Opportunities and Challenges in Sustainability
https://www.acadlore.com/journals/OCS

Strengthening the Sustainability and Resilience of Global Supply Chains: An Integrated Risk Assessment Framework for International Logistics Security

Milan Andrejić, Vukašin Pajić*

Faculty of Transport and Traffic Engineering, University of Belgrade, 11000 Belgrade, Serbia

* Correspondence: Vukašin Pajić (v.pajic@sf.bg.ac.rs)

Received: 12-05-2024 **Revised:** 02-10-2025 **Accepted:** 02-18-2025

Citation: Andrejić, M. & Pajić, V. (2025). Strengthening the sustainability and resilience of global supply chains: An integrated risk assessment framework for international logistics security. *Oppor Chall. Sustain.*, *4*(1), 56-69. https://doi.org/10.56578/ocs040105.

Abstract: Global supply chains face increasing disruption from security-related risks, including cargo theft, illicit trade, document forgery, and cyberattacks—challenges that pose serious threats to sustainable development, especially in vulnerable and emerging economies. This study proposes a comprehensive decision-support framework designed to identify, assess, and rank logistics-related criminal threats, with the goal of strengthening the resilience and sustainability of international logistics systems. The model integrates Failure Mode and Effects Analysis (FMEA) for initial risk detection and prioritization, fuzzy Analytic Hierarchy Process (fuzzy AHP) to determine the relative importance of sustainability-relevant criteria (such as legal, environmental, financial, and reputational impacts), and the Additive Ratio Assessment (ARAS) method to perform final ranking. A real-world case study in international logistics demonstrates the framework's applicability and robustness. Results highlight how this integrated approach can support informed decision-making by governments, port authorities, and global logistics firms to mitigate risk and enhance supply chain continuity. By aligning technical methods with sustainable risk governance principles, this study contributes practical insights into building more adaptive, secure, and sustainable logistics infrastructures across borders.

Keywords: Sustainable logistics; Supply chain resilience; Risk assessment; FMEA; Fuzzy AHP; ARAS; Cross-border threats; International logistics governance

1. Introduction

Around the world, companies and their goods are faced with numerous threats, whether in transit, storage, or even at their final destination. Supply chains are considered extremely vulnerable to these threats, which often stem from human activities and are linked to illicit trade, theft, and terrorism. Criminal risks are ever-present, whether goods are being transported via sea, air, or land. These risks extend beyond the boundaries of the corporate world and impact citizens, national reputation, economic stability, and the integrity of individual companies. Criminal activities present various types of threats, which, when combined with different methods of security and safety management, can be observed across postal systems and logistics operations (Cavusgil et al., 2020; Gurtu & Johny, 2021). This is an area that will be further analyzed and described in this study.

The aim of this paper is to explore the criminal risks that affect international logistics, including the various types of crimes and the management strategies used to ensure the safe and secure execution of logistics activities and processes. To achieve this, companies must be aware of the existence of these risks, be able to recognize them, and take proactive measures to mitigate or completely eliminate their consequences. This study will also discuss the situation in Serbia, focusing on the prevalent type of crime, namely the trade of counterfeit and pirated goods. Additionally, the rise of cybercrime, especially in the aftermath of the ongoing COVID-19 pandemic, will be addressed, as it increasingly impacts logistics systems globally.

By examining these threats and the measures available for managing them, this paper seeks to contribute to the development of a comprehensive risk management framework for international logistics, which is crucial for maintaining security and operational continuity in a highly interconnected and increasingly risky global environment. To achieve this, a decision-making model was developed in this study, based on the integration of the FMEA, fuzzy AHP, and ARAS methods. The FMEA method was first applied to determine the RPN value for each risk, which was subsequently used as one of the evaluation criteria. The fuzzy AHP method was then employed to calculate the weights of the criteria used in the evaluation process, while the ARAS method was finally applied to rank the alternatives.

As previously indicated, the FMEA method was utilized to assess and prioritize risks based on their Risk Priority Number (RPN), where higher RPN values correspond to greater risk significance. In contrast, the fuzzy AHP method was chosen for its capacity to accommodate linguistic variables, making it well-suited for capturing expert judgment under uncertainty, a key requirement in the context of this study. Thanks to its simplicity, transparency, and interpretability, the ARAS method is well-suited for evaluating complex decision problems involving both qualitative and quantitative data. It has been effectively used in various fields, especially logistics, where balancing multiple objectives and handling diverse evaluation criteria are crucial.

The remainder of the paper is organized as follows. Section 2 provides a review of the relevant literature, followed by a discussion on crime in international flows in Section 3. Section 4 focuses on security in international flows, while Section 5 outlines the research methodology. The case study analysis and the results of the proposed model's application are presented in Section 6. Finally, Section 7 offers concluding remarks and suggestions for future research directions.

2. Literature Review

Supply chains often experience performance bottlenecks such as the bullwhip effect, high inventory levels, and limited data flow, which elevate costs and reduce efficiency. Distributed Ledger Technologies (DLT) have emerged as promising solutions to mitigate these challenges by enhancing transparency, decentralization, and data integrity. A review of 111 studies highlights DLT’s potential to transform supply chain operations, particularly in supporting the transition toward circular economic models through improved traceability and trust (Asante et al., 2023). Investigating international transport crimes presents a significant challenge for global security, law enforcement, and economic stability (Kniaziev et al., 2024). Previous research highlights the importance of advanced technologies, international cooperation, and effective customs control in reducing illegal transportation. Statistical analyses from EU customs data demonstrate that integrated legal and technological strategies can play a crucial role in addressing these crimes, with violations ranging from 82 to 106 cases annually across Europe. According to Cedillo-Campos et al. (2024) cargo theft continues to be a major challenge in logistics, with increasing sophistication in theft methods making traditional security measures inadequate. Research emphasizes the need for new analytical models that adapt to different regional contexts, particularly for road transportation. The development of the "Cargo Theft Model" (CTM) based on the Physical Internet framework presents a promising approach to mitigating the risk of theft by optimizing the mix of products in consolidated shipments. This model, tested in real-world scenarios, offers insights into its potential benefits for enhancing supply chain security, reducing logistical costs, and minimizing environmental impact through collaborative freight consolidation.

