the consequent economic loss; creates a dedicated cyclone-hazard database for Kaohsiung Port that can also be used by surrounding terminals and ports; develops cyclone-induced fragility curves for quay cranes, advancing understanding of cyclone impacts on these critical components; estimates throughput loss and the consequent economic loss using objective data fed to a simulation model, thereby reducing the subjectivity present in similar studies; and presents a framework that provides seaport authorities with a vital tool to understand, evaluate, and strengthen resilience against climate-related hazards. The framework also supports informed, risk-based decisions to mitigate disruptions, reduce recovery costs, and enhance long-term operational continuity for sustainable port infrastructure management under climate change.

Future work will consider a multi-hazard analysis of cyclone-induced impacts including storm surge and compound flooding, wave setup, run-up and overtopping. Moreover, chain disruptions throughout the whole terminal, including the yard and intermodal areas, will be examined. In addition, the adoption of different resilience strategies and their contributions to reducing the consequent losses will be assessed.

Chapter 7 : Conclusion

7.1 Summary

Maritime transport and port activity underpin world commerce and economic resilience. Because ports sit at the heart of logistics, keeping them operating reliably is critical for uninterrupted goods movement and robust supply chains domestically and across borders. Disruptions to these systems can have widespread and cascading effects. Evaluating seaport performance, therefore, requires consideration of key principles such as reliability, vulnerability, robustness, survivability, safety, and security. While each of these dimensions contributes uniquely to performance assessment, resilience has emerged as the most comprehensive and critical concept, encompassing a port's ability to withstand, adapt to, and recover from diverse shocks and stresses.

In response to growing threats, particularly those linked to climate change and complex systemic risks, this thesis developed a novel, holistic, risk-informed framework for assessing the safety, security, and resilience of seaports. Grounded in an extensive literature review, the study identified key research gaps and addressed them using a combination of data-driven techniques and innovative methodologies. The framework integrates objective, quantitative analysis to reduce the subjectivity inherent in many existing approaches.

Recognizing the complex socio-technical nature of seaport systems, a Safety-II-based systemic risk assessment method was introduced. This approach enables the examination of performance variability and interdependencies across technological, human, and organizational dimensions, moving beyond traditional safety assessments.

In addition, a simulation-based approach was developed using real-world data to evaluate port resilience against natural hazards, particularly those intensified by climate change. The fragility curves were also developed for quay cranes to represent their failure probability induced by different cyclone intensities. The proposed framework was validated, and applied to a real case study, offering a practical and scalable tool for resilience measurement.

In summary, this research makes significant contributions by developing integrated, validated, and scalable methodologies to support decision-makers in enhancing the safety, security, and resilience of seaport operations. The outcomes provide actionable insights for policymakers, port authorities, and other stakeholders, enabling proactive planning and robust response strategies in an increasingly uncertain risk environment.

7.2 Realization of the research aims and objectives

The research aims and objectives outlined in this study have been addressed in relation to the identified gaps in the literature and the research questions posed. These are detailed in Table 7.1. The objectives were examined in terms of the underlying assumptions, the extent of their achievement, and their broader implications.

Table 7. 1: The summary of the results obtained and implications of the research.

Research objectives	Rational	Contributions	Implications

Comprehensive literature review	A comprehensive literature review will reveal the current research gap in the context of maritime transportation safety, security, risk, and resilience.	The relevant research gaps for each aspect of the topics studied have been identified and are presented primarily in Chapter 2, with additional references included in the introductions of individual chapters, depending on the nature of the topic.	The identified research gaps serve as a foundation and driving force for guiding the current research efforts. They provide both the momentum and direction needed to develop novel models and methodologies aimed at effectively addressing these unresolved issues.
Physical security risk assessment	The application of data-driven learning in constructing a TAN-based BN model for the analysis of maritime terrorism is expected to address the limitations of the current qualitative approaches, as well as the subjectivity of the current quantitative ones.	This section of the study analysed 160 maritime terrorism incidents from the GTD database, identifying 12 key SRIFs and modelling their interactions using a TAN-based BN. Focusing on four attack types, namely assailment, explosion, hijacking, and hostage-taking, the model revealed six dominant SRIFs. Validation through various techniques confirmed its robustness, with over 90% accuracy in predicting two real-world cases. The results demonstrate the model's strong predictive power and practical value for enhancing maritime security and guiding international counterterrorism strategies.	The study underscores the urgent need for a multi-stakeholder, adaptive approach to maritime security. It highlights the importance of recognizing temporal patterns in terrorist activities, investing in advanced detection technologies, and tailoring security strategies based on weapon types and regional risks. Intelligence gathering on perpetrator groups and technological trends is vital, as is international cooperation and information sharing. Strengthening regional and national capabilities, through innovation, capacity-building, and targeted policy interventions is essential to counter evolving maritime terrorism threats effectively and ensure long-term maritime resilience and safety.
Cybersecurity risk assessment	The application of data-driven learning in constructing a TAN-based BN model for the analysis of maritime cyber threats is expected to address the limitations of the current qualitative approaches, as well as the subjectivity of the current quantitative ones.	The key SRIFs are identified, leading to the development of a distinct data-driven BN model. This model enables effective analysis of potential cybersecurity risks across various sectors of the maritime industry. Analysis of the cybersecurity model reveals that ransomware is the most common type of cyberattack targeting stationary maritime infrastructures, followed by hacking, malware, phishing, and DDoS attacks. For vessels, the predominant cyber threats consist of spoofing and jamming, in that order.	The findings of this chapter reinforce the conclusion that effectively addressing cyber threats in the maritime sector requires a comprehensive and integrated approach, encompassing both technological and organizational dimensions. The results highlight that a multifaceted cybersecurity strategy, combining robust technical safeguards with well-defined institutional policies, procedures, and training, is essential for establishing a resilient defence posture. The study underscores that no single measure is sufficient; rather, the interplay between advanced technical solutions and strong organizational frameworks is critical to countering the evolving and complex cyber threat landscape facing the maritime industry.
Systemic risk analysis	Developing a systemic risk analysis framework	The study resulted in an integrated risk analysis framework for seaports,	The implications of this chapter highlight the need for a functional, system-wide

	based on Safety-II concept is expected to address the inherent complexities in complex socio-technical systems like seaports, while tackling the limitations in traditional safety assessment methodologies.	successfully combining FRAM, BN, and advanced analytical techniques. It enabled the identification of key performance variabilities across technological, human, and organizational elements, as well as their critical interdependencies. The framework provided both retrospective and prospective risk insights, allowing for effective visualization and quantification of system-level risks. These outcomes support informed, risk-based decision-making and strengthen the overall resilience of seaport operations.	perspective in managing seaport risks. By capturing performance variability and interdependencies, the framework enables stakeholders to anticipate emergent behaviours and critical system vulnerabilities. It supports proactive, risk-based decision-making and prioritization of interventions. The integration of FRAM and Bayesian Networks promotes a shift toward Safety-II thinking, offering practical, adaptable strategies for enhancing resilience and safety across complex socio-technical systems in the maritime domain.
Risk-informed resilience assessment	Developing a novel simulation-based resilience analysis framework that addresses both the direct and indirect physical damage from natural hazards, as well as the associated economic losses, offers a powerful tool for enhancing the long-term sustainability and reliability of seaports amid increasing climate-related risks.	A simulation-based resilience analysis framework has been developed and applied to Kaohsiung Port, specifically Terminal 7, using 30 years of cyclone data. It quantifies hazard frequency, intensity, and economic impact through probabilistic and mathematical modelling. The framework calculates the raised cost of disruptions and integrates these elements within AnyLogic software to assess the influence of different resilience strategies against cyclone hazards. This enables a data-driven assessment of port functionality under natural hazard scenarios.	The study's framework offers a vital tool for seaport authorities to understand, evaluate, and strengthen resilience against climate-related hazards. By incorporating natural hazard risks, performance metrics, and economic losses into a unified simulation model, stakeholders can proactively identify vulnerabilities and improve adaptive strategies. The framework supports informed, risk-based decisions to mitigate disruptions, reduce recovery costs, and enhance long-term operational continuity, contributing to the sustainable management of critical maritime infrastructure amid climate change.

7.3 Limitations of the research

This research represents a pioneering effort in developing a comprehensive platform for conducting risk-informed resilience analysis in seaports, encompassing various risks such as physical security, cyber-attacks, safety hazards, and natural disasters. However, during the implementation of this framework, several minor issues arose, primarily due to the inherent limitations of data collection process. These constraints stemmed from scope, confidentiality, technical competence, sensitivity of the subject matter, and time constraints.

One notable limitation concerns data accessibility, particularly the confidentiality surrounding specific data related to physical and cybersecurity in seaports. Due to reputational risks and competition among ports, there is reluctance to disclose such information publicly, potentially obscuring the true scope of incidents and accidents. Consequently, this analysis relied primarily on publicly available data, which may not fully capture all relevant incidents.

Moreover, critical operational details essential for simulating seaport operations, such as logistics, equipment specifications, investments in upgrades, crew training levels, and organizational efficiency, remain closely guarded by seaport authorities. This lack of transparency may also affect the fidelity of the results to some extent.

As a result, the final output of this study is constrained by the data accessible through public sources or selectively obtained through connections with seaport authorities. Despite these limitations, it is important to note that these constraints do not significantly undermine the academic rigor of the findings, which still reflect a substantial approximation of reality.

7.4 Future research directions

The present thesis advances seaport resilience assessment by integrating probabilistic, deterministic, and empirical perspectives on disruption and recovery; nevertheless, several substantive avenues remain to consolidate and extend these gains. A priority is to couple resource-allocation decisions with formal optimization, using metaheuristics such as Genetic Algorithms and Particle Swarm Optimization to search across large investment and operations spaces while explicitly balancing risk reduction and cost efficiency. These optimizers should be embedded in the simulation stack so that candidate solutions are stress-tested under uncertainty and time-varying operating conditions, allowing resilience to be treated as an objective rather than a by-product of design.

A second strand concerns the development of seaport digital twins that fuse real-time data with high-fidelity simulation. Such twins can act as continuously updated “what-if” laboratories in which alternative preparedness, response, and recovery strategies are exercised across compound and cascading scenarios before adoption in the field. Beyond improving situational awareness, this capability would enable closed-loop learning, where models recalibrate to new events, databases evolve, and resilience strategies are iteratively refined as operations and threat landscapes change.

Methodological integration should also deepen. At system level, Bayesian Networks can continue to represent probabilistic dependencies among assets, processes, and hazards, while Discrete-Event Simulation captures queueing, capacity, and temporal dynamics; agent-based components can be added to represent human decision-making and organizational behaviour under stress. This triad supports analysis across the absorptive, adaptive, and restorative capacities and can be aligned with functional-interaction views (e.g., FRAM) to expose interdependencies that drive resonance and cascade. Multi-criteria decision methods should sit on top of these models to translate technical performance into value-based trade-offs, including economic, operational, environmental aspects, so that port authorities can rank resilience portfolios transparently and defensibly.

Networked resilience remains under-modelled. Future work should bridge micro-to-macro scales by tracing how local disruptions at one terminal propagate through hinterland links and across the wider port system of systems, quantifying spillovers, substitution, and recovery pathways under centralized, decentralized, and hybrid coordination. This entails representing

inter-port cooperation rules alongside local autonomy so that governance design becomes part of the solution space rather than an external constraint.

Cybersecurity research should be advanced in parallel and tightly integrated with physical risk analysis, given the growing likelihood of coordinated cyber-physical attacks. Data-driven Bayesian Networks, enriched with machine learning and real-time threat intelligence, can power early-warning and attribution by linking indicators across IT, OT, and vessel/terminal systems.

Progress on all fronts depends on data. Priority tasks include curating continuously updated physical- and cybersecurity incident repositories; establishing protocols for secure data sharing that respect privacy and commercial sensitivity; and building pipelines that handle heterogeneous, dynamic data streams without compromising model tractability. These efforts will make the framework adaptive to novel events and ensure that lessons learned feed back into models, metrics, and managerial practice. Collectively, these directions move seaport resilience from static assessment toward a learning, optimized, and network-aware capability that can keep pace with evolving risk.

References

Abou Kasm, O., Diabat, A., Bierlaire, M., 2021. Vessel scheduling with pilotage and tugging considerations. Transp. Res. Part E Logist. Transp. Rev. 148, 102231. https://doi.org/10.1016/j.tre.2021.102231

Achterkamp, J., 2019. Improving Terminal Performance, Mega-ships require mega-terminals. https://www.porttechnology.org/.

Achurra-Gonzalez, P.E., Novati, M., Foulser-Piggott, R., Graham, D.J., Bowman, G., Bell, M.G.H., Angeloudis, P., 2019. Modelling the impact of liner shipping network perturbations on container cargo routing: Southeast Asia to Europe application. Accid. Anal. Prev. 123, 399–410. https://doi.org/10.1016/j.aap.2016.04.030

Adam, E.F., Brown, S., Nicholls, R.J., Tsimplis, M., 2016. A systematic assessment of maritime disruptions affecting UK ports, coastal areas and surrounding seas from 1950 to 2014. Nat. Hazards 83, 691–713. https://doi.org/10.1007/s11069-016-2347-4

Adhita, I.G.M.S., Fuchi, M., Konishi, T., Fujimoto, S., 2023. Ship navigation from a Safety-II perspective: A case study of training-ship operation in coastal area. Reliab. Eng. Syst. Saf. 234, 109140. https://doi.org/10.1016/j.ress.2023.109140

Ahmed, F., Robinson, S., Tako, A.A., 2014. Using the structred analysis and design technique (SADT) in simulation conceptual modeling, in: Proceedings of the Winter Simulation Conference 2014. Presented at the 2014 Winter Simulation Conference - (WSC 2014), IEEE, Savanah, GA, USA, pp. 1038–1049. https://doi.org/10.1109/WSC.2014.7019963

Ahvenjärvi, S., Czarnowski, I., KÁla, J., Kyster, A., Meyer, I., Mogensen, J., Szyman, P., 2019. Safe Information Exchange on Board of the Ship. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 13, 165–171. https://doi.org/10.12716/1001.13.01.17

Al Ali, N.A.R., Chebotareva, A.A., Chebotarev, V.E., 2021. Cyber security in marine transport: opportunities and legal challenges. Pomorstvo 35, 248–255. https://doi.org/10.31217/p.35.2.7

Al-Dhaheri, N., Jebali, A., Diabat, A., 2016. The quay crane scheduling problem with nonzero crane repositioning time and vessel stability constraints. Comput. Ind. Eng. 94, 230–244. https://doi.org/10.1016/j.cie.2016.01.011

Almutairi, A., Collier, Z.A., Hendrickson, D., Palma-Oliveira, J.M., Polmateer, T.L., Lambert, J.H., 2019. Stakeholder mapping and disruption scenarios with application to resilience of a container port. Reliab. Eng. Syst. Saf. 182, 219–232. https://doi.org/10.1016/j.ress.2018.10.010

Alyami, H., Yang, Z., Riahi, R., Bonsall, S., Wang, J., 2019. Advanced uncertainty modelling for container port risk analysis. Accid. Anal. Prev. 123, 411–421. https://doi.org/10.1016/j.aap.2016.08.007

Amirkhani, H., Rahmati, M., Lucas, P.J.F., Hommersom, A., 2017. Exploiting Experts' Knowledge for Structure Learning of Bayesian Networks. IEEE Trans. Pattern Anal. Mach. Intell. 39, 2154–2170. https://doi.org/10.1109/TPAMI.2016.2636828

Angeloudis, P., Bichou, K., Bell, M., 2013. Security and Reliability of the Liner Container-Shipping Network: Analysis of Robustness using a Complex Network Framework. Risk Manag. Port Oper. Logist. Supply Chain Secur. https://doi.org/10.4324/9781315850504-17.

