Marine Research
of the National Academy of Marine Research
ISSN: 2709-6629 (Vol.5 Iss.2)
GPN: 2011200033

DOI: http://dx.doi.org/10.29677/MR.202512_5(2).0003
2025, 5(2),45-75

Enhancing Port Security Management in Taiwan's International Commercial Ports

Chi-Chang Lin [1] Chia-Hsun Chang [2*]

[1] *Department of Business Computing, National Kaohsiung University of Science and Technology, Kaohsiung City, Taiwan*

[2] *School of Engineering, Liverpool John Moores University, Liverpool, UK*

ABSTRACT

Despite not being a member of the International Maritime Organization (IMO), Taiwan voluntarily adheres to the International Ship and Port Facility Security (ISPS) Code to maintain alignment with international maritime security standards. This study aims to identify pivotal factors influencing port security through an analysis of existing security strategies and the proposal of a standardized security inspection framework, thereby bolstering the global competitiveness of Taiwan's commercial ports. A literature review and bibliometric analysis to explore the current research status of port safety strategy formulation were initially conducted to develop a security management framework, encompassing 12 sub-criteria categorized into four critical criteria: Port Management Authority, Facility Lessees, Security Law Enforcement Agencies, and Security Policies and Regulations. An online questionnaire survey was conducted by port authorities, the Coast Guard Administration, Port Police, Customs personnel, and other relevant stakeholders, as well as scholars specializing in port security research. In total, 52 reply samples were collected. This study employs a fuzzy Multi-Criteria Decision-Making (MCDM) method, integrating expert opinions from both academic scholars and industry professionals, to evaluate critical dimensions of port security governance. The responses from academic scholars and industry professionals were compared. Results indicate that academics regard all four criteria as equally important, while industry professionals prioritize Port Management Authority as the most important, closely followed by Security Policies and Regulations. At the sub-criteria level, both groups identified the top two sub-criteria under Port Management Authority, showing strong agreement across sectors. However, a significant difference emerges in the evaluation of "Formulation of a Port Facility Security Plan (PFSP) and vessel protection plan," where academic scholars rank it much higher than industry professionals. This study offers a novel analysis of Taiwan's port security governance by integrating academic and industry perspectives through a fuzzy MCDM framework. The study contributes theoretical value by validating fuzzy logic in maritime security decision-making and provides practical insights for enhancing the implementation, regulatory clarity, and international alignment of PFSPs.

Keywords: International Ship and Port Facility Security (ISPS) Code; International Maritime Organization (IMO); bibliometric analysis; fuzzy Multi-Criteria Decision-Making (MCDM) analysis.

* Corresponding author, e-mail: c.chang@ljmu.ac.uk

Received June 10, 2025; accepted November 4, 2025.

1 INTRODUCTION

In the contemporary context of global economic interdependence, maritime transport remains the foundational infrastructure supporting international trade. According to the United Nations Conference on Trade and Development (UNCTAD, 2024), maritime routes facilitate approximately 80% of global cargo, highlighting ports' essential roles as critical nodes within global supply chains. Beyond their economic contributions, ports significantly influence national security, energy distribution networks, supply logistics, and humanitarian operations. Consequently, ensuring resilience and maintaining security within port operations are paramount not only to national interests but also to sustaining global trade networks.

Traditionally, port functions cantered predominantly on optimizing cargo throughput; however, current paradigms increasingly frame ports as critical security zones. Heightened complexity within global supply chains, extensive digital system integration, and increased transnational threats including terrorism, cyberattacks, piracy, and smuggling have substantially elevated the necessity for stringent port security governance. Ports now face vulnerabilities not solely from accidental disruptions or natural disasters but also from intentional threats capable of precipitating significant regional and international impacts. Hence, a comprehensive approach to port security governance, integrating traditional security measures with a dynamic and resilience framework, is essential (Mohsendokhta et al., 2025).

For Taiwan, an island economy characterized by limited natural resources and a constrained domestic market, maritime trade holds heightened significance. Taiwan's economic stability is intrinsically tied to its maritime logistics infrastructure, particularly through international commercial ports serving as essential gateways for trade flows (Chang & Thai, 2016). Any operational disruptions resulting from external threats, internal failures, or regulatory compliance issues can induce severe economic impacts, reputational harm, and compromised national security. Taiwan's unique geopolitical circumstances, including its exclusion from global entities such as the International Maritime Organization (IMO), further underline the necessity of aligning port security systems with international standards independently.

To mitigate maritime security risks, the IMO implemented a robust regulatory framework through Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS) and the International Ship and Port Facility Security (ISPS) Code. These frameworks provide structured guidelines aimed at protecting vessels, cargo, port infrastructures, and personnel from security threats. Specifically, the ISPS Code outlines standardized protocols for vulnerability assessments, strategic security planning, and effective incident response mechanisms. Despite its non-membership status, Taiwan voluntarily adheres to these international standards, thereby aiming to maintain international confidence, ensure continuous trade, and establish legitimacy as a reliable maritime participant.

Nonetheless, concerns persist regarding the efficacy of port security implementation in Taiwan. While national regulations and institutional frameworks exist, operational challenges remain significant. These challenges include fragmented governance structures, overlapping responsibilities among regulatory agencies, inconsistent enforcement practices, and inadequate public-private coordination. Entities such as the Maritime and Port Bureau, Coast Guard Administration, Customs, and Port Police have defined roles, yet unclear delineation often leads to duplicated efforts or security gaps, potentially delaying detection and response to threats like unauthorized entries, smuggling, human trafficking, and cyber intrusions.

Additionally, the increasing complexity within port ecosystems comprising terminal operators, shipping firms, Customs brokers, logistics providers, and transport personnel necessitates enhanced integration and systematization in security approaches. Effective port security extends beyond physical surveillance and patrol measures to incorporate strategic planning, comprehensive threat assessments, stakeholder education, real-time

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

intelligence dissemination, and systematic audits. Essential elements include the formulation of maritime security policies, port facility security assessments, port facility security plans (PFSPs), structured drills and exercises, and specialized security personnel training, all contributing to a resilient security framework.

Recent discourse within global port security has expanded to address emerging threats, including cybersecurity vulnerabilities, climate-related disruptions, and security concerns linked to digital transformations such as autonomous shipping and AI-enhanced logistics platforms. The European Maritime Safety Agency (EMSA) differentiates maritime safety, addressing accidental risks, from maritime security, targeting deliberate criminal actions. The EMSA (2025) underscores enhancing crew competence, improving inter-agency coordination, and modernizing regulatory frameworks, which are recommendations highly applicable to Taiwan.

This study primarily investigates the current state of port security at international commercial ports under the jurisdiction of the Taiwan International Ports Corporation (TIPC). The motivation for this study stems from a significant organizational restructuring in 2012, during which the port administration system transitioned from a government department, the Port Authority, to the corporatized TIPC, consolidating port governance into a single corporate entity. This transformation necessitated corresponding adjustments in port security management and operational measures. Notably, to ensure compliance with the International Ship and Port Facility Security Code (ISPS Code), the Maritime and Port Bureau (MPB) is required to conduct comprehensive audits, security assessments, and reissuance of Statements of Compliance for Port Facilities every five years for all designated port areas. These audits specifically evaluate individual port facilities (PFs).

In alignment with international standards, Taiwan adopts a tiered port security level system, classifying port facilities into three internationally recognized security levels. Currently, each PFSP is formulated by the designated Port Facility Security Officer (PFSO) of the respective facility. It is the responsibility of the PFSO to develop the PFSP by holistically considering the unique characteristics of the port and assessing its specific risk profile. Based on this assessment, a determination is made as to whether the designation of a PFSO is necessary, and corresponding security plans are drafted accordingly. According to the ISPS Code Part B, recommended elements to be included in a PFSP encompass six key components: control of access to port facilities, management of restricted areas within the facility, procedures for handling ship-borne cargo, delivery of ship stores, handling of unaccompanied baggage, and surveillance of the port facility.

In Taiwan, the responsibility for implementing and maintaining port facility security lies with the lessee of the port facility. Each lessee company is required to appoint a responsible officer for the leased facility and is subject to regular audits conducted by authorized inspection bodies. Upon successful inspection, a Statement of Compliance is issued for the facility. Beyond the administrative and operational responsibilities of the TIPC and individual Facility Lessees, Law Enforcement Agencies also play a critical role in safeguarding port security. In accordance with Article 43 of the Commercial Port Law, the MPB may coordinate with the Port Police and other relevant security authorities when conducting security audits. These developments illustrate that, following the corporatization of Taiwan's international commercial ports, challenges have emerged in integrating institutions, personnel, and legal frameworks within the evolving port security governance structure.

Despite Taiwan's endeavors to comply with international regulations, substantial evidence-based assessments of its port security strategies remain limited. Addressing this gap, the current study systematically investigates critical aspects of port facility security governance in Taiwan's international commercial ports. Guided by the ISPS Code framework, the study identifies and categorizes essential security dimensions and stakeholders involved in port security implementation. Utilizing expert surveys from academic and industry professionals, the study achieves a comprehensive understanding of the relative importance of critical security elements and enforcement-related challenges.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

To systematically analyze the intricate decision-making environment associated with port security governance, which is inherently characterized by hierarchical and subjective criteria, this study employs a multi-criteria decision-making (MCDM) framework with fuzzy logic theory, referred to as fuzzy MCDM analysis. The integration of fuzzy logic further addresses the intrinsic uncertainties and ambiguities inherent in human evaluations, resulting in a robust fuzzy MCDM analytical framework that reliably captures stakeholder priorities under conditions of uncertainty.

The study specifically investigates four primary stakeholder dimensions: (1) Port Management Authority (PM), focusing on regulatory oversight, coordination, and the enforcement of PFSPs; (2) Facility Lessee (FL), emphasizing preparedness and compliance among private operators; (3) Security Law Enforcement Agency (SL), addressing critical functions such as surveillance, access control, and threat response; and (4) Security Policies and Regulations (SP), evaluating the comprehensiveness and adaptability of regulatory frameworks. A total of twelve sub-criteria, informed by the ISPS Code and expert consultations, were meticulously assessed to determine their relative significance. Survey responses collected from domain experts were converted into fuzzy numerical representations, systematically aggregated through fuzzy weighting methodologies, and subsequently analyzed via defuzzification techniques.

Preliminary findings indicate a significant consensus among stakeholders regarding the paramount importance of effective PFSP implementation, emphasizing regular reviews and consistent compliance with ISPS Code standards. However, noteworthy differences emerged in stakeholder priorities; academic respondents particularly underscored the necessity of strategic planning, whereas industry professionals prioritized practical aspects such as operational training and adherence to compliance protocols.

This systematic comparative analysis substantially contributes to both theoretical and practical dimensions within maritime security research. From a theoretical standpoint, the study validates the efficacy of fuzzy MCDM methodologies in reconciling subjective judgments with diverse, heterogeneous data sets. Practically, the findings yield actionable insights and recommendations for Taiwanese authorities and stakeholders, highlighting the critical need for enhanced inter-agency coordination, clear delineation of stakeholder responsibilities, dynamic and responsive regulatory updates, and the establishment of institutionalized, risk-based auditing mechanisms to fortify port security governance.