Rahman et al. (2024) note that the detection and prevention of financial crimes has grown increasingly complex due to global economic integration, online banking, and cryptocurrency usage, highlighting the need for combined machine-learning and network-analysis approaches. Their experiments on a global black-money dataset show that, despite slightly lower overall accuracy, XG-Boost outperforms Logistic Regression and Random Forest in precision, recall, and F1 score, making it the most effective for distinguishing illicit from legitimate transactions.

Lallerstedt (2022) outlines the vast scope of illicit trade—including counterfeit and excise goods, trade misinvoicing, substandard and environmental crimes, illicit drugs, and a shadow service economy and detail its grave harms, from funding organized crime and terrorists to health costs, environmental destruction, and the undermining of Sustainable Development Goals, while noting its low-profile nature contributes to its underprioritization. They propose three remedies: improved data collection for informed policy analysis, “completing globalization” by embedding stronger counter-illicit mechanisms into trade and cybercrime frameworks, and coordinated collective action against key problem states.

3. Crime in International Flows

In recent years, increasing attention has been given to disruptions, interruptions, and other adverse events affecting supply chains. These challenges relate to various aspects of international flows, including decision-making, goods safety and security, financial management, and more. Many of these disruptions occur randomly and are beyond human control, such as natural disasters—tornadoes, floods, and other extreme weather events—that can damage infrastructure, disrupt transport routes, and halt production facilities. Others, while triggered by human activity, are still considered accidental—such as workplace injuries or accidents that lead to production stoppages or transportation delays.

In addition to these, there are intentional disruptions like theft, which significantly increase costs and cause interruptions in global trade flows. A notable example includes piracy on the open seas. All types of disruptions, regardless of their origin, negatively affect both short-term operations and long-term business strategies, as well as financial performance. Beyond financial losses, they can also lead to diminished customer trust, brand devaluation, and legal consequences. Despite growing evidence of the harmful impact of such events, many companies still fail to invest adequately in resilient systems that can effectively respond to supply chain disturbances. Often, businesses focus more on recurring, low-impact risks while neglecting rare but high-impact threats (Speier et al., 2011). Given the vulnerability of international trade flows, a deeper understanding of disruptions and the development of appropriate response strategies is essential. Among these threats are also those related to criminal activities. Management of international logistics flows frequently overlooks issues of safety, security, and crime prevention. The main focus tends to remain on performance indicators such as delivery time, cost, quality, and customer satisfaction, while safety and security measures are often seen as additional burdens or expenses. However, in light of the potential and actual consequences of criminal acts within supply chains, the importance of proactive security management becomes evident. Preventive measures should be embedded into regular control processes, rather than being limited to inspections or border checks. While international trade flows enable legal, efficient production, supply, and delivery of goods, they can also be exploited for illegal purposes. Common crimes include theft, smuggling, counterfeiting, drug and weapon trafficking, human trafficking, and illegal immigration. As globalization advances and global interconnectivity expands, so do opportunities for these illicit activities. The following sections of this paper will explore the general theory of crime, as well as specific criminal acts that have the greatest impact on international trade flows (Ahokas et al., 2010).

The environment in which supply chain participants operate is highly unstable and exposed to numerous threats targeting personnel, cargo, vehicles, and other assets. Various criminal activities—such as cargo theft, terrorism, and piracy—are prevalent and will be examined in more detail below.

3.1 Cargo Loss and Theft

Loss of goods can occur at any stage between the point of production and the final point of sale. The four main causes of cargo loss include employee theft, shoplifting, administrative errors, and supplier fraud—three of which are criminal in nature. Theft represents a widespread and serious issue globally. Despite its prevalence, in many countries, cargo theft is considered a low-priority concern due to the high costs associated with its prevention and resolution. Accurate data collection on cargo loss is often hindered by limited reporting from transport companies and the absence of legal regulations that would enforce consistent and standardized reporting practices. Cargo theft frequently coincides with vehicle theft and the targeting of drivers' personal property. Motivations behind vehicle theft generally fall into three categories: value, utility for transporting stolen goods, and access to personal or sensitive documentation. Vehicles may be stolen for their resale value, for their ability to move stolen cargo, or for personal belongings such as credit cards, mobile phones, or digital cameras stored inside. Even if no items are ultimately taken, such acts are still perceived as threats to the transportation network. Most of these incidents occur between 10 p.m. and 6 a.m., indicating that the time of day plays a significant role in the vulnerability of transport operations within the supply chain. Regardless of the motive, there are numerous well-defined methods used to target trucks, which vary based on the attack location—from the point of dispatch to the final delivery location, including loading and unloading sites (Liang et al., 2022).

Interestingly, one of the greatest risks for companies comes from trusted insiders—namely employees—who are estimated to be involved in around 60% of total losses. This is particularly noteworthy given that most preventive measures are aimed at external threats. Employees may commit theft in response to social or environmental pressures within the workplace, making such incidents difficult to predict or detect. Drivers are often seen as the weakest link in the chain: they are highly exposed to risks yet are also the first line of defense against cargo crime. Therefore, proper training and education on cargo crime and personal safety are essential.

3.2 Terrorism

Terrorism is defined as the deliberate use of unlawful violence or threats with the intent to instill fear, typically for political, religious, or ideological purposes. The maritime sector, and transportation in general, is inherently complex and deeply integrated with global markets—making it susceptible to a range of security threats. Ships can serve both as direct targets and as tools for conducting or planning terrorist acts. Additionally, maritime transport can be exploited as a source of revenue for terrorist organizations. The key risk factors—cargo, vessels, personnel, and finances—are all linked to widespread disruptions in global trade and lead to significant economic costs due to the need for heightened security measures. For this reason, it is critical that governments implement coherent and proactive security policies. These policies should not only address isolated and individual threats but should also recognize and respond to broader, interconnected risks across the global transportation network.

Statistical analysis suggests that the focus should be placed more on the potential for attacks rather than their probability. As such, it becomes increasingly difficult to clearly identify who constitutes a potential terrorist threat.

Whether the effects of a terrorist act—or even the threat of one—are direct or indirect, they will inevitably impact the global supply chain to varying degrees, and consequently, the global economy as a whole (Dobie et al., 2000).

