İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Research Article / Araştırma Makalesi

A DECISION SUPPORT MODEL FOR CYBERSECURITY RISK ASSESSMENT IN MARITIME TRANSPORTATION BASED ON SPHERICAL FUZZY INFORMATION

KÜRESEL BULANIK BİLGİYE DAYALI DENİZ TAŞIMACILIĞINDA SİBER GÜVENLİK RİSK DEĞERLENDİRMESİ İÇİN BİR KARAR DESTEK MODELİ

Veysel TATAR[1]

https://doi.org/10.55071/ticaretfbd.1579978

Corresponding Author (Sorumlu Yazar)	*Received (Geliş Tarihi)*	*Revised (Revizyon Tarihi)*	*Accepted (Kabul Tarihi)*
vtatar@artvin.edu.tr	*05.11.2024*	*18.11.2024*	*29.11.2024*

Abstract

The increasing technological innovations in the maritime industry, which plays an important role in the global supply chain, have the potential to introduce significant risks in terms of cyber threats. Therefore, this study proposes a cybersecurity risk assessment approach using spherical fuzzy (SF) set information based on the Fine-Kinney method to prioritize potential cyber threats/hazards for navigation systems in maritime transportation. The Fine-Kinney risk parameters (probability (P), exposure (E) and consequence (C)) are weighted using SF-based the LOgarithmic DEcomposition of Criteria Importance (LODECI) approach. The ranking of potential cybersecurity threats/hazards is evaluated using SF-based the Alternative Ranking Technique based on Adaptive Standardized Intervals (ARTASI), which provides more adaptability in managing the uncertainty present in expert assessments. The integration of these methodologies with the employment of SF sets results in the formulation of the proposed hybrid SF-LODECI-SF-ARTASI based on Fine-Kinney risk assessment model. Upon evaluation of the proposed model, it becomes evident that the most significant cyber threat/hazard that can impact the cyber security of critical systems on a ship is CYB1 "Accessing the AIS network to obtain vessel position, speed and route information." In general, when the top five most important cybersecurity threats are analyzed, it is determined from the results that the most vulnerable systems to cyber threats/hazards are AIS, GPS and ECDIS, respectively. Finally, a comparative analysis is conducted using an alternative methodology to test the results of the model.

Keywords: Cybersecurity, maritime transportation, risk assessment, spherical fuzzy sets, ARTASI.

Öz

Küresel tedarik zincirinde önemli bir rol oynayan denizcilik sektöründeki artan teknolojik yenilikler, siber tehditler açısından önemli riskler getirme potansiyeline sahiptir. Bu nedenle, bu çalışma, deniz taşımacılığındaki navigasyon sistemleri için olası siber tehditleri/tehlikeleri önceliklendirmek için Fine-Kinney yöntemine dayalı küresel bulanık (SF) küme bilgilerini kullanan bir siber güvenlik risk değerlendirme yaklaşımı önermektedir. Fine-Kinney risk parametreleri (olasılık (P), maruz kalma (E) ve sonuç (C)), SF tabanlı Kriter Öneminin Logaritmik Ayrıştırılması (LODECI) yaklaşımı kullanılarak ağırlıklandırılır. Olası siber güvenlik tehditlerinin/tehlikelerinin sıralaması, uzman değerlendirmelerinde mevcut olan belirsizliği yönetmede daha fazla uyarlanabilirlik sağlayan SF tabanlı Adaptif Standartlaştırılmış Aralıklara Dayalı Alternatif Sıralama Tekniği (ARTASI) kullanılarak değerlendirilir. Bu metodolojilerin SF setlerinin kullanımı ile entegrasyonu, Fine-Kinney risk değerlendirme modeline dayalı olarak önerilen hibrit SF-LODECI-SF-ARTASI modelinin formüle edilmesiyle sonuçlanmıştır. Önerilen model değerlendirildiğinde, bir gemideki kritik sistemlerin siber güvenliğini etkileyebilecek en önemli siber tehdit/tehlikenin CYB1 “Gemi konumu, hızı ve rota bilgilerini elde etmek için AIS ağına erişim” olduğu ortaya çıkmaktadır. Genel olarak, en önemli beş siber güvenlik tehdidi analiz edildiğinde, sonuçlardan siber tehditlere/tehlikelere karşı en savunmasız sistemlerin sırasıyla AIS, GPS ve ECDIS olduğu tespit edilmektedir. Son olarak, modelin sonuçlarını test etmek için alternatif bir metodoloji kullanılarak karşılaştırmalı bir analiz gerçekleştirilmiştir.

Anahtar Kelimeler: Siber güvenlik, deniz taşımacılığı, risk değerlendirmesi, küresel bulanık kümeler, ARTASI.

[1] Artvin Çoruh University, Maritime and Port Management Program, Artvin, Türkiye.
vtatar@artvin.edu.tr, Orcid.org/0000-0003-4285-6854.

1. INTRODUCTION

The issue of cybersecurity represents a crucial security concern for the maritime industry, which plays a substantial role in international trade. The necessity for precise cyber-risk assessments is becoming increasingly crucial in order to guarantee economic and physical security, given the growing technological dependence and sophistication of maritime systems (Tam & Jones, 2019). Maritime cyber risk is defined as the degree to which a technology asset is vulnerable to a potential incident that could result in operational, safety or security failures in the context of shipping. Such incidents may arise from the corruption, loss or compromise of information or systems (IMO, 2022). Maritime cyber security may be defined as the policies, procedures and technologies employed to safeguard vessels, ports, shipping companies and associated infrastructure from the risks resulting from cyber-attacks (Haugli-Sandvik et al., 2024). The remote and secure control of marine system parameters offers a number of advantages with regard to more sustainable operations. These include improved human performance through closer cooperation between ship and shore personnel, a reduction in greenhouse gas emissions, an enhanced emergency response capability, and the ability to determine the location of a vessel (Bolbot et al., 2022a). Nevertheless, despite the aforementioned advantages, it is susceptible to a multitude of cybersecurity risks.

In the publication on cybersecurity on ships by the Baltic and International Maritime Council (BIMCO), the concept of cybersecurity is described as the protection of Information Technology (IT), Operational Technology (OT), information and data against unauthorised access, manipulation and disruption (BIMCO, 2020). In evaluating the cybersecurity of the Ship Security Assessment (SSA), it is essential to consider the distinctive IT and OT configurations of each vessel. In general, a greater reliance on IT and OT systems should be associated with an increased cybersecurity risk, given that the consequences of a potential cyber attack would be significantly more disruptive (EMSA, 2023). The utilization of cybertechnologies has become a fundamental aspect of the operation and management of a multitude of systems that are of paramount importance to the safety and security of maritime transportation and the sustainability of the marine environment. The aforementioned critical systems can be summarised as follows (Svilicic et al., 2019; IMO, 2022):

- Bridge navigation and radio systems
    - RADAR (Radio Detection And Ranging)
    - ECDIS (Electronic Chart Display Information System)
    - AIS (Automatic Identification System)
    - GPS (Global Positioning System)
    - VDR (Voyage Data Recorder)
    - GMDSS (Global Maritime Distress And Safety System)
- Cargo handling and management systems
    - Control systems
    - Monitoring systems
    - Alarm systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems

- Communication systems

Figure 1 presents a summary of the critical systems of ships.

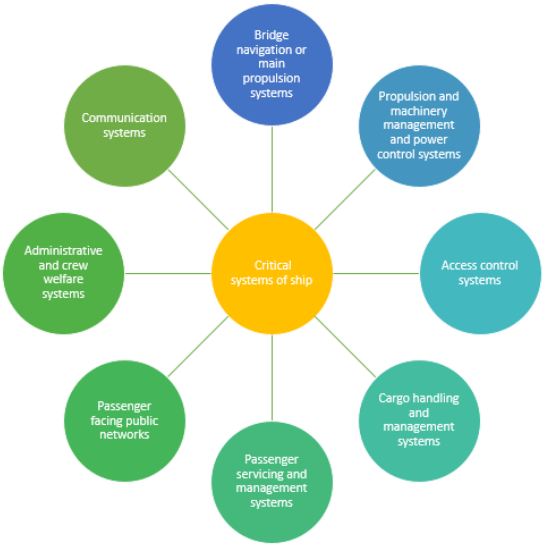

Bridge navigation or main propulsion systems
Propulsion and machinery management and power control systems
Communication systems
Administrative and crew welfare systems
Critical systems of ship
Access control systems
Passenger facing public networks
Cargo handling and management systems
Passenger servicing and management systems

Figure 1. Critical Systems of Ship (IMO, 2022)

The maritime transportation sector has been significantly impacted by cyber attacks, resulting in prolonged operational disruptions and substantial economic and reputational losses for numerous companies (Uflaz et al., 2024). A shipboard incident resulted in the disruption of the vessel's operations and the imposition of significant economic costs due to an infection in the Electronic Chart Display Information System (ECDIS) (Bolbot et al., 2020). The potential for vulnerabilities to arise in the AIS system of a ship, which is of great significance in ensuring the safe passage of maritime traffic, can present significant challenges for the relevant authorities in making critical decisions in the event of an attack involving the use of malware (Soner et al., 2024). In light of the growing importance of autonomous ships in the future of maritime trade, it is imperative to address potential security gaps in the AIS system and guarantee navigational safety. This can be achieved by meticulously examining the interrelationship between safety and cybersecurity (Chaal et al., 2023). In the cyber security guide for ships published by the Baltic and International Maritime Council (BIMCO), the stages of cyber security risk management for the maritime industry are shown in Figure 2.

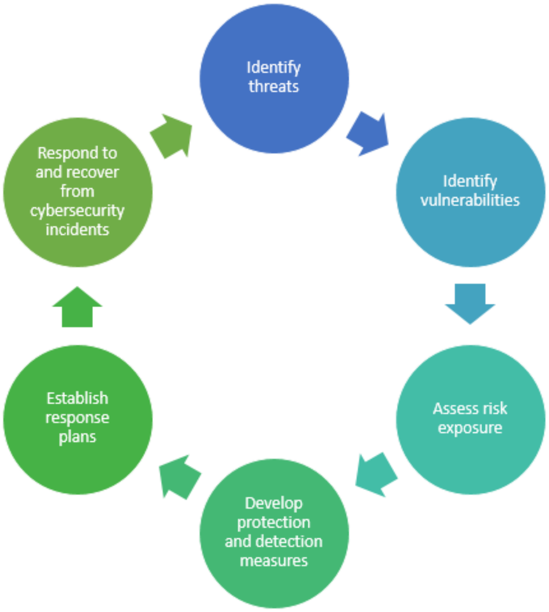

Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish response plans
Respond to and recover from cybersecurity incidents

Figure 2. Cybersecurity Risk Management Framework (BIMCO, 2020)

A variety of methods have been employed in the field of risk assessment of in the maritime sector. Wan et al. (2019) proposed an innovative fuzzy Bayesian-based Failure Mode and Effects Analysis (FMEA) approach for the assessment of maritime supply chain risks. Tam and Jones (2019) proposed the Maritime Cyber-Risk Assessment (MaCRA), a model-based risk assessment framework that considers a combined analysis of cyber and maritime factors. Bayazit and Kaptan (2023) presented a risk assessment model based on the Fuzzy Bayesian Network approach to identify sources of marine pollution from ship operations. Park et al. (2023) developed a new model, FMEA with a Rule-based Bayesian Network (RBN), within the scope of risk management of maritime cyber threats. Bolbot et al. (2020) developed a novel model, designated as the Cyber Preliminary Hazard Analysis (CPHA), for the assessment of cyber risks associated with the navigation and propulsion systems of inland waterway autonomous ships. Bolbot et al. (2022b) utilized a model based on Failure Modes, Vulnerabilities and Effects Analysis to identify potential cyber attack scenarios on a marine dual fuel engine.

