

Research article

Prioritizing cybersecurity initiatives in aviation: A dematel-QSFS methodology

Filiz Mizrak^{a,*}, Gonca Reyhan Akkartal^b

^a Beykoz University, Turkey

^b Istanbul Medipol University, Turkey



ARTICLE INFO

Keywords:

Aviation management
Cybersecurity
Strategic management
Dematel
QSFS
Air Transportation
Logistics Management

ABSTRACT

The aviation industry's growing dependence on digital technologies necessitates robust cybersecurity measures to counter advanced threats. This study integrates the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method with Quantum Spherical Fuzzy Sets (QSFS) to enable precise and reliable decision-making under uncertainty. Key criteria, identified through expert evaluations, include Threat Detection Systems (TDS), Data Encryption Protocols (DEP), Regulatory Compliance (RC), Incident Response Plans (IRP), User Training (UT), Access Control Mechanisms (ACM), and Network Security Solutions (NSS). Analysis using the proposed method revealed that "Regulatory Compliance" and "Threat Detection Systems" are the most influential factors, emphasizing the need for strict adherence to standards and advanced threat detection capabilities. Additionally, the significance of "User Training" and "Data Encryption Protocols" underscores the importance of comprehensive training programs and strong encryption measures. By incorporating strategic management theories such as the Resource-Based View (RBV), Contingency Theory, and Risk Management Theory, this study presents a strategic framework to assist aviation organizations, policymakers, and researchers in developing effective cybersecurity strategies, ensuring the safety and security of global air travel.

1. Introduction

The aviation industry is critical to global transportation and commerce, providing connectivity and facilitating economic growth. As aviation operations become increasingly digitized, the significance of robust cybersecurity measures has never been more crucial. Recent high-profile cybersecurity incidents underscore the urgency and relevance of enhancing aviation cybersecurity.

In July 2024, the Airport and Aviation Services Sri Lanka (AASL) suffered a significant data breach, exposing over 7000 records, including names, national identification numbers, and passport details. This incident highlights the persistent threat posed by cybercriminals targeting sensitive aviation infrastructure (Cyber Security Review, 2024). Furthermore, a July 2023 report from the World Economic Forum emphasized the growing complexity of aviation cybersecurity, noting the industry's vulnerability to diverse cyber threats, including malware, phishing, and ransomware attacks [1].

These incidents are part of a broader trend of escalating cyber threats against the aviation sector. For example, a 2024 breach at AerCap, a major aircraft leasing company, involved hackers accessing sensitive data, though no financial losses were reported (Cyber Security Review). These examples demonstrate the potential for operational disruptions, financial losses, and compromised passenger

* Corresponding author.

E-mail addresses: flzmizrak@gmail.com (F. Mizrak), gonca.akkartal@medipol.edu.tr (G. Reyhan Akkartal).

safety due to cyber-attacks.

This study aims to prioritize cybersecurity initiatives in the aviation sector by evaluating their impacts on system security, operational efficiency, and regulatory compliance. By integrating quantum spherical fuzzy sets (QSFS) into the Decision-Making Trial and Evaluation Laboratory (DEMATEL) technique, the research seeks to analyze the cause-and-effect relationships among various cybersecurity measures such as intrusion detection systems, encryption protocols, and incident response strategies. The goal is to develop a strategic framework that helps aviation organizations enhance their cybersecurity posture effectively.

- What are the most influential cybersecurity initiatives in the aviation sector concerning system security and operational efficiency?
- How do these initiatives interrelate, and what are their cause-and-effect dynamics?
- Which cybersecurity initiative should be prioritized to maximize security and compliance benefits in aviation?

The methodology of this study involves several key steps. Initially, critical cybersecurity initiatives and criteria will be identified and selected. An expert panel of cybersecurity professionals from the aviation industry will provide evaluations through surveys and interviews. The DEMATEL-QSFS methodology will then be applied to construct relational matrices, defuzzify data, normalize relationships, and analyze cause-and-effect interactions among the criteria. Finally, a prioritization framework will be developed based on the analysis to guide strategic cybersecurity initiatives in aviation.

This study's novelty lies in integrating the DEMATEL and QSFS methodologies to address the complexities and uncertainties inherent in aviation cybersecurity. By utilizing QSFS, the study enhances the precision of decision-making under uncertainty, providing a more nuanced understanding of the interrelationships and influences among cybersecurity initiatives. This innovative approach contributes to the theoretical advancement of decision-making methodologies and offers practical insights for aviation cybersecurity management.