Ultimately, Taiwan's international commercial ports operate at the nexus of global trade imperatives, national security considerations, and international regulatory frameworks. Effective port security governance transcends technical concerns, constituting a strategic imperative. This study bridges policy formulation with implementation realities, offering rigorous, empirically grounded insights to enhance resilience, compliance, and international credibility within Taiwan's port security infrastructure.

This study aims to examine the key factors influencing port facility security governance in Taiwan's international commercial ports, particularly under the framework of the ISPS Code. The rest of the paper is organized as follows: Section 2 provides a comprehensive review of pertinent literature and regulatory documents, focusing on port facility security provisions issued related to the ISPS Code and corresponding policies enacted by Taiwan's port authorities; it further investigates potential security threats facing Taiwan's international ports and clarifies the associated regulatory responsibilities, mandates, and inter-agency jurisdictional structures. Section 3 adopts an expert survey methodology to evaluate Taiwan's port security governance in relation to international regulatory standards. Section 4 analyzes the collected data, allowing for the integration of expert judgments under uncertainty and facilitating a robust prioritization of port security criteria. A discussion and conclusions are drawn in Section 5.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

2 LITERATURE REVIEW

This section begins with an overview of the ISPS Code, followed by a bibliometric analysis to explore academic trends related to the ISPS Code. The analysis includes identifying the most relevant journals and affiliations, conducting a thematic review, mapping authors' keyword networks, examining publication trends over time, and reviewing recent scholarly articles. Finally, the section concludes with an examination of compliance practices and security measures in Taiwan's international commercial ports.

2.1 ISPS Code: Framework and Application

The ISPS Code is a comprehensive set of measures developed to enhance the security of ships and port facilities, introduced in response to the heightened perception of maritime threats following the September 11, 2001 terrorist attacks in the United States (IMO, 2003). The ISPS Code was adopted as an amendment to the 1974 SOLAS Convention by the IMO and formally introduced through Conference Resolution 2 in December 2002 (IMO, 2003). This amendment revised Chapter XI-1 of SOLAS and added a new Chapter XI-2, thereby establishing the ISPS Code as an international framework for maritime security. Coming into force on July 1, 2004, the Code sets out mandatory security measures for governments, port authorities, and shipping companies, with the objective of identifying and assessing threats and reducing the risk of security-related incidents that could disrupt global maritime transport (Raunek, 2024).

The ISPS Code is divided into two parts: Part A contains mandatory provisions that Contracting States must implement; whereas Part B provides non-mandatory guidelines that offer recommended best practices to support the implementation of Part A. The objectives of Part A of the ISPS Code are as follows:

- To establish a set of international security standards applicable to contracting governments, administrative agencies, shipping companies, and port operators, ensuring the prevention and response to security incidents.
- To define the roles and responsibilities of contracting governments, administrative bodies, shipping companies, and port operators in implementing security measures.
- To ensure that security-related information concerning port facilities and ships is collected, analyzed, and communicated effectively.
- To provide a structured framework for conducting security assessments and responding to changes in security threat levels.

The ISPS Code applies to: (1) ships engaged in international voyages, including passenger ships, cargo ships of 500 gross tonnage or more, and mobile offshore drilling units; and (2) port facilities serving these categories of ships during international voyages. Contracting States may choose to extend the Code's application to port facilities that primarily handle domestic shipping or receive international ship calls infrequently, based on national security assessments (IMO, 2003). The Code explicitly excludes naval vessels, naval auxiliaries, and government-owned ships used for non-commercial purposes. The ISPS Code defines three security levels:

- Security Level 1: Minimum appropriate protective security measures must be maintained at all times.
- Security Level 2: Additional specific protective measures must be implemented during periods of heightened risk.
- Security Level 3: Further enhanced security measures are required when a security threat is imminent or has occurred.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

While the ISPS Code encompasses multiple objectives, one of its primary goals is to foster international cooperation among Contracting Governments, national administrations, port authorities, and shipping companies. This collaboration is vital for the assessment and management of maritime security threats. Additionally, the Code delineates the responsibilities and obligations of all relevant stakeholders involved in securing ships and port facilities at national, regional, and international levels.

2.2 Bibliometric Analysis on the ISPS Code

In order to gain a comprehensive view of the academic perspective on the ISPS Code, a bibliometric analysis was conducted. Using the database Scopus, the keyword "International Ship and Port Facility Security Code" was searched across "all fields". After excluding non-English publications and those without identifiable authors, a total of 679 relevant publications were identified.

Figure 1 shows a thematic map divided into four quadrants: Basic (bottom right corner), Motor (top right corner), Niche (top left corner), and Emerging or Declining (bottom left corner) themes. Basic themes are foundational and broadly relevant, serving as the basis for further research. This category encompasses security systems, maritime transport, and risk assessment. Motor themes are both highly developed and central to the field, indicating high density and relevance. This category includes two dominant themes: the human and governance approach, and the policy and regulatory framework. These findings reflect a strong research emphasis on human factors and policy-related issues in maritime security. Niche themes are well-developed but peripheral to the core of the research field. In this quadrant, three main topics are identified: economics and investments, gas fuel purification, and cybersecurity. Emerging or Declining themes represent areas that are either newly developing or losing relevance. This quadrant includes two major groups: autonomous ships and environmental conditions.

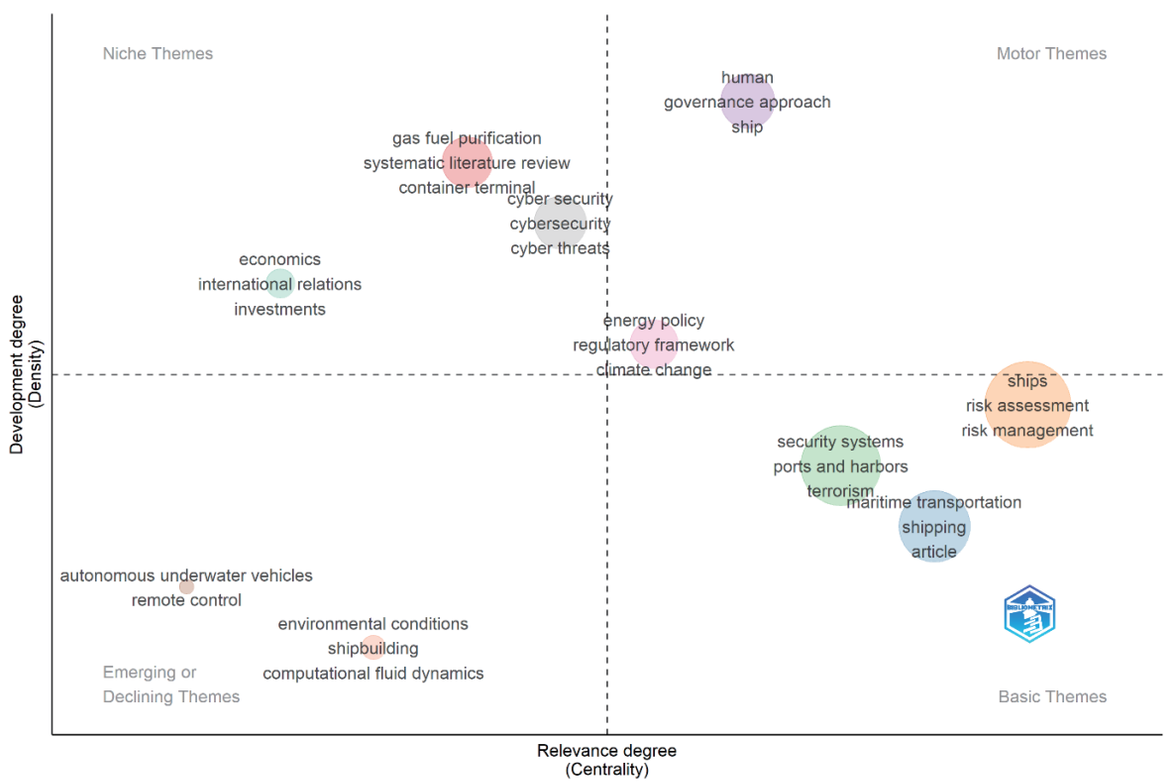

Figure 1. Thematic map.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

In order to understand the temporal trends in keyword usage, VOSviewer was used to visualize the results, as illustrated in Figure 2. The most frequently occurring keywords include maritime security, port security, risk assessment, and ISPS Code. A temporal analysis reveals that these core topics were predominantly discussed prior to 2015 (represented by navy blue nodes). Around 2020, the focus shifted toward risk assessment and regulatory aspects (green nodes). In the most recent years, the literature has increasingly addressed topics such as cybersecurity, decision-making, sustainable and energy efficiency (light green to yellow spots), reflecting broader research trends in the maritime sector that emphasize the importance of digital transformation and sustainable practices. For example, Stavroulakis et al. (2024) analyzed the sustainable maritime legislation, whereas Anyanova (2024) addressed maritime cybersecurity from the perspective of the ISPS Code (see Table 1 for the details of the research).

In order to identify more relevant articles for an in-depth literature review, the keyword "International Ship and Port Facility Security Code" was searched in the Scopus database using the field "Article title, Abstract, Keywords". This search yielded a total of 97 publications identified from 2002 to 2025. These include journal papers, conference papers, reviews, book chapters, notes and books. After removing non-English and unknown authors' publications, there were 84 articles left. Figure 3 shows the trends based on the number of publications by year. It illustrates that the relevant research addresses the ISPS Code, which is limited and outdated. The majority of the research articles were published prior to 2015, with only 29 articles published between 2015 and 2025.