The present study employed the traditional Fine-Kinney methodology for the purpose of conducting a risk assessment. In the classic version of the Fine–Kinney model, as initially proposed, a risk value is derived through a calculation involving the multiplication of probability (P), exposure (E), and consequence (C) parameters (Gul et al., 2021a). Nevertheless, the most significant limitations of the Fine-Kinney risk assessment model are that it fails to account for the inherent uncertainty in expert opinions and that it does not incorporate the relative importance weights of risk parameters in the risk rating (Wang et al., 2024). In this context, numerous studies have addressed the problem of risk assessment by integrating the transformation of uncertain risk rating information, fuzzy set versions, and a number of techniques with the Fine-Kinney method (Ilbahar et al., 2018; Wang et al., 2023; Ayvaz et al., 2024).

The motivation behind this study is to develop a hybrid cyber security risk assessment tool for potential cyber threats/hazards in maritime transport. This is to address the gap in the existing literature on this topic. The assessment tool will use spherical fuzzy set (SFS) information. In this context, a hybrid cybersecurity risk assessment model based on Fine-Kinney is presented, which integrates spherical fuzzy sets (SFSs), Spherical Weighted Geometric Mean (SWGM) operator, ARTASI (Pamucar et al., 2024) and LODECI (Pala, 2024).

1.1. Study Objectives and Contributions

The present study aims to advance the existing literature on maritime transportation cybersecurity in a more nuanced manner. This objective is to be attained by identifying novel perspectives for prospective research and furnishing policymakers with recommendations regarding measures that can be implemented to develop resilient maritime cybersecurity critical infrastructure, designed to address both current and future threats/hazards.

The following is a summary of the contributions made by this study:

- Construction of a Cybersecurity Decision Support System: The study presents a novel cybersecurity decision support model, designated as the SF-LODECI-SF-ARTASI method on the basis of Fine-Kinney, which is proposed as a cybersecurity risk assessment in the maritime sector. This model incorporates SFSs, SWGM, LODECI, ARTASI, and Fine-Kinney methods, thereby offering a novel perspective in the existing literature.

- Reasonable Cybersecurity Risk Assessment: The risk assessment provided by experts can be modelled utilizing the SFSs-based formulation method. The SFSs facilitate the expression of experts' cognitive judgments and subjective assessments of cybersecurity risk in a more reasonable and compelling manner.

- Dynamic Rating of Risks: The ARTASI approach to risk ranking permits the expansion of uncertainty degrees in expert evaluations, thereby facilitating the development of more malleable and adaptable risk analysis in the context of critical maritime transportation systems.

- The Weighting of Risk Parameters Based on Equilibrium: The LODECI methodology has been selected as the risk parameter weighting approach in the hybrid model due to its efficacy in consolidating situations that may be susceptible to instability when utilizing alternative criterion weighting methods. This increases the stability of the risk assessment model based on the element of equilibrium.

- The Reverberations for Theory and Management: The study presents a novel methodology based on spherical fuzzy sets for risk assessment model, while simultaneously paving the way for future research endeavours and offering policymakers a distinctive decision-support model to construct resilient maritime cybersecurity systems that can effectively address both current and future threats/hazards.

1.2. The Organizational Structure of the Study

This study is organized into four sections. In Section 2, the methodological framework is described, including steps of the SF-LODECI-SF-ARTASI based on the Fine-Kinney hybrid model and the preliminary phases of the SF process. Section 3 presents a numerical case study that exemplifies the application of the proposed model to a cybersecurity risk assessment. Furthermore, a comparative analysis is provided, comparing the proposed methodology with an alternative approach. Section 4 presents the conclusion, in which the results are discussed in detail. Additionally, this section addresses the limitations of the research and offers recommendations for future studies in this field.

2. METHODOLOGY

2.1. Spherical Fuzzy Sets (SFSs)

The SFSs theory proposed by Kahraman and Kutlu Gündoğdu (2018), is an integration of Pythagorean fuzzy sets and neutrosophic sets. In SFSs, the levels of membership, non-membership and hesitancy must conform to the constraint $0 \leq \mu^2 + \nu^2 + \pi^2 \leq 1$, where μ , ν and π are the respective values of the aforementioned levels, respectively. Moreover, each parameter can be defined independently in the interval [0,1] (Kutlu Gündoğdu and Kahraman, 2019). The distinctive capacity of the SFS to address uncertainty and ambiguity sets it apart from other fuzzy set models (Akram et al., 2020). An overview of the fundamental terminology, symbols, and functions associated with the SFSs is provided below (Kutlu Gündoğdu and Kahraman, 2020):

Definition I: The description of an SFSs, $\tilde{\mathcal{T}}_s$, of the universe of discourse $\mathcal{U}$ is as follows.

$$\mathrm{p}_{\tilde{\mathcal{T}}_s}: \mathcal{U} \to [0,1], \mathrm{q}_{\tilde{\mathcal{T}}_s}: \mathcal{U} \to [0,1], \mathrm{r}_{\tilde{\mathcal{T}}_s}: \mathcal{U} \to [0,1]$$

and

$$0 \leq \mathrm{p}^2_{\tilde{\mathcal{T}}_s}(\mathrm{u}) + \mathrm{q}^2_{\tilde{\mathcal{T}}_s}(\mathrm{u}) + \mathrm{r}^2_{\tilde{\mathcal{T}}_s}(\mathrm{u}) \leq 1 \quad (\mathrm{u} \in \mathcal{U}) \tag{1}$$

$$\tilde{\mathcal{T}}_s = \left\{ \langle s, \left(\mathrm{p}_{\tilde{\mathcal{T}}_s}(\mathrm{u}), \mathrm{q}_{\tilde{\mathcal{T}}_s}(\mathrm{u}), \mathrm{r}_{\tilde{\mathcal{T}}_s}(\mathrm{u}) \right) \rangle \, | \mathrm{u} \in \mathcal{U} \right\} \tag{2}$$

For each, $\mathfrak{p}_{\tilde{\mathcal{T}}_s}(\mathfrak{u}), \mathfrak{q}_{\tilde{\mathcal{T}}_s}(\mathfrak{u}), and\ \mathfrak{r}_{\tilde{\mathcal{T}}_s}(\mathfrak{u})$ are the degree of membership, nonmembership, and hesitancy of s to $\tilde{\mathcal{T}}_s$, respectively. The degree of refusal is $\vartheta(\mathfrak{u}) = \sqrt{1 - \mathfrak{p}^2(\mathfrak{u}) - \mathfrak{q}^2(\mathfrak{u}) - \mathfrak{r}^2(\mathfrak{u})}$ (Ali and Garg, 2023).

Definition II: The basic mathematical operations are described as follows.

Addition:

$$\tilde{\mathcal{T}}_s \oplus \tilde{V}_s = \left\{\sqrt{\mathfrak{p}_{\tilde{\mathcal{T}}_s}^2 + \mathfrak{p}_{\tilde{V}_s}^2 - \mathfrak{p}_{\tilde{\mathcal{T}}_s}^2 . \mathfrak{p}_{\tilde{V}_s}^2}, \mathfrak{q}_{\tilde{\mathcal{T}}_s}^2 . \mathfrak{q}_{\tilde{V}_s}^2, \sqrt{\left(\left(1 - \mathfrak{p}_{\tilde{V}_s}^2\right)\mathfrak{r}_{\tilde{\mathcal{T}}_s}^2 + \left(1 - \mathfrak{p}_{\tilde{\mathcal{T}}_s}^2\right)\mathfrak{r}_{\tilde{V}_s}^2 - \mathfrak{r}_{\tilde{\mathcal{T}}_s}^2 . \mathfrak{r}_{\tilde{V}_s}^2\right)}\right\} \tag{3}$$

Multiplication:

$$\tilde{\mathcal{T}}_s \otimes \tilde{V}_s = \left\{\mathfrak{p}_{\tilde{\mathcal{T}}_s}^2 . \mathfrak{p}_{\tilde{V}_s}^2, \sqrt{\mathfrak{q}_{\tilde{\mathcal{T}}_s}^2 + \mathfrak{q}_{\tilde{V}_s}^2 - \mathfrak{q}_{\tilde{\mathcal{T}}_s}^2 . \mathfrak{q}_{\tilde{V}_s}^2}, \sqrt{\left(\left(1 - \mathfrak{q}_{\tilde{V}_s}^2\right)\mathfrak{r}_{\tilde{\mathcal{T}}_s}^2 + \left(1 - \mathfrak{q}_{\tilde{\mathcal{T}}_s}^2\right)\mathfrak{r}_{\tilde{V}_s}^2 - \mathfrak{r}_{\tilde{\mathcal{T}}_s}^2 . \mathfrak{r}_{\tilde{V}_s}^2\right)}\right\} \tag{4}$$

Multiplication by a scalar:

$$\tilde{\mathcal{T}}_s \otimes x = \left\{\sqrt{1 - \left(1 - \mathfrak{p}_{\tilde{\mathcal{T}}_s}^2\right)^x}, \mathfrak{q}_{\tilde{\mathcal{T}}_s}^x, \sqrt{\left(1 - \mathfrak{p}_{\tilde{\mathcal{T}}_s}^2\right)^x - \left(1 - \mathfrak{p}_{\tilde{\mathcal{T}}_s}^2 - \mathfrak{r}_{\tilde{\mathcal{T}}_s}^2\right)^x}\right\} \tag{5}$$

x. Power of $\tilde{\mathcal{T}}_s$:

$$\tilde{\mathcal{T}}_s^x = \left\{\mathfrak{p}_{\tilde{\mathcal{T}}_s}^x, \sqrt{1 - \left(1 - \mathfrak{q}_{\tilde{\mathcal{T}}_s}^2\right)^x}, \sqrt{\left(1 - \mathfrak{q}_{\tilde{\mathcal{T}}_s}^2\right)^x - \left(1 - \mathfrak{q}_{\tilde{\mathcal{T}}_s}^2 - \mathfrak{r}_{\tilde{\mathcal{T}}_s}^2\right)^x}\right\} \tag{6}$$

Definition III: The formulation of SWGM with $\mathfrak{w}$=$(\mathfrak{w}_1, \mathfrak{w}_2, \ldots \mathfrak{w}_n)$; $\sum_{i:1}^n \mathfrak{w}_i = 1$ is described as follows:

$$\text{SWGM}\mathfrak{w}(\tilde{\mathcal{T}}_{s1}, \tilde{\mathcal{T}}_{s2}, \ldots., \tilde{\mathcal{T}}_{sn}) = \tilde{\mathcal{T}}_{s1}^{\mathfrak{w}_1} + \tilde{\mathcal{T}}_{s2}^{\mathfrak{w}_2} + \cdots + \tilde{\mathcal{T}}_{sn}^{\mathfrak{w}_n}$$
$$= \left\{\prod_{i:1}^n \mathfrak{p}_{\tilde{\mathcal{T}}_{sn}}^{\mathfrak{w}_i}, \sqrt{1 - \prod_{i:1}^n \left(1 - \mathfrak{q}_{\tilde{\mathcal{T}}_{sn}}^2\right)^{\mathfrak{w}_i}}, \sqrt{\prod_{i:1}^n \left(1 - \mathfrak{q}_{\tilde{\mathcal{T}}_{sn}}^2\right)^{\mathfrak{w}_i} - \prod_{i:1}^n \left(1 - \mathfrak{q}_{\tilde{\mathcal{T}}_{sn}}^2 - \mathfrak{r}_{\tilde{\mathcal{T}}_{sn}}^2\right)^{\mathfrak{w}_i}}\right\} \tag{7}$$