Asadabadi, A., Miller-Hooks, E., 2020. Maritime port network resiliency and reliability through co-opetition. Transp. Res. Part E Logist. Transp. Rev. 137, 101916. https://doi.org/10.1016/j.tre.2020.101916

Asadabadi, A., Miller-Hooks, E., 2018. Co-opetition in enhancing global port network resiliency: A multi-leader, common-follower game theoretic approach. Transp. Res. Part B Methodol. 108, 281–298. https://doi.org/10.1016/j.trb.2018.01.004

Asal, V., Hastings, J.V., 2015. When Terrorism Goes to Sea: Terrorist Organizations and the Move to Maritime Targets. Terror. Polit. Violence 27, 722–740. https://doi.org/10.1080/09546553.2013.855636

Ashraf, I., Park, Y., Hur, S., Kim, S.W., Alroobaea, R., Zikria, Y.B., Nosheen, S., 2022. A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. IEEE Trans. Intell. Transp. Syst. 1–14. https://doi.org/10.1109/TITS.2022.3164678

Association, I.N. (Ed.), 2002. Seismic Design Guidelines for Port Structures. Taylor & Francis. https://doi.org/10.1201/NOE9026518188

Athukorala, P., Resosudarmo, B.P., 2005. The Indian Ocean Tsunami: Economic Impact, Disaster Management, and Lessons. Asian Econ. Pap. 4, 1–39. https://doi.org/10.1162/asep.2005.4.1.1

Aven, T., 2022. A risk science perspective on the discussion concerning Safety I, Safety II and Safety III. Reliab. Eng. Syst. Saf. 217, 108077. https://doi.org/10.1016/j.ress.2021.108077

Baroud, H., Barker, K., Ramirez-Marquez, J.E., Rocco S., C.M., 2014. Importance measures for inland waterway network resilience. Transp. Res. Part E Logist. Transp. Rev. 62, 55–67. https://doi.org/10.1016/j.tre.2013.11.010

Baxter, G., Sommerville, I., 2011. Socio-technical systems: From design methods to systems engineering. Interact. Comput. 23, 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Bayramova, A., Edwards, D.J., Roberts, C., Rillie, I., 2023. Enhanced safety in complex socio-technical systems via safety-in-cohesion. Saf. Sci. 164, 106176. https://doi.org/10.1016/j.ssci.2023.106176

BBC, 2018. UK and US blame Russia for "malicious" NotPetya cyber-attack. https://www.bbc.co.uk/news/uk-politics-43062113.

Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X., 2022. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information 13, 22. https://doi.org/10.3390/info13010022

Benmalek, M., 2024. Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet Things Cyber-Phys. Syst. 4, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

Berghout, T., Benbouzid, M., 2022. EL-NAHL: Exploring labels autoencoding in augmented hidden layers of feedforward neural networks for cybersecurity in smart grids. Reliab. Eng. Syst. Saf. 226, 108680. https://doi.org/10.1016/j.ress.2022.108680

Bhimani, A., Soderberg, E., 2006. Crane Loads & Wharf Structure Design: Putting the Two Together. AAPA Facilities Engineering Seminar.

Bierwirth, C., Meisel, F., 2010. A survey of berth allocation and quay crane scheduling problems in container terminals. Eur. J. Oper. Res. 202, 615–627. https://doi.org/10.1016/j.ejor.2009.05.031

BIMCO, 2018. The Guidelines on Cyber Security Onboard Ships, Version 4.

Biringer, B., Vugrin, E., Warren, D., 2013. Critical infrastructure system security and resilience (1st ed.). FL: CRC Press, Taylor & Francis Group.

Błaszczyk, T., Nowak, M., 2009. THE TIME-COST TRADE-OFF ANALYSIS IN CONSTRUCTION PROJECT USING COMPUTER SIMULATION AND INTERACTIVE PROCEDURE. Technol. Econ. Dev. Econ. 15, 523–539. https://doi.org/10.3846/1392-8619.2009.15.523-539

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O.V., Musharraf, M., 2022. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. Int. J. Crit. Infrastruct. Prot. 39, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Bolbot, V., Theotokatos, G., Boulougouris, E., Vassalos, D., 2020. A novel cyber-risk assessment method for ship systems. Saf. Sci. 131, 104908. https://doi.org/10.1016/j.ssci.2020.104908

Boudehenn, C., Jacq, O., Lannuzel, M., Cexus, J.-C., Boudraa, A., 2021. Navigation anomaly detection: An added value for Maritime Cyber Situational Awareness, in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). Presented at the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, Dublin, Ireland, pp. 1–4. https://doi.org/10.1109/CyberSA52016.2021.9478189

Bouejla, A., Chaze, X., Guarnieri, F., Napoli, A., 2014. A Bayesian network to manage risks of maritime piracy against offshore oil fields. Saf. Sci. 68, 222–230. https://doi.org/10.1016/j.ssci.2014.04.010

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A., Von Winterfeldt, D., 2003. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthq. Spectra 19, 733–752. https://doi.org/10.1193/1.1623497

Bytheway, C.W., 2007. FAST creativity and innovation: Rapidly Improving Processes, Product Development and Solving Complex Problems. J. Ross Publishing.
Cao, X., Lam, J.S.L., 2019. A fast reaction-based port vulnerability assessment: Case of Tianjin Port explosion. Transp. Res. Part Policy Pract. 128, 11–33. https://doi.org/10.1016/j.tra.2019.05.019
Cao, X., Lam, J.S.L., 2018. Simulation-based catastrophe-induced port loss estimation. Reliab. Eng. Syst. Saf. 175, 1–12. https://doi.org/10.1016/j.ress.2018.02.008
Caprolu, M., Pietro, R.D., Raponi, S., Sciancalepore, S., Tedeschi, P., 2020. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. IEEE Commun. Mag. 58, 90–96. https://doi.org/10.1109/MCOM.001.1900632
Carlo, H.J., Vis, I.F.A., Roodbergen, K.J., 2015. Seaside operations in container terminals: literature overview, trends, and research directions. Flex. Serv. Manuf. J. 27, 224–262. https://doi.org/10.1007/s10696-013-9178-3
Carreras Guzman, N.H., Wied, M., Kozine, I., Lundteigen, M.A., 2020. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Syst. Eng. 23, 189–210. https://doi.org/10.1002/sys.21509
Central Weather Administration (CWA) Taiwan., 2015. Typhoon Database. Typhoon General Summary. (https://rdc28.cwa.gov.tw/TDB/public/typhoon_detail?typhoon_id=201513) Last accessed July 19, 2024.
Ceylan, B.O., Akyuz, E., Arslan, O., 2021. Systems-Theoretic Accident Model and Processes (STAMP) approach to analyse socio-technical systems of ship allision in narrow waters. Ocean Eng. 239, 109804. https://doi.org/10.1016/j.oceaneng.2021.109804
Chalk, P., 2008. The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States. RAND Corporation. https://doi.org/10.7249/MG697
Chang, C.-H., Kontovas, C., Yu, Q., Yang, Z., 2021. Risk assessment of the operations of maritime autonomous surface ships. Reliab. Eng. Syst. Saf. 207, 107324. https://doi.org/10.1016/j.ress.2020.107324
Chang, W., Li, N., Zhao, Y., 2024. Resilience of regional container port network: based on projection correlation and dynamic spatial Markov Chain. Marit. Policy Manag. 1–17. https://doi.org/10.1080/03088839.2024.2385846
Chavas, D.R., Emanuel, K.A., 2010. A QuikSCAT climatology of tropical cyclone size. Geophys. Res. Lett. 37. https://doi.org/10.1029/2010gl044558
Cheng, T., Veitch, E.A., Utne, I.B., Ramos, M.A., Mosleh, A., Alsos, O.A., Wu, B., 2024. Analysis of human errors in human-autonomy collaboration in autonomous ships operations through shore control experimental data. Reliab. Eng. Syst. Saf. 246, 110080. https://doi.org/10.1016/j.ress.2024.110080
Cho, H., Park, H., 2017. Constructing resilience model of port infrastructure based on system dynamics. Int. J. Saf. Secur. Eng. 7, 352–360. https://doi.org/10.2495/SAFE-V7-N3-352-360
Cho, H.S., Lee, J.S., Moon, H.C., 2018. Maritime Risk in Seaport Operation: A Cross-Country Empirical Analysis with Theoretical Foundations. Asian J. Shipp. Logist. 34, 240–247. https://doi.org/10.1016/j.ajsl.2018.09.010
Choi, J.S., Jin, H.H., Lee, J.J., 2022. Basic study on the improvement of cargo vehicle parking capacity and parking correction coefficient in port using literature research method. J. Korean Asph. Inst. 12, 90–99. https://doi.org/10.22702/JKAI.2022.12.1.8
Chua, C.T., Otake, T., Li, T., Cheng, A.-C., Qiu, Q., Li, L., Suppasri, A., Imamura, F., Switzer, A.D., 2024. An approach to assessing tsunami risk to the global port network under rising sea levels. Npj Nat. Hazards 1, 38. https://doi.org/10.1038/s44304-024-00039-2
Cohen, J., 1960. A Coefficient of Agreement for Nominal Scales. Educ. Psychol. Meas. 20, 37–46. https://doi.org/10.1177/001316446002000104
Cooper, M.D., 2022. The Emperor has no clothes: A critique of Safety-II. Saf. Sci. 152, 105047. https://doi.org/10.1016/j.ssci.2020.105047
Cormen, T.H., 2009. Introduction to algorithms. MIT press.
Cover, T.M., Thomas, J.A., 2005. Elements of Information Theory, 1st ed. Wiley. https://doi.org/10.1002/047174882X
Critical infrastructure resilience: Final report and recommendations., 2009.

Cui, H., Notteboom, T., 2018. A game theoretical approach to the effects of port objective orientation and service differentiation on port authorities' willingness to cooperate. Res. Transp. Bus. Manag. 26, 76–86. https://doi.org/10.1016/j.rtbm.2018.03.007

D'Agostino, R.B., 1986. Goodness-of-Fit-Techniques. CRC Press.

Darbra, R.-M., Casal, J., 2004. Historical analysis of accidents in seaports. Saf. Sci. 42, 85–98. https://doi.org/10.1016/S0925-7535(03)00002-X

DARMAWAN, D., 2024. Distribution of Six Major Factors Enhancing Organizational Effectiveness. J. Distrib. Sci. 22, 47–58. https://doi.org/10.15722/JDS.22.04.202404.47

De Neira, A.B., Kantarci, B., Nogueira, M., 2023. Distributed denial of service attack prediction: Challenges, open issues and opportunities. Comput. Netw. 222, 109553. https://doi.org/10.1016/j.comnet.2022.109553

Đelović, D., 2024. Criticality Analysis of A Sea Port`s Shore Cranes Using Analytic Hierarchy Process Method. Open Transp. J. 18, e26671212293095. https://doi.org/10.2174/0126671212293095240314040205

Deng, Z.Z.W., 2000. Crane Design Manual(Chinese Edition). ZHANG ZHI WEN DENG: 9787113025717 - AbeBooks. https://www.abebooks.co.uk/9787113025717/Crane-Design-ManualChinese-Edition-ZHANG-7113025714/plp.

Deryugina, T., Kawano, L., Levitt, S., 2018. The Economic Impact of Hurricane Katrina on Its Victims: Evidence from Individual Tax Returns. Am. Econ. J. Appl. Econ. 10, 202–233. https://doi.org/10.1257/app.20160307

Di Ludovico, M., De Martino, G., Prota, A., Manfredi, G., Dolce, M., 2022. Relationships between empirical damage and direct/indirect costs for the assessment of seismic loss scenarios. Bull. Earthq. Eng. 20, 229–254. https://doi.org/10.1007/s10518-021-01235-5

Diao, X., Zhao, Y., Smidts, C., Vaddi, P.K., Li, R., Lei, H., Chakhchoukh, Y., Johnson, B., Blanc, K.L., 2024. Dynamic probabilistic risk assessment for electric grid cybersecurity. Reliab. Eng. Syst. Saf. 241, 109699. https://doi.org/10.1016/j.ress.2023.109699

Díez, F.J., 1993. Parameter adjustment in Bayes networks. The generalized noisy OR–gate, in: Uncertainty in Artificial Intelligence. Elsevier, pp. 99–105. https://doi.org/10.1016/B978-1-4832-1451-1.50016-0

Diez, F.J., Druzdzel, M.J., 2006. Canonical probabilistic models for knowledge engineering. Technical report, UNED. http://www.cisiad.uned.es.

Dillon, R.L., Liebe, R.M., Bestafka, T., 2009. Risk-Based Decision Making for Terrorism Applications. Risk Anal. 29, 321–335. https://doi.org/10.1111/j.1539-6924.2008.01196.x

DNV GL, 2018. Port & Terminal Incident Database – 2018 Annual Report. (Open PDF at https://rules.dnvgl.com/PortIncidentDB2018.pdf).

Du, X., Hajjar, J.F., 2024. Methodology for collapse fragility development for hurricane events: Electrical transmission towers. J. Constr. Steel Res. 223, 109005. https://doi.org/10.1016/j.jcsr.2024.109005

Eberechukwu Onwuegbuchunam, D., Okechukwu Okeke, K., Olatude Aponjolosun, M., Igboanusi, C., 2021. Impacts of Terrorism and Piracy on Maritime Activities: An Exploratory Study. Int. J. Transp. Eng. Technol. 7, 104. https://doi.org/10.11648/j.ijtet.20210704.13

Emanuel, K., 2006. Climate and Tropical Cyclone Activity: A New Model Downscaling Approach. J. Clim. 19, 4797–4802. https://doi.org/10.1175/JCLI3908.1

Emanuel, K., 2005. Increasing destructiveness of tropical cyclones over the past 30 years. Nature 436, 686–688. https://doi.org/10.1038/nature03906

Engineers, A.S.O.C., 2014. Seismic design of Piers and Wharves. American Society of Civil Engineers. ISBN: 9780784413487.

Erik, H., 2017. FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems, 1st ed. CRC Press. https://doi.org/10.1201/9781315255071

European Committee for Standardization (CEN), 2014. EN 13001-2: Cranes—General Design—Part 2: Load Actions. (SIST EN 13001-2:2014 adoption).