3.3 Smuggling of Goods

Illicit goods are funneled into the black market, a space where items of questionable or outright illegal origin are exchanged for money. Buyers for such products can be found across the globe. It is important to note that smuggling does not necessarily imply that the goods themselves are illegal in every location. What is deemed legal in one country may be prohibited in another, allowing smugglers to operate through legitimate companies attempting to penetrate restricted markets.

The "grey market" refers to the illegal trade of counterfeit goods, typically known only to authorities. This market includes goods that have been diverted from legitimate supply chains. The risk of detection is primarily posed by government agencies or companies whose products are being counterfeited. Production sites for these knockoffs are often situated in regions where the likelihood of discovery is low, and where they can blend into regular business environments—though often with added costs and issues related to quality control.

Counterfeit goods travel the same logistical pathways and use the same ports as legal goods. Certain regions, particularly in Central and South America, act as hubs for counterfeit products, where purchasing fake items is commonly used as a method of money laundering. The nature of counterfeit goods seized at the EU's external borders often differs from those found elsewhere, which underscores the fact that fake products are tailored to the cultural preferences, trends, and habits of specific regions.

Both types of illicit supply chains—those dealing in counterfeits and in banned substances like drugs—rely heavily on global container flows. Smugglers deliberately avoid direct or well-known routes in an effort to bypass detection by customs and law enforcement. The counterfeiting business demands continuous monitoring of market trends and technological advancements to remain effective. The infiltration of illegal products into legitimate logistics channels poses a significant threat. One of the most widely used countermeasures is the inspection of cargo vehicles crossing borders. However, even when no illegal goods are found, these inspections can cause disruptions throughout the transportation network (Najafi et al., 2023).

3.4 Piracy

Piracy is considered an international crime against all nations, and offenders can be prosecuted anywhere. In recent years, piracy has been most prevalent at sea, particularly affecting maritime trade flows that depend on this mode of transport (Hosen, 2024). The threat of piracy has grown significantly, especially in areas like the Horn of Africa, where it has forced rerouting of shipping lanes. Modern pirates are constantly adapting their tactics and selecting new targets, using increasingly sophisticated weapons and advanced techniques to ensure successful attacks. Violence and the kidnapping of crew members are becoming more common in piracy operations. The resulting costs are substantial, including the diversion of ships to avoid high-risk zones, ransom payments, and logistical support from various agencies and organizations. Piracy thus imposes financial, operational, and security burdens on the global maritime supply chain.

4. Security in International Goods Flows

The primary objective of managing the security of international flows is to mitigate or eliminate the consequences of criminal activities occurring within these flows. Consequently, it is necessary to define performance indicators that can effectively measure the efficiency of implemented solutions aimed at combating crime. Within these flows, three main types of criminal activities are commonly identified: theft, smuggling, and direct attacks. Theft involves the unauthorized appropriation of any form of assets within the flow of goods. Smuggling refers to the illegal transportation of goods or people and represents a significant threat to the integrity and safety of the supply chain. Direct attacks target assets, infrastructure, or individuals involved in the flow process (Männistö, 2015). When considering maritime transport and port operations, security performance can be evaluated based on the capability of inspection systems to detect nuclear materials or weapons potentially hidden within shipping containers. Additionally, performance can be assessed by examining the effectiveness of deterrence against terrorist organizations. The deterrence effect is reflected in situations where these organizations abandon planned actions due to the high perceived risk of failure. One key performance indicator relevant to the entire supply chain is the threat detection probability, which measures the proportion of actual threats detected in a timely manner versus those identified too late. Employees play a pivotal role in managing flow security. Their motivation is crucial to the detection and prevention of criminal activities of any nature. Effective security management also contributes to ensuring the continuity of supply chains while reducing both the probability and duration of potential disruptions. Across all modes of transportation, the fundamental goals of security management include prevention, monitoring, detection, and response to anomalies and failures. These goals can also be interpreted as performance metrics—such as incident frequency, detection capabilities, and recovery efficiency. The following sections of this paper will explore the diversity of existing security solutions and introduce a performance model designed to evaluate the security of international cargo flows.

A wide range of solutions is employed to enhance the safety and security of international flows. Many of these solutions involve the application of technologies such as alarms, CCTV cameras, and electronic access cards designed to protect facilities. In the context of transportation—including ships, trucks, and other transport modes—logistics operators use RFID tags, GPS devices, security seals, and tracking technologies to monitor cargo throughout transit. These tracking systems enable rapid detection and response to routing issues, unauthorized container openings, or unexplained vehicle stoppages. Such technologies are particularly valuable at border crossings, where automated computer systems are increasingly used to assess the risk of inbound and outbound cargo traffic. For inspection purposes, technologies based on X-rays, gamma rays, material detection devices, and passive radiation detectors are also applied. In addition to technological solutions, adherence to standardized procedures and protocols by employees plays a vital role in maintaining supply chain security. Examples of such procedures include: Background checks for job applicants, which may involve contact with law enforcement and financial institutions to assess candidate reliability; Regular training and awareness programs for employees; Organized guard patrols; Verification of security seals; Compliance checks; Arrangement of secure escorts (Männistö, 2015).

Many of these solutions represent upgrades to existing systems. For instance, adapting existing alarm systems or repositioning surveillance and tracking equipment can significantly improve the speed and security of logistics operations, particularly within port environments. A key distinction between traditional and modern approaches lies in the increased accessibility and visibility of information. Whereas information was previously exchanged by phone, today much of it is digitized and instantly available upon request. Although many solutions can function independently, they are often integrated into more complex systems. A limitation of this integration is that the impact of a single solution may be difficult to isolate, as it is influenced by the presence and interaction with other technologies already in use. Researchers have sought to frame the diversity of these solutions within conceptual models. According to one classification, solutions can be categorized as either protecting facilities, information, or cargo—each at either a basic or advanced level. The basic level refers to commonly applied standard practices, while the advanced level includes solutions capable of anticipating events and “thinking ahead.” In conclusion, these solutions encompass a broad spectrum of technologies, procedures, and principles that enable companies to reduce or eliminate criminal risks in international flows. They are almost always implemented in combination, forming part of a larger security system. Security-related projects in international logistics are often built upon existing systems, leading to gradual yet meaningful improvements over time (Ekwall, 2012).