Definition IV: The score function, designated as $\mathcal{S}\left(\tilde{\mathcal{T}}_s\right)$, can be defined as follows (Ashraf and Abdullah, 2019):

$$\mathcal{S}\left(\tilde{\mathcal{T}}_s\right) = \left(\frac{1}{3}\right)\left(2 + \left(\mathfrak{p}_{\tilde{\mathcal{T}}_s}\right) - \left(\mathfrak{q}_{\tilde{\mathcal{T}}_s}\right) - \left(\mathfrak{r}_{\tilde{\mathcal{T}}_s}\right)\right); \mathcal{S}\left(\tilde{\mathcal{T}}_s\right) \in [0,1]. \tag{8}$$

2.2. The LODECI Technique

The LODECI (Pala, 2024) technique is predicated on the principle of maximal decomposition of each alternative in relation to all other alternatives with respect to each criterion. The decomposition value (DV) of an alternative can be readily determined for each criterion by calculating the maximum distance between the alternative and the others. LODECI utilizes the decision matrix $X = \left\|x_{ij}\right\|_{(nxm)}$

comprising of $A_i(i = 1, \dots, n)$ alternatives and $C_j(j = 1, \dots, m)$ benefit criteria $a_{ij} = \frac{x_{ij}}{x_j^{max}}$ and cost criteria $a_{ij} = \frac{x_j^{min}}{x_{ij}}$ is the maximum normalization techniques. Normalized decision matrix components are utilized to compute each decision matrix element's DV $\left(DV_{ij} = max\{|a_{ij} - a_{rj}|\} \; (r \neq i, r = 1, \dots, n)\right)$. Subsequently, the logarithmic DV $\left(LDV_j = \ln\left(1 + \frac{\sum_{i=1}^{n} DV_{ij}}{n}\right)\right)$ is calculated. Finally, the relative importance of the criteria $\mathbb{W}_j = \frac{LDV_j}{\sum_{j=1}^{m} LDV_j}$ are calculated.

2.3. The ARTASI Concept

The ARTASI (Pamucar et al., 2024) method is recommended as an alternative to traditional normalization techniques for standardizing the elements of decision matrices when the decision maker's subjective evaluations and the specificity of the addressed problem are taken into account. This method is particularly suited to the standardization of criteria values in multi-criteria models with more than ten alternatives, where it is appropriate to set the range of values to [1, 100]. This allows for a sufficient range to be established for matching the original criteria values. In the case of smaller-scale multi-criteria models, it is possible to adopt a smaller range threshold for the criteria. The method calculates the aggregated utility levels of the alternatives by defining the utility level of the alternatives with respect to the ideal and anti-ideal value. Finally, it ranks the alternatives according to their aggregated utility levels. Two parameters, ϕ and , ψ are used to to define the alternatives' utility function. The stabilization parameter of the aggregation function, denoted by the parameter ϕ, which can assume values within the range $[1, +\infty]$. The parameter $\psi \in [0, 1]$ is employed to define the influence of the aggregated levels of the utility of the alternatives in the ultimate decision-making process.

2.4. The Proposed Model for Cybersecurity Risk Assessment Based Fine-Kinney

The Fine-Kinney technique is a methodology that offers an analytical approach to the quantitative assessment of risk (Gul et al., 2018). The calculation of each risk is based on the multiplication of the risk parameters probability (P), exposure (E) and consequence (C). In the proposed hybrid method, the Fine-Kinney risk parameters (P, E and C) are weighted by the SF-LODECI (Yalçın et al., 2024) method and subsequently integrated into the SF-ARTASI (Yalçın et al., 2024) method, thereby determining the cyber threat ranking. The proposed hybrid cybersecurity risk assessment framework is presented in Figure 3.

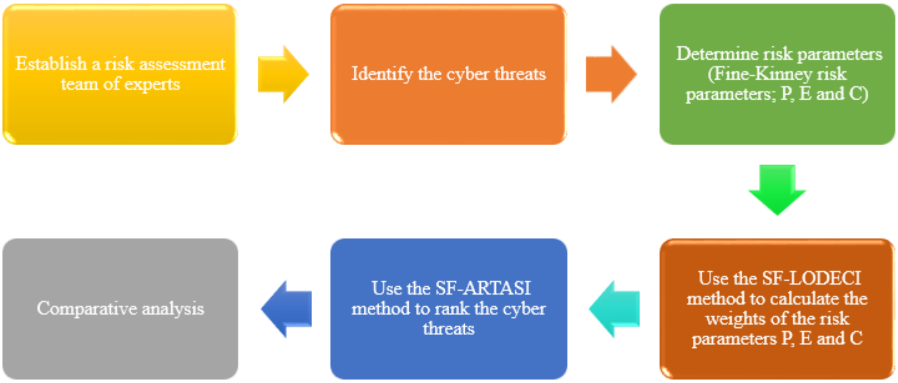
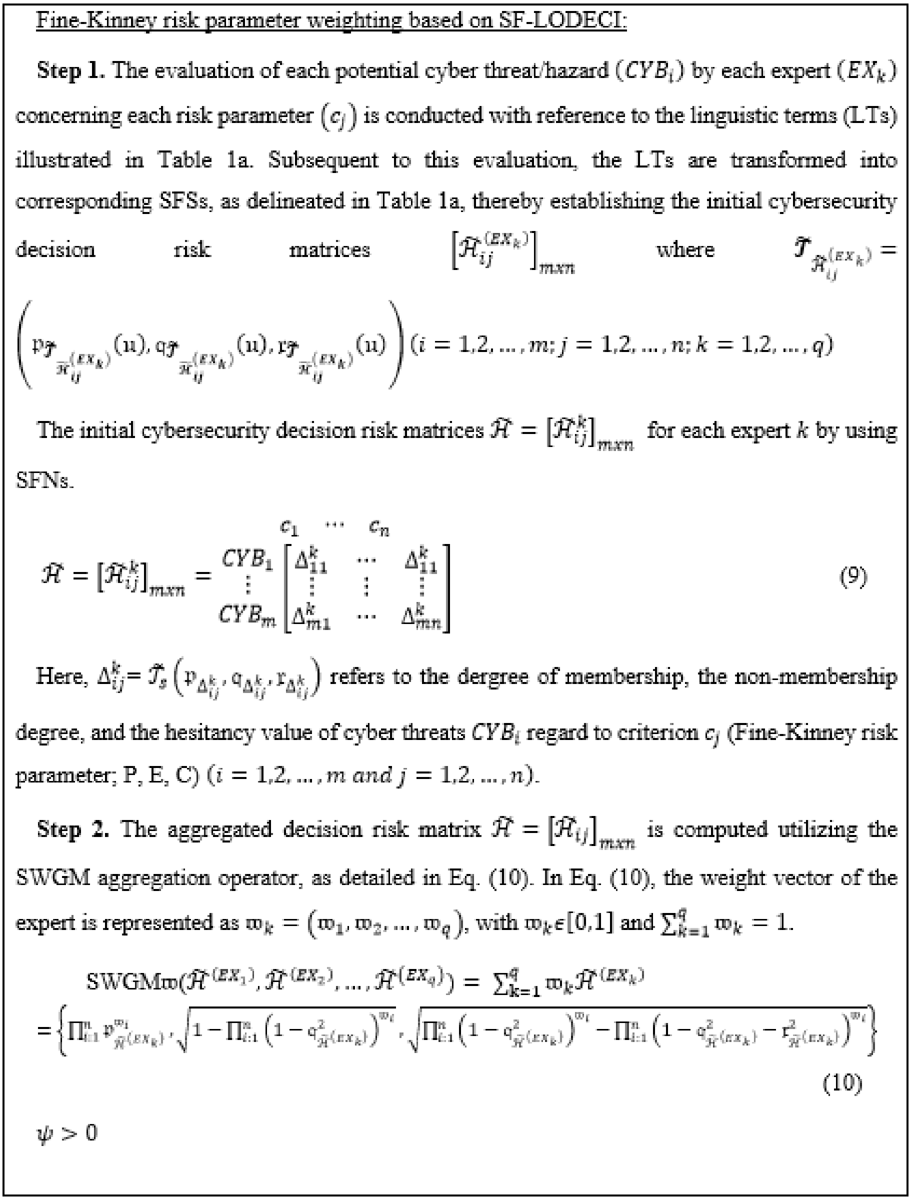

Establish a risk assessment team of experts
Identify the cyber threats
Determine risk parameters (Fine-Kinney risk parameters; P, E and C)
Use the SF-LODECI method to calculate the weights of the risk parameters P, E and C
Use the SF-ARTASI method to rank the cyber threats
Comparative analysis

Figure 3. The Proposed Hybrid Cybersecurity Risk Assessment Framework

The cybersecurity risk assessment problem with spherical fuzzy risk information addressed by the ARTASI hybrid model, which is based on the Fine-Kinney approach. Let $(CYB_i) = \{CYB_1, CYB_2, \dots, CYB_m\}(i = 1,2, \dots, m)$ be cyber threats/ hazards and n risk parameters $(c_j) = \{c_1, c_2, \dots, c_n\}(j = 1,2, \dots, n)$, and experts $(EX_k) = \{EX_1, EX_2, \dots, EX_q\}(k = 1,2, \dots, q)$ for the cybersecurity risk assessment problem. The proposed hybrid model consists of the following steps detailed in Table 1.

Table 1. The Steps of the Proposed Hybrid Cybersecurity Risk Assessment Model



Fine-Kinney risk parameter weighting based on SF-LODECI:

Step 1. The evaluation of each potential cyber threat/hazard (CYB_i) by each expert (EX_k) concerning each risk parameter (c_j) is conducted with reference to the linguistic terms (LTs) illustrated in Table 1a. Subsequent to this evaluation, the LTs are transformed into corresponding SFSs, as delineated in Table 1a, thereby establishing the initial cybersecurity decision risk matrices $\left[\hat{\mathcal{H}}_{ij}^{(EX_k)}\right]_{mxn}$ where $\mathcal{T}_{\hat{\mathcal{H}}_{ij}^{(EX_k)}} = \left(\mathfrak{p}_{\mathcal{T}_{\tilde{\mathcal{H}}_{ij}^{(EX_k)}}}(\mathfrak{u}), \mathfrak{q}_{\mathcal{T}_{\tilde{\mathcal{H}}_{ij}^{(EX_k)}}}(\mathfrak{u}), \mathfrak{r}_{\mathcal{T}_{\tilde{\mathcal{H}}_{ij}^{(EX_k)}}}(\mathfrak{u})\right) (i = 1,2, \dots, m; j = 1,2, \dots, n; k = 1,2, \dots, q)$

The initial cybersecurity decision risk matrices $\hat{\mathcal{H}} = \left[\hat{\mathcal{H}}_{ij}^{k}\right]_{mxn}$ for each expert k by using SFNs.

$$\hat{\mathcal{H}} = \left[\hat{\mathcal{H}}_{ij}^{k}\right]_{mxn} = \begin{array}{c c} & \begin{array}{ccc} c_1 & \cdots & c_n \end{array} \\ \begin{array}{c} CYB_1 \\ \vdots \\ CYB_m \end{array} & \begin{bmatrix} \Delta_{11}^{k} & \cdots & \Delta_{11}^{k} \\ \vdots & \vdots & \vdots \\ \Delta_{m1}^{k} & \cdots & \Delta_{mn}^{k} \end{bmatrix} \end{array} \tag{9}$$

Here, $\Delta_{ij}^{k} = \mathcal{T}_s\left(\mathfrak{p}_{\Delta_{ij}^{k}}, \mathfrak{q}_{\Delta_{ij}^{k}}, \mathfrak{r}_{\Delta_{ij}^{k}}\right)$ refers to the dergree of membership, the non-membership degree, and the hesitancy value of cyber threats CYB_i regard to criterion c_j (Fine-Kinney risk parameter; P, E, C) $(i = 1,2, \dots, m \; and \; j = 1,2, \dots, n)$.