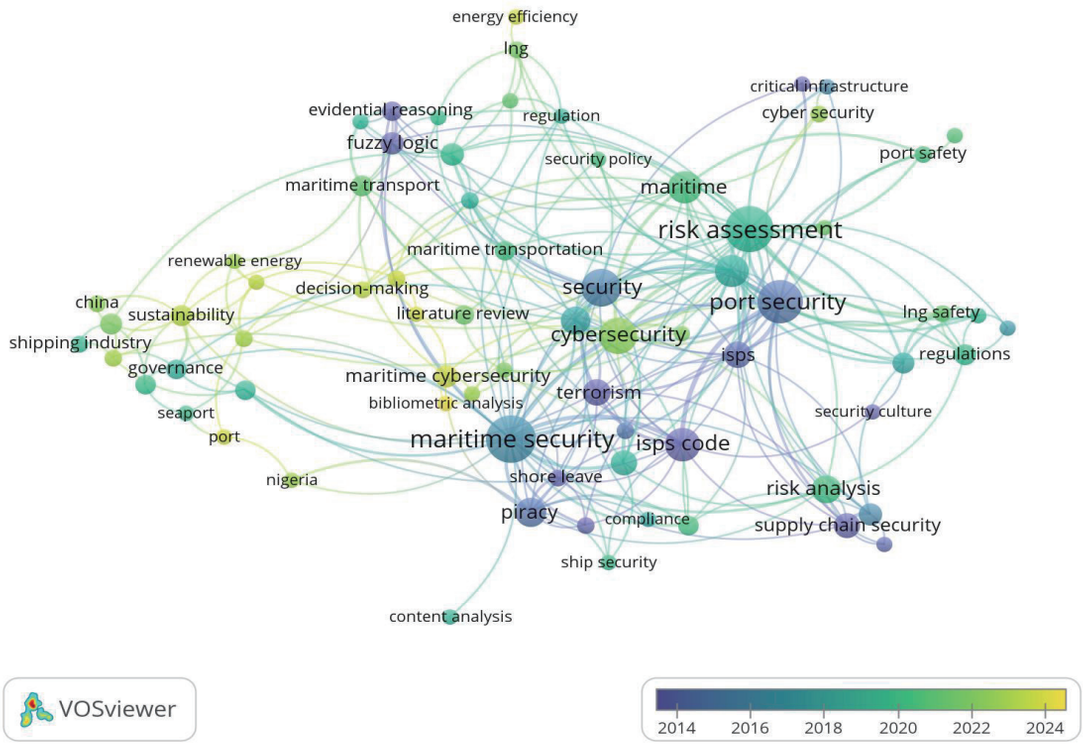

Figure 2. Authors keyword network.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

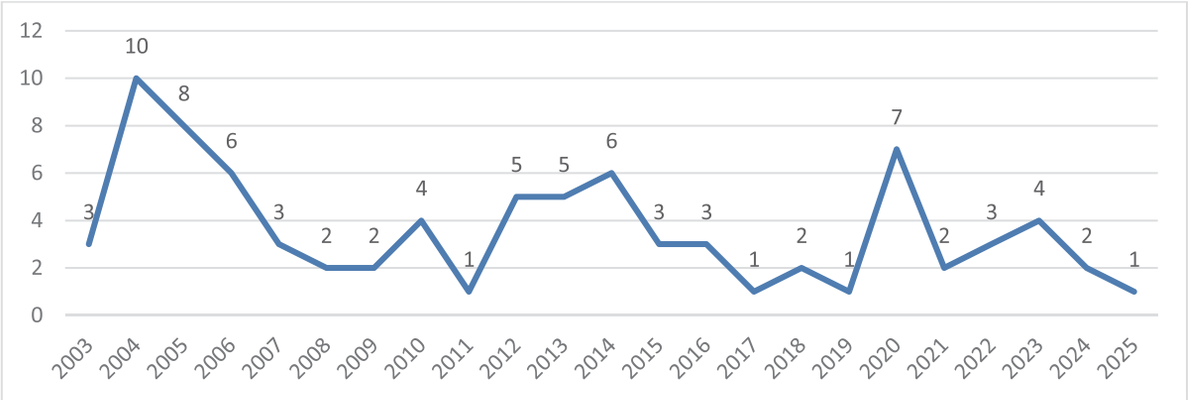

Figure 3. Selected publications.

After excluding inaccessible journals, 10 relevant papers were selected for detailed review. Table 1 provides a summary of these articles, including their key findings and research methodologies. Several noteworthy insights emerge from this literature. For instance, Stavroulakis et al. (2024) identified a significant difference in perceptions between academic scholars and industry professionals regarding the implementation of the ISPS Code. This is an issue that needs to be further explored in this study within the context of Taiwan's international ports. Other studies examine the application of the ISPS Code in various national contexts, including Indonesia (Wiko et al., 2023; Farisi et al., 2020), Azerbaijan (Hasanov & Alsulaiman, 2021), Mexico (Ávila-Zúñiga-Nordfjeld & Dalaklis, 2019), and Malaysia (Arof & Khadzi, 2018). Further details are presented in Table 1.

Table 1. Summary of selected journal papers.

Author	Journal	Summary	Methodology
Stavroulakis et al. (2024)	WMU Journal of Maritime Affairs	This study examines the ISPS and finds a significant divergence in perceptions between academics and practitioners regarding its implementation, highlighting a need for alignment to ensure effectiveness and sustainability in international maritime legislation.	The study used a Google Forms survey with 102 respondents (63 practitioners, 39 academics) to assess ISPS Code awareness, importance, and implementation. Reliability was tested via Cronbach's alpha and intraclass correlation coefficient (ICC); t-tests, Analysis of Variance (ANOVA), and Hotelling's T-square supported analysis.
Anyanova (2024)	Maritime Cyber Security	The paper examines the need for amending international law to achieve cyber resilience in the maritime industry, analyzing the impact of cybersecurity on shipping and discussing legal frameworks and proposed amendments to existing regulations like the ISPS Code.	The methodology involves international legal research and analysis of data, focusing on laws, cyber attacks, and international documents like the ISPS Code and IMO guidance, as well as evaluating countermeasures in cybersecurity.
Moran (2023)	European Journal of Legal Studies	The paper concludes that absolute freedom of the seas is impractical and proposes that regulation and enforcement, particularly through strengthening coastal state support, are necessary to balance maritime security with freedom of navigation.	The methodology involves analyzing the legal and security framework of maritime security and freedom of navigation, reviewing types of freedom of navigation under international law, examining maritime terrorism and piracy, and analyzing legal instruments to offer suggestions for reconciliation.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Author	Journal	Summary	Methodology
Wiko et al. (2023)	Indonesian Journal of International Law	The paper discusses the development of Tanjungpura Port, Kijing Terminal, an international hub port, focusing on legal regulations and governance to enhance economic competitiveness and regional development in Indonesia.	A normative research methodology was employed using an in-concreto legal approach, examining bibliographic sources and secondary data. A qualitative lens was applied to explore and understand the efforts of various stakeholders involved in maritime security practices.
Adams et al. (2021)	Journal of Transportation Security	The paper provides guidance to ports on understanding and mitigating hybrid cyber-physical security threats, emphasizing the importance of interdependencies between cyber and physical domains and offering recommendations to enhance security situational awareness and reduce vulnerabilities.	This study developed a Hybrid Situational Awareness (HSA) system comprising four key modules to assess cascading cyber-physical attacks on port infrastructure. Using modeling and simulation techniques, it analyzed potential impacts on port operations and integrated real-time data with dynamic threat assessment to enhance situational awareness and response effectiveness.
Hasanov and Alsulaiman (2021)	Maritime Technology and Research	The paper evaluates the successful implementation of the ISPS Code in Azerbaijan, highlighting a high security level but also areas for improvement, with the State Maritime Agency playing a key role in training and exceeding international standards.	A mixed-methods approach was used, combining qualitative and quantitative techniques. It included a literature review, interviews with key security personnel, and a survey of 115 maritime security stakeholders across two ports, gathering data from both industry professionals and governmental agencies.
Farisi et al. (2020)	Indonesian Journal of International Law	The paper reviews the facility security measures at Ujung Jabung Port in terms of the ISPS Code, discussing its strategic location, construction, and compliance with international security standards.	The methodology involves a review of existing regulations and legal frameworks related to the construction and development of the Samudera Ujung Jabung Port, focusing on the implementation of the ISPS Code. The study includes an analysis of discrepancies in port categorization based on different regulations.
Ávila Zúñiga-Nordfjeld and Dalaklis (2019)	WMU Journal of Maritime Affairs	This paper aims to improve port security measures in developing countries by integrating incident reporting and investigation procedures, focusing on the Mexican experience, and develops a "transparent port security incident reporting tool" that significantly improves incident reporting and contributes to a national maritime security policy.	Qualitative semi-structured interviews with stakeholders were used to explore port security challenges and opportunities. Data were analyzed through thematic analysis and constant comparison. An action research approach supported practical implementation, with regular assessments to refine the incident reporting tool.
Arof and Khadzi (2018)	International Journal of Supply Chain Management	This study identifies two additional factors (monitoring/assessment/audit and access control) for effective ISPS Code implementation and concludes that Vale Malaysia Minerals has satisfactorily adhered to the general ISPS Code requirements, with suggestions for improvement in regular drills and security exercises.	A Delphi technique was used to collect primary data. The Delphi technique involved two rounds of questionnaires: the first round used open-ended questions, and the second round used closed-ended questions. The questionnaire was pilot tested before being disseminated to respondents via email.
Malcolm (2016)	The British Journal of Politics and International Relations	The study examines how the "war on terror" led to the securitization of UK ports, detailing a typology of counter-terrorism practices that are constantly evolving and expansive in scope, with a focus on spatial and temporal dimensions of control.	This study analyzed legislation, regulatory texts, and academic sources, supplemented by site visits to three UK ports and interviews with security stakeholders. Ports were strategically selected for diversity, and documents were collected from the IMO library and online platforms.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

3 RESEARCH METHOD

3.1 Research Framework

This study follows a structured approach to examining Taiwan's international commercial ports' security management. First, a literature review was conducted to analyze international port security regulations, with a focus on the ISPS Code. The study then examined Taiwan's port security policies, the roles of relevant agencies, and potential gaps in international regulations. From the ISPS Code provisions, port security roles can be categorized into three primary sectors: Management-Port Management Authorities, Operations-Port Facility Lessee Agencies, and Government-Port Law Enforcement Agencies. To ensure a comprehensive evaluation of port security measures, this study will structure its questionnaire design based on these three dimensions. Moreover, an additional dimension "Security Policies and Regulations" will be included to assess the legal and regulatory frameworks that support security responsibilities within ports. This framework will provide a structured approach to analyzing Taiwan's compliance with ISPS Code regulations and identifying areas for enhancement in port security management. To ensure an objective assessment, this questionnaire survey was distributed to senior officials from the maritime and shipping industry, government, and academia. Their opinions will then be analyzed to understand the importance of the port security measures in Taiwan. This study is important as it helps port authorities as well as the maritime industry focus on the most critical port security measures.

3.2 Sampling

This study employs an online questionnaire survey to analyze Taiwan's international commercial port security policies and relevant international regulations, with a particular focus on the ISPS Code. Selected provisions from the ISPS Code were categorized and incorporated into the questionnaire, which was distributed via email to industry professionals and academic experts. The target samples included representatives from port authorities, the Coast Guard Administration, Port Police, Customs personnel, and other relevant stakeholders, as well as scholars specializing in port security research, contributing to assessing the perceived importance of the security dimensions (the criteria and sub-criteria) for different stakeholders, and improving security measures and regulatory alignment in Taiwan's international commercial ports.

In total, 52 replies were collected. Upon collection, the responses underwent an initial consistency check to ensure reliability. Valid responses were then analyzed using Excel and R software to determine the weighting of key factors in port security.

3.3 Analytical Framework

This study develops a structured hierarchical model for evaluating the importance of port security management. The model consists of three levels:

- Goal Level: Enhancing the security management of international commercial ports.
- Criteria Level: Four primary security dimensions.
- Sub-criteria Level: Twelve critical security factors.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

The questionnaire required experts to evaluate the relative importance of security factors in commercial ports. Table 2 presents the four major port security criteria identified in this study, aligned with the provisions of Part A of the ISPS Code, as well as the corresponding roles of port stakeholders in Taiwan.

Table 2. Comparison of dimensions, ISPS Code, and agencies.