Ezell, B.C., Bennett, S.P., Von Winterfeldt, D., Sokolowski, J., Collins, A.J., 2010. Probabilistic Risk Analysis and Terrorism Risk. Risk Anal. 30, 575–589. https://doi.org/10.1111/j.1539-6924.2010.01401.x

Fan, H., Lyu, J., Wang, S., Gong, X., 2024. Leverage rule-based Bayesian network on assessing straits/canals resilience performance on a risk coupling analysis perspective. Marit. Policy Manag. 1–19. https://doi.org/10.1080/03088839.2024.2306952

Fan, S., Blanco-Davis, E., Yang, Z., Zhang, J., Yan, X., 2020. Incorporation of human factors into maritime accident analysis using a data-driven Bayesian network. Reliab. Eng. Syst. Saf. 203, 107070. https://doi.org/10.1016/j.ress.2020.107070

Fan, S., Yang, Z., 2024. Accident data-driven human fatigue analysis in maritime transport using machine learning. Reliab. Eng. Syst. Saf. 241, 109675. https://doi.org/10.1016/j.ress.2023.109675

Fan, S., Yang, Z., Wang, J., Marsland, J., 2022. Shipping accident analysis in restricted waters: Lesson from the Suez Canal blockage in 2021. Ocean Eng. 266, 113119. https://doi.org/10.1016/j.oceaneng.2022.113119

Farrell, R., 2007. Maritime terrorism: focusing on the probable. Nav War Coll Rev 603 46–60.

Faturechi, R., Miller-Hooks, E., 2015. Measuring the Performance of Transportation Infrastructure Systems in Disasters: A Comprehensive Review. J. Infrastruct. Syst. 21, 04014025. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000212

FEMA, 2024a. Hazus_6.1_Hurricane_Model_Technical_Manual. Federal Emergency Management Agency.

FEMA, 2024b. Hazus Earthquake Model Technical Manual Hazus 6.1.

FEMA, 2020. Hazus Maritime Addendum – Hurricane Fragility Functions. https://www.fema.gov/sites/default/files/documents/fema_hazus-maritime-appendix-c.pdf.

FEMA, 2018. HAZUS Hurricane User Model Guide. https://www.fema.gov/.

Flynn, D., 2023. Mariner's Tropical Cyclone Guide. Tropical Analysis and Forecast Branch; National Hurricane Center National Weather; Service National Oceanic and Atmospheric Administration.

Folkman, D., Gharehgozli, A., Mileski, J., Galvao, C.B., 2021. Port resiliency and the effects of hurricanes on port operations. Int. J. Adv. Oper. Manag. 13, 409. https://doi.org/10.1504/IJAOM.2021.120779

Freire, W.P., Melo, W.S., Do Nascimento, V.D., Nascimento, P.R.M., De Sá, A.O., 2022. Towards a Secure and Scalable Maritime Monitoring System Using Blockchain and Low-Cost IoT Technology. Sensors 22, 4895. https://doi.org/10.3390/s22134895

Friedman, N., Geiger, D., Goldszmidt, M., 1997. Bayesian Network Classifiers. Machine Learning 131–163. https://doi.org/10.1023/A:1007465528199

Galbusera, L., Giannopoulos, G., Argyroudis, S., Kakderi, K., 2018. A Boolean Networks Approach to Modeling and Resilience Analysis of Interdependent Critical Infrastructures. Comput.-Aided Civ. Infrastruct. Eng. 33, 1041–1055. https://doi.org/10.1111/mice.12371

Ganor, B., 2002. Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? Police Pract. Res. 3, 287–304. https://doi.org/10.1080/1561426022000032060

Geerlings, H., Kuipers, B., Zuidwijk, R. (Eds.), 2017. Ports and Networks: Strategies, Operations and Perspectives, 1st ed. Routledge, Abingdon, Oxon ; New York, NY : Routledge, 2018. https://doi.org/10.4324/9781315601540

Geiger, T., Frieler, K., Bresch, D.N., 2018. A global historical data set of tropical cyclone exposure (TCE-DAT). Earth Syst. Sci. Data 10, 185–194. https://doi.org/10.5194/essd-10-185-2018

George, P.G., Renjith, V.R., 2021. Evolution of Safety and Security Risk Assessment methodologies towards the use of Bayesian Networks in Process Industries. Process Saf. Environ. Prot. 149, 758–775. https://doi.org/10.1016/j.psep.2021.03.031

Global Terrorism Database (GTD), Codebook: methodology, inclusion criteria, and variables, 2021.

Gourisetti, S.N.G., Mylrea, M., Patangia, H., 2020. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Gener. Comput. Syst. 105, 410–431. https://doi.org/10.1016/j.future.2019.12.018

Grainger, A., Achuthan, K., 2014. Port resilience: a primer.

Greenberg, M., Chalk, P., Willis, H., Khilko, I., Ortiz, D., 2006. Maritime Terrorism: Risk and Liability. RAND Corporation. https://doi.org/10.7249/MG520

Grigoryev, I., 2015. AnyLogic 7 in three days: A Quick Course in Simulation Modeling. CreateSpace Independent Publishing Platform.

Gros, X.E., 1997. Data Fusion – A Review, in: NDT Data Fusion. Elsevier, pp. 5–42. https://doi.org/10.1016/B978-034067648-6/50004-9
Gu, B., Liu, J., 2023. A systematic review of resilience in the maritime transport. Int. J. Logist. Res. Appl. 1–22. https://doi.org/10.1080/13675567.2023.2165051
Gunes, B., Kayisoglu, G., Bolat, P., 2021. Cyber security risk assessment for seaports: A case study of a container port. Comput. Secur. 103, 102196. https://doi.org/10.1016/j.cose.2021.102196
Guo, Y., Jin, Y., Hu, S., Yang, Z., Xi, Y., Han, B., 2023. Risk evolution analysis of ship pilotage operation by an integrated model of FRAM and DBN. Reliab. Eng. Syst. Saf. 229, 108850. https://doi.org/10.1016/j.ress.2022.108850
Guthery, F.S., Burnham, K.P., Anderson, D.R., 2003. Model Selection and Multimodel Inference: A Practical Information-Theoretic Approach. J. Wildl. Manag. 67, 655. https://doi.org/10.2307/3802723
Haas, J., 2016. Gard guidance on freight containers. Gard, ISBN: 978-82-90344-35-6.
Hacaga, M., 2020. An easy target?Types of attack on oil tankers by state actors. Secur. Def. Q. 28, 54–69. https://doi.org/10.35467/sdq/118147
Ham, D.-H., Park, J., 2020. Use of a big data analysis technique for extracting HRA data from event investigation reports based on the Safety-II concept. Reliab. Eng. Syst. Saf. 194, 106232. https://doi.org/10.1016/j.ress.2018.07.033
Han, D.-S., Han, G.-J., 2011. Force coefficient at each support point of a container crane according to the wind direction. Int. J. Precis. Eng. Manuf. 12, 1059–1064. https://doi.org/10.1007/s12541-011-0141-5
Hao, Z., Xu, Z., Zhao, H., Yang, L., 2023. Risk assessment model with probabilistic linguistic fuzzy inference methods for maritime piracy crime and applications. Appl. Soft Comput. 140, 110262. https://doi.org/10.1016/j.asoc.2023.110262
Henrion, M., 1989. Some Practical Issues in Constructing Belief Networks. in: Uncertainty in Artificial Intelligence. Elsevier Science Publisher B.V, North Holland, pp. 161-174.
Henriques De Gusmão, A.P., Mendonça Silva, M., Poleto, T., Camara E Silva, L., Cabral Seixas Costa, A.P., 2018. Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. Int. J. Inf. Manag. 43, 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008
Hirose, T., Sawaragi, T., 2020. Extended FRAM model based on cellular automaton to clarify complexity of socio-technical systems and improve their safety. Saf. Sci. 123, 104556. https://doi.org/10.1016/j.ssci.2019.104556
Hirose, T., Sawaragi, T., 2019. Development of FRAM Model Based on Structure of Complex Adaptive Systems to Visualize Safety of Socio-Technical Systems. IFAC-Pap. 52, 13–18. https://doi.org/10.1016/j.ifacol.2019.12.075
Hoaglin, D.C., Mosteller, F., Tukey, J.W., 2000. Understanding robust and exploratory data analysis. John Wiley & Sons.
Hoite, S., McCarthy, P., Jordan, M., 2018. Tie-Down Design Considerations for STS Container Cranes." Port Technology International 77.
Holland, G.J., 1980. An analytic model of the wind and pressure profiles in hurricanes. Monthly Weather Review, 108(8), 1212–1218.
Hollnagel, E., 2018. Safety–I and Safety–II: The Past and Future of Safety Management, 1st ed. CRC Press. https://doi.org/10.1201/9781315607511
Hollnagel, E., 1998. Cognitive Reliability and Error Analysis Method (CREAM). Elsevier. https://doi.org/10.1016/B978-0-08-042848-2.X5000-3
Hollnagel, E., Rees Hill, Slater, D., 2023. The FRAM model Visualiser (FMV)-The Web Version. https://doi.org/10.13140/RG.2.2.23719.32162
Hollnagel, E., Wears, R.L., Braithwaite, J., 2015. From Safety-I to Safety-II: A White Paper. https://doi.org/10.13140/RG.2.1.4051.5282
Hong, N., 2012. Charting a Maritime Security Cooperation Mechanism in the Indian Ocean: Sharing Responsibilities among Littoral States and User States. Strateg. Anal. 36, 400–412. https://doi.org/10.1080/09700161.2012.670539
Hossain, N.U.I., Amrani, S.E., Jaradat, R., Marufuzzaman, M., Buchanan, R., Rinaudo, C., Hamilton, M., 2020. Modeling and assessing interdependencies between critical infrastructures using

Bayesian network: A case study of inland waterway port and surrounding supply chain network. Reliab. Eng. Syst. Saf. 198, 106898. https://doi.org/10.1016/j.ress.2020.106898

Hossain, N.U.I., Nur, F., Hosseini, S., Jaradat, R., Marufuzzaman, M., Puryear, S.M., 2019. A Bayesian network based approach for modeling and assessing resilience: A case study of a full service deep water port. Reliab. Eng. Syst. Saf. 189, 378–396. https://doi.org/10.1016/j.ress.2019.04.037

Hosseini, S., Barker, K., 2016. Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. Comput. Ind. Eng. 93, 252–266. https://doi.org/10.1016/j.cie.2016.01.007

Hosseini, S., Barker, K., Ramirez-Marquez, J.E., 2016. A review of definitions and measures of system resilience. Reliab. Eng. Syst. Saf. 145, 47–61. https://doi.org/10.1016/j.ress.2015.08.006

Hu, J.-L., Tang, X.-W., Qiu, J.-N., 2016. Assessment of seismic liquefaction potential based on Bayesian network constructed from domain knowledge and history data. Soil Dyn. Earthq. Eng. 89, 49–60. https://doi.org/10.1016/j.soildyn.2016.07.007

Huang, Z., He, Z., Zhao, P., Zhang, C., Niu, Y., Guo, W., Cui, Y., Shao, W., 2024. The effects of tropical cyclone on the container shipping network: A case study of typhoon Ma-on (2022). Transp. Res. Part Transp. Environ. 136, 104449. https://doi.org/10.1016/j.trd.2024.104449

Iai, S., 2019. Evaluation of performance of port structures during earthquakes. Soil Dyn. Earthq. Eng. 126, 105192. https://doi.org/10.1016/j.soildyn.2018.04.055

IMO, 2022. GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.

International Taskforce, 2019. International Taskforce Port Call Optimization, Port Call Process Handbook. Appendix to Port Call Process. Sect. 17-18.

Izaguirre, C., Losada, I.J., Camus, P., Vigh, J.L., Stenek, V., 2021. Climate change risk to global port operations. Nat. Clim. Change 11, 14–20. https://doi.org/10.1038/s41558-020-00937-z

Jensen, A., Aven, T., 2018. A new definition of complexity in a risk analysis setting. Reliab. Eng. Syst. Saf. 171, 169–173. https://doi.org/10.1016/j.ress.2017.11.018

Ji, Z., Xia, Q., Meng, G., 2015. A Review of Parameter Learning Methods in Bayesian Network, in: Huang, D.-S., Han, K. (Eds.), Advanced Intelligent Computing Theories and Applications, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 3–12. https://doi.org/10.1007/978-3-319-22053-6_1

Jian, W., Liu, C., Lam, J.S.L., 2019. Cyclone risk model and assessment for East Asian container ports. Ocean Coast. Manag. 178, 104796. https://doi.org/10.1016/j.ocecoaman.2019.04.023

Jian-Bo Yang, Dong-Ling Xu, 2002. On the evidential reasoning algorithm for multiple attribute decision analysis under uncertainty. IEEE Trans. Syst. Man Cybern. - Part Syst. Hum. 32, 289–304. https://doi.org/10.1109/TSMCA.2002.802746

Jiang, L., Cai, Z., Wang, D., Zhang, H., 2012. Improving Tree augmented Naive Bayes for class probability estimation. Knowl.-Based Syst. 26, 239–245. https://doi.org/10.1016/j.knosys.2011.08.010

Jiang, M., Lu, J., 2020. The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. Transp. Res. Part E Logist. Transp. Rev. 139, 101965. https://doi.org/10.1016/j.tre.2020.101965

Jo, J.-H., Kim, S., 2019. Key Performance Indicator Development for Ship-to-Shore Crane Performance Assessment in Container Terminal Operations. J. Mar. Sci. Eng. 8, 6. https://doi.org/10.3390/jmse8010006

John, A., Paraskevadakis, D., Bury, A., Yang, Z., Riahi, R., Wang, J., 2014a. An integrated fuzzy risk assessment for seaport operations. Saf. Sci. 68, 180–194. https://doi.org/10.1016/j.ssci.2014.04.001

John, A., Yang, Z., Riahi, R., Wang, J., 2014b. Application of a collaborative modelling and strategic fuzzy decision support system for selecting appropriate resilience strategies for seaport operations. J. Traffic Transp. Eng. Engl. Ed. 1, 159–179. https://doi.org/10.1016/S2095-7564(15)30101-X

Jones, B., Jenkinson, I., Yang, Z., Wang, J., 2010. The use of Bayesian network modelling for maintenance planning in a manufacturing industry. Reliab. Eng. Syst. Saf. 95, 267–277. https://doi.org/10.1016/j.ress.2009.10.007

Joyner, C.C., 1989. Suppression of Terrorism on the High Seas: The 1988 IMO Convention on the Safety of Maritime Navigation, in: Israel Yearbook on Human Rights. Brill Nijhoff, pp. 343–369. https://doi.org/10.1163/9789004423039_019

Kabir, S., Papadopoulos, Y., 2019. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review. Saf. Sci. 115, 154–175. https://doi.org/10.1016/j.ssci.2019.02.009

Kamal, B., Çakır, E., 2022. Data-driven Bayes approach on marine accidents occurring in Istanbul strait. Appl. Ocean Res. 123, 103180. https://doi.org/10.1016/j.apor.2022.103180

Kang, J.-H., Lee, S.-J., 2008. Experimental study of wind load on a container crane located in a uniform flow and atmospheric boundary layers. Eng. Struct. 30, 1913–1921. https://doi.org/10.1016/j.engstruct.2007.12.013

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.-H., 2022. Maritime cybersecurity: are onboard systems ready? Marit. Policy Manag. 1–19. https://doi.org/10.1080/03088839.2022.2124464

Karnon, J., Stahl, J., Brennan, A., Caro, J.J., Mar, J., Möller, J., 2012. Modeling Using Discrete Event Simulation: A Report of the ISPOR-SMDM Modeling Good Research Practices Task Force–4. Med. Decis. Making 32, 701–711. https://doi.org/10.1177/0272989X12455462

Kavallieratos, G., Katsikas, S., Gkioulos, V., 2019. Cyber-Attacks Against the Autonomous Ship, in: Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Antón, A., Gritzalis, S., Mylopoulos, J., Kalloniatis, C. (Eds.), Computer Security, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 20–36. https://doi.org/10.1007/978-3-030-12786-2_2

Kavallieratos, G., Spathoulas, G., Katsikas, S., 2021. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. Sensors 21, 1691. https://doi.org/10.3390/s21051691

Kaya, G.K., Ozturk, F., Sariguzel, E.E., 2021. System-based risk analysis in a tram operating system: Integrating Monte Carlo simulation with the functional resonance analysis method. Reliab. Eng. Syst. Saf. 215, 107835. https://doi.org/10.1016/j.ress.2021.107835

Kazama, M., Noda, T., 2012. Damage statistics (Summary of the 2011 off the Pacific Coast of Tohoku Earthquake damage). Soils Found. 52, 780–792. https://doi.org/10.1016/j.sandf.2012.11.003

Kenneth, R., Howard, J., James, P., Michael, C., Carl, J., 2019. International Best Track Archive for Climate Stewardship (IBTrACS) Project, Version 4. https://doi.org/10.25921/82TY-9E16

Kessler, G.C., 2021. The CAN Bus in the Maritime Environment – Technical Overview and Cybersecurity Vulnerabilities. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 15, 531–540. https://doi.org/10.12716/1001.15.03.05

Kessler, G.C., Craiger, P., Haass, J.C., 2018. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 12, 429–437. https://doi.org/10.12716/1001.12.03.01

Kim, D., Oh, B., Han, S., Shim, J., 2004. Collapse of Container Cranes at Busan Ports under Typhoon Maemi. In Proceedings of the Fourteenth International Offshore and Polar Engineering Conference (ISOPE).