5. Methodology

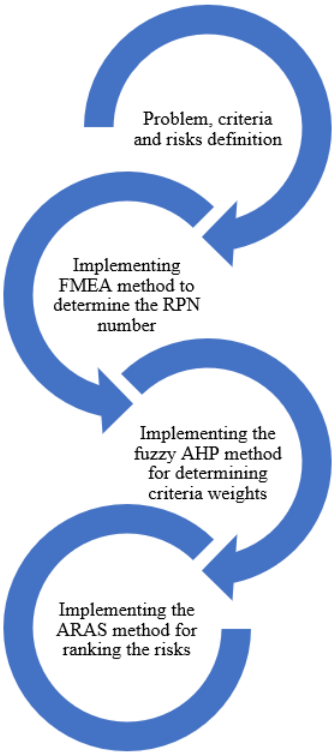
Problem, criteria and risks definition
Implementing FMEA method to determine the RPN number
Implementing the fuzzy AHP method for determining criteria weights
Implementing the ARAS method for ranking the risks

Figure 1. Methodology of the paper

For the purpose of risk evaluation and ranking, a comprehensive model was developed in this study, based on the integration of the FMEA, fuzzy AHP, and ARAS methods. The fuzzy AHP method was employed to determine the weights of the evaluation criteria, while the FMEA method was used to assess the significance of risks by calculating the Risk Priority Number (RPN), which was also included as one of the criteria in the ARAS-based evaluation and ranking process. The proposed model, along with the implementation steps, is illustrated in Figure 1.

5.1 FMEA Method

FMEA is a systematic technique originally developed to investigate potential failures across various systems and processes. It focuses on the structural aspects and failure characteristics of the system being examined. The core aim of FMEA is to identify possible faults and determine preventive or corrective actions that can mitigate associated risks. By applying this method, organizations can achieve several advantages, such as improved operational safety, enhanced service reliability, lower warranty and maintenance costs, reduced development time, better adherence to project timelines, more efficient processes, and increased customer satisfaction. FMEA evaluates and ranks failure modes using the Risk Priority Number (RPN). This value is obtained by multiplying three key risk factors: Severity (S), Occurrence (O), and Detection (D). Severity reflects the impact or seriousness of a failure. Each effect is rated on a scale from 1 (no impact) to 10 (catastrophic impact). In this study, the severity scale defined by Chin et al. (2009) was used (Table 1).

Occurrence measures how likely it is that a failure will happen. The probability scale used in this study is also adapted from Chin et al. (2009) and is presented in Table 2.

Table 1. Severity ratings (Chin et al., 2009)

Rating	Effect	Severity of Effect
10	Hazardous without warning	Extremely severe, affects safety without prior indication
9	Hazardous with warning	Extremely severe, safety affected but with some warning
8	Very high	System fails destructively without endangering safety
7	High	Equipment failure with damage
6	Moderate	Operational failure with minor damage
5	Low	System stops functioning without physical damage
4	Very low	Reduced performance, but the system remains operational
3	Minor	Slight performance degradation
2	Very minor	Minimal performance interference
1	None	No noticeable effect

Table 2. Probability ratings (Chin et al., 2009)

Rating	Probability of Occurrence	Failure Probability
10	Very high: failure is almost certain	>1 in 2
9		1 in 3
8	High: failures occur frequently	1 in 8
7		1 in 20
6	Moderate: failures occur occasionally	1 in 80
5		1 in 400
4		1 in 2000
3	Low: rare failures	1 in 15,000
2		1 in 150,000
1	Remote: failure is very unlikely	<1 in 1,500,000

Table 3. Detection ratings (Chin et al., 2009)

Rating	Detection Capability	Probability of Detection
10	Absolute uncertainty	No chance of detection
9	Very remote	Extremely low likelihood of detection
8	Remote	Low likelihood of detection
7	Very low	Slight chance of detection
6	Low	Limited chance of detection
5	Moderate	Moderate ability to detect
4	Moderately high	Fairly reliable detection possible
3	High	High chance of detecting the issue
2	Very high	Very likely to detect potential cause
1	Almost certain	Design control almost always detects the potential cause

Detection refers to the likelihood that a failure will be discovered before reaching the end user. The detection rating indicates the effectiveness of existing controls in identifying potential failures. A higher score represents lower chances of detection. The detection scale used in this study is outlined in Table 3.

Once severity, occurrence, and detection are rated, the RPN is determined by multiplying these three values: RPN = S × O × D. Failure modes with the highest RPNs are considered the most critical and should be addressed with priority in the risk management process.

5.2 Fuzzy AHP Method

The fuzzy AHP method according to some studies (Holecek & Talašová, 2016; Tadić et al., 2023) is implemented through several steps as follows.

Step 1 - Structuring the Decision Hierarchy - The first phase involves building a hierarchical structure of the decision problem. This structure should clearly define the overall objective at the top level, followed by the relevant criteria and sub-criteria, and finally, the possible alternatives at the lowest level.

Step 2 - Pairwise Comparisons Using Fuzzy Logic - Next, decision-makers compare elements in pairs at each level of the hierarchy with respect to the element directly above them. While traditional AHP uses Saaty's 1–9 scale, the FAHP version replaces this with triangular fuzzy numbers to handle uncertainty in judgments. The linguistic terms and their corresponding fuzzy numbers are listed in Table 4.