ISPS Code	Criteria	Agency
Contracting State Responsibilities Declaration of Security Records	Port Management Authorities	Maritime Port Bureau Taiwan International Ports Corp.
Company responsibilities Company security personnel Vessel security personnel Vessel security Vessel security training and drills Vessel security assessment Vessel security plan Port facility security plan Port facility security Port facility security personnel Port facility security training and drills	Facility Lessee	Terminal operator Shipping companies
Port facility security assessment Vessel security assessment	Security Enforcement Agencies	Port policy Coast Guard Administration Customs
Responsibilities of Contracting States Ship inspection and certification Record keeping	Security Policies and Regulations	IMO

Table 3 provides a detailed explanation of the four key criteria employed in this study, including Port Management Authority, Facility Lessee, Security Law Enforcement Agency, and Security Policies and Regulations. This table serves to clarify the conceptual framework of each criterion, ensuring that respondents have a comprehensive understanding of their significance within the study.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Table 3. The criteria level.

Criteria	Code	Contents	Source
Port Management Authority	PM	The Port Management Authority shall issue security levels for port security and review port security plans.	European Union (2020); IMO (2021)
Facility Lessee	FL	Port Facility Lessees must prepare relevant security plans and conduct security plan drills to ensure that company personnel and ship personnel understand the contents of the security plans.	European Union (2020); IMO (2021)
Security Law Enforcement Agency	SL	As the primary law enforcement entity in the port, the port law enforcement agency must intervene in response to any illegal activity within the port area.	European Union (2020); IMO (2021); Inter-American Committee on Ports (2025)
Security Policies and Regulations	SP	The government should establish security policies and regulations for international commercial ports, providing a foundation for enforcement and compliance by Port Management Authorities, Law Enforcement Agencies, and Facility Lessees.	European Union (2020); IMO (2021); Australian Government (2021); Departamento de Seguridad Nacional (2024)

Table 4 provides a detailed explanation of the sub-criteria. As each criterion comprises three sub-criteria, a total of 12 sub-criteria are defined. This table serves to enhance respondents' understanding of the research framework and its significance before completing the questionnaire, thereby minimizing potential errors in responses. In hierarchical analytic frameworks, each sub-criterion must be mutually exclusive, collectively exhaustive, and contextually bounded within its parent dimension to ensure conceptual clarity and prevent redundancy across dimensions (Ishizaka & Nemery, 2013).

The Port Management Authority (PM) dimension encompasses policy execution, plan approval, and supervisory oversight. Its sub-criteria, namely PM1, PM2, and PM3, represent administrative functions that cannot be assigned to other entities. PM1 concerns establishing port security regulations in line with the ISPS Code, a legislative mandate unique to government authorities. PM2 involves reviewing and approving PFSPs, a task reserved for authorized management agencies rather than lessees or enforcement bodies. PM3 entails ensuring PFSP implementation through supervision and drills, reflecting a system-level oversight distinct from the lessee's internal operational practices. Thus, PM sub-criteria collectively define the governance mechanism of port security. The Facility Lessee (FL) dimension represents terminal operators responsible for translating approved plans into practice. FL1 covers formulating the PFSP and vessel protection plan, which only lessees and shipping companies can design, subject to PM approval. FL2 addresses ensuring personnel comprehension of PFSP contents through internal communication and training, while FL3 involves conducting regular security drills to maintain operational readiness. These sub-criteria emphasize internal execution and workforce

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

preparedness, distinguishing FL from the regulatory or enforcement functions of other dimensions. The Security Law Enforcement (SL) dimension reflects state enforcement units such as Customs, Coast Guards, and Port Police. SL1 involves inspecting vessels entering or leaving ports, SL2 covers safety inspections within port areas, and SL3 pertains to verifying the identities of individuals and vehicles accessing restricted zones. These tasks require formal enforcement authority, differentiating them from administrative or managerial oversight. Collectively, SL sub-criteria capture the coercive and preventive dimensions of maritime law enforcement. The Security Policies (SP) dimension defines the macro-level institutional environment. SP1 involves establishing a unified business platform for inter-agency coordination, SP2 focuses on developing comprehensive national security inspection regulations, and SP3 concerns forming specialized port security units. These sub-criteria describe policy design and institutional integration, providing the regulatory foundation for the PM, FL, and SL dimensions to function effectively.

Methodologically, the strict attribution of each sub-criterion to a single criterion ensures the independence of judgments in pairwise comparisons, enhances traceability to specific decision domains (policy, management, enforcement, and operation), and maintains hierarchical consistency across governance levels. The twelve sub-criteria thus constitute a mutually exclusive yet collectively exhaustive framework, a necessary condition for analytical precision, interpretive clarity, and reliable weighting in multi-criteria evaluation.

Table 4. Explanation of each dimension factor.

Crit	Sub-criteria	Code	Content	Source
PM	Participate in and comply with the provisions of the ISPS Code	PM1	Contracting Governments should establish relevant security regulations for international ports within their jurisdiction, ensuring compliance with the ISPF Code.	IMO (2021); Organization of American States (2021); Nippon Kaiji Kyokai (2023)
	Review PFSP of each port facility	PM2	The designated government management agencies must inspect the PFSP of each facility to ensure they comply with relevant regulations.	
	Ensure that all units and agencies implement the PFSP	PM3	The designated port management agencies must ensure that all port units implement the PFSP and conduct regular drills and inspections.	
FL	Formulate PFSP and vessel protection plan	FL1	Port facility lessees must develop a PFSP, while shipping companies must also develop ship security plans.	Inter-American Committee on Ports (2025); Curvey (2024); Organization of American States (2021)
	Ensure that the company and port site personnel understand the PFSP	FL2	Port facility lessees should ensure that company personnel and on-site port staff fully understand the content of the PFSP.	

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Crit	Sub-criteria	Code	Content	Source
	Regularly conduct port security plan drills	FL3	Port facility lessees should regularly conduct drills for the port security plan to ensure its effective implementation.	
SL	Inspection of import and export vessels	SL1	Port law enforcement agencies must inspect vessels entering and leaving the port to ensure the identity of crew members and that there are no prohibited items on board.	IMO (2021); Organization of American States (2021)
	Enforce port security inspection	SL2	In addition to inspecting vessels entering and leaving the port, port law enforcement agencies must also conduct safety inspections within the port area to prevent unauthorized entry.	
	Ensure the identity of people and vehicles entering the port area	SL3	The verification of people and vehicles entering the port area is the primary checkpoint before entering the port, ensuring that personnel match the application data.	
SP	Establish a unified business handling platform	SP1	Establishing a unified business handling platform can effectively reduce the ambiguity issues that arise among multiple units and make it easier for businesses to find the responsible agency.	Government of the Netherlands (2015, pp. 12–13)
	Establish comprehensive domestic security inspection regulations	SP2	The government should construct a comprehensive set of security inspection regulations to provide a complete basis for implementation by all port units.	
	Establish a specialized unit for port security	SP3	Regulations should be established to set up specialized units for port security, allowing security to be implemented by dedicated departments and reducing potential ambiguity among different units.	

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Figure 4 illustrates the structure for this study, derived from the contents of Tables 3 and 4. The research framework is organized into an objective, four criteria, and three sub-criteria under each criterion.

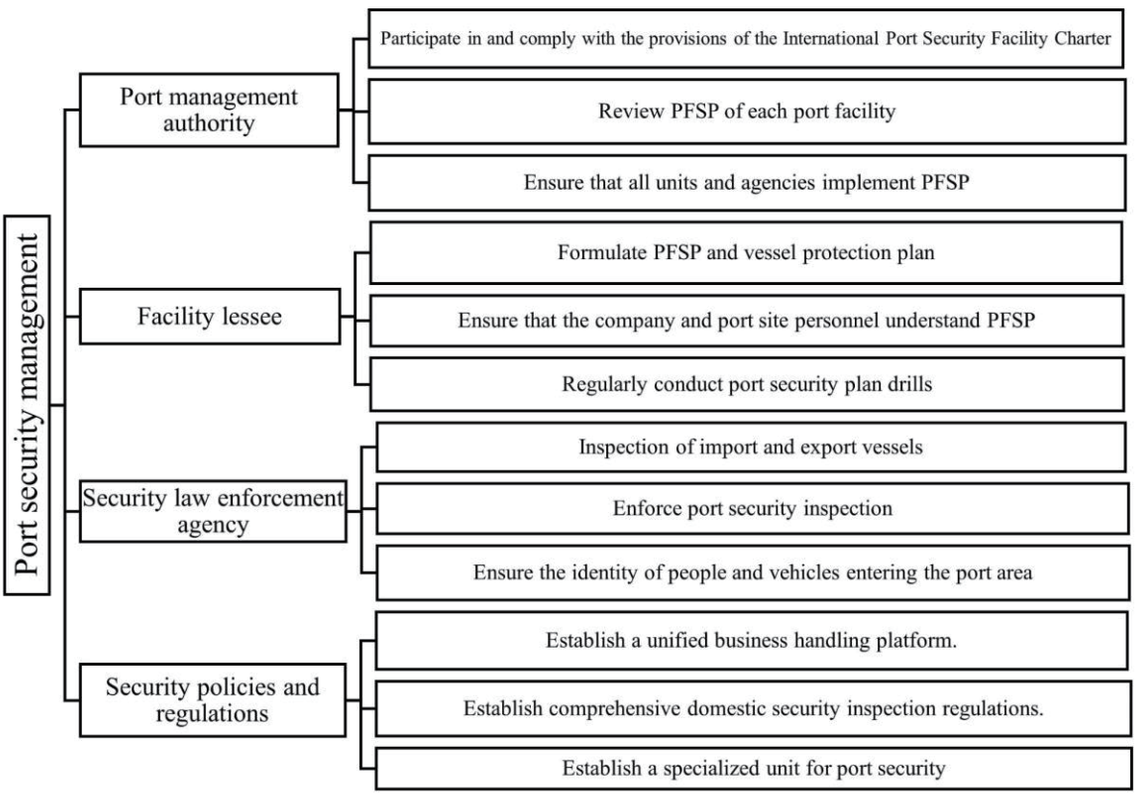

Figure 4. Research framework diagram.

3.4 Data Collection Method

The data necessary for the analysis was collected using an online questionnaire with three sections. In the first section, experts were asked to rate the importance of each criterion (5 levels ranging from 'very unimportant' to 'very important') for port security measures in Taiwan. In the second section, experts were asked to assess the importance of each sub-criterion (5 levels ranging from 'very unimportant' to 'very important'). The last section requested respondents to provide details about their professional background, e.g., occupation type (i.e., academic scholar or industry professional), position, work experience (years), and department.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

3.5 Data Analysis Method

In this study, a fuzzy Multi-Criteria Decision-Making (MCDM) method was employed to analyze the relative importance of the identified criteria and sub-criteria. The MCDM method is well-suited for this study as it allows for the systematic evaluation of complex and interrelated factors, which is essential when assessing multiple safety and security criteria in port operations. Although all sub-criteria are expected to be implemented in international ports in accordance with the ISPS Code, the associated costs and management efforts may vary depending on the respondent's industry background. Given that companies operating in the port sector often face limited capital and resources for addressing safety and security concerns, understanding the prioritization of these criteria is crucial. This enables organizations to allocate their efforts and resources more effectively, focusing on the most critical areas.