Step 2. The aggregated decision risk matrix $\hat{\mathcal{H}} = \left[\hat{\mathcal{H}}_{ij}\right]_{mxn}$ is computed utilizing the SWGM aggregation operator, as detailed in Eq. (10). In Eq. (10), the weight vector of the expert is represented as $\varpi_k = \left(\varpi_1, \varpi_2, \dots, \varpi_q\right)$, with $\varpi_k \epsilon [0,1]$ and $\sum_{k=1}^{q} \varpi_k = 1$.

$$\text{SWGM}\varpi(\hat{\mathcal{H}}^{(EX_1)}, \hat{\mathcal{H}}^{(EX_2)}, \dots, \hat{\mathcal{H}}^{(EX_q)}) = \sum_{k=1}^{q} \varpi_k \hat{\mathcal{H}}^{(EX_k)}$$
$$= \left\{\prod_{i:1}^{n} \mathfrak{p}_{\hat{\mathcal{H}}^{(EX_k)}}^{\varpi_i}, \sqrt{1 - \prod_{i:1}^{n}\left(1 - \mathfrak{q}_{\hat{\mathcal{H}}^{(EX_k)}}^{2}\right)^{\varpi_i}}, \sqrt{\prod_{i:1}^{n}\left(1 - \mathfrak{q}_{\hat{\mathcal{H}}^{(EX_k)}}^{2}\right)^{\varpi_i} - \prod_{i:1}^{n}\left(1 - \mathfrak{q}_{\hat{\mathcal{H}}^{(EX_k)}}^{2} - \mathfrak{r}_{\hat{\mathcal{H}}^{(EX_k)}}^{2}\right)^{\varpi_i}}\right\} \tag{10}$$

$\psi > 0$

Table 1. Continued

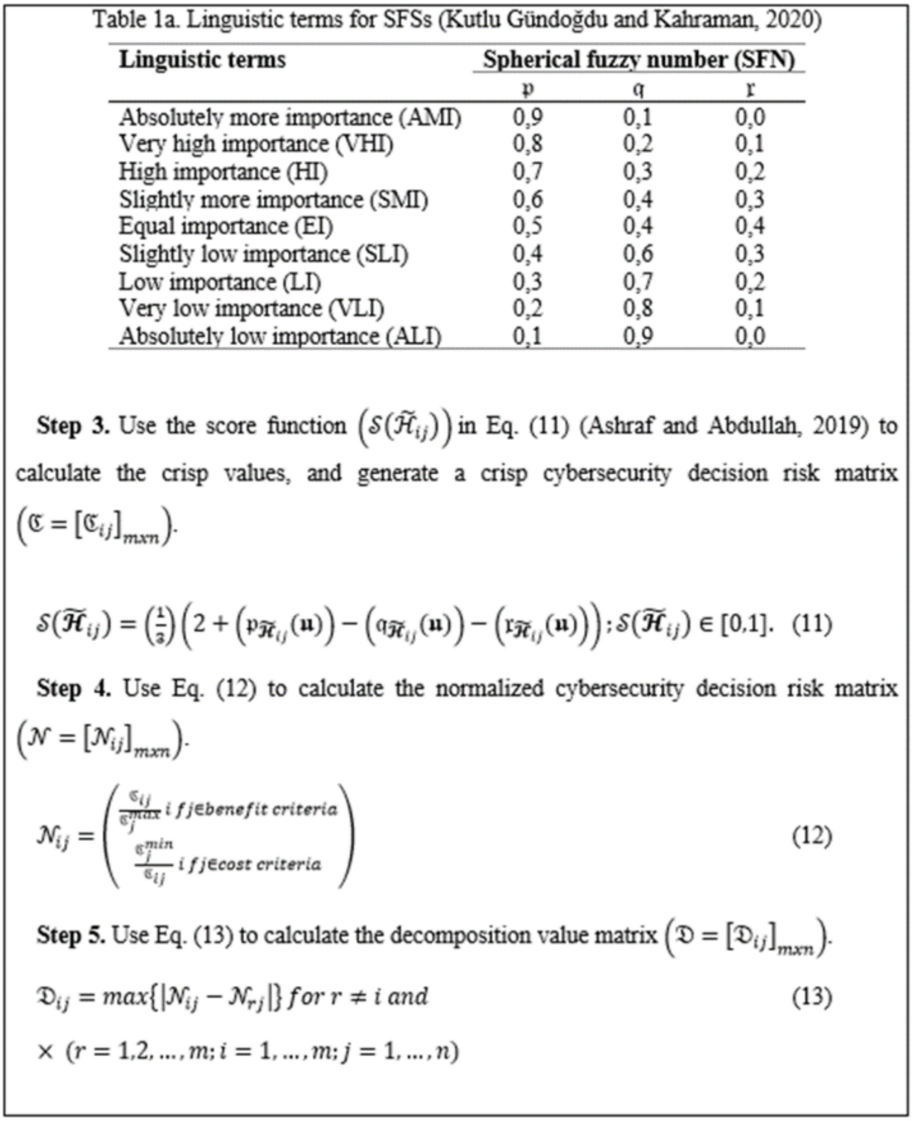


Table 1a. Linguistic terms for SFSs (Kutlu Gündoğdu and Kahraman, 2020)

Linguistic terms	Spherical fuzzy number (SFN)		
	p	q	r
Absolutely more importance (AMI)	0,9	0,1	0,0
Very high importance (VHI)	0,8	0,2	0,1
High importance (HI)	0,7	0,3	0,2
Slightly more importance (SMI)	0,6	0,4	0,3
Equal importance (EI)	0,5	0,4	0,4
Slightly low importance (SLI)	0,4	0,6	0,3
Low importance (LI)	0,3	0,7	0,2
Very low importance (VLI)	0,2	0,8	0,1
Absolutely low importance (ALI)	0,1	0,9	0,0

Step 3. Use the score function $\left(\mathcal{S}(\widetilde{\mathcal{H}}_{ij})\right)$ in Eq. (11) (Ashraf and Abdullah, 2019) to calculate the crisp values, and generate a crisp cybersecurity decision risk matrix $\left(\mathfrak{C} = [\mathfrak{C}_{ij}]_{mxn}\right)$.

$$\mathcal{S}(\widetilde{\mathcal{H}}_{ij}) = \left(\frac{1}{3}\right)\left(2 + \left(\mathfrak{p}_{\widetilde{\mathcal{H}}_{ij}}(\mathfrak{u})\right) - \left(\mathfrak{q}_{\widetilde{\mathcal{H}}_{ij}}(\mathfrak{u})\right) - \left(\mathfrak{r}_{\widetilde{\mathcal{H}}_{ij}}(\mathfrak{u})\right)\right); \mathcal{S}(\widetilde{\mathcal{H}}_{ij}) \in [0,1]. \quad (11)$$

Step 4. Use Eq. (12) to calculate the normalized cybersecurity decision risk matrix $\left(\mathcal{N} = [\mathcal{N}_{ij}]_{mxn}\right)$.

$$\mathcal{N}_{ij} = \begin{pmatrix} \frac{\mathfrak{C}_{ij}}{\mathfrak{C}_j^{max}} \, i\,f j \in benefit\ criteria \\ \frac{\mathfrak{C}_j^{min}}{\mathfrak{C}_{ij}} \, i\,f j \in cost\ criteria \end{pmatrix} \quad (12)$$

Step 5. Use Eq. (13) to calculate the decomposition value matrix $\left(\mathfrak{D} = [\mathfrak{D}_{ij}]_{mxn}\right)$.

$$\mathfrak{D}_{ij} = max\{|\mathcal{N}_{ij} - \mathcal{N}_{rj}|\}\ for\ r \neq i\ and \quad (13)$$

$$\times\ (r = 1,2, \dots, m; i = 1, \dots, m; j = 1, \dots, n)$$

Table 1. Continued

Step 6. Use Eq. (14) to calculate the logarithmic decomposition matrix $\left(\mathbb{L} = \left[\mathbb{L}_j\right]_n\right)$.

$$\mathbb{L}_j = \ln\left(1 + \frac{\sum_{i=1}^{m}\mathfrak{D}_{ij}}{m}\right) \tag{14}$$

Step 7. Use Eq. (15) to calculate the final weighting of the risk parameter matrix $\left(\mathbb{W} = \left[\mathbb{W}_j\right]_n\right)$.

$$\mathbb{W}_j = \frac{\mathbb{L}_j}{\sum_{j=1}^{n}\mathbb{L}_j} \tag{15}$$

Threat/hazard ranking based on SF-ARTASI:

Step 8. The crisp cybersecurity decision risk matrix $\left(\mathfrak{C} = \left[\mathfrak{C}_{ij}\right]_{mxn}\right)$, calculated in accordance with the procedures in Step 3, provides an initial cybersecurity decision risk assessment matrix for the SF-ARTASI method. The crisp cybersecurity decision risk matrix employed in order to calculate the absolute maximum values matrix$\left(\mathfrak{C}^{max} = \left[\mathfrak{C}_j^{max}\right]_n\right)$ and the absolute minimum values matrix $\left(\mathfrak{C}^{min} = \left[\mathfrak{C}_j^{min}\right]_n\right)$, as per the formulae provided in Eqs. (16) and (17), respectively.

$$\mathfrak{C}_j^{max} = \max_{1\le i\le m}\mathfrak{C}_{ij} + \left\{\max_{1\le i\le m}\mathfrak{C}_{ij}\right\}^{1/m} \tag{16}$$

$$\mathfrak{C}_j^{min} = \min_{1\le i\le m}\mathfrak{C}_{ij} - \left\{\min_{1\le i\le m}\mathfrak{C}_{ij}\right\}^{1/m} \tag{17}$$

Table 1. Continued

Step 9. In the following step, the standardized cybersecurity decision risk assessment matrix is derived by applying it to two sub-steps.