2. Conceptual framework

2.1. Definition of cyber attacks

A cyber-attack is a deliberate attempt by malicious entities to disrupt, damage, or gain unauthorized access to computer systems or networks with the motive of exploitation. They are generally aimed at the software, hardware, and information on a shared network. Common goals for a cyber-attack include data exfiltration, disruption of operations, as well as corruption/destruction and availability of information and services. Businesses operating within sectors that have been hit hardest by the pandemic, such as aviation, are further exposed to these threats as digital transformation continues across all industries. Thus, it is very important that we know how to detect and eliminate them – without these measures inclusions being the preservation of the integrity, confidentiality, availability of information systems and digitization process [2,3]

Cyber-attacks are actions with malicious intents directed at information systems to breach data by reducing the integrity, confidentiality, and availability. Examples of these actions are usually centered around data theft and operational disruptions. The increasing penetration of digital technologies into everyday life and business, from personal communications to essential critical infrastructure and national defense systems, has broadened digitally connected environments that can be targeted by cyber threats. This is why we need to know the basics of what cyber-attacks are and how they occur [4].

This trust is the foundation of digital systems working effectively; users need to know that their personal information, financial transactions, and communications are protected. Whilst some argue cyber-attacks need not concern those with nothing to hide—terrorists who ought to be caught or bank fraudsters who deserve to get robbed, for example—it is clear even then that by exposing sensitive information and exploiting system vulnerabilities, these attacks undermine a wider societal trust. Deterioration in trust for the digital systems can obstruct from using online services, which eventually stifles the users from adopting any new technology digitally [5].

Cyber-attacks are costly, and the impacts on a business compound with every new attack. Direct Costs: Changes and costs occur to alleviate an attack, such as hiring cybersecurity professionals, deploying countermeasures as well as paying for ransom loss in case of a successful ransomware incident. This covers things like reputational damage, loss of customer trust, and consequently reduced market share that has long-term effects. Whether they cause a company to earn less money, lay off employees, or go out of business entirely, these can have catastrophic financial impacts on businesses. The true economic impact of cyber-attacks is shown by the average data breach in 2021 costing \$4.24 million [6].

Cyber-attacks can represent a real danger for the national defense. Digital interconnected systems are also being used for critical infrastructure (i.e., power grids, water supply networks, transportation channels, and communication, etc.). Cyber-attacks on these are successful and can result in widespread disruption, economic collapse, and even deaths. Of course, the specter of state-sponsored cyber-attacks that could disrupt a nation's security or economy — or even undermine its political processes is particularly troubling. One example was the Stuxnet worm, designed to infect Iran's nuclear installations, showing that cyber weapons could do actual physical damage and impede critical national ventures [7].

Essential services are vulnerable, too, as evidenced in the compromise of public safety. In the same manner, if a person's data is not protected, their healthcare can be affected via attacks that compromise patient records or even sometimes just disrupt medical access and care with risky results. It is illustrated by a massive ransomware attack WannaCry, 2017, affecting hospitals across the globe and resulting in canceled surgeries and diverted ambulances. That is how much real-world life-threatening affect public health systems can experience due to cyber-attacks. Moreover, the cybersecurity of transportation systems like air traffic control or railway networks is a

real concern since even a single cyber-attack can threaten passenger safety and cause catastrophic accidents.

These days, how can we responsibly assess risks in the absence of insightful cyber-attack understanding when, at the same time, it is becoming more important than ever to understand cyber-attacks with new legal and regulatory landscape developments occurring? Given the need to safeguard our critical infrastructure, coupled with massive scandals regarding data privacy in recent times, it is no surprise that government regulations around the globe are tightening on cybersecurity. For instance, the European Union's General Data Protection Regulation (GDPR) carries some of the toughest data protection requirements and penalties for non-compliance. These are the standards that organizations have to follow, and they should have adequate security measures in place if they do not want to face legal steps or might require you to request them. Organizations need to learn about these rules and ensure cybersecurity compliance (Voigt & von dem Bussche, 2017).

Understanding cyber-attacks also fosters innovation and development in cybersecurity technologies. Researchers and developers can design security solutions with greater resilience by examining the tactics, techniques, and procedures that cyber attackers employ. This proactive nature also generates newer technologies such as AI/ML for threat hunting, Blockchain for loot protection, and Quantum cryptography for better encryption [8]. To be able to engage in this new cyber realm successfully takes ensured investment and commitment into digital resilience from all sectors if we are going to keep growing while having the necessary protection in place for our systems.