In the field of decision-making, numerous studies have highlighted the presence of uncertainty and ambiguity in human judgments. To address this challenge, fuzzy theory has emerged as a widely accepted approach for dealing with imprecision, vagueness, and subjectivity in decision-making processes (Chang, 2013). Fuzzy logic has been extensively applied in combination with various MCDM methods in the maritime domain. For instance, Chang et al. (2019) utilized fuzzy Analytic Hierarchy Process (AHP) to evaluate risk mitigation strategies in container shipping operations, while Belabyad et al. (2025) applied the fuzzy Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to prioritize skill requirements for future maritime education and training, particularly in the context of autonomous shipping. Additional applications of fuzzy MCDM approaches in the maritime sector can be found in Yazır (2023). The following section introduces the principles of fuzzy theory and outlines the steps involved in the fuzzy MCDM method used in this study.

3.5.1 Introduction to fuzzy theory and basic arithmetic

Fuzzy models, such as those utilizing triangular fuzzy numbers, have proven highly effective in addressing decision-making problems where information is imprecise. Below, some fundamental definitions of fuzzy sets and fuzzy arithmetic are outlined per Belabyad et al. (2025).

Definition 1. "A fuzzy set $\tilde{A}$ in a universe of discourse X is characterised by a membership function that assigns a real number in the interval [0;1] to each element x.

Definition 2. A triangular fuzzy number $\tilde{a}$ is defined by a triplet $\tilde{a} = (a_1, a_2, a_3)$ as shown in Figure 5.

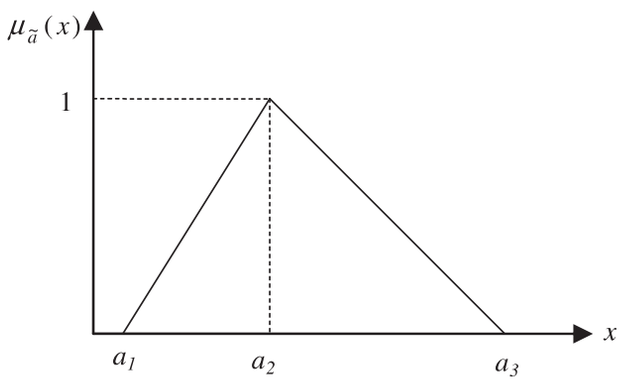

Figure 5. Triangular fuzzy number.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

The membership function for a triangular fuzzy number is defined as follows:

$$\mu_{\tilde{a}}(x) = \begin{cases} 0, & x < a_1 \\ \frac{x-a_1}{a_2-a_1}, & a_2 \geqslant x \geqslant a_1 \\ \frac{x-a_3}{a_2-a_3}, & a_3 \geqslant x \geqslant a_2 \\ 0, & x > a_3 \end{cases}$$

where a_2 is the value for which $\mu_{\tilde{a}}(a_2) = 1$, and a_1 and a_3 are the extreme values on the left and right of the fuzzy number $\tilde{a}$, respectively, with $\mu_{\tilde{a}}(a_1) = \mu_{\tilde{a}}(a_3) = 0$.

Definition 3. Operations involving fuzzy numbers, $\tilde{a} = (a_1, a_2, a_3)$ and $\tilde{b} = (b_1, b_2, b_3)$, such as addition, subtraction, multiplication, and division, can be represented as follows (Chang, 2013):

$$\tilde{a} \oplus \tilde{b} = (a_1, a_2, a_3) \oplus (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$$
$$\tilde{a} \ominus \tilde{b} = (a_1, a_2, a_3) \ominus (b_1, b_2, b_3) = (a_1 - b_3, a_2 - b_2, a_3 - b_1)$$
$$\tilde{a} \otimes \tilde{b} = (a_1, a_2, a_3) \otimes (b_1, b_2, b_3) = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3)$$
$$\tilde{a} \oslash \tilde{b} = (a_1, a_2, a_3) \oslash (b_1, b_2, b_3) = \left(\frac{a_1}{b_3}, \frac{a_2}{b_2}, \frac{a_3}{b_1}\right)$$
$$k\tilde{a} = k(a_1, a_2, a_3) = (ka_1, ka_2, ka_3).$$

3.5.2 Fuzzy Multi-Criteria Decision-Making (MCDM) analysis

As mentioned previously, this study uses the weight of the criterion times the weight of the sub-criterion under the relevant criterion to obtain the final global weight of each sub-criterion. The analysis process is described as the following steps:

Step 1: Transform crisp values to fuzzy values

To conduct the fuzzy weighting analysis, the crisp values provided by the respondents must first be converted into fuzzy values. The linguistic variables and corresponding fuzzy numbers for both criteria and sub-criteria are adapted from Chen (2000) and Belabyad et al. (2025), who employed a seven-level linguistic scale. However, this study adopts a five-level scale, as described in Section 3.4. These five linguistic levels are converted into their respective fuzzy numbers, as presented in Table 5 for the criteria and Table 6 for the sub-criteria. Different fuzzy numbers are used for the criteria (Table 5) and sub-criteria (Table 6) to ensure that the calculated global weights in Step 3 fall within the range of 1 to 5, aligning with the scale of a 5-point Likert system.

Table 5. Linguistic variables for the weight of each criterion.

Linguistic Variable	Fuzzy Number
Very unimportant	(0, 0.1, 0.3)
Unimportant	(0.1, 0.3, 0.5)
Medium	(0.3, 0.5, 0.7)
Important	(0.5, 0.7, 0.9)
Very important	(0.7, 0.9, 1)

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Table 6. Linguistic variables for the importance weight of each sub-criterion.

Linguistic Variable	Fuzzy Number
Very unimportant	(1, 1, 2)
Unimportant	(1, 2, 3)
Medium	(2, 3, 4)
Important	(3, 4, 5)
Very important	(4, 5, 5)

Step 2: Calculate fuzzy weight criteria and sub-criteria

After transforming the crisp values obtained from the respondents into fuzzy values, the fuzzy weights of each criterion ($\widetilde{wc}$) can be calculated using Equation 1 below:

$$\widetilde{Wc}^{\iota} = \frac{\sum_1^n \widetilde{Wc_n^{\iota}}}{n} \quad (1)$$

Where n is the number of respondents, and i=1,2,…,4 is the criterion.

Simultaneously, the fuzzy weight of sub-criteria ($\widetilde{wsc}$) can be obtained using Equation 2 below:

$$\widetilde{Wsc}^{\iota J} = \frac{\sum_1^n \widetilde{Wsc_n^{\iota J}}}{n} \quad (2)$$

Where j = 1, 2, and 3 is the sub-criterion

Step 3: Calculate the global weight of sub-criteria

When calculating the global weights of the sub-criteria, it is essential to account for the importance of their corresponding criteria. Adopting the concept from the Analytic Hierarchy Process (AHP) approach, the global weight of each sub-criterion is determined by multiplying its local weight by the weight of its associated criterion. Accordingly, the global weights of the sub-criteria ($\widetilde{Gsc}$) can be calculated using Equation 3 below:

$$\widetilde{Gsc} = \widetilde{Wc}^{\iota} \times \widetilde{Wsc}^{\iota J} \quad (3)$$

Where $\widetilde{Wsc}^{\iota J}$ is the $\widetilde{Wsc}^{J}$ under the relevant criterion i

Step 4: Defuzzy the fuzzy values to crisp values

After obtaining the global weight of sub-criteria, they are converted into crisp values in order to determine the priority of each sub-criterion under its corresponding criterion. Various defuzzification methods have been employed in existing research to achieve this conversion such as $DF = \frac{a_1+2a_2+a_3}{4}$ (Durán & Aguilo, 2008), $DF = \frac{a_1+4a_2+a_3}{6}$ (Ding, 2010) and $DF = \frac{((a_3-a_1)+(a_2-a_1))}{3} + a_1$(Ali et al., 2012). In this study, the method proposed by Ali et al. (2012) was adopted, which applies the center of gravity approach for defuzzification. In addition, the other two methods were also employed to validate the results obtained from the approach of Ali et al.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

4 RESEARCH ANALYSIS RESULTS

4.1 Respondents' Background

A total of 52 replies were collected, including 40 industry professionals and 12 academic scholars. Table 7 provided detailed information on the respondents' background. Ten of the 12 academic scholars (83.3%) hold positions of Associate Professors or above, and the same proportion has more than 11 years of port-related work experience. In terms of their academic affiliation, eight work in Business school, one works in Law school, and three work in Engineering and Science school, indicating a multidisciplinary perspective, and thus minimizing the bias from a single perspective. The selected sample was initially screened to verify whether the participating scholars possessed relevant experience in port safety education and policy development, thereby ensuring their capability to provide informed and meaningful responses to the questionnaire items. Among industry professionals, 36 out of 40 (90%) occupy positions at the level of Director or higher. The majority (60%) have over 11 years of experience in the port industry, which shows that most of them have rich work experience related to the port industry, and thus their opinions on the security measures for Taiwan's ports are reliable. In terms of their department, 12 of them work at port authorities, six work at law enforcement agencies, and 22 work at facility leasing units.

Table 7. Respondents' background.

		Academic Scholars		Industry Professionals	
		N=12	%	N=40	%
Position	Professor	3	25.0%		
	Associate Professor	7	58.3%		
	Assistant Professor	2	16.7%		
	Vice General Manager or above			3	7.5%
	Manager			15	37.5%
	Director			18	45.0%
	Staff			4	10.0%
Work Experience	1-5 years	2	16.6%	2	5.0%
	6-10 years	0	0.0%	7	17.5%
	11-15 years	5	41.7%	15	37.5%
	16+ years	5	41.7%	16	40.0%
Department	Business school	8	66.7%		
	Law school	1	8.3%		
	Engineering and Science school	3	25.0%		
	Port authority			12	30.0%
	Law enforcement			6	15.0%
	Leasing			22	55.0%

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

4.2 Results of Descriptive Analysis

The results of the questionnaire survey were first analyzed using descriptive statistics (see Table 8). At the criteria level, Port Management Authority was ranked as the most important criterion overall, followed closely by Security Policies and Regulations, Security Law Enforcement Agency, and Facility Lessee, with mean values between 4.38 and 4.58. In addition, while the overall ranking of Port Management is the most important, Security Policies and Regulations exhibit a higher level of consensus among respondents, as indicated by the lower standard deviation (S.D.). To gain deeper insights, the results were further examined from the perspectives of academic scholars (Aca Mean) and industry professionals (Ind Mean). Interestingly, the results from two groups of respondents are different. Academic scholars rated Security Policies and Regulations as the most important criterion, while the remaining three criteria have received identical or nearly identical mean scores. In terms of industry professionals, the most important criterion was Port Management Authority, followed by Security Policies and Regulations, Security Law Enforcement Agency, and Facility Lessee. The ranking from industry professionals aligned with the overall results. This ranking suggests that industry professionals generally believe the Port Management Authority should be the primary entity responsible for security management in international commercial ports. This preference is likely due to the Port Management Authority's role as the operational hub of the port, particularly after privatization, where it has assumed responsibility for managing and enhancing port competitiveness, thus warranting a higher priority in industrial assessments. Industry professionals also placed significant emphasis on Security Policies and Regulations, likely due to the fact that, although Taiwan's commercial ports are privatized, their management still heavily relies on the establishment of comprehensive legal frameworks, such as the Commercial Port Law. Without sufficient and well-established legal regulations, management agencies may face challenges in effectively governing the ports. When combining the results from both the academic and industry questionnaires, it is evident that while there are slight differences in perspectives, both groups overall place considerable importance on "Port Management Authority" and "Security Policies and Regulations" in the security management of international commercial ports.