Table 4. Linguistic scale used for assessment

Linguistic Term	Fuzzy Number (Triangular)
Absolutely preferable (AP)	(8,9,10)
Very preferable (VP)	(7,8,9)
Strongly preferable (SP)	(6,7,8)
Pretty preferable (PP)	(5,6,7)
Quite preferable (QP)	(4,5,6)
Moderately preferable (MP)	(3,4,5)
Remotely preferable (RP)	(2,3,4)
Barely preferable (BP)	(1,2,3)
Equally important (EI)	(1,1,2)

Step 3 - Developing the Fuzzy Comparison Matrix - For each group of criteria or sub-criteria, a fuzzy comparison matrix is created. This matrix includes triangular fuzzy numbers that capture the level of preference between each pair of elements.

$$\tilde{\in}=\begin{bmatrix}\tilde{a}_{11} & \cdots & \tilde{a}_{in}\\ \vdots & \ddots & \vdots\\ \tilde{a}_{n1} & \cdots & \tilde{a}_{nn}\end{bmatrix}, \tag{1}$$

Step 4 – Computing Criteria Weights with LFPP - To derive the relative importance of each criterion, the Logarithmic Fuzzy Preference Programming (LFPP) method is applied. Each matrix entry is a triangular fuzzy number $\tilde{a}_{ij} = (l_{ij}, m_{ij}, u_{ij})$, and the logarithmic transformation is used to linearize the relationships between comparisons.

$$\ln \tilde{a}_{ij} \approx (\ln l_{ij}, \ln m_{ij}, \ln u_{ij})\,; i,j = 1,\dots,n, \tag{2}$$

$$Min\,J = (1-\lambda)^2 + M \times \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}(\delta_{ij}^2 + \eta_{ij}^2), \tag{3}$$

$$s.t.\begin{cases} x_i - x_j - \lambda\ln(m_{ij}/l_{ij}) + \delta_{ij} \geq \ln l_{ij}, i = 1,\dots,n-1; j = i+1,\dots,n\\ -x_i + x_j - \lambda\ln(u_{ij}/m_{ij}) + \eta_{ij} \geq -\ln u_{ij}, i = 1,\dots,n-1; j = i+1,\dots,n\\ \lambda, x_i \geq 0, i = 1,\dots,n\\ \delta_{ij}, \eta_{ij} \geq 0, i = 1,\dots,n-1; j = i+1,\dots,n \end{cases}, \tag{4}$$

where, x_i^* represents the optimal score for criterion i, and $M = 10^3$ is a large constant ensuring feasibility. On the other hand, the variables δ_{ij} and η_{ij} are included to maintain non-negativity and to satisfy the following logarithmic inequalities:

$$\ln w_i - \ln w_j - \lambda \ln\left(\frac{m_{ij}}{l_{ij}}\right) + \delta_{ij} \geq \ln l_{ij}, i = 1, \dots, n-1; j = i+1, \dots, n, \tag{5}$$

$$-\ln w_i + \ln w_j - \lambda \ln\left(m_{ij}/l_{ij}\right) + \eta_{ij} \geq -\ln u_{ij}, i = 1, \dots, n-1; j = i+1, \dots, n, \tag{6}$$

Once the optimization is complete, normalized crisp weights for each criterion are calculated using:

$$w_j = \frac{w_j^l + 4w_j^m + w_j^u}{6}, j = 1, 2, \dots, n \tag{7}$$

Step 5 – Consistency Check - To validate the reliability of the comparisons, the Consistency Ratio (CR) is evaluated using:

$$CR = \frac{CI}{RI}, \tag{8}$$

The Consistency Index (CI) is defined as (Wind & Saaty, 1980):

$$CI = \frac{Z_{max}-0}{0-1}, \tag{9}$$

where, Z_{max} is the principal eigenvalue of the matrix, and *RI* is the Random Index value from standard AHP tables. A CR value below 0.10 indicates acceptable consistency in the pairwise comparisons.

5.3 ARAS Method

The ARAS method is an MCDM technique that evaluates and ranks alternatives based on their relative closeness to the ideal solution. This method enables integration of all criteria and their respective weights into a single utility function, thereby simplifying complex decision-making, and consists of the following steps (Hatefi et al., 2021; Kozoderović et al., 2025; Sihombing et al., 2021).

Step 1-Constructing the Initial Decision Matrix - The process begins with the development of a decision matrix X, consisting of *m* alternatives and *n* criteria.

$$X = \begin{bmatrix} x_{01} & x_{02} & \cdots & x_{0n} \\ x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix}, \quad i = 0, 1, \dots, m, \quad j = 1, 2, \dots, n \tag{10}$$

where, x_{0j} denotes the ideal value for criterion j. If the ideal value is not predefined, it is determined as:

$$x_{0j} = \max_i x_{ij}, \quad for\ benefit\ criteria \tag{11}$$

$$x_{0j} = \min_i x_{ij}, \quad for\ cost\ criteria \tag{12}$$

Step 2-Normalizing the Decision Matrix - The matrix is normalized to eliminate the effects of different scales, resulting in a normalized matrix $\bar{X}$. The elements $\bar{x}_{ij}$ are calculated as follows:

$$\bar{X} = \begin{bmatrix} \bar{x}_{01} & \bar{x}_{02} & \cdots & \bar{x}_{0n} \\ \bar{x}_{11} & \bar{x}_{12} & \dots & \bar{x}_{1n} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{m1} & \bar{x}_{m2} & \cdots & \bar{x}_{mn} \end{bmatrix}, \quad i = 0, 1, \dots, m, \quad j = 1, 2, \dots, n \tag{13}$$

For benefit-type criteria:

$$\bar{x}_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \tag{14}$$

For cost-type criteria:

$$\bar{x}_{ij} = \frac{1}{x_{ij}^*}, \qquad \bar{x}_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \tag{15}$$

Step 3-Forming the Weighted Normalized Matrix - The normalized values are multiplied by the corresponding weights w_j of each criterion, producing the weighted matrix $\hat{X}$:

$$\hat{X} = \begin{bmatrix} \hat{x}_{01} & \hat{x}_{02} & \cdots & \hat{x}_{0n} \\ \hat{x}_{11} & \hat{x}_{12} & \cdots & \hat{x}_{1n} \\ \hat{x}_{21} & \hat{x}_{22} & \cdots & \hat{x}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{x}_{m1} & \hat{x}_{m2} & \cdots & \hat{x}_{mn} \end{bmatrix}, \quad i = 0,1,\dots,m, \quad j = 1,2,\dots,n \tag{16}$$

$$\hat{x}_{ij} = \bar{x}_{ij} \times w_j, \qquad i = 0,1,\dots,m \tag{17}$$

Step 4-Calculating the Optimality Function and Utility Degree - The optimality function S_i is calculated for each alternative:

$$Si = \sum_{j=1}^{n} \hat{x}_{ij}, \qquad i = 0,1,\dots,m \tag{18}$$

where, S_i represents the optimality function for alternative *i*. The alternative with the highest S_i is considered the most desirable. The utility degree K_i of each alternative is then determined by comparing it to the ideal alternative S_0.

$$K_i = \frac{S_i}{S_0}, \qquad i = 0,1,\dots,m \tag{19}$$

The utility degree K_i ranges between 0 and 1, with higher values indicating more favorable alternatives.