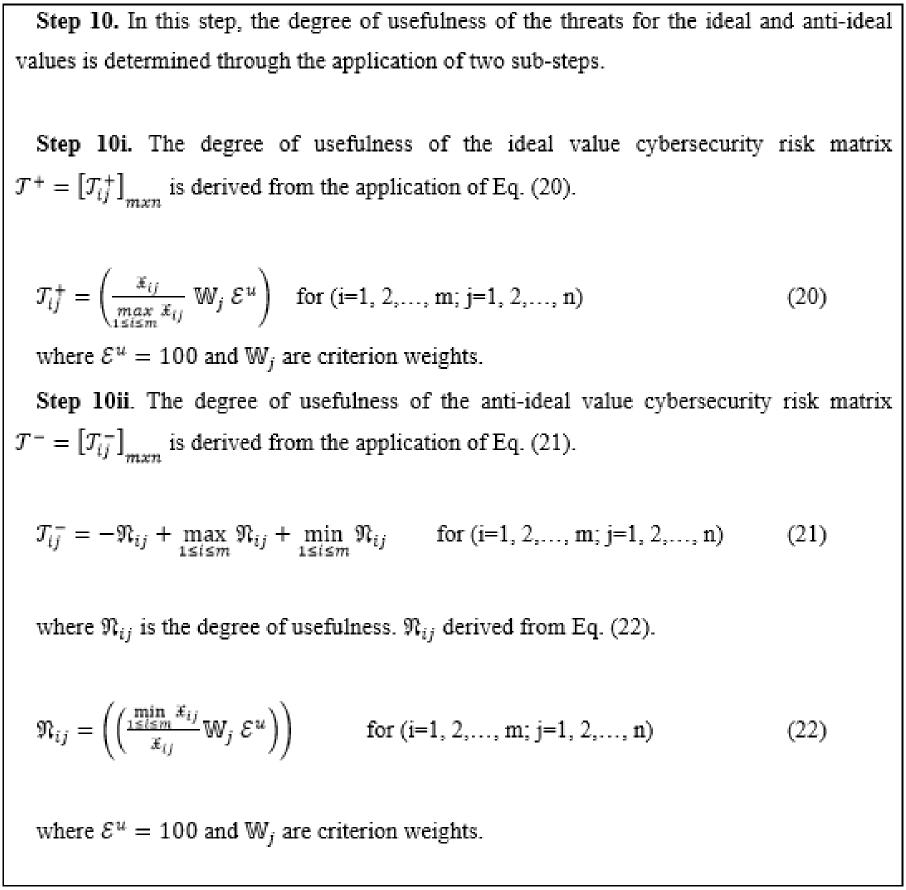
Step 9i. The cybersecurity risk assessment matrix can have two types of criteria: cost and benefit. The criteria values must be transformed to a standard base or interval. This approach uses subjective preferences to convert criterion values into a standardized range, unlike traditional normalizing methods that use a criteria interval of [0,1]. The components of the defuzzified cybersecurity decision risk matrix $\left[\mathfrak{C}_{ij}\right]_{mxn}$ are assigned to a randomized range of criteria $[\mathcal{E}^{l}, \mathcal{E}^{u}]$, where $(\mathcal{E}^{l})$ represents the lower limit of the range and $(\mathcal{E}^{u})$ represents the upper limit. The first level of the standardized cybersecurity decision risk matrix $\left[\mathfrak{B}_{ij}\right]_{mxn}$, standardize each element of the defuzzified cybersecurity risk matrix is computed via the application of Eq. (18). Furthermore, the standardized interval $[\mathcal{E}^{l}, \mathcal{E}^{u}]$ values equal [1, 100] (Pamucar et al., 2024).

$$\mathfrak{B}_{ij} = \frac{\mathcal{E}^{u} - \mathcal{E}^{l}}{\mathfrak{C}_{j}^{max} - \mathfrak{C}_{j}^{min}}\, \mathfrak{C}_{ij} + \frac{\mathfrak{C}_{j}^{max} . \mathcal{E}^{l} - \mathfrak{C}_{j}^{min} . \mathcal{E}^{u}}{\mathfrak{C}_{j}^{max} - \mathfrak{C}_{j}^{min}} \tag{18}$$

Step 9ii. The second-level standardized cybersecurity decision risk matrix $\left[\mathfrak{X}_{ij}\right]_{mxn}$ is derived from the application of Eq. (19).

$$\mathfrak{X}_{ij} = \begin{pmatrix} (\mathfrak{X}_{ij}) = \left(-\mathfrak{B}_{ij} + \max_{1 \le i \le m} \mathfrak{B}_{ij} + \min_{1 \le i \le m} \mathfrak{B}_{ij}\right) : if j \in cost\ criteria \\ (\mathfrak{X}_{ij}) = (\mathfrak{B}_{ij}) \, ; \, if j \in benefit\ criteria \end{pmatrix} \tag{19}$$

Table 1. Continued



Step 10. In this step, the degree of usefulness of the threats for the ideal and anti-ideal values is determined through the application of two sub-steps.

Step 10i. The degree of usefulness of the ideal value cybersecurity risk matrix $\mathcal{T}^{+} = [\mathcal{T}_{ij}^{+}]_{mxn}$ is derived from the application of Eq. (20).

$$\mathcal{T}_{ij}^{+} = \left(\frac{\mathscr{x}_{ij}}{\underset{1\le i\le m}{max}\ \mathscr{x}_{ij}}\ \mathbb{W}_j\ \mathcal{E}^{u}\right) \quad \text{for (i=1, 2,…, m; j=1, 2,…, n)} \qquad (20)$$

where $\mathcal{E}^{u} = 100$ and $\mathbb{W}_j$ are criterion weights.

Step 10ii. The degree of usefulness of the anti-ideal value cybersecurity risk matrix $\mathcal{T}^{-} = [\mathcal{T}_{ij}^{-}]_{mxn}$ is derived from the application of Eq. (21).

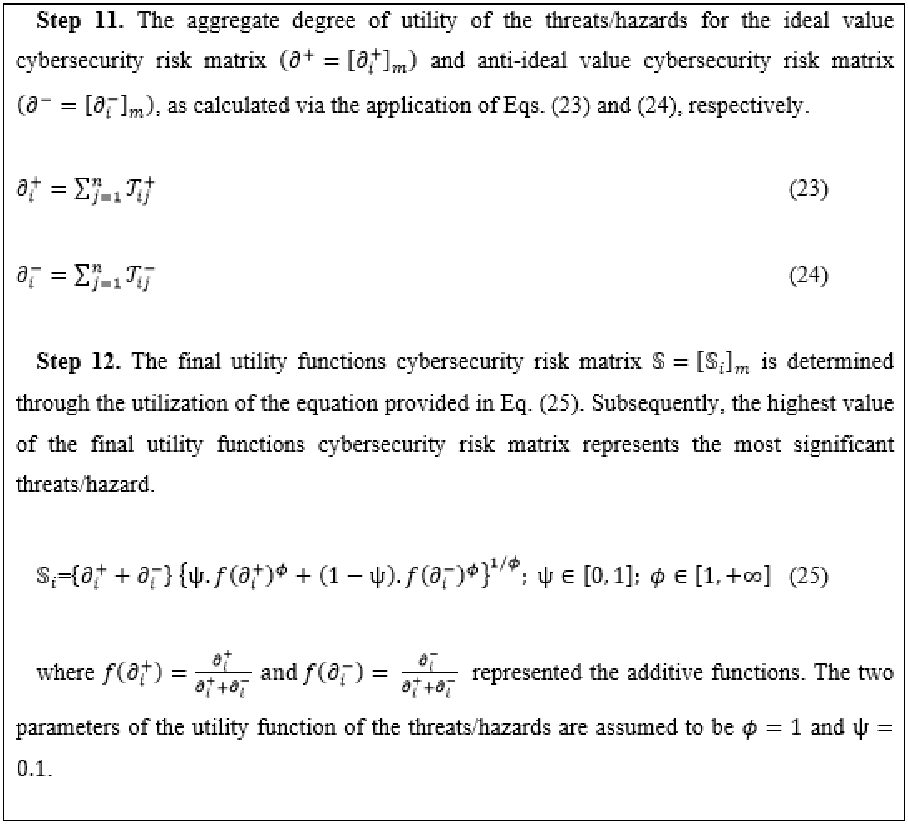
$$\mathcal{T}_{ij}^{-} = -\mathfrak{R}_{ij} + \max_{1\le i\le m} \mathfrak{R}_{ij} + \min_{1\le i\le m} \mathfrak{R}_{ij} \quad \text{for (i=1, 2,…, m; j=1, 2,…, n)} \qquad (21)$$

where $\mathfrak{R}_{ij}$ is the degree of usefulness. $\mathfrak{R}_{ij}$ derived from Eq. (22).

$$\mathfrak{R}_{ij} = \left(\left(\frac{\min_{1\le i\le m} \mathscr{x}_{ij}}{\mathscr{x}_{ij}} \mathbb{W}_j\ \mathcal{E}^{u}\right)\right) \quad \text{for (i=1, 2,…, m; j=1, 2,…, n)} \qquad (22)$$

where $\mathcal{E}^{u} = 100$ and $\mathbb{W}_j$ are criterion weights.

Table 1. Continued



Step 11. The aggregate degree of utility of the threats/hazards for the ideal value cybersecurity risk matrix ($\partial^{+} = [\partial_i^{+}]_m$) and anti-ideal value cybersecurity risk matrix ($\partial^{-} = [\partial_i^{-}]_m$), as calculated via the application of Eqs. (23) and (24), respectively.

$$\partial_i^{+} = \sum_{j=1}^{n} \mathcal{T}_{ij}^{+} \qquad (23)$$

$$\partial_i^{-} = \sum_{j=1}^{n} \mathcal{T}_{ij}^{-} \qquad (24)$$

Step 12. The final utility functions cybersecurity risk matrix $\mathbb{S} = [\mathbb{S}_i]_m$ is determined through the utilization of the equation provided in Eq. (25). Subsequently, the highest value of the final utility functions cybersecurity risk matrix represents the most significant threats/hazard.

$$\mathbb{S}_i=\{\partial_i^{+} + \partial_i^{-}\}\,\{\psi.f(\partial_i^{+})^{\phi} + (1-\psi).f(\partial_i^{-})^{\phi}\}^{1/\phi};\ \psi \in [0,1];\ \phi \in [1,+\infty] \quad (25)$$

where $f(\partial_i^{+}) = \frac{\partial_i^{+}}{\partial_i^{+}+\partial_i^{-}}$ and $f(\partial_i^{-}) = \frac{\partial_i^{-}}{\partial_i^{+}+\partial_i^{-}}$ represented the additive functions. The two parameters of the utility function of the threats/hazards are assumed to be $\phi = 1$ and $\psi = 0.1$.

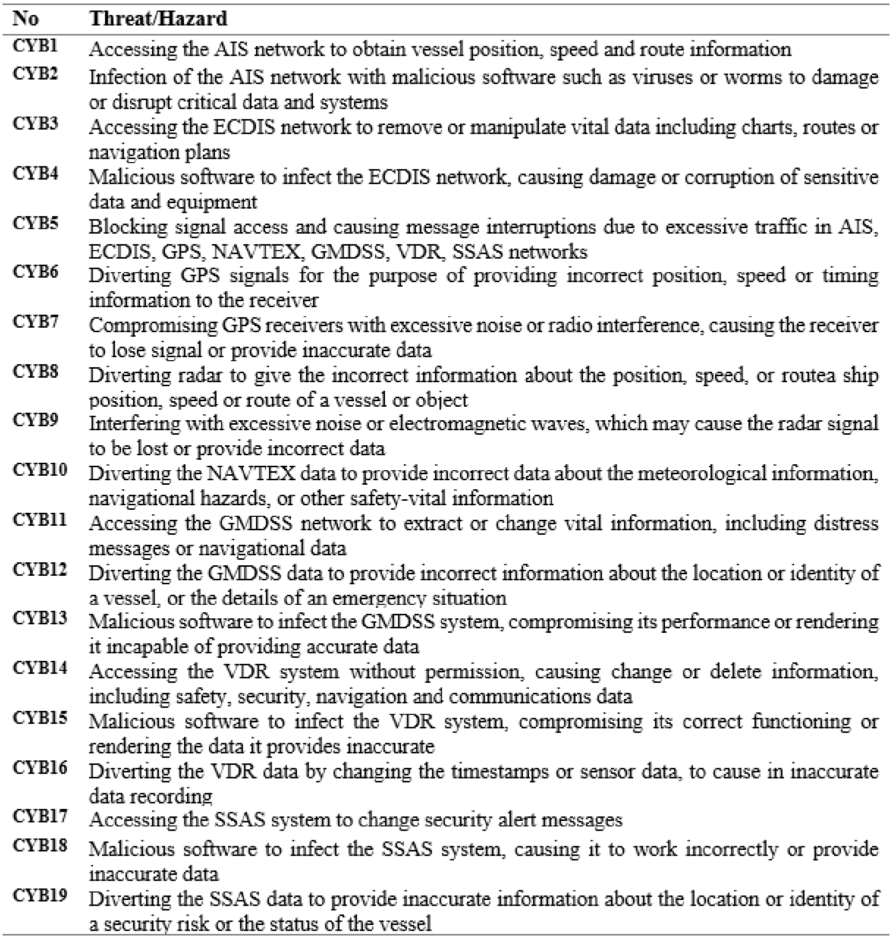
3. NUMERICAL CASE FOR CYBERSECURITY RISK ASSESSMENT

This section presents a numerical case of the application and usability of the proposed cybersecurity risk assessment model, specifically focusing on the evaluation of cybersecurity risks associated with cyber threats in the maritime transportation systems sector. In order to provide the comparability of the implementation of the Fine-Kinney based SF-LODECI-SF-ARTASI hybrid model, a numerical case was adapted from the study conducted by Uflaz et al. (2024) in the literature. Furthermore, this numerical case is employed to assess the validity and dependability of the proposed framework through a comparative analysis. The sub-sections that follow are structured to illustrate a particular application and comparative analysis process.