Kim, K.H., Park, Y.-M., 2004. A crane scheduling method for port container terminals. Eur. J. Oper. Res. 156, 752–768. https://doi.org/10.1016/S0377-2217(03)00133-4

Kim, S., Choi, S., Kim, C., 2021. The Framework for Measuring Port Resilience in Korean Port Case. Sustainability 13, 11883. https://doi.org/10.3390/su132111883

Kizilay, D., Eliiyi, D.T., 2021. A comprehensive review of quay crane scheduling, yard operations and integrations thereof in container terminals. Flex. Serv. Manuf. J. 33, 1–42. https://doi.org/10.1007/s10696-020-09385-5

Knaff, J.A., Sampson, C.R., DeMaria, M., Marchok, T.P., Gross, J.M., McAdie, C.J., 2007. Statistical Tropical Cyclone Wind Radii Prediction Using Climatology and Persistence. Weather Forecast. 22, 781–791. https://doi.org/10.1175/waf1026.1

Knyazeva, N.A., Korobeev, A.I., 2015. Maritime Terrorism and Piracy: The Threat to Maritime Security. Mediterr. J. Soc. Sci. https://doi.org/10.5901/mjss.2015.v6n6s3p226

Koks, E.E., Bočkarjova, M., De Moel, H., Aerts, J.C.J.H., 2015. Integrated Direct and Indirect Flood Risk Modeling: Development and Sensitivity Analysis. Risk Anal. 35, 882–900. https://doi.org/10.1111/risa.12300

Kołowrocki, K., Soszyńska-Budny, J., 2011. Reliability and safety of complex technical systems and processes: Modeling – Identification – Prediction - Optimization. Springer.

Komal, 2023. Fuzzy attack tree analysis of security threat assessment in an internet security system using algebraic t-norm and t-conorm, in: Engineering Reliability and Risk Assessment. Elsevier, pp. 53–64. https://doi.org/10.1016/B978-0-323-91943-2.00003-4

Konecranes, 2024. Ship-to-Shore Crane (STS): Monobox Technical Document.

Konecranes, 2021. STS Crane—Typical Technical Specification for the fastest ship turnaround time.

Kong, D., Lin, Z., Li, W., He, W., 2024. Development of an improved Bayesian network method for maritime accident safety assessment based on multiscale scenario analysis theory. Reliab. Eng. Syst. Saf. 251, 110344. https://doi.org/10.1016/j.ress.2024.110344

Konstandinidou, M., Nivolianitou, Z., Kiranoudis, C., Markatos, N., 2006. A fuzzy modeling application of CREAM methodology for human reliability analysis. Reliab. Eng. Syst. Saf. 91, 706–716. https://doi.org/10.1016/j.ress.2005.06.002

Kuhn, K., McIlhatton, D., Malcolm, J.A., Chapsos, I., 2023. Protective security at sea: a counter terrorism framework for cruise and passenger ships. WMU J. Marit. Aff. 22, 345–363. https://doi.org/10.1007/s13437-022-00296-w

Kuo, T.-C., Huang, W.-C., Wu, S.-C., Cheng, P.-L., 2006. A CASE STUDY OF INTER-ARRIVAL TIME DISTRIBUTIONS OF CONTAINER SHIPS. J. Mar. Sci. Technol. 14. https://doi.org/10.51400/2709-6998.2069

Kwesi-Buor, J., Menachof, D.A., Talas, R., 2019. Scenario analysis and disaster preparedness for port and maritime logistics risk management. Accid. Anal. Prev. 123, 433–447. https://doi.org/10.1016/j.aap.2016.07.013

Lagoudis, I.N., Naim, M.M., Potter, A.T., 2010. Strategic flexibility choices in the ocean transportation industry. Int. J. Shipp. Transp. Logist. 2, 187. https://doi.org/10.1504/IJSTL.2010.030866

Lai, K.K., Shih, K., 1992. A study of container berth allocation. J. Adv. Transp. 26, 45–60. https://doi.org/10.1002/atr.5670260105

Lam, J.S.L., Su, S., 2015. Disruption risks and mitigation strategies: an analysis of Asian ports. Marit. Policy Manag. 42, 415–435. https://doi.org/10.1080/03088839.2015.1016560

Landis, J.R., Koch, G.G., 1977. The Measurement of Observer Agreement for Categorical Data. Biometrics 33, 159. https://doi.org/10.2307/2529310

Larsen, M.H., Lund, M.S., 2021. Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. IEEE Access 9, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433

Laso, P.M., Salmon, L., Bozhilova, M., Ivanov, I., Stoianov, N., Velev, G., Claramunt, C., Yanakiev, Y., 2022. ISOLA: An Innovative Approach to Cyber Threat Detection in Cruise Shipping, in: Rocha, Á., Fajardo-Toro, C.H., Rodríguez, J.M.R. (Eds.), Developments and Advances in Defense and Security, Smart Innovation, Systems and Technologies. Springer Singapore, Singapore, pp. 71–81. https://doi.org/10.1007/978-981-16-4884-7_7

Lau, Y., Chen, Q., Poo, M.C.-P., Ng, A.K.Y., Ying, C.C., 2024. Maritime transport resilience: A systematic literature review on the current state of the art, research agenda and future research directions. Ocean Coast. Manag. 251, 107086. https://doi.org/10.1016/j.ocecoaman.2024.107086

Lavelle, F.M., Goodhue, C., Lyons, D., 2020. Critical path method assessment of community recovery (No. NIST GCR 20-023). National Institute of Standards and Technology (U.S.), Gaithersburg, MD. https://doi.org/10.6028/NIST.GCR.20-023

Lee, J., Chung, H., 2018. A new methodology for accident analysis with human and system interaction based on FRAM: Case studies in maritime domain. Saf. Sci. 109, 57–66. https://doi.org/10.1016/j.ssci.2018.05.011

Lee, K., 2019. Ductile link tie-down systems for quay cranes. Liftech Consultants. (www.porttechnology.org).

Lee, S.-J., Kang, J.-H., 2008. Wind load on a container crane located in atmospheric boundary layers. J. Wind Eng. Ind. Aerodyn. 96, 193–208. https://doi.org/10.1016/j.jweia.2007.04.003

León-Mateos, F., Sartal, A., López-Manuel, L., Quintás, M.A., 2021. Adapting our sea ports to the challenges of climate change: Development and validation of a Port Resilience Index. Mar. Policy 130, 104573. https://doi.org/10.1016/j.marpol.2021.104573

Li, H., Çelik, C., Bashir, M., Zou, L., Yang, Z., 2024a. Incorporation of a global perspective into data-driven analysis of maritime collision accident risk. Reliab. Eng. Syst. Saf. 249, 110187. https://doi.org/10.1016/j.ress.2024.110187

Li, H., Ren, X., Yang, Z., 2023. Data-driven Bayesian network for risk analysis of global maritime accidents. Reliab. Eng. Syst. Saf. 230, 108938. https://doi.org/10.1016/j.ress.2022.108938

Li, H., Yang, Z., 2023. Towards safe navigation environment: The imminent role of spatio-temporal pattern mining in maritime piracy incidents analysis. Reliab. Eng. Syst. Saf. 238, 109422. https://doi.org/10.1016/j.ress.2023.109422

Li, H., Zhou, K., Zhang, C., Bashir, M., Yang, Z., 2024b. Dynamic evolution of maritime accidents: Comparative analysis through data-driven Bayesian Networks. Ocean Eng. 303, 117736. https://doi.org/10.1016/j.oceaneng.2024.117736

Li, P., Chen, G., Dai, L., Zhang, L., 2012. A fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks. Saf. Sci. 50, 1569–1583. https://doi.org/10.1016/j.ssci.2012.03.017

Li, W., Asadabadi, A., Miller-Hooks, E., 2022. Enhancing resilience through port coalitions in maritime freight networks. Transp. Res. Part Policy Pract. 157, 1–23. https://doi.org/10.1016/j.tra.2022.01.015

Li, W., Zhang, L., Liang, W., 2017. An Accident Causation Analysis and Taxonomy (ACAT) model of complex industrial system from both system safety and control theory perspectives. Saf. Sci. 92, 94–103. https://doi.org/10.1016/j.ssci.2016.10.001

Li, Y., Ellingwood, B.R., 2006. Hurricane damage to residential construction in the US: Importance of uncertainty modeling in risk assessment. Eng. Struct. 28, 1009–1018. https://doi.org/10.1016/j.engstruct.2005.11.005

Liang, M., Li, H., Liu, R.W., Lam, J.S.L., Yang, Z., 2024. PiracyAnalyzer: Spatial temporal patterns analysis of global piracy incidents. Reliab. Eng. Syst. Saf. 243, 109877. https://doi.org/10.1016/j.ress.2023.109877

Liang, X., Fan, S., Lucy, J., Yang, Z., 2022. Risk analysis of cargo theft from freight supply chains using a data-driven Bayesian network. Reliab. Eng. Syst. Saf. 226, 108702. https://doi.org/10.1016/j.ress.2022.108702

Liebherr Container Cranes, 2025. Technical Description: Ship-to-Shore Gantry Cranes (STS).

Lin, J., Qian, T., Klotzbach, P., 2022. Tropical Cyclones. Atmosphere-Ocean 60, 360–398. https://doi.org/10.1080/07055900.2022.2086849

Liu, K., Yu, Q., Yang, Zhisen, Wan, C., Yang, Zaili, 2022. BN-based port state control inspection for Paris MoU: New risk factors and probability training using big data. Reliab. Eng. Syst. Saf. 224, 108530. https://doi.org/10.1016/j.ress.2022.108530

Liu, K., Yu, Q., Yuan, Z., Yang, Z., Shu, Y., 2021. A systematic analysis for maritime accidents causation in Chinese coastal waters using machine learning approaches. Ocean Coast. Manag. 213, 105859. https://doi.org/10.1016/j.ocecoaman.2021.105859

Liu, L., 2021. The Politics of (No) Compromise: Information Acquisition, Policy Discretion, and Reputation. https://doi.org/10.48550/ARXIV.2111.00522

Liu, Y., Fu, X., Wang, K., Zheng, S., Xiao, Y., 2024. Bibliometric analysis and literature review on maritime transport resilience and its associated impacts on trade. Marit. Policy Manag. 1–38. https://doi.org/10.1080/03088839.2024.2367971

Loh, H.S., Thai, V.V., 2015a. Management of disruptions by seaports: preliminary findings. Asia Pac. J. Mark. Logist. 27, 146–162. https://doi.org/10.1108/APJML-04-2014-0053

Loh, H.S., Thai, V.V., 2015b. Cost Consequences of a Port-Related Supply Chain Disruption. Asian J. Shipp. Logist. 31, 319–340. https://doi.org/10.1016/j.ajsl.2015.09.001

Lu, X., Wong, W., Yu, H., Yang, X., 2022. Tropical Cyclone Size Identification over the Western North Pacific Using Support Vector Machine and General Regression Neural Network. J. Meteorol. Soc. Jpn. Ser II 100, 927–941. https://doi.org/10.2151/jmsj.2022-048

LÜScher, L.S., Lewis, M.W., 2008. Organizational Change and Managerial Sensemaking: Working Through Paradox. Acad. Manage. J. 51, 221–240. https://doi.org/10.5465/amj.2008.31767217

Madhusudan, C., Ganapathy, G.P., 2011. Disaster resilience of transportation infrastructure and ports – An overview. Int. J. Geomat. Geosci. Vol. 2 Issue 2.

Majumdar, A., Manole, I., Nalty, R., 2022. Analysis of Port Accidents and Calibration of Heinrich's Pyramid. Transp. Res. Rec. J. Transp. Res. Board 2676, 476–489. https://doi.org/10.1177/03611981211044447

Mansouri, M., Nilchiani, R., Mostashari, A., 2010. A policy making framework for resilient port infrastructure systems. Mar. Policy 34, 1125–1134. https://doi.org/10.1016/j.marpol.2010.03.012

Mansouri, M., Sauser, B., Boardman, J., 2009. Applications of systems thinking for resilience study in Maritime Transportation System of Systems, in: 2009 3rd Annual IEEE Systems Conference. Presented at the 2009 3rd Annual IEEE Systems Conference, IEEE, Vancouver, BC, Canada, pp. 211–217. https://doi.org/10.1109/SYSTEMS.2009.4815800

Martinetti, A., Chatzimichailidou, M.M., Maida, L., Van Dongen, L., 2019. Safety I–II, resilience and antifragility engineering: a debate explained through an accident occurring on a mobile elevating work platform. Int. J. Occup. Saf. Ergon. 25, 66–75. https://doi.org/10.1080/10803548.2018.1444724

Martins, J.B., Carim, G., Saurin, T.A., Costella, M.F., 2022. Integrating Safety-I and Safety-II: Learning from failure and success in construction sites. Saf. Sci. 148, 105672. https://doi.org/10.1016/j.ssci.2022.105672

MCAD, 2023. Maritime Cyber Attack Database.

McCarthy, P., Soderberg, E., Dix, A., 2009. Wind damage to dockside cranes: recent failures and recommendations. TCLEE conference.