2.2. Types of cyberattacks in aviation

Malware, including viruses, worms, trojans, ransomware, spyware, and adware, is one of the major cyber threats encountered online. Malware can enter systems by various means such as phishing emails, compromised websites, or infected USB devices, causing system errors or data breaches [2]. Phishing involves deceptive attempts to acquire sensitive information by posing as a trustworthy entity through emails, messages, or websites. These attacks often target aviation personnel to gain unauthorized access to valuable systems and data Lee & Kim, 2023b. DDoS attacks, on the other hand, flood a service with excessive internet traffic, making it unavailable to genuine users and interfering with critical online services at airports, thereby debilitating airport operations [9].

Ransomware also represents a major menace by encrypting data and demanding payment for the decryption key. In the aviation sector, ransomware can lock key systems, causing operational delays and financial costs [10]. Supply chain attacks can further leverage vulnerabilities in third-party vendors to access larger, more secure targets such as airline and airport systems Bitsight, 2020. The aviation industry has had plenty of mishaps to show the importance of solid cybersecurity in the past decade.

For instance, in July 2015, a DDoS attack paralyzed Heathrow Airport's online services by saturating its web infrastructure with traffic and causing significant system downtime. Airports should deploy solutions for protection against denial-of-service attacks, ensure redundancy in critical services, and conduct regular stress testing to prevent similar incidents ACI World, 2023. In May 2018, the Polish LOT airline's ground operations systems were hacked, causing flight delays and cancellations. This breach illustrates the need for isolating critical systems, conducting regular security audits, and investing in advanced intrusion detection systems Atlantic Council, 2017.

In September 2018, Bristol Airport had its flight information display systems disrupted in a supply chain attack through a compromised third-party service. This event underscored the need for thorough vendor assessments, a robust supply chain cybersecurity framework, and ongoing oversight of third-party access Bitsight, 2020. Ransomware attacks have also significantly impacted airport operations. In April 2020, San Francisco International Airport's web servers were compromised by ransomware, leading to operational issues. Addressing these risks involves reliable backup solutions, regular patching, and employee training on phishing [10].

In October 2020, phishing emails targeting European airports aimed to gain unauthorized access to systems. Essential measures include enhancing email filtering, implementing multi-factor authentication (MFA), and conducting regular phishing simulations for staff Atlantic Council, 2020. Data breaches have posed significant threats as well. In November 2020, sensitive data from the top 100 airports was found exposed on the Dark Web, highlighting the importance of encrypting sensitive data, implementing data loss prevention (DLP) tools, and conducting regular security audits Bitsight, 2020.

3. Literature review

The aviation sector is widely dependent on computing technology used to control vital functions; the most evident part would be air traffic control, but various other aspects, including those within airplanes (in-flight), can be compromised by cyber-related means. Cybersecurity in aviation incorporates measures to ensure the security of these systems and networks from cyber events, including attacks on or unauthorized access to them. Benefits like a reduction in pilot workload and improvements to crew situational awareness can also be seen as constraints when advanced technologies like satellite communications, GPS, and onboard network systems integration improve operational efficiencies but create new vulnerabilities (European Union Aviation Safety Agency [11].

Securing air traffic management (ATM) systems is crucial to ensuring safe and secure air travel. As digital data exchange in ATM processes becomes more important, these systems are increasingly subjected to risks such as unauthorized access and manipulation attacks (International Air Transport Association [12]. Moreover, aircraft themselves have become networked, driven by the Internet of Things (IoT), enabling real-time data transfer between onboard systems and ground control. While this technology enhances communication, it also presents new entry points for cyber attackers [13].

Examples of cyber threats in the aviation domain include attacks against critical infrastructure or vulnerabilities within passenger information systems. Notable events such as the WannaCry ransomware attack and numerous Distributed Denial of Service (DDoS)

attacks have exposed vulnerabilities within the industry, highlighting the need for continuous monitoring and advanced security measures (Federal Aviation Administration [10,14]. Recent studies indicate a growing trend in sophisticated cyber-attacks targeting aviation systems, further emphasizing the urgency for robust cybersecurity frameworks [1].