3.1. The Description of the Procedure to Assess Cybersecurity Risk

The issue of cyber risk represents a significant security threat in the maritime sector, as in all other domains. A potential cyberattack on a maritime vessel could have ramifications for the vessel's safety and personnel, the company in terms of economic cost and reputation, the cargo, and potentially the environmental impact in terms of pollution (Kechagias et al., 2022). In this context, a risk assessment is conducted with the objective of identifying and ranking potential cyber threats/hazards to a ship's critical systems. This is a process of analysing the potential vulnerability of digital systems on a vessel, with the intention of reducing the risk of cyber attacks. The potential nineteen cybersecurity threats/hazards (CYB1,CYB2,…,CYB19) outlined in this paper adapted from cyber attacks against ships, as described in Ref. Uflaz et al. (2024). The potential cybersecurity threats/hazards are presented in tabular form in Table 2.

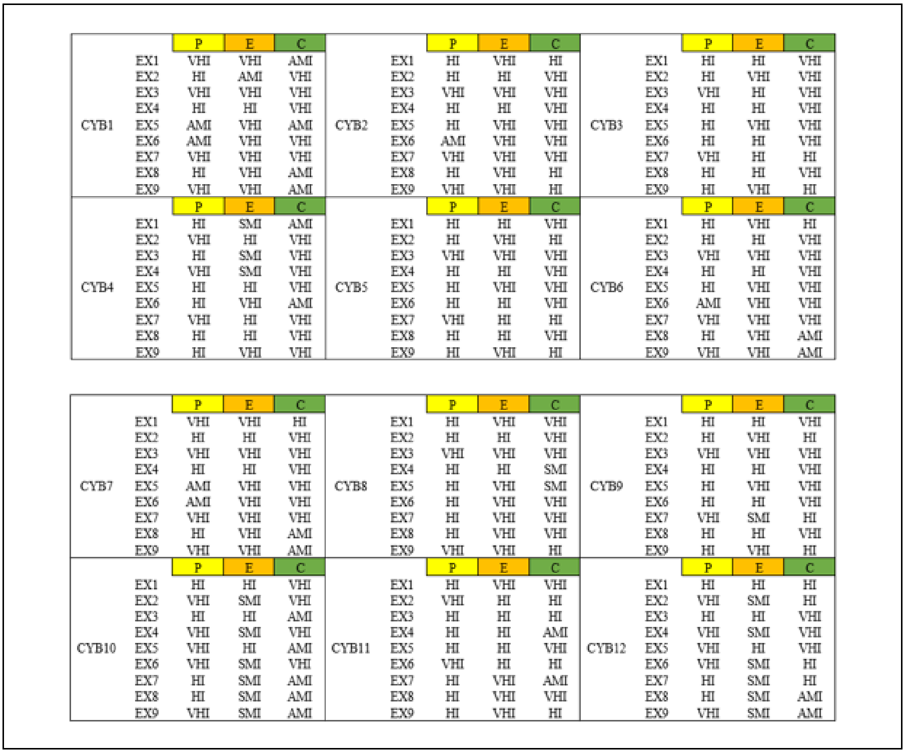
Table 2. The Potential Cybersecurity Threats/Hazards to the Ship's Critical Systems



No	Threat/Hazard
CYB1	Accessing the AIS network to obtain vessel position, speed and route information
CYB2	Infection of the AIS network with malicious software such as viruses or worms to damage or disrupt critical data and systems
CYB3	Accessing the ECDIS network to remove or manipulate vital data including charts, routes or navigation plans
CYB4	Malicious software to infect the ECDIS network, causing damage or corruption of sensitive data and equipment
CYB5	Blocking signal access and causing message interruptions due to excessive traffic in AIS, ECDIS, GPS, NAVTEX, GMDSS, VDR, SSAS networks
CYB6	Diverting GPS signals for the purpose of providing incorrect position, speed or timing information to the receiver
CYB7	Compromising GPS receivers with excessive noise or radio interference, causing the receiver to lose signal or provide inaccurate data
CYB8	Diverting radar to give the incorrect information about the position, speed, or routea ship position, speed or route of a vessel or object
CYB9	Interfering with excessive noise or electromagnetic waves, which may cause the radar signal to be lost or provide incorrect data
CYB10	Diverting the NAVTEX data to provide incorrect data about the meteorological information, navigational hazards, or other safety-vital information
CYB11	Accessing the GMDSS network to extract or change vital information, including distress messages or navigational data
CYB12	Diverting the GMDSS data to provide incorrect information about the location or identity of a vessel, or the details of an emergency situation
CYB13	Malicious software to infect the GMDSS system, compromising its performance or rendering it incapable of providing accurate data
CYB14	Accessing the VDR system without permission, causing change or delete information, including safety, security, navigation and communications data
CYB15	Malicious software to infect the VDR system, compromising its correct functioning or rendering the data it provides inaccurate
CYB16	Diverting the VDR data by changing the timestamps or sensor data, to cause in inaccurate data recording
CYB17	Accessing the SSAS system to change security alert messages
CYB18	Malicious software to infect the SSAS system, causing it to work incorrectly or provide inaccurate data
CYB19	Diverting the SSAS data to provide inaccurate information about the location or identity of a security risk or the status of the vessel

In order to conduct the risk assessment for potential cybersecurity threats/hazards identified through the proposed framework, a cybersecurity risk assessment team was constituted, comprising nine experts $\{EX_1, EX_2, \ldots, EX_9\}$ in maritime and IT fields, selected on the basis of their competence and experience. Following that, experts are asked to evaluate the risk associated with the aforementioned potential cybersecurity threats/hazards, according to the three risk parameters of the Fine-Kinney method (i.e., probability (P), exposure (E), and consequence (C)), using the linguistic scale provided in Table 1a. P, E, and C risk parameters are all considered to be benefit criteria (Gul et al., 2021b). The SFN-based risk evaluation matrix for each expert is presented in Table 3.

Table 3. The SFNs-based Risk Evaluation Matrix of Experts



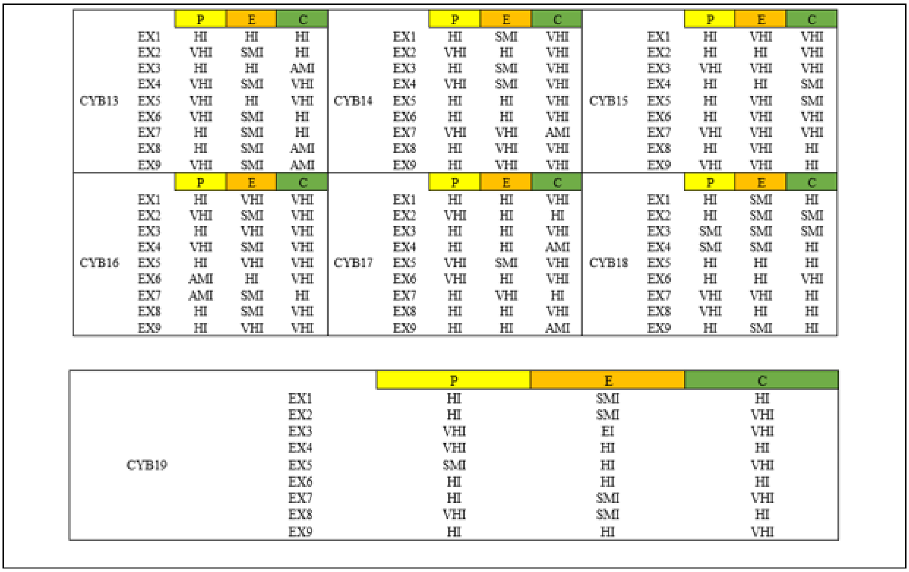
		P	E	C			P	E	C			P	E	C
CYB1	EX1	VHI	VHI	AMI	CYB2	EX1	HI	VHI	HI	CYB3	EX1	HI	HI	VHI
	EX2	HI	AMI	VHI		EX2	HI	HI	VHI		EX2	HI	VHI	VHI
	EX3	VHI	VHI	VHI		EX3	VHI	VHI	VHI		EX3	VHI	HI	VHI
	EX4	HI	HI	VHI		EX4	HI	HI	VHI		EX4	HI	HI	VHI
	EX5	AMI	VHI	AMI		EX5	HI	VHI	VHI		EX5	HI	VHI	VHI
	EX6	AMI	VHI	VHI		EX6	AMI	VHI	VHI		EX6	HI	HI	VHI
	EX7	VHI	VHI	VHI		EX7	VHI	VHI	VHI		EX7	VHI	HI	HI
	EX8	HI	VHI	AMI		EX8	HI	VHI	HI		EX8	HI	HI	VHI
	EX9	VHI	VHI	AMI		EX9	VHI	VHI	HI		EX9	HI	VHI	HI

		P	E	C			P	E	C			P	E	C
CYB4	EX1	HI	SMI	AMI	CYB5	EX1	HI	HI	VHI	CYB6	EX1	HI	VHI	HI
	EX2	VHI	HI	VHI		EX2	HI	VHI	HI		EX2	HI	HI	VHI
	EX3	HI	SMI	VHI		EX3	VHI	VHI	VHI		EX3	VHI	VHI	VHI
	EX4	VHI	SMI	VHI		EX4	HI	HI	VHI		EX4	HI	HI	VHI
	EX5	HI	HI	VHI		EX5	HI	VHI	VHI		EX5	HI	VHI	VHI
	EX6	HI	VHI	AMI		EX6	HI	HI	VHI		EX6	AMI	VHI	VHI
	EX7	VHI	HI	VHI		EX7	VHI	HI	HI		EX7	VHI	VHI	VHI
	EX8	HI	HI	VHI		EX8	HI	HI	VHI		EX8	HI	VHI	AMI
	EX9	HI	VHI	VHI		EX9	HI	VHI	HI		EX9	VHI	VHI	AMI

		P	E	C			P	E	C			P	E	C
CYB7	EX1	VHI	VHI	HI	CYB8	EX1	HI	VHI	VHI	CYB9	EX1	HI	HI	VHI
	EX2	HI	HI	VHI		EX2	HI	HI	VHI		EX2	HI	VHI	HI
	EX3	VHI	VHI	VHI		EX3	VHI	VHI	VHI		EX3	VHI	VHI	VHI
	EX4	HI	HI	VHI		EX4	HI	HI	SMI		EX4	HI	HI	VHI
	EX5	AMI	VHI	VHI		EX5	HI	VHI	SMI		EX5	HI	VHI	VHI
	EX6	AMI	VHI	VHI		EX6	HI	VHI	VHI		EX6	HI	HI	VHI
	EX7	VHI	VHI	VHI		EX7	HI	VHI	VHI		EX7	VHI	SMI	HI
	EX8	HI	VHI	AMI		EX8	HI	VHI	VHI		EX8	HI	HI	VHI
	EX9	VHI	VHI	AMI		EX9	VHI	VHI	HI		EX9	HI	VHI	HI