Meland, P.Há., Bernsmed, K., Wille, E., Rødseth, Ø.J., Nesheim, D.A., 2021. A Retrospective Analysis of Maritime Cyber Security Incidents. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 15, 519–530. https://doi.org/10.12716/1001.15.03.04

Meng, H., An, X., Xing, J., 2022. A data-driven Bayesian network model integrating physical knowledge for prioritization of risk influencing factors. Process Saf. Environ. Prot. 160, 434–449. https://doi.org/10.1016/j.psep.2022.02.010

Merz, B., Hall, J., Disse, M., Schumann, A., 2010. Fluvial flood risk management in a changing world. Nat. Hazards Earth Syst. Sci. 10, 509–527. https://doi.org/10.5194/nhess-10-509-2010

Miller, V., Bear-Crozier, A.N., Newey, V., Horspool, N., Weber, R., 2016. Probabilistic Volcanic Ash Hazard Analysis (PVAHA) II: assessment of the Asia-Pacific region using VAPAH. J. Appl. Volcanol. 5, 4. https://doi.org/10.1186/s13617-016-0044-3

Mitra, A., Youdon, C., Chauhan, P., Shaw, R., 2024. Systemic risk capability assessment methodology: A new approach for evaluating inter-connected risks in seaport ecosystems. Prog. Disaster Sci. 22, 100325. https://doi.org/10.1016/j.pdisas.2024.100325

Mitrani, I., 2008. Probabilistic Modelling. Cambridge University Press; 2nd edition. 978-0521585309.

Mkrtchyan, L., Podofillini, L., Dang, V.N., 2016. Methods for building Conditional Probability Tables of Bayesian Belief Networks from limited judgment: An evaluation for Human Reliability Application. Reliab. Eng. Syst. Saf. 151, 93–112. https://doi.org/10.1016/j.ress.2016.01.004

Modarres, M., Kaminskiy, M., Krivtsov, V., 2016. Reliability Engineering and Risk Analysis: A Practical Guide. CRC Press; 3rd edition.

Mohaghegh, Z., Kazemi, R., Mosleh, A., 2009. Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization. Reliab. Eng. Syst. Saf. 94, 1000–1018. https://doi.org/10.1016/j.ress.2008.11.006

Mohsendokht, M., Kontovas, C., Chang, C.-H., Qu, Z., Li, H., Yang, Z., 2025. Resilience analysis of seaports: a critical review of development and research directions. Marit. Policy Manag. 1–36. https://doi.org/10.1080/03088839.2025.2483410

Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., Yang, Z., 2024. Enhancing maritime transportation security: A data-driven Bayesian network analysis of terrorist attack risks. Risk Anal. risa.15750. https://doi.org/10.1111/risa.15750

Monroe, J., Ramsey, E., Berglund, E., 2018. Allocating countermeasures to defend water distribution systems against terrorist attack. Reliab. Eng. Syst. Saf. 179, 37–51. https://doi.org/10.1016/j.ress.2018.02.014

Mostashari, A., Nilchiani, R., Omer, M., Andalibi, N., Heydari, B., 2011. A Cognitive Process Architecture Framework for Secure and Resilient Seaport Operations. Mar. Technol. Soc. J. 45, 120–127. https://doi.org/10.4031/MTSJ.45.3.13

Mutombo, K., Ölçer, A.I., Kuroshi, L., 2017. A new approach to assessing port infrastructure resilience to climate risks and adaptive solutions prioritization. Journal of Maritime Research. https://doi.org/Vol XIV. No. III, pp 56–67.

Na, U.J., Shinozuka, M., 2009. Simulation-based seismic loss estimation of seaport transportation system. Reliab. Eng. Syst. Saf. 94, 722–731. https://doi.org/10.1016/j.ress.2008.07.005

Nalebuff, B., Brandenburger, A., Maulana, A., 1996. Co-Opetition. London: HarperCollins Business.

Nelson, E.S., 2012. Maritime Terrorism and Piracy: Existing and Potential Threats.

Netica (Version 607)., 2019.

Nincic, D.J., 2005. The challenge of maritime terrorism: Threat identification, WMD and regime response. J. Strateg. Stud. 28, 619–644. https://doi.org/10.1080/01402390500301020

Notteboom, T., Pallis, A., Rodrigue, J.-P., 2021. Port Economics, Management and Policy, 1st ed. Routledge, London. https://doi.org/10.4324/9780429318184

Öğütçü, G., Testik, Ö.M., Chouseinoglou, O., 2016. Analysis of personal information security behavior and awareness. Comput. Secur. 56, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Olalla, O.R., 2012. Assessing the Resilience of Global Sea Routes.

Omer, M., Mostashari, A., Nilchiani, R., Mansouri, M., 2012. A framework for assessing resiliency of maritime transportation systems. Marit. Policy Manag. 39, 685–703. https://doi.org/10.1080/03088839.2012.689878

Oruc, A., Gkioulos, V., Katsikas, S., 2022. Towards a Cyber-Physical Range for the Integrated Navigation System (INS). J. Mar. Sci. Eng. 10, 107. https://doi.org/10.3390/jmse10010107

Pan, Q., 2015. Estimating the Economic Losses of Hurricane Ike in the Greater Houston Region. Nat. Hazards Rev. 16, 05014003. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000146

Pan, S., Yan, H., He, J., He, Z., 2021. Vulnerability and resilience of transportation systems: A recent literature review. Phys. Stat. Mech. Its Appl. 581, 126235. https://doi.org/10.1016/j.physa.2021.126235

Panahi, R., Sadeghi Gargari, N., Lau, Y., Ng, A.K.Y., 2022. Developing a resilience assessment model for critical infrastructures: The case of port in tackling the impacts posed by the Covid-19 pandemic. Ocean Coast. Manag. 226, 106240. https://doi.org/10.1016/j.ocecoaman.2022.106240

Papadimitriou, E., Pooyan Afghari, A., Tselentis, D., Van Gelder, P., 2022. Road-safety-II: Opportunities and barriers for an enhanced road safety vision. Accid. Anal. Prev. 174, 106723. https://doi.org/10.1016/j.aap.2022.106723

Park, C., Kontovas, C., Yang, Z., Chang, C.-H., 2023. A BN driven FMEA approach to assess maritime cybersecurity risks. Ocean Coast. Manag. 235, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Park, J., Kim, Ji-tae, Lee, S., Kim, Jonghyun, 2018. Modeling Safety-II based on unexpected reactor trips. Ann. Nucl. Energy 115, 280–293. https://doi.org/10.1016/j.anucene.2018.01.044

Patriarca, R., Di Gravio, G., Costantino, F., 2017. A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems. Saf. Sci. 91, 49–60. https://doi.org/10.1016/j.ssci.2016.07.016

Patriarca, R., Falegnami, A., Costantino, F., Bilotta, F., 2018. Resilience engineering for socio-technical risk analysis: Application in neuro-surgery. Reliab. Eng. Syst. Saf. 180, 321–335. https://doi.org/10.1016/j.ress.2018.08.001

Patriarca, R., Ramos, M., Paltrinieri, N., Massaiu, S., Costantino, F., Di Gravio, G., Boring, R.L., 2020. Human reliability analysis: Exploring the intellectual structure of a research field. Reliab. Eng. Syst. Saf. 203, 107102. https://doi.org/10.1016/j.ress.2020.107102

Patriarca, R., Simone, F., Di Gravio, G., 2022. Modelling cyber resilience in a water treatment and distribution system. Reliab. Eng. Syst. Saf. 226, 108653. https://doi.org/10.1016/j.ress.2022.108653

Pearl, J., 1988. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Morgan Kaufmann Publishers, Inc., San Mateo, Calif.

PEMA, 2019. Recommended Minimum Safety Features for Quay Container Cranes. A joint initiative from TT Club, ICHCA International and Port Equipment Manufacturers Association. ISBN 978-1-85330-034-9.

Pence, J., Mohaghegh, Z., 2020. A Discourse on the Incorporation of Organizational Factors into Probabilistic Risk Assessment: Key Questions and Categorical Review. Risk Anal. 40, 1183–1211. https://doi.org/10.1111/risa.13468

Peng, Y., Wang, W., Guo, Z., Song, X., Zhang, Q., 2016. A stochastic seaport network retrofit management problem considering shipping routing design. Ocean Coast. Manag. 119, 169–176. https://doi.org/10.1016/j.ocecoaman.2015.10.013

PIANC, 2020. Climate Change Adaptation Planning for Ports and Inland Waterways. Code: EnviCom WG 178.

PIANC WG-174, 2022. Resilience of Maritime and Inland Waterway Transport, Annex A—Port Resilience Scorecard, Tables A-2 & A-3.

Poo, M.C.-P., Yang, Z., 2022. Optimising the resilience of shipping networks to climate vulnerability. Marit. Policy Manag. 1–20. https://doi.org/10.1080/03088839.2022.2094488

Poo, M.C.-P., Zhang, W., Kamalian, L., Wang, T., Lau, Y., Xu, T.Z., 2024. Resilience of Chinese Ports to Tropical Cyclones: Operational Efficiency and Strategic Importance. Climate 12, 214. https://doi.org/10.3390/cli12120214

Port Technology International, 2024. Evergreen opens Kaohsiung Port's first automated container terminal. Port Technology International. https://www.porttechnology.org/news/evergreen-opens-kaohsiung-ports-first-automated-container-terminal/.

Prieto, C., Patel, D., Han, D., Dewals, B., Bray, M., Molinari, D., 2024. Preface: Advances in pluvial and fluvial flood forecasting and assessment and flood risk management. Nat. Hazards Earth Syst. Sci. 24, 3381–3386. https://doi.org/10.5194/nhess-24-3381-2024

Pristrom, S., Yang, Z., Wang, J., Yan, X., 2016. A novel flexible model for piracy and robbery assessment of merchant ship operations. Reliab. Eng. Syst. Saf. 155, 196–211. https://doi.org/10.1016/j.ress.2016.07.001

Progoulakis, I., Rohmeyer, P., Nikitakos, N., 2021. Cyber Physical Systems Security for Maritime Assets. J. Mar. Sci. Eng. 9, 1384. https://doi.org/10.3390/jmse9121384

Provan, D.J., Woods, D.D., Dekker, S.W.A., Rae, A.J., 2020. Safety II professionals: How resilience engineering can transform safety practice. Reliab. Eng. Syst. Saf. 195, 106740. https://doi.org/10.1016/j.ress.2019.106740

Python, G.C., Wakeman, T.H., 2016. Collaboration of Port Members for Supply Chain Resilience, in: Ports 2016. Presented at the 14th Triennial International Conference, American Society of Civil Engineers, New Orleans, LA, pp. 371–380. https://doi.org/10.1061/9780784479902.038

Qiao, W., Liu, Y., Ma, X., Lan, H., 2021. Cognitive Gap and Correlation of Safety-I and Safety-II: A Case of Maritime Shipping Safety Management. Sustainability 13, 5509. https://doi.org/10.3390/su13105509

Rajput, A., 2022. Maritime Security and Threat of a Terrorist Attack. Pace Int. Law Rev. 34, 1. https://doi.org/10.58948/2331-3536.1418

Rausand, M., Barros, A., Hoyland, A., 2020. System Reliability Theory: Models, Statistical Methods, and Applications, 1st ed, Wiley Series in Probability and Statistics. Wiley. https://doi.org/10.1002/9781119373940

Refaeilzadeh, P., Tang, L., Liu, H., 2009. Cross-Validation, in: Liu, L., Özsu, M.T. (Eds.), Encyclopedia of Database Systems. Springer US, Boston, MA, pp. 532–538. https://doi.org/10.1007/978-0-387-39940-9_565

Regens, J.L., Mould, N., Jensen, C.J., Graves, M.A., Edger, D.N., 2015. Probabilistic Graphical Modeling of Terrorism Threat Recognition Using Bayesian Networks and Monte Carlo Simulation. J. Cogn. Eng. Decis. Mak. 9, 295–311. https://doi.org/10.1177/1555343415592730

Reggiani, A., 2013. Network resilience for transport security: Some methodological considerations. Transp. Policy 28, 63–68. https://doi.org/10.1016/j.tranpol.2012.09.007

Ren, H., Guo, Q., 2023. Flexible learning tree augmented naïve classifier and its application. Knowl.-Based Syst. 260, 110140. https://doi.org/10.1016/j.knosys.2022.110140

Rezazadeh, A., Talarico, L., Reniers, G., Cozzani, V., Zhang, L., 2019. Applying game theory for securing oil and gas pipelines against terrorism. Reliab. Eng. Syst. Saf. 191, 106140. https://doi.org/10.1016/j.ress.2018.04.021

Rice, J., Trepte, K., 2012. The MIT CTL port resilience survey report.

Richardson, M., 2004. A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction. ISEAS Publishing. https://doi.org/10.1355/9789812305381

Riemersma, B., Correljé, A.F., Künneke, R.W., 2024. Incorporating Safety-II in future gas systems. Saf. Sci. 173, 106462. https://doi.org/10.1016/j.ssci.2024.106462

Robinson, S., 2005. Discrete-event simulation: from the pioneers to the present, what next? J. Oper. Res. Soc. 56, 619–629. https://doi.org/10.1057/palgrave.jors.2601864

Rodrigue, J.-P., 2024. The Geography of Transport Systems, 6th ed. Routledge, London. https://doi.org/10.4324/9781003343196

Rosa, L.V., Haddad, A.N., De Carvalho, P.V.R., 2015. Assessing risk in sustainable construction using the Functional Resonance Analysis Method (FRAM). Cogn. Technol. Work 17, 559–573. https://doi.org/10.1007/s10111-015-0337-z

Rosca, E., Rusca, F., Carlan, V., Stefanov, O., Dinu, O., Rusca, A., 2025. Assessing the Influence of Equipment Reliability over the Activity Inside Maritime Container Terminals Through Discrete-Event Simulation. Systems 13, 213. https://doi.org/10.3390/systems13030213

Rose, A., Wei, D., 2013. ESTIMATING THE ECONOMIC CONSEQUENCES OF A PORT SHUTDOWN: THE SPECIAL ROLE OF RESILIENCE. Econ. Syst. Res. 25, 212–232. https://doi.org/10.1080/09535314.2012.731379

Rousset, L., Ducruet, C., 2020. Disruptions in Spatial Networks: a Comparative Study of Major Shocks Affecting Ports and Shipping Patterns. Netw. Spat. Econ. 20, 423–447. https://doi.org/10.1007/s11067-019-09482-5

Salmon, P., Jenkins, D., Stanton, N., Walker, G., 2010. Hierarchical task analysis vs. cognitive work analysis: comparison of theory, methodology and contribution to system design. Theor. Issues Ergon. Sci. 11, 504–531. https://doi.org/10.1080/14639220903165169

Schauer, S., Polemi, N., Mouratidis, H., 2019. MITIGATE: a dynamic supply chain cyber risk assessment methodology. J. Transp. Secur. 12, 1–35. https://doi.org/10.1007/s12198-018-0195-z

Schinas, O., Metzger, D., 2023. Cyber-seaworthiness: A critical review of the literature. Mar. Policy 151, 105592. https://doi.org/10.1016/j.marpol.2023.105592

Schneider, P., 2020. Recent Trends in Global Maritime Terrorism.

Schneider, P., 2013. Maritime Terrorism: Governance and Non-State Actors, in: Jakobi, A.P., Wolf, K.D. (Eds.), The Transnational Governance of Violence and Crime. Palgrave Macmillan UK, London, pp. 172–192. https://doi.org/10.1057/9781137334428_9

Schott, T., Landsea, C., Hafele, G., Lorens, J., 2019. The Saffir-Simpson Hurricane Wind Scale. https://www.nhc.noaa.gov/pdf/sshws.pdf.pre20210528.