In terms of the ranking of sub-criteria, the top three overall sub-criteria are "Regularly conduct port security plan drills (FL3)", "Ensure that the company and port site personnel understand the PFSP (FL2)", and "Ensure that all units and agencies implement the PFSP (PM3)". In addition, when considering the S.D., although FL3 has a slightly higher average importance, the responses for FL2 are more dispersed, suggesting that some respondents perceive FL2 to be more important than FL3. When further breaking down the results of the above two groups, academic scholars ranked the top three important sub-criteria as follows: "Ensure that all units and agencies implement the PFSP (PM3)", "Formulate PFSP and vessel protection plan (FL1)", and "Review PFSP of each port facility (PM2)". In contrast, the most important sub-criteria from industry professionals' perspective were: FL3, followed by FL2 and SL3.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Table 8. Results of descriptive analysis.

	Overall Mean	Overall S.D.	Overall Rank	Aca Mean	Aca S.D.	Aca Rank	Ind Mean	Ind S.D.	Ind Rank
Criteria									
Port Management Authority (PM)	4.58	0.54	1	4.67	0.49	2	4.55	0.55	1
Facility Lessee (FL)	4.38	0.60	4	4.67	0.49	2	4.3	0.60	4
Security Law Enforcement Agency (SL)	4.40	0.60	3	4.67	0.49	2	4.33	0.61	3
Security Policies and Regulations (SP)	4.54	0.50	2	4.75	0.45	1	4.48	0.50	2
Sub-criteria									
Participate in and comply with the provisions of the ISPS Code (PM1)	4.46	0.58	9	4.58	0.51	5	4.43	0.59	8
Review PFSP of each port facility (PM2)	4.52	0.58	5	4.75	0.45	2	4.45	0.59	7
Ensure that all units and agencies implement the PFSP (PM3)	4.60	0.57	3	4.83	0.39	1	4.53	0.59	5
Formulate PFSP and vessel protection plan (FL1)	4.48	0.61	7	4.75	0.45	2	4.40	0.62	9
Ensure that the company and port site personnel understand the PFSP (FL2)	4.62	0.57	2	4.67	0.49	4	4.60	0.58	2
Regularly conduct port security plan drills (FL3)	4.65	0.52	1	4.50	0.52	6	4.70	0.51	1
Inspection of import and export vessels (SL1)	4.48	0.67	7	4.25	0.65	12	4.55	0.67	4
Enforce port security inspection (SL2)	4.50	0.54	6	4.42	0.51	7	4.53	0.55	5
Ensure the identity of people and vehicles entering the port area (SL3)	4.54	0.58	4	4.33	0.49	9	4.60	0.58	2
Establish a unified business handling platform (SP1)	4.37	0.63	12	4.33	0.65	9	4.38	0.62	11
Establish comprehensive domestic security inspection regulations (SP2)	4.38	0.63	10	4.33	0.65	9	4.40	0.62	9
Establish a specialized unit for port security (SP3)	4.38	0.53	10	4.42	0.67	7	4.38	0.49	11

4.3 Results of Fuzzy Weighting

As the results in Table 8 reflect only the relative importance of sub-criteria without accounting for the varying importance of the four main criteria, the fuzzy MCDM method is employed to address this issue. Additionally, given the inherent uncertainty in human decision-making, fuzzy theory is commonly used to enhance the robustness of such analyses.

After converting respondents' answers into fuzzy values using the fuzzy numbers defined in Tables 5 and 6 (Step 1 in Section 3.5.2), the fuzzy weights of criteria and sub-criteria were calculated using Equations 1 and 2, as outlined in Step 2. Table 9 presents the fuzzy weights of the main criteria based on the fuzzy numbers in Table 5. Interestingly, academic scholars assigned equal weight to all four criteria, whereas industry professionals displayed slight variations in their assessments. Table 10 shows the fuzzy weights of sub-criteria based on the fuzzy numbers in Table 6.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Table 9. Results of fuzzy weight of the criteria.

Criteria	Academic Scholars	Industry Professionals	Overall
Port Management Authority (PM)	(0.63, 0.83, 0.97)	(0.61, 0.81, 0.95)	(0.62, 0.82, 0.96)
Facility Lessee (FL)	(0.63, 0.83, 0.97)	(0.56, 0.76, 0.92)	(0.58, 0.78, 0.93)
Security Law Enforcement Agency (SL)	(0.63, 0.83, 0.97)	(0.57, 0.77, 0.93)	(0.58, 0.78, 0.93)
Security Policies and Regulations (SP)	(0.63, 0.83, 0.97)	(0.60, 0.80, 0.95)	(0.61, 0.81, 0.95)

Table 10. Results of fuzzy weight of the sub-criteria.

Sub-criteria	Academic Scholars	Industry Professionals	Overall
PM1	(3.58, 4.58, 5.00)	(3.43, 4.43, 4.95)	(3.46, 4.46, 4.96)
PM2	(3.75, 4.75, 5.00)	(3.45, 4.45, 4.95)	(3.52, 4.52, 4.96)
PM3	(3.83, 4.83, 5.00)	(3.53, 4.53, 4.95)	(3.60, 4.60, 4.96)
FL1	(3.75, 4.75, 5.00)	(3.40, 4.40, 4.93)	(3.48, 4.48, 4.94)
FL2	(3.67, 4.67, 5.00)	(3.60, 4.60, 4.95)	(3.62, 4.62, 4.96)
FL3	(3.50, 4.50, 5.00)	(3.70, 4.70, 4.98)	(3.65, 4.65, 4.98)
SL1	(3.25, 4.25, 4.92)	(3.55, 4.55, 4.90)	(3.48, 4.48, 4.90)
SL2	(3.42, 4.42, 5.00)	(3.53, 4.53, 4.98)	(3.50, 4.50, 4.98)
SL3	(3.33, 4.33, 5.00)	(3.60, 4.60, 4.95)	(3.54, 4.54, 4.96)
SP1	(3.33, 4.33, 4.92)	(3.38, 4.38, 4.93)	(3.37, 4.37, 4.92)
SP2	(3.33, 4.33, 4.92)	(3.40, 4.40, 4.93)	(3.38, 4.38, 4.92)
SP3	(3.42, 4.42, 4.92)	(3.38, 4.38, 5.00)	(3.38, 4.38, 4.98)

Using Equation 3 in Step 3, the global fuzzy weights of the sub-criteria could be calculated, with the results presented in Table 11. These fuzzy weights were then converted into crisp values using the defuzzification method proposed by Ali et al. (2012), as shown in Table 12. The analysis reveals that "Ensure that all units and agencies implement the PFSP (PM3)" is considered the most important sub-criterion among the academic scholars, industry professionals, and in the overall ranking. "Review PFSP of each port facility (PM2)" is ranked as the second across both groups and in the overall results. The third-ranked sub-criterion is the same for both industry professionals and the overall ranking: "Participate in and comply with the provisions of the ISPS Code (PM1)". The least important criterion, "Inspection of import and export vessels (SL1)," is ranked last by both academic scholars and in the overall results, and 11th out of 12 by industry professionals. A notable divergence is observed in the ranking of "Formulate PFSP and vessel protection plan (FL1)," which academic scholars considered the second most important, while industry professionals ranked it as the least important sub-criterion.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

Table 11. Results of fuzzy global weights of sub-criteria.

Sub-criteria	Academic Scholars	Industry Professionals	Overall
PM1	(2.27, 3.82, 4.83)	(2.09, 3.58, 4.71)	(2.13, 3.64, 4.74)
PM2	(2.38, 3.96, 4.83)	(2.10, 3.60, 4.71)	(2.17, 3.68, 4.74)
PM3	(2.43, 4.03, 4.83)	(2.15, 3.67, 4.71)	(2.21, 3.75, 4.74)
FL1	(2.38, 3.96, 4.83)	(1.90, 3.34, 4.54)	(2.01, 3.48, 4.61)
FL2	(2.32, 3.89, 4.83)	(2.02, 3.50, 4.57)	(2.09, 3.59, 4.63)
FL3	(2.22, 3.75, 4.83)	(2.07, 3.57, 4.59)	(2.11, 3.62, 4.65)
SL1	(2.06, 3.54, 4.75)	(2.01, 3.48, 4.53)	(2.02, 3.50, 4.58)
SL2	(2.16, 3.68, 4.83)	(1.99, 3.46, 4.60)	(2.03, 3.51, 4.66)
SL3	(2.11, 3.61, 4.83)	(2.03, 3.52, 4.58)	(2.06, 3.54, 4.64)
SP1	(2.17, 3.68, 4.79)	(2.01, 3.48, 4.67)	(2.05, 3.53, 4.70)
SP2	(2.17, 3.68, 4.79)	(2.02, 3.50, 4.67)	(2.06, 3.54, 4.70)
SP3	(2.22, 3.75, 4.79)	(2.01, 3.48, 4.74)	(2.06, 3.54, 4.75)

Table 12. Results of crisp global weights of sub-criteria.

Sub-criteria	Academic Scholars		Industry Professionals		Overall	
	Weight	Rank	Weight	Rank	Weight	Rank
PM1	3.64	5	3.46	3	3.5	3
PM2	3.72	2	3.47	2	3.53	2
PM3	3.76	1	3.51	1	3.57	1
FL1	3.72	2	3.26	12	3.37	11
FL2	3.68	4	3.36	9	3.43	6
FL3	3.60	6	3.41	4	3.46	4
SL1	3.45	12	3.34	11	3.37	11
SL2	3.56	8	3.35	10	3.40	10
SL3	3.52	11	3.38	7	3.41	9
SP1	3.55	9	3.38	7	3.42	8
SP2	3.55	9	3.40	6	3.43	6
SP3	3.59	7	3.41	4	3.45	5

DOI: 10.29677/MR.202512_5(2).0003

As discussed in Section 3.5.2, the results are compared with three defuzzification methods (i.e., Durán & Aguilo, 2008; Ding, 2010; Ali et al., 2012) across academic scholars, industry professionals, and the overall ranking. As illustrated in Figure 6, the results indicate that, in general, academic scholars tend to assign slightly higher importance to the sub-criteria compared to industry professionals, although the general trend remains consistent between the two groups. Notably, a significant difference emerges in the evaluation of "Formulate PFSP and vessel protection plan (FL1)," where academic scholars rank it much higher than industry professionals. This discrepancy may be attributed to the fact that academic scholars typically adopt a strategic and policy-oriented perspective, viewing the formulation of PFSPs and vessel protection plans as fundamental components of maritime security. These planning instruments serve as critical blueprints for conducting risk assessments, establishing preventive measures, and coordinating emergency responses. This perspective aligns with theoretical frameworks that underscore the centrality of planning and compliance mechanisms in fostering comprehensive and resilient security systems. In contrast, industry professionals tend to emphasize the implementation and operational aspects of port security. Their priorities are often centered on the execution of security measures, regulatory compliance, and the enforcement of protocols. Consequently, the formulation of the PFSP may be perceived by practitioners as a routine or completed administrative obligation, rather than an ongoing strategic necessity. From their standpoint, the PFSP is often regarded as a static regulatory document that is formulated once and subject only to periodic review, thereby rendering it less salient in the context of day-to-day operational concerns.