		P	E	C			P	E	C			P	E	C
CYB10	EX1	HI	HI	VHI	CYB11	EX1	HI	VHI	VHI	CYB12	EX1	HI	HI	HI
	EX2	VHI	SMI	VHI		EX2	VHI	HI	HI		EX2	VHI	SMI	HI
	EX3	HI	HI	AMI		EX3	HI	HI	HI		EX3	HI	HI	VHI
	EX4	VHI	SMI	VHI		EX4	HI	HI	AMI		EX4	VHI	SMI	VHI
	EX5	VHI	HI	AMI		EX5	HI	HI	VHI		EX5	VHI	HI	VHI
	EX6	VHI	SMI	VHI		EX6	VHI	HI	HI		EX6	VHI	SMI	HI
	EX7	HI	SMI	AMI		EX7	HI	VHI	AMI		EX7	HI	SMI	HI
	EX8	HI	SMI	AMI		EX8	HI	VHI	VHI		EX8	HI	SMI	AMI
	EX9	VHI	SMI	AMI		EX9	HI	VHI	HI		EX9	VHI	SMI	AMI

Table 3. Continued



		P	E	C
CYB13	EX1	HI	HI	HI
	EX2	VHI	SMI	HI
	EX3	HI	HI	AMI
	EX4	VHI	SMI	VHI
	EX5	VHI	HI	VHI
	EX6	VHI	SMI	HI
	EX7	HI	SMI	HI
	EX8	HI	SMI	AMI
	EX9	VHI	SMI	AMI
CYB14	EX1	HI	SMI	VHI
	EX2	VHI	HI	VHI
	EX3	HI	SMI	VHI
	EX4	VHI	SMI	VHI
	EX5	HI	HI	VHI
	EX6	HI	HI	VHI
	EX7	VHI	VHI	AMI
	EX8	HI	VHI	VHI
	EX9	HI	VHI	VHI
CYB15	EX1	HI	VHI	VHI
	EX2	HI	HI	VHI
	EX3	VHI	VHI	VHI
	EX4	HI	HI	SMI
	EX5	HI	VHI	SMI
	EX6	HI	VHI	VHI
	EX7	VHI	VHI	VHI
	EX8	HI	VHI	HI
	EX9	VHI	VHI	HI
CYB16	EX1	HI	VHI	VHI
	EX2	VHI	SMI	VHI
	EX3	HI	VHI	VHI
	EX4	VHI	SMI	VHI
	EX5	HI	VHI	VHI
	EX6	AMI	HI	VHI
	EX7	AMI	SMI	HI
	EX8	HI	SMI	VHI
	EX9	HI	VHI	VHI
CYB17	EX1	HI	HI	VHI
	EX2	VHI	HI	HI
	EX3	HI	HI	VHI
	EX4	HI	HI	AMI
	EX5	VHI	SMI	VHI
	EX6	VHI	HI	VHI
	EX7	HI	VHI	HI
	EX8	HI	HI	VHI
	EX9	HI	HI	AMI
CYB18	EX1	HI	SMI	HI
	EX2	HI	SMI	SMI
	EX3	SMI	SMI	SMI
	EX4	SMI	SMI	HI
	EX5	HI	HI	HI
	EX6	HI	HI	VHI
	EX7	VHI	VHI	HI
	EX8	VHI	HI	HI
	EX9	HI	SMI	HI
CYB19	EX1	HI	SMI	HI
	EX2	HI	SMI	VHI
	EX3	VHI	EI	VHI
	EX4	VHI	HI	HI
	EX5	SMI	HI	VHI
	EX6	HI	HI	HI
	EX7	HI	SMI	VHI
	EX8	VHI	SMI	HI
	EX9	HI	HI	VHI

Based on Table 3, the aggregated cybersecurity decision risk matrix is computed utilizing the SWGM aggregation operator, as presented in Eq. (10). The aggregated cybersecurity decision matrix is provided in Table 4. The weights of the risk parameters (P, E, and C) are calculated by applying the equations in Steps 3, 4, 5, 6, and 7 of SF-LODECI, as outlined in Table 1. The calculated risk parameter weights are presented in Table 5.

Table 4. The Aggregated Cybersecurity Decision Risk Matrix

No	P			E			C		
CYB1	0,785	0,225	0,136	0,799	0,206	0,112	0,843	0,164	0,075
CYB2	0,753	0,255	0,162	0,777	0,227	0,131	0,765	0,239	0,143
CYB3	0,721	0,281	0,184	0,732	0,271	0,175	0,777	0,227	0,131
CYB4	0,732	0,271	0,175	0,685	0,322	0,229	0,821	0,183	0,089
CYB5	0,721	0,281	0,184	0,743	0,261	0,165	0,765	0,239	0,143
CYB6	0,753	0,255	0,162	0,777	0,227	0,131	0,809	0,198	0,107
CYB7	0,785	0,225	0,136	0,777	0,227	0,131	0,809	0,198	0,107
CYB8	0,721	0,281	0,184	0,777	0,227	0,131	0,739	0,271	0,184
CYB9	0,721	0,281	0,184	0,730	0,276	0,184	0,765	0,239	0,143
CYB10	0,754	0,250	0,155	0,632	0,371	0,273	0,854	0,153	0,067
CYB11	0,721	0,281	0,184	0,743	0,261	0,165	0,774	0,237	0,148
CYB12	0,754	0,250	0,155	0,632	0,371	0,273	0,774	0,237	0,148
CYB13	0,754	0,250	0,155	0,632	0,371	0,273	0,784	0,230	0,145
CYB14	0,732	0,271	0,175	0,695	0,313	0,222	0,811	0,192	0,094
CYB15	0,732	0,271	0,175	0,777	0,227	0,131	0,729	0,281	0,192
CYB16	0,762	0,248	0,159	0,694	0,317	0,229	0,788	0,214	0,116
CYB17	0,732	0,271	0,175	0,698	0,304	0,208	0,797	0,212	0,122

CYB18	0,697	0,309	0,215	0,652	0,353	0,258	0,687	0,317	0,222
CYB19	0,719	0,286	0,192	0,630	0,360	0,279	0,754	0,250	0,155

Table 5. The Weights of the Risk Parameters

$\mathbb{W}$	P	E	C
$\mathbb{W}_j$	0,1908	0,4030	0,4062

Subsequently, following the calculation of the risk parameter weights, the SF-ARTASI steps are implemented. Eqs. (16) and (17) are used to compute the absolute maximum values matrix and the absolute minimum values matrix, respectively. Table 6 provides the absolute maximum values and minimum values matrices.

Table 6. The Absolute Maximum and Minimum Values

$\mathfrak{C}$	P	E	C
$\mathfrak{C}_j^{max}$	1,7972	1,8170	1,8710
$\mathfrak{C}_j^{min}$	-0,2589	-0,3160	-0,2668

The utility functions of threats/hazards for the ideal value cybersecurity risk matrix are calculated by applying steps 9, 10, 11, and 12 of SF-ARTASI, as outlined in Table 1. Table 7 presents the final utility functions cybersecurity risk matrix. The most significant threat/hazard is indicated by the final utility functions cybersecurity risk matrix's highest value.

Table 7. The Utility Functions and Ranking Threats/Hazards

No	∂_i^+	∂_i^-	$\mathbb{S}_i$	Rank
CYB1	0,49989	0,50011	99,699	1
CYB2	0,49915	0,50085	96,160	4
CYB3	0,49885	0,50115	94,671	5
CYB4	0,49912	0,50088	94,521	9
CYB5	0,49888	0,50112	94,599	7
CYB6	0,49929	0,50071	97,517	3
CYB7	0,49937	0,50063	98,014	2
CYB8	0,49923	0,50077	94,513	10
CYB9	0,49881	0,50119	94,080	13
CYB10	0,49993	0,50007	93,893	15
CYB11	0,49888	0,50112	94,665	6
CYB12	0,49935	0,50065	91,243	17
CYB13	0,49936	0,50064	91,479	16
CYB14	0,49902	0,50098	94,553	8
CYB15	0,49928	0,50072	94,327	11
CYB16	0,49891	0,50109	94,075	14

CYB17	0,49886	0,50114	94,194	12
CYB18	0,49975	0,50025	87,891	19
CYB19	0,49934	0,50066	90,181	18

As seen from Table 7, CYB1, CYB7 and CYB6 represent the most significant threat/hazard to be considered respectively. Figure 4 provides a visual representation of the utility functions associated with the identified threats/hazards.

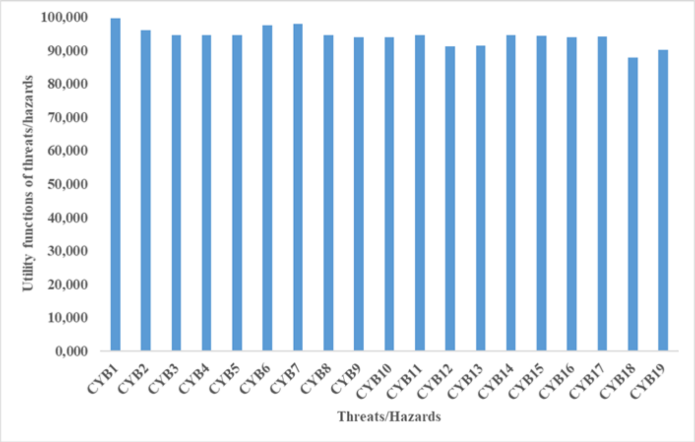


Figure 4. The Utility Functions of Threats/Hazards

3.2. Comparative Analysis

The findings of the risk assessment model proposed in this study are compared in this section with a different ranking method applied in the literature, which is Fine-Kinney based and employs SFSs. A comparative analysis was conducted to evaluate the efficacy of the proposed model in relation to the Fine-Kinney-based SF-TOPSIS methodology, as presented by Tatar et al. (2023). The results of the analysis are presented in Figure 5.

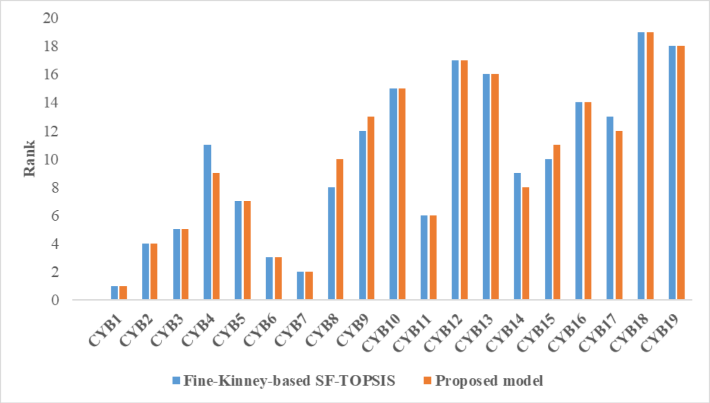


Figure 5. The Results of the Comparative Analysis

Figure 5 illustrates that the threat/hazard rankings are highly similar, as revealed by the findings of the comparison analysis. This stability underscores the efficacy and reliability of the proposed Fine-Kinney-based SF-ARTASI hybrid model.

4. CONCLUSION

The maritime sector is of critical importance in the global supply chain, representing approximately 90% of global trade in the transportation of goods (Alcaide and Llave, 2020). While the pervasive implementation of digital technologies in the maritime industry facilitates operational advancement, it concurrently engenders a series of disadvantages pertaining to cybersecurity (Uflaz et al., 2024). The maritime industry is susceptible to a range of cyber risks, particularly those targeting ship critical systems, and in-port information systems (Ben Farah et al., 2022).