Schwenkenbecher, A., 2012. Terrorism: A Philosophical Enquiry. Palgrave Macmillan UK, London. https://doi.org/10.1057/9781137024220

Shafieezadeh, A., Ivey Burden, L., 2014. Scenario-based resilience assessment framework for critical infrastructure systems: Case study for seismic resilience of seaports. Reliab. Eng. Syst. Saf. 132, 207–219. https://doi.org/10.1016/j.ress.2014.07.021

Shah, R., 2013. Maritime Counter-terrorism: The Challenges of Centre–State Relations in India. Marit. Aff. Natl. Marit. Found. India 9, 20–41. https://doi.org/10.1080/09733159.2013.837246

Shannon, C.E., S., C.E., 1949. The Mathematical Theory of Communication; University of Illinois Press: Champaign, IL, USA,.

Shaw, D.R., Grainger, A., Achuthan, K., 2017. Multi-level port resilience planning in the UK: How can information sharing be made easier? Technol. Forecast. Soc. Change 121, 126–138. https://doi.org/10.1016/j.techfore.2016.10.065

Sheng, T., Weng, J., Shi, K., Han, B., 2024. Analysis of human errors in maritime accidents: A Bayesian spatial multinomial logistic model. J. Transp. Saf. Secur. 16, 594–610. https://doi.org/10.1080/19439962.2023.2235323

Shipmentlink, 2025. Shipment dashboard. https://ss.shipmentlink.com.

Simsekler, M.C.E., Qazi, A., 2022. Adoption of a Data-Driven Bayesian Belief Network Investigating Organizational Factors that Influence Patient Safety. Risk Anal. 42, 1277–1293. https://doi.org/10.1111/risa.13610

Slim, H., Nadeau, S., 2020. A Mixed Rough Sets/Fuzzy Logic Approach for Modelling Systemic Performance Variability with FRAM. Sustainability 12, 1918. https://doi.org/10.3390/su12051918

Srinivas, S., 1993. A generalization of the noisy-or model. In: Proceedings of the Ninth international conference on Uncertainty in artificial intelligence. Elsevier, pp. 208-215.

Stanton, N.A., 2006. Hierarchical task analysis: Developments, applications, and extensions. Appl. Ergon. 37, 55–79. https://doi.org/10.1016/j.apergo.2005.06.003

Stanton, N.A., 2004. Systematic human error reduction and prediction approach (SHERPA). In Handbook of human factors and ergonomics methods (pp. 394-403). CRC Press.

START (National consortium for the study of terrorism and responses to terrorism), Global Terrorism Database (GTD) [Dataset], 2023.

Struck, M.C., Stoppe, J., 2021. A Backwards Compatible Approach to Authenticate Automatic Identification System Messages, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). Presented at the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, Rhodes, Greece, pp. 524–529. https://doi.org/10.1109/CSR51186.2021.9527954

Sturgis, L., Smythe, T., Tucci, A., 2014. Port Recovery in the Aftermath of Hurricane Sandy. Center for a New American Security.

Sunaryo, Hamka, M.A., 2017. Safety Risks Assessment on Container Terminal Using Hazard Identification and Risk Assessment and Fault Tree Analysis Methods. Procedia Eng. 194, 307–314. https://doi.org/10.1016/j.proeng.2017.08.150

Svilicic, B., Kamahara, J., Rooks, M., Yano, Y., 2019. Maritime Cyber Risk Management: An Experimental Ship Assessment. J. Navig. 72, 1108–1120. https://doi.org/10.1017/S0373463318001157

Tam, K., Jones, K., 2019. MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J. Marit. Aff. 18, 129–163. https://doi.org/10.1007/s13437-019-00162-2

Tan, A.T.H., 2012. The Emergence of Naval Power in the Straits of Malacca. Def. Stud. 12, 106–135. https://doi.org/10.1080/14702436.2012.683975

Tang, D., Fang, Y.-P., Zio, E., 2023. Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods. Reliab. Eng. Syst. Saf. 235, 109212. https://doi.org/10.1016/j.ress.2023.109212

Tang, Y., Zhang, X., Zhou, Y., Huang, Y., Zhou, D., 2023. A new correlation belief function in Dempster-Shafer evidence theory and its application in classification. Sci. Rep. 13, 7609. https://doi.org/10.1038/s41598-023-34577-y

Tanoue, M., Taguchi, R., Nakata, S., Watanabe, S., Fujimori, S., Hirabayashi, Y., 2020. Estimation of Direct and Indirect Economic Losses Caused by a Flood With Long-Lasting Inundation: Application to the 2011 Thailand Flood. Water Resour. Res. 56, e2019WR026092. https://doi.org/10.1029/2019WR026092

TDB, 2024. CWA RDC28 Typhoon Database web tool. (https://rdc28.cwa.gov.tw/TDB/public/basic_query/).

Tertia, J., Perwita, A.A.B., 2018. Maritime Security in Indo-Pacific: Issues, Challenges, and Prospects. J. Ilm. Hub. Int. 14, 77. https://doi.org/10.26593/jihi.v14i1.2795.77-95

Thomas, C.M., Featherstone, W.E., 2005. Validation of Vincenty's Formulas for the Geodesic Using a New Fourth-Order Extension of Kivioja's Formula. J. Surv. Eng. 131, 20–26. https://doi.org/10.1061/(ASCE)0733-9453(2005)131:1(20)

Tilly, C., 2004. Terror, Terrorism, Terrorists. Sociol. Theory 22, 5–13. https://doi.org/10.1111/j.1467-9558.2004.00200.x

Toğan, V., Eirgash, M.A., 2019. Time-Cost Trade-Off Optimization with a New Initial Population Approach. Tek. Dergi 30, 9561–9580. https://doi.org/10.18400/tekderg.410934

Touzinsky, K.F., Scully, B.M., Mitchell, K.N., Kress, M.M., 2018. Using Empirical Data to Quantify Port Resilience: Hurricane Matthew and the Southeastern Seaboard. J. Waterw. Port Coast. Ocean Eng. 144, 05018003. https://doi.org/10.1061/(ASCE)WW.1943-5460.0000446

Trabing, B.C., Penny, A.B., Martinez, J., Fritz, C., 2024. Are Forecasts of the Tropical Cyclone Radius of Maximum Wind Skillful? Geophys. Res. Lett. 51, e2024GL109663. https://doi.org/10.1029/2024GL109663

Trepte, K., James, B.R., 2014. An initial exploration of port capacity bottlenecks in the USA port system and the implications on resilience. Int. J. Shipp. Transp. Logist. 6, 339. https://doi.org/10.1504/IJSTL.2014.060800

TT CLUB, 2009. Wind storm II. Practical risk management guidance for marine and inland terminals. Second Edition.

Tunçel, A.L., Sezer, S.I., Elidolu, G., Uflaz, E., Akyuz, E., Arslan, O., 2024. A rule-based Bayesian network modelling under evidential reasoning theory for risk analysis of anchoring operation in maritime transportation. Ocean Eng. 292, 116521. https://doi.org/10.1016/j.oceaneng.2023.116521

Tusher, H.M., Munim, Z.H., Notteboom, T.E., Kim, T.-E., Nazir, S., 2022. Cyber security risk assessment in autonomous shipping. Marit. Econ. Logist. 24, 208–227. https://doi.org/10.1057/s41278-022-00214-0

Uflaz, E., Sezer, S.I., Tunçel, A.L., Aydin, M., Akyuz, E., Arslan, O., 2024. Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling. Reliab. Eng. Syst. Saf. 243, 109825. https://doi.org/10.1016/j.ress.2023.109825

UNCTAD, 2022a. Review of Maritime Transport.

UNCTAD, 2022b. BUILDING CAPACITY TO MANAGE RISKS AND ENHANCE RESILIENCE A Guidebook for Ports.

UNCTAD, 2010. Review of Maritime Transport 2010 (UNCTAD/RMT/2010). United Nations Conference on Trade and Development.*

USACE, 2019. EP 1100-1-5 Guide to Resilience Practices. https://www.publications.usace.army.mil/Portals/76/EP%201100-1-5.pdf.

Vanlaer, N., Albers, S., Guiette, A., Van Den Oord, S., Marynissen, H., 2022. 100% Operational! An organizational resilience perspective on ports as critical infrastructures. Case Stud. Transp. Policy 10, 57–65. https://doi.org/10.1016/j.cstp.2021.11.002

Verschuur, J., Koks, E.E., Hall, J.W., 2020. Port disruptions due to natural disasters: Insights into port and logistics resilience. Transp. Res. Part Transp. Environ. 85, 102393. https://doi.org/10.1016/j.trd.2020.102393

Verschuur, J., Koks, E.E., Li, S., Hall, J.W., 2023. Multi-hazard risk to global port infrastructure and resulting trade and logistics losses. Commun. Earth Environ. 4, 5. https://doi.org/10.1038/s43247-022-00656-7

Verschuur, J., Pant, R., Koks, E., Hall, J., 2022. A systemic risk framework to improve the resilience of port and supply-chain networks to natural hazards. Marit. Econ. Logist. 24, 489–506. https://doi.org/10.1057/s41278-021-00204-8

Wahl, A., Kongsvik, T., Antonsen, S., 2020. Balancing Safety I and Safety II: Learning to manage performance variability at sea using simulator-based training. Reliab. Eng. Syst. Saf. 195, 106698. https://doi.org/10.1016/j.ress.2019.106698

Wan, C., Yang, Z., Yan, X., Zhang, D., Blanco-Davis, E., Ren, J., 2019. Risk-Based Resilience Analysis of Maritime Container Transport Networks, in: Proceedings of the 29th European Safety and Reliability Conference (ESREL). Presented at the Proceedings of the 29th European Safety and Reliability Conference (ESREL), Research Publishing Services, pp. 3667–3674. https://doi.org/10.3850/978-981-11-2724-3_0213-cd

Wan, C., Yang, Z., Zhang, D., Yan, X., Fan, S., 2018. Resilience in transportation systems: a systematic review and future directions. Transp. Rev. 38, 479–498. https://doi.org/10.1080/01441647.2017.1383532

Wan, C., Yuan, J., Cao, D., Wang, T., Ng, A.K., 2024. A fuzzy evidential reasoning-based model for evaluating resilience of ports to typhoons. Transp. Res. Part Transp. Environ. 133, 104228. https://doi.org/10.1016/j.trd.2024.104228

Wang, F., Tian, J., Lin, Z., 2020. Empirical study of gap and correlation between philosophies Safety-I and Safety-II: A case of Beijing taxi service system. Appl. Ergon. 82, 102952. https://doi.org/10.1016/j.apergo.2019.102952

Wang, L., Yang, Z., 2018. Bayesian network modelling and analysis of accident severity in waterborne transportation: A case study in China. Reliab. Eng. Syst. Saf. 180, 277–289. https://doi.org/10.1016/j.ress.2018.07.021

Wang, N., Wu, M., Yuen, K.F., 2023. Assessment of port resilience using Bayesian network: A study of strategies to enhance readiness and response capacities. Reliab. Eng. Syst. Saf. 237, 109394. https://doi.org/10.1016/j.ress.2023.109394

Wei, L., 2022. Application of Bayesian Algorithm in Risk Quantification for Network Security. Comput. Intell. Neurosci. 2022, 1–10. https://doi.org/10.1155/2022/7512289

Wendler-Bosco, V., Nicholson, C., 2020. Port disruption impact on the maritime supply chain: a literature review. Sustain. Resilient Infrastruct. 5, 378–394. https://doi.org/10.1080/23789689.2019.1600961

Weng, J., Du, J., Shi, K., Liao, S., 2023. Effects of ship domain shapes on ship collision risk estimates considering collision frequency and severity. Ocean Eng. 283, 115070. https://doi.org/10.1016/j.oceaneng.2023.115070

Wu, J., 2018. A generalized tree augmented naive Bayes link prediction model. J. Comput. Sci. 27, 206–217. https://doi.org/10.1016/j.jocs.2018.04.006

Wu, L., Jia, S., Wang, S., 2020. Pilotage planning in seaports. Eur. J. Oper. Res. 287, 90–105. https://doi.org/10.1016/j.ejor.2020.05.009

Wu, X., Sun, Y., Wu, Y., Su, N., Peng, S., 2022. The Interference Effects of Wind Load and Wind-Induced Dynamic Response of Quayside Container Cranes. Appl. Sci. 12, 10969. https://doi.org/10.3390/app122110969

Xu, X., Wu, B., Man, J., Soares, C.G., 2024. Bayesian network modelling for navigation status control of cargo ships in the Three Gorges Waterway. Reliab. Eng. Syst. Saf. 245, 110018. https://doi.org/10.1016/j.ress.2024.110018

Xue, L., Li, Y., Yao, S., 2023. A Statistical Analysis of Tropical Cyclone-Induced Low-Level Winds near Taiwan Island. Atmosphere 14, 715. https://doi.org/10.3390/atmos14040715

Yamamura, E., 2016. Natural disasters and social capital formation: The impact of the Great Hanshin-Awaji earthquake. Pap. Reg. Sci. 95, S143–S165. https://doi.org/10.1111/pirs.12121

Yang, Q., Tian, J., Zhao, T., 2017. Safety is an emergent property: Illustrating functional resonance in Air Traffic Management with formal verification. Saf. Sci. 93, 162–177. https://doi.org/10.1016/j.ssci.2016.12.006

Yang, Zhisen, Yang, Zaili, Yin, J., 2018. Realising advanced risk-based port state control inspection using data-driven Bayesian networks. Transp. Res. Part Policy Pract. 110, 38–56. https://doi.org/10.1016/j.tra.2018.01.033

Yang, Z.L., Bonsall, S., Wall, A., Wang, J., Usman, M., 2013. A modified CREAM to human reliability quantification in marine engineering. Ocean Eng. 58, 293–303. https://doi.org/10.1016/j.oceaneng.2012.11.003

Yin, J., Khan, R.U., Wang, X., Asad, M., 2024. A data-centered multi-factor seaport disruption risk assessment using Bayesian networks. Ocean Eng. 308, 118338. https://doi.org/10.1016/j.oceaneng.2024.118338

Yoo, Y., Park, H.-S., 2021. Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. J. Mar. Sci. Eng. 9, 565. https://doi.org/10.3390/jmse9060565

Yu, M., Quddus, N., Kravaris, C., Mannan, M.S., 2020. Development of a FRAM-based framework to identify hazards in a complex system. J. Loss Prev. Process Ind. 63, 103994. https://doi.org/10.1016/j.jlp.2019.103994

Yu, Q., Liu, K., Yang, Zhisen, Wang, H., Yang, Zaili, 2021. Geometrical risk evaluation of the collisions between ships and offshore installations using rule-based Bayesian reasoning. Reliab. Eng. Syst. Saf. 210, 107474. https://doi.org/10.1016/j.ress.2021.107474

Zarei, E., Khan, F., Abbassi, R., 2022. A dynamic human-factor risk model to analyze safety in sociotechnical systems. Process Saf. Environ. Prot. 164, 479–498. https://doi.org/10.1016/j.psep.2022.06.040

Zelenkov, M., Laamarti, Y., Charaeva, M., Rogova, T., Novoselova, O., Mongush, A., 2022. Maritime terrorism as a threat to confidence in water transport and logistics systems. Transp. Res. Procedia 63, 2259–2267. https://doi.org/10.1016/j.trpro.2022.06.256

Zhang, D., Yan, X.P., Yang, Z.L., Wall, A., Wang, J., 2013. Incorporation of formal safety assessment and Bayesian network in navigational risk estimation of the Yangtze River. Reliab. Eng. Syst. Saf. 118, 93–105. https://doi.org/10.1016/j.ress.2013.04.006

Zhen, L., Lin, S., Zhou, C., 2022. Green port oriented resilience improvement for traffic-power coupled networks. Reliab. Eng. Syst. Saf. 225, 108569. https://doi.org/10.1016/j.ress.2022.108569

Zhou, C., Xu, J., Miller-Hooks, E., Zhou, W., Chen, C.-H., Lee, L.H., Chew, E.P., Li, H., 2021. Analytics with digital-twinning: A decision support system for maintaining a resilient port. Decis. Support Syst. 143, 113496. https://doi.org/10.1016/j.dss.2021.113496

Zhou, K., Xing, W., Wang, J., Li, H., Yang, Z., 2024. A data-driven risk model for maritime casualty analysis: A global perspective. Reliab. Eng. Syst. Saf. 244, 109925. https://doi.org/10.1016/j.ress.2023.109925

Zhu, R., Hu, X., Li, X., Ye, H., Jia, N., 2020. Modeling and Risk Analysis of Chemical Terrorist Attacks: A Bayesian Network Method. Int. J. Environ. Res. Public. Health 17, 2051. https://doi.org/10.3390/ijerph17062051

Zong, Y., Chen, X., 1999. Typhoon Hazards in the Shanghai Area. Disasters 23, 66–80. https://doi.org/10.1111/1467-7717.00105

Appendix

Table Ap. 1: Description of resilience strategies in the context of seaports.