6. Numerical Example

As outlined in the methodology section, the first step involved the application of the FMEA method in order to calculate the Risk Priority Number (RPN) for each identified risk. These RPN values served as input data for the subsequent Multi-Criteria Decision-Making (MCDM) evaluation process, specifically during the construction of the initial decision matrix. Each risk was assessed using the scales defined in the Methodology section, resulting in the quantification of individual RPN scores (Table 5). For the purposes of this study, the following risks were analyzed, each of which also represents an alternative in the MCDM framework:

- R1: Theft Risk (A1) – the risk of goods being stolen during transportation
- R2: Smuggling Risk (A2) – the risk associated with the illegal movement of goods
- R3: Terrorism Risk (A3) – potential threats stemming from terrorist activities
- R4: Corruption Risk (A4) – the risk of unlawful involvement of employees or institutions in illicit practices
- R5: Documentation Fraud (A5) – the risk of forgery involving paperwork, invoices, customs documentation, etc.
- R6: Cyber-attacks on IT Systems (A6) – risks arising from hacking, data breaches, or software manipulation
- R7: Sabotage in Supply Chains (A7) – intentional disruption or damage to logistics processes by employees or third parties
- R8: Unauthorized Transport of Hazardous Materials (A8) – the risk of transporting materials in violation of international safety regulations
- R9: Human Errors (A9) – risks resulting from incorrect handling, documentation errors, or procedural failures

Based on the obtained results, it can be concluded that the risk with the highest RPN value—and thus the highest priority—is R1 (Theft Risk), while the risk with the lowest RPN value is R7 (Sabotage in Supply Chains). These RPN values were subsequently used in the development of the initial decision matrix.

In the next phase of the model implementation, the fuzzy AHP method was applied to determine the weights of the criteria used in the risk evaluation process. Specifically, the risks considered in this study were assessed according to the following criteria:

- C1: Security Impact – potential harm to the physical safety of people and goods
- C2: Cost Impact – financial consequences associated with the risk
- C3: Reputation Impact – the extent to which the risk can damage the company's reputation
- C4: Legal Risk – the degree to which the risk involves legal violations or regulatory consequences

- C5: Historical Occurrence – frequency of past occurrences of the risk
- C6: Recovery Time – the time required for the logistics system to recover from the impact
- C7: Spread – whether the risk is localized or has broader, possibly global, implications
- C8: FMEA (RPN) Rating – defines the severity and priority level of the risk

The application of the fuzzy AHP method began with pairwise comparisons of the criteria, using the linguistic scale presented in Table 4. Based on this, the corresponding fuzzy pairwise comparison matrix was constructed and is shown in Table 6.

Subsequently, by applying Eqs. (1) through (7), the weights of each criterion were calculated, as presented in Table 7.

Based on the values from Table 7, it can be concluded that criterion C2 has the greatest weight and, therefore, importance, while criterion C7 has the least weight. After defining the input parameters, each of the identified risks was evaluated against all the criteria, resulting in the formation of the initial decision matrix (Table 8).

Table 5. FMEA results

Risks	S	O	D	RPN
R1: Theft Risk	8	8	10	640
R2: Smuggling Risk	8	6	5	240
R3: Terrorism Risk	10	3	10	300
R4: Corruption Risk	7	5	7	245
R5: Documentation Fraud	6	4	7	168
R6: Cyber-attacks on IT systems	10	4	6	240
R7: Sabotage in supply chains	8	3	6	144
R8: Unauthorized transport of hazardous materials	10	6	4	240
R9: Human errors	8	9	5	360

Table 6. Pairwise comparison

	C1	C2	C3	C4	C5	C6	C7	C8
C1	/	1 1 2	4 5 6	2 3 4	3 4 5	1 2 3	5 6 7	2 3 4
C2		/	3 4 5	3 4 5	4 5 6	2 3 4	4 5 6	2 3 4
C3			/	1 1 2	1 2 3	1 1 2	2 3 4	1 1 2
C4				/	2 3 4	2 3 4	3 4 5	1 2 3
C5					/	1 1 2	2 3 4	1 1 2
C6						/	3 4 5	1 1 2
C7							/	1 1 2
C8								/

Table 7. Criteria weights

Criteria	Lower	Medium	Upper	w_{crisp}
C1	0.235	0.261	0.29	0.2615
C2	0.24	0.278	0.278	0.27165
C3	0.084	0.086	0.109	0.0895
C4	0.102	0.125	0.133	0.1225
C5	0.062	0.063	0.08	0.067
C6	0.07	0.083	0.094	0.082666667
C7	0.035	0.035	0.04	0.037183
C8	0.052	0.07	0.071	0.068

Table 8. Initial decision-making matrix

	C1	C2	C3	C4	C5	C6	C7	C8
Weights	0.2615	0.27165	0.0895	0.1225	0.067	0.082666667	0.037183	0.068
A1	6	7	6	4	8	5	8	640
A2	5	6	7	7	6	4	7	240
A3	9	8	9	9	2	2	6	300
A4	4	6	8	8	7	4	7	245
A5	3	7	7	9	6	5	6	168
A6	7	8	8	6	5	6	9	240
A7	8	7	7	6	3	3	5	144
A8	9	9	8	9	4	3	4	240
A9	5	6	5	4	9	6	6	360

As shown in the table, all alternatives were evaluated across all criteria—except for the last one—using a scale from 1 to 10. The first step in applying the ARAS method involved determining the optimal value for each criterion (Table 9).

Thereafter, the initial decision matrix was normalized using Eqs. (14)-(15), resulting in the normalized decision matrix (Table 10).

In the next step, the criterion weights obtained through the fuzzy AHP method were applied in order to construct the weighted decision matrix (Table 11).

In the penultimate step, the value of the optimality function was determined, which served as the basis for ranking the alternatives in the final step (Table 12).