The Fine-Kinney approach provides an efficacious methodology for risk assessment problems (Wang et al., 2023). Nevertheless, this approach is limited in its ability to accurately reflect the judgments of experts under conditions of uncertainty. In order to address the aforementioned cyber security risk assessment problem, which is based in Fine and Kinney, the SWGM operator, LODECI and ARTASI methods are integrated using spherical fuzzy sets. Subsequently, the model is utilized to conduct a risk assessment study for potential cyber threats/hazards to critical maritime transportation systems. Furthermore, the proposed model's robustness and reliability are tested by comparing it to another approach that has been employed in the literature. The findings demonstrate that the proposed model has the potential to provide a beneficial tool for stakeholders engaged in the cybersecurity risk assessment process. Accordingly, the hybrid model developed in this study will guide risk managers and other stakeholders in the identification and ranking of cybersecurity risks related to maritime transportation operations.

The present study has determined 19 potential cyber threats/hazards. According to the study results, the threat/hazard CYB1 "Accessing the AIS network to obtain vessel position, speed and route information" represents the most significant cyber threat/hazard and necessitates the most rigorous attention and protective measures. AIS-transmitted signals lack both encryption and verification, which renders them susceptible to exploitation by malicious actors. This deficiency can facilitate a range of attacks, including the spoofing of messages, the fabrication of ghost ships, the dissemination of false alerts or meteorological data, and other forms of interference (Ribeiro et al., 2023). AIS systems play an important role in maritime communication, providing information about a ship's route and location using GPS coordinates. However, AIS is one of the electronic communication equipment vulnerable to potential cyber attacks (Alcaide and Llave, 2020). Infection of the ECDIS system and its subsequent manipulation have the potential to significantly impact ship operations, resulting in considerable financial losses (Bolbot et al., 2020). The systems that facilitate the navigation of maritime vessels, including AIS, GPS and ECDIS, are dependent on signal processing and transmission principles. Consequently, this structure can make these systems vulnerable to cyber threats (Tusher et al., 2022). Organizations in the maritime sector must to take a proactive stance against cyber threats (Afenyo and Caesar, 2023). In the maritime transportation, weaknesses in a vessel's bridge system (Uflaz et al., 2024) may give rise to considerable issues with regard to cyber threats to navigation systems. Such challenges have the potential to result in significant financial losses with global trade.

The remaining ones have been ranked as follows: CYB7 “Compromising GPS receivers with excessive noise or radio interference, causing the receiver to lose signal or provide inaccurate data”>CYB6 “Diverting GPS signals for the purpose of providing incorrect position, speed or timing information to the receiver”>CYB2 “Infection of the AIS network with malicious software such as viruses or worms to damage or disrupt critical data and systems”>CYB3 “Accessing the ECDIS network to remove or manipulate vital data including charts, routes or navigation plans”>CYB11 “Accessing the GMDSS network to extract or change vital information, including distress messages or navigational data”>CYB5 “Blocking signal access and causing message interruptions due to excessive traffic in AIS, ECDIS, GPS, NAVTEX, GMDSS, VDR, SSAS networks”>CYB14 “Accessing the VDR system without permission, causing change or delete information, including safety, security, navigation and communications data”>CYB4 “Malicious software to infect the ECDIS network, causing damage or corruption of sensitive data and equipment”>CYB8 “Diverting radar to give the incorrect information about the position, speed, or routea ship position, speed or route of a vessel or object”>CYB15 “Malicious software to infect the VDR system, compromising its correct functioning or rendering the data it provides inaccurate”>CYB17 “Accessing the SSAS system to change security alert messages”>CYB9 “Interfering with excessive noise or electromagnetic waves, which may cause the radar signal to be lost or provide incorrect data”>CYB16 “Diverting the VDR data by changing the timestamps or sensor data, to cause in inaccurate data recording”>CYB10 “Diverting the NAVTEX data to provide incorrect data about the meteorological information, navigational hazards, or other safety-vital information”>CYB13 “Malicious software to infect the GMDSS system, compromising its performance or rendering it incapable of providing accurate data”>CYB12 “Diverting the GMDSS data to provide incorrect information about the location or identity of a vessel, or the details of an emergency situation”>CYB19 “Diverting the SSAS data to provide inaccurate information about the location or identity of a security risk or the status of the vessel”>CYB18 “Malicious software to infect the SSAS system, causing it to work incorrectly or provide inaccurate data”.

It is recommended that future research address the limitations of the proposed approach, which are as follows: First, the incorporation of data concerning cyber threats to ship navigation systems, in addition to the potential for cyber attacks on satellite link systems between land and sea, may have an impact on the results. Second, the different parameters can be added in addition to the three risk parameters. Furthermore, the integration of diverse weighting methodologies may provide a more rational approach to parameter weight calculation. In addition, for future research, the Fine-Kinney based ARTASI risk assessment strategy can be integrated with various ranking techniques using different fuzzy sets rather than spherical fuzzy sets. Moreover, future studies may utilize the presented hybrid methodology in disparate domains, such as finance and energy, and subsequently undertake a comparative analysis of the outcomes.

Statement of Research and Publication Ethics
Research and publication ethics were observed in the study.

REFERENCES

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*, *236*, 106493.

Akram, M., Alsulami, S., Khan, A., & Karaaslan, F. (2020). Multi-criteria group decision-making using spherical fuzzy prioritized weighted aggregation operators. *International Journal of Computational Intelligence Systems*, *13*(1), 1429-1446.

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547-554.

Ali, J., & Garg, H. (2023). On spherical fuzzy distance measure and TAOV method for decision-making problems with incomplete weight information. *Engineering Applications of Artificial Intelligence*, *119*, 105726.

Ashraf, S., & Abdullah, S. (2019). Spherical aggregation operators and their application in multiattribute group decision-making. *International Journal of Intelligent Systems*, 34(3), 493-523.

Ayvaz, B., Tatar, V., Sağır, Z., & Pamucar, D. (2024). An integrated Fine-Kinney risk assessment model utilizing Fermatean fuzzy AHP-WASPAS for occupational hazards in the aquaculture sector. *Process Safety and Environmental Protection*, *186*, 232-251.

Baltic and International Maritime Council (BIMCO), (2020). The Guidelines on Cyber Security Onboard Ships- Version 4. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Bayazit, O., & Kaptan, M. (2023). Evaluation of the risk of pollution caused by ship operations through bow-tie-based fuzzy Bayesian network. *Journal of Cleaner Production*, *382*, 135386.

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*(1), 22.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022a). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, *39*, 100571.

Bolbot, V., Methlouthi, O., Banda, O. V., Xiang, L., Ding, Y., & Brunou, P. (2022b). Identification of cyber-attack scenarios in a marine Dual-Fuel engine. *Trends in Maritime Technology and Engineering*, 503-510.

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science*, *131*, 104908.

Chaal, M., Ren, X., BahooToroody, A., Basnet, S., Bolbot, V., Banda, O. A. V., & Van Gelder, P. (2023). Research on risk, safety, and reliability of autonomous ships: A bibliometric review. *Safety science*, *167*, 106256.

European Maritime Safety Agency (EMSA), (2023). Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections- MARSEC Doc. 9209. https://www.emsa.europa.eu/publications/inventories/item/5074-guidance-on-how-to-address-cybersecurity-onboard-ships-during-audits,-controls,-verifications-and-inspections.html

Gul, M., Guven, B., & Guneri, A. F. (2018). A new Fine-Kinney-based risk assessment framework using FAHP-FVIKOR incorporation. *Journal of Loss Prevention in the Process Industries*, *53*, 3-16.

Gul, M., Mete, S., Serin, F., Celik, E. (2021a). Fine–Kinney Occupational Risk Assessment Method and Its Extensions by Fuzzy Sets: A State-of-the-Art Review. Fine–Kinney-Based Fuzzy Multi-Criteria Occupational Risk Assessment: Approaches, Case Studies and Python Applications, 1-11, Springer, Cham.

Gul, M., Mete, S., Serin, F., Celik, E. (2021b). Fine–Kinney-Based Occupational Risk Assessment Using Intuitionistic Fuzzy TODIM. Fine–Kinney-Based Fuzzy Multi-Criteria Occupational Risk Assessment: Approaches, Case Studies and Python Applications, 69-89, Springer, Cham.

Haugli-Sandvik, M., Lund, M. S., & Bjørneseth, F. B. (2024). Maritime decision-makers and cyber security: deck officers' perception of cyber risks towards IT and OT systems. *International Journal of Information Security*, 23, 1721–1739.

Ilbahar, E., Karaşan, A., Cebi, S., & Kahraman, C. (2018). A novel approach to risk assessment for occupational health and safety using Pythagorean fuzzy AHP & fuzzy inference system. *Safety Science*, *103*, 124-136.

International Maritime Organisation (IMO), (2022). Guidelines On Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2.

Kahraman, C., and Kutlu Gündoğdu, F. (2018). From 1D to 3D membership:spherical fuzzy sets. BOS / SOR 2018 Conference, Warsaw, Poland.

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*, 100526.

Kutlu Gündoğdu, F., & Kahraman, C. (2020). A novel spherical fuzzy analytic hierarchy process and its renewable energy application. *Soft Computing*, *24*, 4607-4621.

Kutlu Gündoğdu, F., and Kahraman, C. (2019). A novel fuzzy TOPSIS method using emerging interval-valued spherical fuzzy sets. *Engineering Applications of Artificial Intelligence*, 85, 307-323.

Pala, O. (2024). Assessment of the social progress on European Union by logarithmic decomposition of criteria importance. *Expert Systems With Applications*, *238*, 121846.

Pamucar, D., Simic, V., Görçün, Ö. F., & Küçükönder, H. (2024). Selection of the best Big Data platform using COBRAC-ARTASI methodology with adaptive standardized intervals. *Expert Systems with Applications*, *239*, 122312.

Park, C., Kontovas, C., Yang, Z., & Chang, C. H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480.

Ribeiro, C. V., Paes, A., & de Oliveira, D. (2023). AIS-based maritime anomaly traffic detection: A review. *Expert Systems with Applications*, *231*, 120561.

Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research*, *142*, 103855.

Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, *18*, 509-520.

Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*, 129-163.

Tatar, V., Yazicioglu, O., & Ayvaz, B. (2023). A novel risk assessment model for work-related musculoskeletal disorders in tea harvesting workers. *Journal of Intelligent & Fuzzy Systems*, *44*(2), 2305-2323.

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime economics & Logistics*, *24*, 208-227.

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. *Reliability Engineering & System Safety*, *243*, 109825.

Wan, C., Yan, X., Zhang, D., Qu, Z., & Yang, Z. (2019). An advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks. *Transportation Research Part E: Logistics and Transportation Review*, *125*, 222-240.

Wang, W., Han, X., Ding, W., Wu, Q., Chen, X., & Deveci, M. (2023). A Fermatean fuzzy Fine–Kinney for occupational risk evaluation using extensible MARCOS with prospect theory. *Engineering Applications of Artificial Intelligence*, *117*, 105518.

Wang, Y., Wang, W., Deveci, M., & Yu, X. (2024). An integrated interval-valued spherical fuzzy Choquet integral based decision making model for prioritizing risk in Fine-Kinney. *Engineering Applications of Artificial Intelligence*, *127*, 107437.

Yalçın, G. C., Kara, K., & Senapati, T. (2024). A hybrid spherical fuzzy logarithmic decomposition of criteria importance and alternative ranking technique based on Adaptive Standardized Intervals model with application. *Decision Analytics Journal*, *11*, 100441.