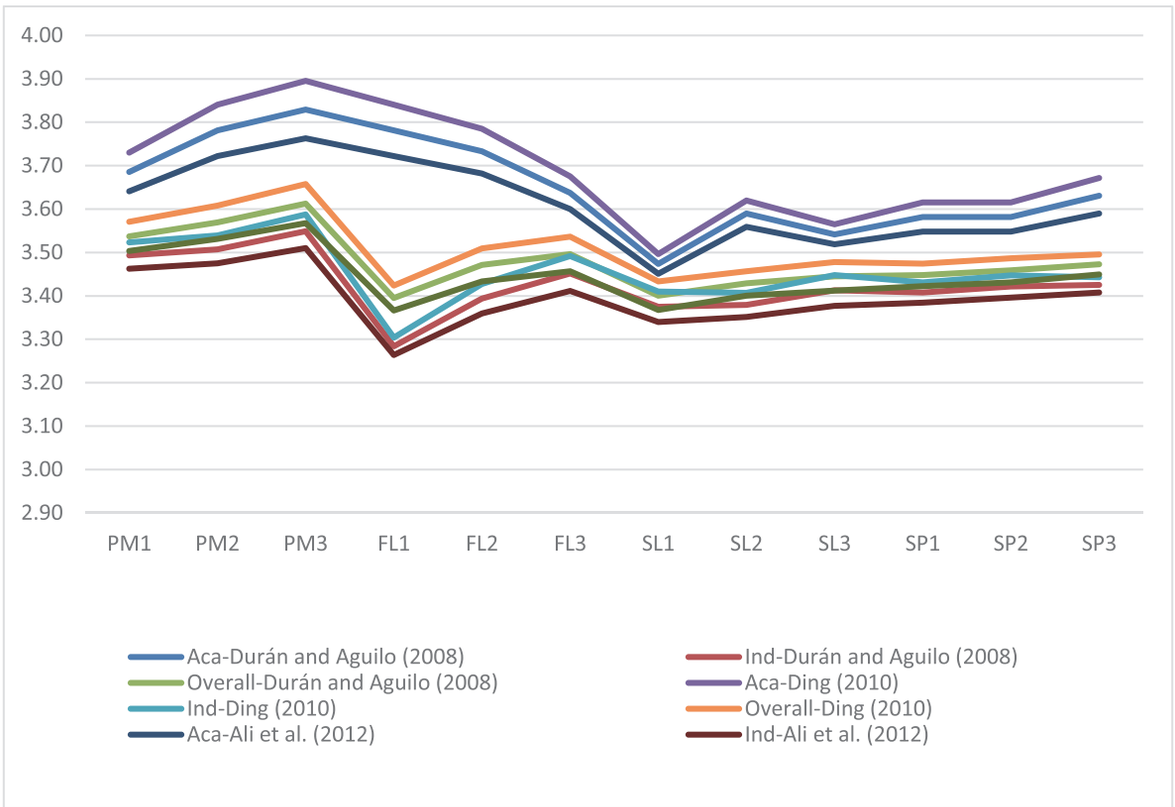

Figure 6. Comparison of the three defuzzification methods.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

5 CONCLUSION AND DISCUSSION

5.1 Conclusion

This study aimed to identify and evaluate the key factors influencing port facility security management in international commercial ports through the application of fuzzy MCDM analysis. By integrating expert opinions from both academia and industry, the study provides a comprehensive and multi-dimensional understanding of the critical elements necessary to ensure effective and sustainable port security governance. The results yield valuable insights into the relative importance of stakeholder roles and regulatory instruments in the maritime security domain.

The analysis confirmed that among the four main criteria, namely Port Management Authority (PM), Facility Lessee (FL), Security Law Enforcement Agency (SL), and Security Policies and Regulations (SP), while academics think all four criteria are equally important, industry professionals identified PM and SP as the most significant contributors to enhancing port security. This reflects a shared recognition that administrative leadership and the existence of clear, enforceable regulations are the foundation upon which operational security practices are built. In particular, the coordination capacity of port authorities and the adequacy of existing legal frameworks are perceived as the most critical enablers of security assurance in a complex, multi-actor environment.

At the sub-criteria level, the consensus centered on the paramount importance of "Ensure that all units and agencies implement the PFSP (PM3)." This sub-criterion ranked first among both academic and industry respondents, underscoring the centrality of consistent and coordinated implementation of the PFSP. The second most important sub-criterion, "Review PFSP of each port facility (PM2)," was also consistently ranked across both groups. This prioritization illustrates the need for regular oversight, auditing, and evaluation mechanisms to ensure that the evolving security landscape is met with updated and context-specific plans. A third key sub-criterion, "Participate in and comply with the provisions of the ISPS Code (PM1)," also gained significant importance, particularly among industry professionals. This indicates that industry professionals place considerable emphasis on practice-oriented codes of conduct, highlighting the importance of practical implementation of regulatory requirements within real-world operational contexts. Furthermore, the academic scholars generally recognize compliance with international regulations and alignment with global standards as fundamental objectives in ensuring port safety.

Furthermore, the comparative evaluation of the sub-criteria under the Facility Lessee (FL) dimension reveals a marked divergence in emphasis between academic scholars and industry professionals. Academic scholars assign higher importance to strategic planning and conceptual preparation, as evidenced by the elevated rankings of FL1 (Formulate PFSP and vessel protection plan) and FL2 (Ensure that the company and port site personnel understand the PFSP). This prioritization reflects the academic inclination toward formalized structures, theoretical underpinnings, and comprehensive planning as foundational elements of effective port facility security management. Conversely, industry professionals exhibit a pronounced preference for operationally focused and actionable measures, as demonstrated by the relatively high ranking of FL3 (Regularly conduct port security plan drills). The notably low prioritization of FL1 by practitioners suggests a degree of skepticism regarding the practical utility of planning documents in the absence of concrete implementation, highlighting a pragmatic orientation grounded in immediate operational demands and experiential insights. These contrasting perspectives underscore the necessity of integrating both strategic foresight and practical execution in the formulation of port security governance frameworks. While the academic emphasis on planning and communication establishes a necessary structural basis, the industry's focus on drills and performance-based validation ensures that security measures are effectively internalized and

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

operationalized. Therefore, a comprehensive and balanced port facility security model should harmonize rigorous preparatory planning with continuous practical training to achieve both strategic alignment and operational resilience.

The ranking of the sub-criteria under the Security Law Enforcement Agency (SL) and Security Policies and Regulations (SP) from both groups is similar with slightly different ranking. The global weights of these sub-criteria are slightly higher from academic scholars' perspective compared to that of industry professionals. This is also reflected in the results as shown in Figure 6.

5.2 Discussion

The IMO has established comprehensive international standards aimed at enhancing the safety and security of maritime transportation and trade. This international framework provides a crucial communication platform for member countries, enabling them to benchmark and subsequently adjust their national policies and regulations in alignment with global best practices and specific national contexts. Such mechanisms ensure that national maritime and port management agencies have well-defined safety and security standards to guide their operations effectively.

Although Taiwan is currently unable to obtain formal membership within the IMO, adherence to these international standards remains vital for facilitating smooth international trade and ensuring robust port safety. In response to this global trend, it is essential for Taiwan's port authority to proactively review and continuously update its maritime transport and port security policies and regulatory frameworks. Aligning national standards with international practices will not only enhance the operational safety of Taiwan's ports but also significantly strengthen their international competitiveness and strategic capability within the global maritime industry.

Moreover, Taiwanese legislative bodies and policy-making institutions should systematically engage with frontline personnel and managers responsible for implementing the ISPS Code. Regular consultations and interviews should be conducted to identify practical challenges, conflicts, or limitations that these personnel face when applying existing laws and regulations in operational contexts. Through ongoing dialogue and iterative revisions of regulatory provisions, policies can be optimized to better reflect practical realities and operational demands, thus ensuring the effective implementation and continuous enhancement of port safety and security standards across Taiwan's international commercial ports. Based on the findings, this section outlines five key suggestions to improve the effectiveness, coordination, and adaptability of port security management systems.

1. Strengthen the execution and integration of PFSPs

The highest-ranked sub-criterion "Ensure that all units and agencies implement the PFSP" demonstrates the pressing need for effective horizontal and vertical coordination in executing port security strategies. While planning and policy design are essential, their true value lies in the integrity and consistency of implementation. Port authorities should thus establish dedicated cross-agency coordination task forces and standard operating procedures (SOPs) for the deployment, auditing, and adaptation of PFSPs. Moreover, security compliance audits should be institutionalized at regular intervals. These audits should not only focus on checking the presence of documents and certifications but also include simulated scenarios (e.g., emergency drills or red team testing) to evaluate actual preparedness and responsiveness.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

2. Establish dynamic, risk-based regulatory frameworks

While both groups underscored the importance of comprehensive security regulations, existing frameworks should evolve into dynamic, risk-sensitive systems. Security threats are increasingly asymmetric, ranging from cyber intrusions to insider threats and geopolitical disruptions. Hence, static regulations must give way to adaptable frameworks capable of responding to both known and emergent risks. An approach would be to adopt modular regulations with scenario-based appendices, allowing port authorities to rapidly adjust protocols based on intelligence updates, international alerts, or local threat assessments. Additionally, a formal feedback loop should be established between the regulatory drafting units and operational stakeholders to ensure policies remain relevant and feasible.

3. Institutionalize port-wide risk assessment and surveillance innovation

To enhance proactive defense and optimize resource allocation, ports should institutionalize risk assessment procedures using quantitative methods, such as threat likelihood matrices, vulnerability scoring, and consequence-based modelling. These assessments should be conducted periodically and include both physical and cyber domains. In tandem, investments in smart surveillance systems, including AI-enabled video analytics, biometric access control, and data fusion platforms can substantially improve the visibility and efficiency of port operations. However, these technologies must be embedded within clearly defined policy and ethical frameworks to ensure transparency, privacy, and lawful usage.