Resilience Strategies	Description	Sources
Regular maintenance	Regular preventative and corrective maintenance activities of a) structures: berths, quays, jetties, and piers, seawalls, revetments, breakwaters, b): machineries: cranes, hoists, forklifts, conveyors. and other cargo-handling equipment, c) electrical systems: lighting, power distribution, and backup generators, d) dockside infrastructure for vessel mooring, such as bollards, fenders, and mooring lines, e) dredging of channels, basins, and berths to maintain required depths, to name but a few.	Tsinker, G. P. (2004). Port Engineering: Planning, Construction, Maintenance, and Security. John Wiley & Sons.
Strong coastal protection	Consideration of the measures to effectively reduce the potential risks associated with coastal erosion, floods, sea level rise, etc., that have the potential to adversely affect the port infrastructure, vessels, cargo, and employees, including seawalls, breakwaters, Groynes, Revetments, Gabions, Dunes and Sand Dikes, Vegetation and Salt Marshes, and the relevant protective structures.	Tripak S., Willey S., Stokes J. Coastal Texas protection and restoration project; (2014). Available from: https://pdfs.semanticscholar.org/presentation/215d/b6290470d28f6656e57629a3866823e26357.pdf.
Strong cyber-secure infrastructure	Given the heavy reliance of seaports on digital technology for their operations, it is essential to implement the cybersecurity measures for mitigation of any interruptions and data breaches. The measures are as follows: Identification of cyber threats and vulnerabilities, isolating critical systems from non-critical ones by network segmentation, implementing strong authentication methods such as multi-factor authentication, deploying the Intrusion Detection and Prevention Systems (IDPS), cybersecurity training for personnel, among others.	ENISA (European Union Agency for Cybersecurity), (2019). Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector. ISBN 978-92-9204-314-8.
Safety management	Including a range of strategies, processes, and activities that are performed to ensure the well-being of personnel, safeguard assets, avoid accidents, and environmental damage. The essential safety management practices can be succinctly outlined as follows: a) meticulous planning and comprehensive training of personnel, b) establishment of clear safety policies and procedures encompassing personnel safety, cargo handling, equipment maintenance, and emergency response, c) enforcement of the use of suitable personal protective equipment, including helmets, safety vests, gloves, and respiratory protection, d) Proper handling and disposal of hazardous materials, compliance with environmental regulations, e) staying abreast of pertinent safety regulations and guidelines.	Maritime and coastguard agency, (2017). A Guide to Good Practice on Port Marine Operations. https://www.southamptonvts.co.uk/admin/content/files/PDF_Downloads/170508_Port_Marine_Guide_To_Good_Practice__Rev_Sept_2017.pdf
Security management	Including measures that are adopted to protect port superstructures, personnel, assets, and cargo from various security threats, including terrorism, smuggling, theft, and unauthorized access. some key security measures applied in seaports are: a) Implementing access control systems such as identification badges and biometric verification, b) Securing the port with physical barriers such as walls, fences, gates, c) Monitoring the critical areas with CCTVs and motion sensors along with video analytics techniques, d) Employing trained security personnel to guard the port	Christopher, K. (2014). Port Security Management. In CRC Press eBooks. https://doi.org/10.1201/b17142.

	facilities, e) Identification of hidden threats within containers using advanced scanning technologies, such as X-ray machines and radiation detectors, f) Proper implementation of ISPS code to enhance the security of vessels entering and leaving the port, g) Providing security awareness and training programs for port personnel.	
Resource conservation	Resource conservation practices bolster the resilience of seaports against the disruptions through minimization of environmental impacts, improving cost efficiency and mitigating the potential for further financial losses. Some key practices are: a) Conserving resources such as energy and water to maintain essential operations during crises, b) Allocating the saved funds to invest in disaster preparedness and infrastructure upgrades, c) Reducing emissions and waste to contribute to protecting the environment, d) Gaining positive reputation through demonstrating a commitment to resource conservation and sustainability.	Hossain, T., Adams, M., & Walker, T. R. (2021). Role of sustainability in global seaports. Ocean & Coastal Management, 202, 105435. https://doi.org/10.1016/j.ocecoaman.2020.105435.
Redundant energy infrastructure	Equipped with redundant or backup systems to guarantee the continuous and reliable energy supply during the failures or disruptions. Some examples of redundant energy infrastructures in seaports are: a) Emergency diesel generators, b) Uninterruptible Power Supply Systems, c) Emergency Battery Systems, d) Parallel power feeders from different sub-stations, e) redundant fuel storage tanks.	Berle, Ø., Rice, J. D., & Asbjørnslett, B. E. (2011). Failure modes in the maritime transportation system: a functional approach to throughput vulnerability. Maritime Policy & Management, 38(6), 605–632. https://doi.org/10.1080/03088839.2011.615870.
Redundant facility	Equipped with redundant or backup facilities to ensure the continued operation of essential functions during disruptions. The examples of redundant facilities in a seaport are: Backup terminal operations, backup berths, backup storage areas, backup IT infrastructures, backup communication systems including radio, satellite and internet connections.	Berle, Ø., Rice, J. D., & Asbjørnslett, B. E. (2011). Failure modes in the maritime transportation system: a functional approach to throughput vulnerability. Maritime Policy & Management, 38(6), 605–632. https://doi.org/10.1080/03088839.2011.615870.
Backup main equipment	Equipped with redundant or spare machinery, vehicles, and tools including backup cranes, forklifts, loaders, additional trucks and trailers, spare tugboats, backup cargo handlers, such as reach stackers and straddle carriers.	J. Rice and K. Trepte, "The MIT CTL port resilience survey report." MIT Center for Transportation & Logistics, Cambridge, MA, 2012. [Online]. Available: http://ctl. mit. edu/sites/default/files/Port% 20resilience% 20survey% 20report% 20v27% 20sans% 20SEM. p df.
Reserved space	The allocation of additional specified areas inside a port, referred to as reserved spaces, is typically carried out by port authorities with the aim of mitigating congestion, maximizing the usage of resources, and improving the overall performance of the port. Within a container port, providing specialized sections for the storage of additional containers is advisable. Alternatively, designated zones may be allocated for the purpose of accommodating vehicles that are awaiting access to the terminal for cargo collection or distribution, hence mitigating the occurrence of congestion at entry gates. From a security perspective, it is recommended that designated areas be developed for the purpose of screening and inspecting potentially suspect cargoes in order to enhance port security.	Christopher, K. (2014). Port Security Management. In CRC Press eBooks. https://doi.org/10.1201/b17142.

Diverse energy systems	The use of renewable energy sources, such as solar, wind, hydro, tidal and wave power serves to enhance the energy supply diversification of a port. In the case of potential interruptions to conventional energy supplies, the use of alternative energy sources may provide a more reliable and consistent energy supply, hence guaranteeing uninterrupted operations.	Berle, Ø., Rice, J. D., & Asbjørnslett, B. E. (2011). Failure modes in the maritime transportation system: a functional approach to throughput vulnerability. Maritime Policy & Management, 38(6), 605–632. https://doi.org/10.1080/03088839.2011.615870.
Diverse equipment	The complex and multifaceted nature of port operations necessitates the use of a varied array of equipment in order to effectively and efficiently handle a broad spectrum of tasks. In the case of an emergency and the malfunction of a system components, it may be possible to use alternative equipment that has been developed or built for a different purpose to perform the function of the failed system. For some kinds of cargo and certain circumstances, mobile cranes or Automated Guided Vehicle (AGVs) may serve as a viable alternative to main equipment.	J. Rice and K. Trepte, "The MIT CTL port resilience survey report." MIT Center for Transportation & Logistics, Cambridge, MA, 2012. [Online]. Available: http://ctl. mit. edu/sites/default/files/Port% 20resilience% 20survey% 20report% 20v27% 20sans% 20SEM. p df.
Equipment/cargo tracking systems	Seaport equipment/cargo tracking systems which are based on various technologies such as RFID, GPS, sensors, and data analytics, are deployed for the purpose of providing real-time information and monitoring the movement, location, status, and condition of equipment, containers, and cargos.	Yau, K. A., Peng, S., Qadir, J., Low, Y. C., & Ling, M. H. (2020). Towards smart port infrastructures: Enhancing port activities using information and communications technology. IEEE Access, 8, 83387–83404. https://doi.org/10.1109/access.2020.2990961.
Real-time data management systems	A real-time data management system implemented at a seaport is a technologically advanced solution that collects, processes, evaluates, and demonstrates data pertaining to diverse port operations and activities in real-time. These systems use cutting-edge technology, including sensors, IoT devices, data analytics, and communication networks.	Yang, Y., Zhong, M., Yao, H., Yu, F., Fu, X., & Postolache, O. (2018). Internet of things for smart ports: Technologies and challenges. IEEE Instrumentation & Measurement Magazine, 21(1), 34–43. https://doi.org/10.1109/mim.2018.8278808.
Data analysis program	Data analysis programs used in seaports refer to data analysis software tools or systems that are employed for the purpose of processing, interpreting, and comprehending the extensive volumes of data that are created within the operations of seaports. They deploy high-performance processing engines and advanced analytics algorithms, including machine learning and AI, to provide real-time insights into many facets of port operations. These programs are of utmost importance in the optimization of port efficiency, the enhancement of security measures, and the facilitation of informed decision-making for the managers via the use of data-driven insights.	Yang, Y., Zhong, M., Yao, H., Yu, F., Fu, X., & Postolache, O. (2018). Internet of things for smart ports: Technologies and challenges. IEEE Instrumentation & Measurement Magazine, 21(1), 34–43. https://doi.org/10.1109/mim.2018.8278808.
Preparedness Management	Preparedness management within a seaport context is the systematic and thorough process of strategizing, coordinating, and executing a range of initiatives with the objective of assuring the port's capacity promptly and efficiently address and alleviating diverse emergency situations and critical events. The multifaceted nature of preparedness management in seaports could be represented by following examples: a) the effective preparedness management may serve as a deterrent to worker strikes occurring inside the port, b) The establishment of collaborative partnerships with local emergency services, police enforcement agencies,	Çetin, Ç. K., & Cerit, A. G. (2010). Organizational effectiveness at seaports: a systems approach. Maritime Policy & Management, 37(3), 195–219. https://doi.org/10.1080/03088831003700611.

	fire departments, and other pertinent entities guarantees seamless coordination and reciprocal assistance in times of disaster, c) the implementation of methods aimed at expeditiously mobilizing supplementary resources during emergencies, such as the establishment of contractual agreements with external organizations or corporations to acquire specialist equipment or employees, has the potential to ease the burden on port workers and enhance the effectiveness of emergency response efforts.	
Communication	During emergency situations, it is essential to establish efficient communication and coordination among many stakeholders, including port authorities, terminal operators, government agencies, emergency services, shipping agents, weather service, and community partners. Establishing effective channels of communication and clearly delineating roles and responsibilities are crucial factors in ensuring a prompt and efficient response. An illustrative case in history is the dynamic communication that took place between port officials in New York and New Jersey within the occurrence of Hurricane Sandy. This particular instance highlighted the pivotal significance of coordination and the interchange of information in the realms of disaster planning, response, and recovery. The implementation of this measure had a significant role in mitigating the adverse effects of the storm on port operations and bolstering the capacity to recover swiftly in the aftermath of the calamity.	Sturgis L.A., Smythe T.C., Tucci A.E. (2013). Port recovery in the aftermath of hurricane sandy: improving port resiliency in the era of climate change; Available from: https://s3.amazonaws.com/files.cnas.org/documents/CNAS_HurricaneSandy_VoicesFromTheField.pdf?mtime=20160906081313.
Alternative means of transportation	Alternative modes of transportation refer to diverse means of conveyance that extend beyond conventional approaches for transporting commodities inside or in relation to the port setting. These alternate solutions are designed to improve efficiency and tackle the difficulties related to congestion and restricted transportation choices. For instance, in the event of a disruption at a destination port, railroads and trucks may serve as viable alternate modes of transit. In alternative scenarios, barges and other marine vessels possess the capability to convey substantial amounts of goods, therefore alleviating congestion on roadways and railroads.	MacKenzie, C. A., Barker, K., & Grant, F. H. (2012). Evaluating the consequences of an inland waterway port closure with a dynamic multiregional interdependence model. IEEE Transactions on Systems, Man, and Cybernetics, 42(2), 359–370. https://doi.org/10.1109/tsmca.2011.2164065.
Container repositioning	Container repositioning during a disastrous scenario is the deliberate and tactical relocation of containers within a port to effectively respond to and mitigate the unique problems and demands that arise as a result of the disaster. For example, during severe weather conditions such as storms or hurricanes, it is advisable to relocate containers to a lower location on the ground, preventing them from toppling over. Conversely, in the event of a flood, it is recommended to reposition objects at an elevated height that is beyond the reach of the floodwaters. Additional instances may be cited in scenarios such as fire, seismic events, and similar circumstances. In a quite different situation, such as explosions or chemical spills, the strategic relocation of containers may be used to establish protective barriers or buffer zones, so safeguarding adjacent regions of the port from possible damage.	S. Hosseini and K. Barker, “Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports,” Comput. Ind. Eng., vol. 93, pp. 252–266, Mar. 2016, doi: 10.1016/j.cie.2016.01.007.