Finally, in the last step, the degree of utility was calculated, based on which the final ranking of the alternatives was performed (Table 13). As shown, A5 emerged as the best-ranked alternative, followed by A9, A4, A2, A1, A7, A6, A3, and lastly, A8, which was identified as the worst-ranked alternative.

Table 9. Optimal values

	C1	C2	C3	C4	C5	C6	C7	C8
Optimal value	3	6	5	4	2	6	4	144

Table 10. Normalized decision-making matrix

	C1	C2	C3	C4	C5	C6	C7	C8
Optimal value	0.1689	0.1144	0.1350	0.1484	0.2003	0.1364	0.1452	0.1575
A1	0.0845	0.0981	0.1125	0.1484	0.0501	0.1136	0.0726	0.0354
A2	0.1013	0.1144	0.0964	0.0848	0.0668	0.0909	0.0830	0.0945
A3	0.0563	0.0858	0.0750	0.0660	0.2003	0.0455	0.0968	0.0756
A4	0.1267	0.1144	0.0844	0.0742	0.0572	0.0909	0.0830	0.0926
A5	0.1689	0.0981	0.0964	0.0660	0.0668	0.1136	0.0968	0.1350
A6	0.0724	0.0858	0.0844	0.0989	0.0801	0.1364	0.0645	0.0945
A7	0.0633	0.0981	0.0964	0.0989	0.1336	0.0682	0.1162	0.1575
A8	0.0563	0.0763	0.0844	0.0660	0.1002	0.0682	0.1452	0.0945
A9	0.1013	0.1144	0.1350	0.1484	0.0445	0.1364	0.0968	0.0630

Table 11. Weighted normalized decision-making matrix

	C1	C2	C3	C4	C5	C6	C7	C8
Optimal value	0.0442	0.0311	0.0121	0.0182	0.0134	0.0113	0.0054	0.0107
A1	0.0221	0.0266	0.0101	0.0182	0.0034	0.0094	0.0027	0.0024
A2	0.0265	0.0311	0.0086	0.0104	0.0045	0.0075	0.0031	0.0064
A3	0.0147	0.0233	0.0067	0.0081	0.0134	0.0038	0.0036	0.0051
A4	0.0331	0.0311	0.0076	0.0091	0.0038	0.0075	0.0031	0.0063
A5	0.0442	0.0266	0.0086	0.0081	0.0045	0.0094	0.0036	0.0092
A6	0.0189	0.0233	0.0076	0.0121	0.0054	0.0113	0.0024	0.0064
A7	0.0166	0.0266	0.0086	0.0121	0.0089	0.0056	0.0043	0.0107
A8	0.0147	0.0207	0.0076	0.0081	0.0067	0.0056	0.0054	0.0064
A9	0.0265	0.0311	0.0121	0.0182	0.0030	0.0113	0.0036	0.0043

Table 12. Optimality function values

Alternatives	S_i
Optimal value	0.1463
A1	0.0948
A2	0.0981
A3	0.0788
A4	0.1016
A5	0.1142
A6	0.0874
A7	0.0936
A8	0.0753
A9	0.1100

Table 13. Degree utility and alternative ranking

Alternatives	K_i	Ranking
A1	0.6481	5
A2	0.6705	4
A3	0.5382	8
A4	0.6943	3
A5	0.7803	1
A6	0.5972	7
A7	0.6395	6
A8	0.5143	9
A9	0.7517	2

7. Conclusions

This study introduces a comprehensive and methodologically sound approach to managing criminal risks in the field of international logistics. By combining the analytical capabilities of FMEA, the expert-driven prioritization of Fuzzy AHP, and the decision-support functionality of the ARAS method, the framework addresses key vulnerabilities in modern, globally connected supply networks. Threats such as cargo theft, smuggling, organized fraud, and corruption continue to jeopardize operational continuity, financial outcomes, and brand credibility, necessitating a systematic and data-centric method for risk mitigation.

The framework initiates with the recognition and categorization of criminal threats using FMEA, which structures potential failure points and highlights areas of concern. Fuzzy AHP builds upon this by translating expert insight and ambiguity into a quantifiable prioritization of risk factors, effectively managing the uncertainty inherent in subjective evaluations. The final step employs ARAS to assess and rank those risks. To evaluate the proposed model, a ranking of nine criminal risks (theft risk, smuggling risk, terrorism risk, corruption risk, documentation fraud, cyber-attacks on IT systems, sabotage in supply chains, unauthorized transport of hazardous materials, and human errors) was conducted based on eight criteria: security impact, cost impact, reputation impact, legal risk, historical occurrence, recovery time, spread, and the FMEA (RPN) rating.

The results of the model's application showed that the risk with the highest RPN, and thus the highest priority, is R1 (theft risk). Conversely, the risk with the lowest RPN value is R7 (sabotage in supply chains). Furthermore, following the application of the Fuzzy AHP method and the determination of criteria weights, it was concluded that criterion C2 (cost impact) holds the greatest weight, indicating its dominant influence in the decision-making process. In contrast, criterion C7 (spread) received the lowest weight, suggesting it has the least influence among the evaluated criteria.

This research highlights the urgent need for forward-thinking risk strategies, particularly in high-exposure areas such as international entry points, customs facilities, and major transportation routes. The synergy of these three methods allows for a layered and nuanced risk profile that can guide logistics professionals toward optimal resource allocation and targeted risk prevention actions. Operationally, the model contributes to the establishment of best practices for managing logistics security threats. It is applicable across a wide range of transportation and trade sectors, including sea, air, and land logistics, as well as within customs operations and regulatory oversight frameworks. Additionally, the methodology can be tailored to suit specific regional or organizational conditions, making it flexible and scalable. Ultimately, the integration of FMEA, Fuzzy AHP, and ARAS in this research provides a forward-looking and practical tool for confronting criminal risk in global logistics. The framework enhances organizational preparedness, supports smarter decision-making, and reinforces the integrity of international supply chains in an era of increasing complexity and risk exposure.

For future applications, there is a strong case for testing the framework in real-world scenarios, especially across various logistical systems and geographic regions. The integration of dynamic technologies such as real-time monitoring tools, predictive modeling through artificial intelligence, and adaptive criteria systems could significantly enhance the model's responsiveness and accuracy. Broader engagement with stakeholders, ranging from insurance companies and government agencies to global trade institutions, could also ensure that the framework remains inclusive and relevant. Additionally, combining the proposed approach with other methods to develop new hybrid models is also highlighted as a promising direction for future research.