4. Clarify roles and enhance accountability among stakeholders

The findings indicate that while port management authorities are perceived as central actors, the roles of Facility Lessees and Law Enforcement Agencies are equally critical to achieving integrated port security. A lack of clarity or overlap in responsibilities can hinder timely responses and lead to operational inefficiencies. To address this, port authorities should develop a responsibility assignment matrix outlining who is responsible, accountable, consulted, and informed for each PFSP sub-component. This matrix should be disseminated across agencies and reviewed annually to reflect institutional changes or new threat landscapes.

5. Promote international collaboration and benchmarking

Given Taiwan's participation in the global maritime trade network despite its non-membership in the IMO, proactive alignment with international best practices is essential. This can be achieved through bilateral agreements, technical exchanges, and participation in regional port security forums.

In sum, the recommended actions should be implemented in the following order of priority: (1) PFSP execution and coordination, (2) regulatory adaptability, (3) risk assessment and surveillance innovation, (4) stakeholder role clarification, and (5) international alignment. This sequence reflects both urgency and feasibility in addressing current security gaps while ensuring sustainable and globally compatible port security governance.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202512_5(2).0003

In advancing Taiwan's maritime security governance, governmental focus should extend beyond port facility management by the Taiwan International Ports Corporation (TIPC) to encompass the coordinated oversight of commercial shipping by maritime authorities such as the Maritime and Port Bureau (MPB) and the Ocean Affairs Council (OAC). Specifically, information control related to Ship Security Plans (SSPs) and Ship Security Officers (SSOs) must be integrated into the supervisory framework for Taiwan-flagged vessels. Based on prior findings, several strategies are proposed: (1) the MPB should establish a centralized digital platform for collecting and reviewing SSP and SSO records in line with ISPS Code requirements; (2) an inter-agency task force involving TIPC, MPB, OAC, and law enforcement should be created to coordinate PFSP and SSP implementation, auditing, and enforcement; (3) joint review mechanisms for PFSPs and SSPs should be institutionalized through periodic evaluations; (4) mandatory simulation-based training and joint drills should be implemented to enhance operational preparedness; (5) a maritime security intelligence system should be developed to consolidate compliance data, threat intelligence, and vessel movement for informed decision-making; and (6) legal frameworks should be revised to clearly delineate inter-agency responsibilities for ship security oversight. Together, these measures provide a comprehensive and risk-responsive foundation for strengthening Taiwan's maritime and port security system.

Additionally, regular benchmarking against major ports in Asia, Europe, and North America can offer valuable insights into emerging practices, technology adoption, and policy innovations. Such comparisons can serve as a catalyst for local improvements and enhance the international credibility of Taiwan's port security governance system. In conclusion, this study offers a structured, empirically grounded framework for prioritizing and improving port security efforts in Taiwan and similar maritime contexts. By incorporating the perspectives of both academia and industry, and applying a rigorous fuzzy MCDM analysis methodology, it identifies critical leverage points for enhancing the efficacy, coherence, and responsiveness of security operations at international commercial ports. While the current study has provided meaningful insights, future research could explore additional variables, such as the role of digital infrastructure, supply chain integration, and inter-agency information sharing platforms. Expanding the sample to include international experts and port operators would also enhance the generalizability of the findings. To further inform policy and operational decision-making, future studies could apply performance-based evaluation methods, such as gap analysis or importance performance analysis (IPA), to prioritize which factors most urgently require improvement. As port security continues to evolve in response to both conventional and hybrid threats, such multi-disciplinary, data-driven approaches will be increasingly vital to sustaining global maritime safety and economic resilience.

ACKNOWLEDGEMENTS

This study was partially supported by the Royal Society (IEC\NSFC\223196).

REFERENCES

Adams, N., Chisnall, R., Pickering, C., Schauer, S., Peris, R. C., & Papagiannopoulos, I. (2021). Guidance for ports: Security and safety against physical, cyber and hybrid threats. *Journal of Transportation Security, 14*(3), 197–225. https://doi.org/10.1007/s12198-021-00234-6

Ali, N. H., Sabri, I. A. A., Noor, N. M. M., & Ismail, F. (2012). Rating and ranking criteria for selected islands using Fuzzy Analytic Hierarchy Process (FAHP). *International Journal of Applied Mathematics and Informatics, 1*(6), 57–65. https://www.naun.org/main/UPress/ami/17-907.pdf

Anyanova, E. (2024). Maritime cyber security. *Law, State and Telecommunications Review/Revista de Direito, Estado e Telecomunicações, 16*(2), 69–82. https://doi.org/10.26512/lstr.v16i2.47018

Arof, A. M., & Khadzi, A. F. A. (2018). A Delphi study to identify important factors for determining the level of adherence to ISPS Code implementation. *International Journal of Supply Chain Management, 7*(4), 279–287. https://doi.org/10.59160/ijscm.v7i4.2199

Australian Government. (2021). *Australian government civil maritime security strategy.* Department of Home Affairs. https://www.homeaffairs.gov.au/nat-security/files/australian-government-civil-maritime-security-strategy.pdf

Ávila-Zúñiga-Nordfjeld, A., & Dalaklis, D. (2019). Integrating the procedures of reporting port security incidents and the follow-up investigation to build a national maritime security policy: A case study in Mexico. *WMU Journal of Maritime Affairs, 18*, 25–40. https://doi.org/10.1007/s13437-018-0154-3

Belabyad, M., Kontovas, C., Pyne, R., Shi, W., Li, N., Szwed, P., & Chang, C. H. (2025). The human element in autonomous shipping: A study on skills and competency requirements. *WMU Journal of Maritime Affairs*, 1–31. https://doi.org/10.1007/s13437-025-00366-9

Chang, C. H. (2013). *Container shipping risk management: A case study of Taiwan container shipping industry.* [Doctoral dissertation, University of Plymouth]. http://dx.doi.org/10.24382/4509

Chang, C. H., & Thai, V. V. (2016). Do port security quality and service quality influence customer satisfaction and loyalty?. *Maritime Policy & Management, 43*(6), 720–736. https://doi.org/10.1080/03088839.2016.1151086

Chang, C. H., Xu, J., Dong, J., & Yang, Z. (2019). Selection of effective risk mitigation strategies in container shipping operations. *Maritime Business Review, 4*(4), 413–431. https://doi.org/10.1108/MABR-04-2019-0013

Chen, C. T. (2000). Extensions of the TOPSIS for group decision-making under fuzzy environment. *Fuzzy Sets and Systems, 114*(1), 1–9. https://doi.org/10.1016/S0165-0114(97)00377-1

Curvey, E. (2024, April 18). *International ship and port facility security requirements.* Tideworks Technology. https://tideworks.com/international-ship-and-port-facility-security-requirements/

Departamento de Seguridad Nacional. (2024). *National strategy for maritime security.* https://www.dsn.gob.es/sites/default/files/2025-01/Accesible%20ENSM2024%20EN_0.pdf

DOI: 10.29677/MR.202512_5(2).0003

Ding, J. F. (2010). Critical factors influencing customer value for global shipping carrier-based logistics service providers using Fuzzy AHP approach. *African Journal of Business Management, 4*(7), 1299–1307. https://doi.org/10.5897/AJBM.9000167

Durán, O., & Aguilo, J. (2008). Computer-aided machine-tool selection based on a Fuzzy-AHP approach. *Expert Systems with Applications, 34*(3), 1787–1794. https://doi.org/10.1016/j.eswa.2007.01.046

European Maritime Safety Agency. (2025). *EMSA outlook 2025.* https://www.emsa.europa.eu/publications/download/8044/5402/23.html

European Union. (2020, May 4). *Port infrastructure: enhancing port security.* EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:l24162

Farisi, M., Putra, A. K., Ardianto, B., & Harahap, R. R. (2020). Facility security measures at Ujung Jabung Port: A review in terms of the International Ship and Port Facility Security Code. *Indonesian Journal International Law, 17*(3), 341–356. https://doi.org/10.17304/IJIL.VOL17.3.790

Government of the Netherlands. (2015). *The Dutch maritime strategy 2015–2025.* https://www.government.nl/binaries/government/documenten/reports/2015/07/07/the-dutch-maritime-strategy-2015-2025/150604-maritieme-strategie-uk-lr-2.pdf

Hasanov, N., & Alsulaiman, M. F. (2021). Evaluating the implementation framework of the International Ship and Port Facility Security Code in the Republic of Azerbaijan. *Maritime Technology and Research, 3*(2), 185–201. https://doi.org/10.33175/mtr.2021.247419

Inter-American Committee on Ports. (2025). *Port protection and security informative bulletin.* https://portalcip.org/wp-content/uploads/2025/02/Port-Protection-and-Security-Informative-Bulletin.pdf

International Maritime Organization. (2003). *International Ship and Port Facility Security Code* (2003 ed.). https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

International Maritime Organization. (2021). Guide to maritime security and the ISPS Code. https://doi.org/10.62454/KB116E

Ishizaka, A., & Nemery, P. (2013). *Multi-criteria decision analysis: Methods and software.* John Wiley & Sons. https://doi.org/10.1002/9781118644898

Malcolm, J. A. (2016). Responding to international terrorism: The securitisation of the United Kingdom's ports. *The British Journal of Politics and International Relations, 18*(2), 443–462. https://doi.org/10.1177/1369148115623211

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

Moran, C. (2023). Navigating between Scylla and Charybdis: International law, maritime security and freedom of navigation. *European Journal of Legal Studies, 15*(1), 9–28. https://doi.org/10.2924/EJLS.2023.010

Nippon Kaiji Kyokai. (2023). *ISPS Code Part B: Guidance regarding the provisions of chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as amended and part A of this Code.* https://www.classnk.or.jp/hp/pdf/activities/statutory/isps/code/ISPS_CodeB.pdf

Organization of American States. (2021). Verification and compliance manual for port security officials. https://www.oas.org/en/sms/cicte/docs/Verification-and-Compliance-Manual-for-Port-Security-Officers-Drafting-Guide.pdf

Raunek. (2024, February 1). *The ultimate guide to the ISPS Code for ships–Enhancing maritime security.* Marine Insight. https://www.marineinsight.com/maritime-law/the-isps-code-for-ships-a-quick-guide/

Stavroulakis, P. J., Georgoulas, D., Gerakoudi-Ventouri, K., Iosifidi, G., & Papadimitriou, S. (2024). Sustainable maritime legislation: The case of the International Ship and Port Facility Security Code. *WMU Journal of Maritime Affairs, 23*, 575–602. https://doi.org/10.1007/s13437-024-00348-3

United Nations Conference on Trade and Development. (2024, October 22). *Review of Maritime Transport 2024.* https://unctad.org/publication/review-maritime-transport-2024

Wiko, G., Kinanti, F. M., Syafei, M., Darajati, M. R., & Sudagung, A. D. (2023). Tanjungpura port as an international hub port to improve economic competitiveness: An overview from international law. *Indonesian Journal of International Law, 21*(1), Article 3. https://doi.org/10.17304/ijil.vol21.1.4

Yazır, D. (2023). A survey on MCDM approaches for maritime problems. *Mersin Üniversitesi Denizcilik ve Lojistik Araştırmaları Dergisi, 5*(1), 1–37. https://doi.org/10.54410/denlojad.1325664

DOI: 10.29677/MR.202512_5(2).0003