Alternate functioning manner	When a seaport faces a disruptive event, alternate functioning manner is attributed to the operational strategies and adaptations that seaports can implement to continue or modify their operations. For instance, seaports have the ability to curtail their operations to a limited capacity, prioritizing the processing of essential cargo or urgent provisions such as medical supplies, food, water, and emergency equipment to facilitate reaction and recovery actions. Or, in the case of an outbreak of a highly contagious disease, with utilization of advanced technologies, the remote management of some port services, including the remote operation of cranes and monitoring systems are possible.	N. Wang, M. Wu, and K. F. Yuen, "Assessment of port resilience using Bayesian network: A study of strategies to enhance readiness and response capacities," Reliab. Eng. Syst. Saf., vol. 237, p. 109394, Sep. 2023, doi: 10.1016/j.ress.2023.109394.
Timely evacuation	The concept of timely evacuation entails the quick relocation of personnel, goods, cargos and facilities from a disrupted port to an alternative port or secure area, with the aim of minimizing possible losses and damages. For instance, a port situated in a region prone to floods has identified an impending hazard of river inundation as a result of intense precipitation. In order to mitigate potential losses, perishable commodities, equipment, and other critical cargo are promptly transferred to a more secure port in close proximity. Or, a seaport situated in an area characterized by political instability has received information suggesting the possibility of forthcoming disturbances. As a proactive measure, valuable cargoes and sensitive commodities are expeditiously redirected to a secure off-site storage facility until the situation attains stability.	Lee, P. T., & Flynn, M. (2011). Charting a new paradigm of container hub port Development Policy: The Asian Doctrine. Transport Reviews, 31(6), 791806. https://doi.org/10.1080/01441647.2011.597005.
Emergency unit	The establishment of an emergency unit inside a seaport serves the objective of facilitating a prompt and efficient reaction to a diverse range of emergencies, events, and crises that may arise within the port area or have an influence on port functionality. An emergency unit refers to a specialized group that has the requisite expertise, training, and resources to effectively handle, alleviate, and organize reactions to critical situations, with the ultimate goal of reducing potential damage to individuals, superstructures and assets.	N. Wang, M. Wu, and K. F. Yuen, "Assessment of port resilience using Bayesian network: A study of strategies to enhance readiness and response capacities," Reliab. Eng. Syst. Saf., vol. 237, p. 109394, Sep. 2023, doi: 10.1016/j.ress.2023.109394.
Rerouting	The establishment of a strategic alliance among proximate ports is an initiative of collaboration with the objective of mitigating possible economic setbacks and operational disturbances in the case of emergencies. Through collaboration, ports have the ability to collectively use resources, capabilities, and infrastructure to ensure the continuity of maritime commerce, particularly in situations when one of the ports is facing a disruption. For instance, let's consider two ports A and B have a strategic alliance. In instances involving natural disasters, labor strikes, capacity overload, port infrastructure maintenance, geopolitical instability, and similar factors, cargo ships intended for disrupted port A are rerouted to port B for the purposes of unloading and processing.	Lee, P. T., & Flynn, M. (2011). Charting a new paradigm of container hub port Development Policy: The Asian Doctrine. Transport Reviews, 31(6), 791806. https://doi.org/10.1080/01441647.2011.597005.
Effective information sharing	The utilization of effective information sharing mechanism enables the effective synchronization of activities, well-informed decision-making, and preemptive measures to address disruptive scenarios. For instance, the prompt dissemination of information on meteorological forecasts, the occurrences of natural	Sturgis L.A., Smythe T.C., Tucci A.E. (2013). Port recovery in the aftermath of hurricane sandy: improving port resiliency in the era of climate change; Available from:

	disasters, or security risks enables seaport authorities and relevant parties to make necessary preparations and execute steps aimed at minimizing adverse impacts. This may include activities such as ensuring the safety of goods, facilitating the evacuation of workers, and fortifying infrastructure in order to mitigate potential harm and minimize any resulting disturbances. Or from an optimized resource allocation perspective, it is possible to improve the allocation of berths, distribution of manpower, and use of equipment, therefore mitigating bottlenecks and improving the overall efficiency of port operations.	https://s3.amazonaws.com/files.cnas.org/documents/CNAS_HurricaneSandy_VoicesFromTheField.pdf?mtime=20160906081313.
Budget restoration	The objective of budget restoration during the recovery phase of a seaport is to guarantee the availability of essential financial resources for the purpose of restoring the port to its regular operational state. The process of restoring the budget of a seaport is contingent upon its financial structure, and may need the use of many sources, including reserves, insurance claims, government help, or emergency money that have been specifically allocated for such circumstances.	Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. Risk Analysis, 29(4), 498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x.
Service restoration	Refers to the systematic recovery of critical services and activities necessary for the continued operation of the port after a disruptive event. These services cover a diverse array of activities that together facilitate the efficient functioning of the port, including cargo handling, vessel operations, customs clearance, security measures, logistics management, among others. The service restoration relies heavily on a resumption of the human workforce, including engineers, technical teams, operators, and workers.	Burns, M. G. (2018). Port Management and Operations. In CRC Press eBooks. https://doi.org/10.4324/9781315275215.
Facility recovery	Refers to the process of restoring and bringing back to operational status the affected and damaged seaport facilities such as cranes, docks, berths, container yards, warehouses, machineries, etc. The restoration of port operations at a seaport necessitates a synchronized and cooperative endeavor that engages many stakeholders, aiming to guarantee the effective and prompt recovery of facility functions.	S. Hosseini and K. Barker, “Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports,” Comput. Ind. Eng., vol. 93, pp. 252–266, Mar. 2016, doi: 10.1016/j.cie.2016.01.007.
Technology recovery	Seaports heavily rely on technologies such as TOS (terminal operating systems), EDI (electronic data interchange), RTU (remote terminal unit), PLC (programmable logic control), AGV (automated guided vehicles), VTMS (Vessel Traffic Management Systems), Cargo Inspection and Scanning to facilitate cargo handling, vessel operations, security, communication, and various administrative functions. Technology restoration ensures that these systems are functional and operational, allowing the port to resume its activities efficiently and effectively.	Agatić, A., & Kolanović, I. (2020). Improving the seaport service quality by implementing digital technologies. Pomorstvo, 34(1), 93–101. https://doi.org/10.31217/p.34.1.11.

Table Ap. 2: The expert's profile and their related experience and expertise.

Number	Title	Educational level	Experience (years)	Location	Specialization
1	General Manager	MSc	20	Iran	Port master planning; concession/PPP contract management; stakeholder engagement; ESG & sustainability; business continuity & resilience.
2	Operations Manager	MSc	15	Iran	Berth planning & vessel scheduling; quay-crane assignment; yard planning & resource optimization; stowage coordination with shipping lines.
3	Operations Manager	Ph.D	12	Canada	Container terminal management; stevedoring planning; turnaround-time optimization.
4	HSE Director	Ph.D	10	Belgium	ISO 45001/14001 systems; HAZID/HAZOP/JSA risk assessment; emergency response & oil-spill (ICS) planning; contractor HSE auditing.
5	Harbour Master	MSc	18	USA	VTS & navigational safety; pilotage & towage coordination; mooring/lines safety; ISPS drills & security interface; incident investigation & root-cause analysis.
6	Port Planning	MSc	16	UK	Berth/yard capacity modelling; approach-channel design & navigational risk; asset management (PIANC/ICE standards).
7	Terminal Systems & Automation Manager	MSc	14	Australia	TOS configuration; yard optimization & equipment dispatching (ASC/RTG/AGV); EDI/port community systems; operational analytics & dashboarding.

Table Ap. 3: The established resilience measure for critical path items.

Critical path item	Measure / technology	Resilience capacity*	Capability band	Source
Quay cranes	Ductile-link tie-downs & rail clips that prevent boom lift-off	A	High	Typhoon *Maemi* post-mortem shows five-crane domino collapse would have been avoided with these links (Port Technology International)
	Boom anti-collision radar / LiDAR sensors	A	High	Port-wide fit cuts wind-damage claims; PTI sensor trials report zero boom-ship strikes after retrofit (wpassets.porttechnology.org)

	Spare boom cradle + onsite boom ready for swap	Ad/R	High	TT-Club/ICHCA benchmark lists spare-boom strategy as best practice; swap cuts DS4 rebuild from 90 d to < 7 d (wpassets.porttechnology.org)
	Private-5G IoT vibration sensors for predictive maintenance	R	World class	Felixstowe 5G pilot predicts gearbox faults days ahead, quoting 30–50 % downtime cut on 31 STS cranes (Port Technology International)
	Remote-diagnostics & remote crane operation centre	Ad/R	World class	ABB case study reports 60 % of faults cleared without site visit; remote ops keep labour out of the storm zone (ABB Group)
	Mobile harbour / floating crane retained on site	Ad	World class	Port New Orleans reopened three days after *Gustav* by shifting cargo to a mobile crane while STS inspections ran (FreightWaves)
Berth & mooring gear	Quick-release hooks (QRH) with integrated load pins	A	High	Field data: QRH reset in minutes, limiting berth outage after surge; load-pin alarms avert line parting (Trelleborg, Interface)
	Modular composite fender panels stored on barge	Ad	High	Gulf terminals report swap-out in < 24 h versus 7–10 d cast-in repair (Superyacht Mooring Products)
	Floating crane for berth bypass (same as above)	Ad	High	See New Orleans *Gustav* example (FreightWaves)
	UAV / LiDAR rapid-damage survey team on standby	R	World class	Post-Harvey levee survey cut inspection time by 48 % over rope-access methods (LIDAR Magazine)
Power & electrical	Dual 11 kV feeder loop and auto-transfer switchgear	A	High	Specified in Bayport hurricane manual; keeps crane rails emphasize through single-circuit fault (Port Houston)
	Islandable PV + battery micro-grid for control & reefers	A	World class	Port of Long Beach micro-grid designed to give 0 h outage to command centre & security hub (2022 press release) (Polb)
	Pre-staged mobile substation (MTS) 115/230 kV	R	World class	US-DOE study: energises blown yard transformer in 12–24 h vs 3–8 weeks full rebuild (The Department of Energy's Energy.gov)
	Hardened UPS + diesel gensets for SCADA racks	A/R	High	Hurricane-season UPS checklist notes 72–120 h generator autonomy for critical controls (Joe Powell and Associates, watertechonline.com)
Backbone IT / SCADA	Redundant fibre-optic ring + dual control rooms	A	High	RUGGEDCOM case: county-wide fibre ring provides path diversity and PoE for OT devices (assets.new.siemens.com)
	Hot-standby SCADA servers with automatic fail-over	Ad/R	High	VTScada guidance emphasizes N-way fail-over; no server reboot required after power dip (VTScada by Trihedral)

	OT network segmentation & hardening per NIST 800-82	A	High	Latest revision maps cyber & physical threats; widely adopted in U.S. critical infrastructure (NIST Publications)
	Daily off-site backups & disaster-recovery playbook	R	High	IAPH Cyber-security Guidelines mandate tested backup/restore for port-wide PCS and SCADA (World Port Sustainability Program)
	SATCOM / LTE-sat hybrid for control-centre fail-over	Ad/R	World class	Iridium & Hughes case studies show SATCOM terminals kept ops online when terrestrial links failed in Cat-4 storms (Iridium Satellite Communications, hughes.com)
	Secondary (cold) control centre & credentialed staff	R	World class	PNNL Business-continuity guideline for high-impact control centres, incl. pre-hurricane staff-up procedures (PNNL)

∗ A, Ad, and R stand for Absorptive, Adaptive, and Restorative capabilities, respectively.

Table Ap. 4: Estimated throughput loss for various cyclone classes at different strike distances (RCF=Low).

CWA class	Output	Strike Distance				
		Ring 1	Ring 2	Ring 3	Ring 4	Ring 5
TS	Processed TEU	3632951	3637171	3640572	3647709	3647709
	TEU loss	14758	10538	7137	0	0
	Loss ratio	0.40 %	0.29 %	0.20 %	≈0	≈0
	Rerouted vessels	7	5	3	0	0
STS	Processed TEU	3619340	3630575	3636874	3646207	3647644
	TEU loss	28369	17134	10835	1502	65
	Loss ratio	0.78 %	0.47 %	0.30 %	0.04 %	≈0
	Rerouted vessels	15	6	5	1	0
TY	Processed TEU	3565790	3607513	3633455	3643241	3647362
	TEU loss	81919	40196	14254	4468	347
	Loss ratio	2.25 %	1.10 %	0.39 %	0.12 %	0.01 %
	Rerouted vessels	39	17	8	3	0
VST	Processed TEU	3489751	3531878	3560446	3628314	3642232
	TEU loss	157958	115831	87263	19395	5477
	Loss ratio	4.33%	3.18%	2.45%	0.61%	0.15%
	Rerouted vessels	81	52	37	9	3
VTY	Processed TEU	3368514	3444284	3495889	3577564	3626817
	TEU loss	279195	203425	151820	70145	20892
	Loss ratio	7.65 %	5.58 %	4.16 %	1.92 %	0.57 %
	Rerouted vessels	144	93	65	30	7

Table Ap. 5: Estimated throughput loss for various cyclone classes at different strike distances (RCF=High).

CWA class	Output	Strike Distance				
		Ring 1	Ring 2	Ring 3	Ring 4	Ring 5
TS	Processed TEU	3639231	3641650	3643618	3647709	3647709
	TEU loss	8478	6059	4091	0	0
	Loss ratio	0.23 %	0.17 %	0.11 %	≈0	≈0
	Rerouted vessels	4	3	2	0	0
STS	Processed TEU	3631412	3637858	3641498	3646850	3647672
	TEU loss	16297	9851	6211	859	37

	Loss ratio	0.45 %	0.27 %	0.17 %	0.02 %	≈0
	Rerouted vessels	9	4	3	1	0
TY	Processed TEU	3600650	3624598	3639538	3645155	3647510
	TEU loss	47059	23111	8171	2554	199
	Loss ratio	1.29 %	0.63 %	0.22 %	0.07 %	0.01 %
	Rerouted vessels	23	10	5	1	0
VST	Processed TEU	3556969	3581110	3597689	3636624	3644561
	TEU loss	90740	66599	50020	11085	3148
	Loss ratio	2.49%	1.83%	1.37%	0.31%	0.08%
	Rerouted vessels	47	30	22	5	2
VTY	Processed TEU	3487324	3530747	3560685	3607618	3635705
	TEU loss	160385	116962	87024	40091	12004
	Loss ratio	4.40 %	3.21 %	2.39 %	1.10 %	0.33 %
	Rerouted vessels	83	54	37	17	4

Table Ap. 6: Estimated throughput loss for various cyclone classes at different strike distances (RCF=World-class).

CWA class	Output	Strike Distance				
		Ring 1	Ring 2	Ring 3	Ring 4	Ring 5
TS	Processed TEU	3640414	3642475	3644175	3647709	3647709
	TEU loss	7295	5234	3534	0	0
	Loss ratio	0.20 %	0.14 %	0.10 %	≈0	≈0
	Rerouted vessels	4	2	2	0	0
STS	Processed TEU	3634213	3639198	3642345	3646966	3647677
	TEU loss	13496	8511	5364	743	32
	Loss ratio	0.37 %	0.23 %	0.15 %	0.02 %	≈0
	Rerouted vessels	7	3	2	1	0
TY	Processed TEU	3606855	3627743	3640652	3645499	3647537
	TEU loss	40854	19966	7057	2210	172
	Loss ratio	1.12 %	0.55 %	0.19 %	0.06 %	≈0
	Rerouted vessels	20	9	4	1	0
VST	Processed TEU	3576396	3590174	3604506	3638117	3644986
	TEU loss	71313	57535	43203	9592	2723
	Loss ratio	1.96%	1.58%	1.18%	0.27%	0.07%
	Rerouted vessels	41	25	18	6	1
VTY	Processed TEU	3526970	3546621	3572496	3613059	3637334
	TEU loss	120739	101088	75213	34650	10375
	Loss ratio	3.31%	2.77%	2.06%	0.94%	0.29%
	Rerouted vessels	64	43	33	18	5