Author Contributions

Conceptualization, M.A. and V.P.; methodology, M.A. and V.P.; software, M.A. and V.P.; writing—original draft preparation, M.A. and V.P.; writing—review and editing, M.A. and V.P. All authors have read and agreed to the published version of the manuscript.

Data Availability

The data supporting our research results are included within the article or supplementary material.

Conflicts of Interest

The authors declare no conflicts of interest.

References

Ahokas, J., Laiho, A., Hintsa, J., Männistö, T., & Holmström, J. (2010). A conceptual model for crime prevention in supply chain management. *In 17th International Annual EurOMA Conference, Porto, Portugal*, 6-9.

Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., & Ghafoor, K. Z. (2023). Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Trans. Eng. Manag.*, *70*(2), 713-739. https://doi.org/10.1109/TEM.2021.3053655.

Cavusgil, S. T., Deligonul, S., Ghauri, P. N., Bamiatzi, V., Park, B. I., & Mellahi, K. (2020). Risk in international business and its mitigation. *J. World Bus.*, *55*(2), 101078. https://doi.org/10.1016/j.jwb.2020.101078.

Cedillo-Campos, M. G., Flores-Franco, J. E., & Covarrubias, D. (2024). A physical internet-based analytic model for reducing the risk of cargo theft in road transportation. *Comput. Ind. Eng.*, *190*, 110016. https://doi.org/10.1016/j.cie.2024.110016.

Chin, K. S., Wang, Y. M., Poon, G. K. K., & Yang, J. B. (2009). Failure mode and effects analysis by data envelopment analysis. *Decis. Support Syst.*, *48*(1), 246–256. https://doi.org/10.1016/j.dss.2009.08.005.

Dobie, K., Glisson, L. M., & Grant, J. (2000). Terrorism and the global supply chain: Where are your weak links? *J. Transp. Manag.*, *12*(1), 57-66. https://doi.org/10.22237/jotm/954547560.

Ekwall, D. (2012). Supply chain risk management: Literature review. *In Risk Management-Current Issues and Challenges*. IntechOpen. http://doi.org/10.5772/48365.

Gurtu, A. & Johny, J. (2021). Supply chain risk management: Literature review. *Risks*, *9*(1), 16. https://doi.org/10.3390/risks9010016.

Hatefi, S. M., Asadi, H., Shams, G., Tamošaitienė, J., & Turskis, Z. (2021). Model for the sustainable material selection by applying integrated dempster-shafer evidence theory and additive ratio assessment (ARAS) method. *Sustainability*, *13*(18), 10438. https://doi.org/10.3390/su131810438.

Holecek, P. & Talašová, J. (2016). A free software tool implementing the fuzzy AHP method. *In Proceedings of the 34th International Conference on Mathematical Methods in Economics*, *6*, 266–271.

Hosen, M. F. (2024). Piracy: Assessing threats to global trade and legal responses through case studies. *Pak. J. Criminol.*, *16*(4), 1167-1188.

Kniaziev, S., Shulzhenko, A., Tymchyshyn, A., Vedenyapina, M., & Stepanova, H. (2024). Investigation of international transport crimes. *Pak. J. Criminol.*, *16*(2), 1-8.

Kozoderović, J., Pajić, V., & Andrejić, M. (2025). A multi-criteria analysis for e-commerce warehouse location selection using SWARA and ARAS methods. *J. Eng. Manag. Syst. Eng.*, *4*(2), 122-132. https://doi.org/10.56578/jemse040204.

Lallerstedt, K. (2022). Global Trade of "Illicit Goods" Its Scale, Consequences, and Addressing the Problem. In *Handbook of Security Science* (pp. 933-954). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-91875-4_73

Liang, X., Fan, S., Lucy, J., & Yang, Z. (2022). Risk analysis of cargo theft from freight supply chains using a data-driven Bayesian network. *Reliab. Eng. Syst. Saf.*, *226*, 108702. https://doi.org/10.1016/j.ress.2022.108702

Männistö, T. A. (2015). *Mitigating crime risks in the international logistics network: The Case of Swiss Post* [Doctoralthesis, EPFL]. https://infoscience.epfl.ch/entities/publication/c373ff9f-b862-4312-9484-80405fc747b0

Najafi, M., Zolfagharinia, H., & Asadi, F. (2023). Angels against demons: Fight against smuggling in an illicit supply chain with uncertain outcomes and unknown structure. *Comput. Ind. Eng.*, *176*, 109007. https://doi.org/10.1016/j.cie.2023.109007.

Rahman, A., Debnath, P., Ahmed, A., Dalim, H. M., Karmakar, M., Sumon, M. F. I., & Khan, M. A. (2024). Machine learning and network analysis for financial crime detection: Mapping and identifying illicit transaction patterns in global black money transactions. *Gulf J. Adv. Bus. Res.*, *2*(6), 250-272. https://doi.org/10.51594/gjabr.v2i6.49

Sihombing, V., Nasution, Z., Al Ihsan, M. A., Siregar, M., Munthe, I. R., Mulia Siregar, V. M., Fatmawati, I., & Asfar, D. A. (2021). Additive Ratio Assessment (ARAS) method for selecting English course branch locations. *J. Phys.: Conf. Ser.*, *1933*(1), 012070. https://doi.org/10.1088/1742-6596/1933/1/012070

Speier, C., Whipple, J. M., Closs, D. J., & Voss, M. D. (2011). Global supply chain design considerations:

Mitigating product safety and security risks. *J. Oper. Manag.*, *29*(7–8), 721-736. https://doi.org/10.1016/j.jom.2011.06.003

Tadić, S., Krstić, M., Dabić-Miletić, S., & Božić, M. (2023). Smart material handling solutions for city logistics systems. *Sustainability*, *15*(8), 6693. https://doi.org/10.3390/su15086693.

Wind, Y. & Saaty, T. L. (1980). Marketing applications of the analytic hierarchy process. *Manag. Sci.*, *26*(7), 641-658. https://doi.org/10.1287/mnsc.26.7.641.