Recent advancements in the Decision-Making Trial and Evaluation Laboratory (DEMATEL) methodology have significantly contributed to enhancing safety management systems in the aviation sector. Yazdi et al. [15] introduced an improved DEMATEL methodology for effective safety management decision-making, highlighting its application in identifying and prioritizing critical safety factors. Similarly, Ye et al. (2017) applied a FCM-DEMATEL-based approach for flight safety evaluation, demonstrating its effectiveness in improving safety protocols. Further studies by Meng et al. [16] utilized the DEMATEL-ISM method to investigate influencing factors on flight crew safety, providing valuable insights into crew training and safety management. These studies collectively underscore the importance of improving safety management through advanced methodologies.

Transitioning to a focus on resilience, Huang et al. [17] explored the mutual influence relationships of international airport resilience factors using a fermatean fuzzy DEMATEL approach, emphasizing the importance of resilience in aviation safety. This study is complemented by Sharma and Sharma [18], who analyzed the role of multi-agent technology in preventing airplane crashes using AHP and DEMATEL, underlining the technological advancements in aviation safety. Li and Yazdi [19] further developed a dynamic decision-making trial and evaluation laboratory (DEMATEL) to enhance safety management systems, offering a dynamic approach to safety management. The dynamic capabilities of DEMATEL were also explored by Shi et al. [20], who developed an evolutionary model and risk analysis for ship collision accidents using complex networks and DEMATEL, demonstrating its applicability in various high-risk industries.

The application of DEMATEL extends beyond static analysis, incorporating dynamic decision-making approaches. Wagner et al. [21] analyzed the interaction between safety and cybersecurity management systems in automated driving systems using dynamic DEMATEL, offering insights into its application in integrated management systems. Similarly, Torbacki [22] combined DANP and PROMETHEE II methods to assess cybersecurity in Industry 4.0, showcasing the integration of dynamic decision-making methodologies. These studies highlight the evolving nature of decision-making tools in addressing complex safety and cybersecurity challenges.

Further enhancing the decision-making framework, the integration of game theory with DEMATEL has provided new perspectives in safety and reliability decision-making. Li and Yazdi [19] explored progressive decision-making methods in system safety and reliability problems, emphasizing the use of game theory for risk prioritization. Yazdi [23] discussed reliability-centered design and system resilience, highlighting the role of game theory in enhancing system reliability. Li et al. [24] applied Nash equilibrium-based FMEA for risk prioritization in hydrogen refueling station design, demonstrating the practical applications of progressive DEMATEL-game theory in safety management. This approach was further exemplified in their analysis of critical barriers in well-drilling blowouts, providing a robust framework for risk management.

Recent studies post-2020 about cybersecurity have been included to incorporate the latest trends and developments in aviation cybersecurity. Filinovich and Hu [25] discussed cybersecurity threats in aviation, providing a foundational understanding of current challenges. Babu et al. [26] emphasized the importance of proactive cybersecurity measures, while Kumar and Mohanty [27] analyzed current trends in cybersecurity for drones, highlighting emerging threats. Pyzynski and Balcerzak [28] explored the cybersecurity of unmanned aircraft systems, offering insights into protecting these systems from cyber-attacks. Mizrak [29] conducted a comprehensive study on cybersecurity in air traffic control, integrating expert perspectives and literature insights. Janson [30] proposed a multi-layered approach for enhancing cyberspace monitoring in the United States aviation industry, addressing emerging threats. Lastly, Kuleshov et al. (2024) investigated cyber-attacks on avionics networks in a digital twin environment, providing advanced methodologies for detection and defense.

Recent studies further highlight the ongoing challenges and advancements in aviation cybersecurity. Shah, Jhanjhi, and Brohi [31] outline the persistent cybersecurity issues and challenges in civil aviation security, emphasizing the need for integrated cybersecurity strategies that can address both technical and organizational vulnerabilities. They underscore the significance of maintaining robust security measures to prevent unauthorized access and potential disruptions to aviation operations. Sabillon and Bermejo Higuera, (2023) stress the importance of cybersecurity awareness training in the aviation industry. Their study highlights how early detection of cyber threats and vulnerabilities can be significantly improved through comprehensive training programs, which empower aviation personnel to recognize and respond to potential cyber-attacks more effectively.

Pearson and Oni [32] explore the disconnects between cybersecurity and safety in United States Army aviation. Their findings suggest that bridging these gaps through enhanced communication and integrated safety and cybersecurity protocols can lead to more resilient and secure aviation operations. This exploratory qualitative case study provides valuable insights that can be applied to civil aviation contexts to improve overall cybersecurity posture. Asbaş and Tuzlukaya [33] discuss the role of aviation cybersecurity in shielding against cyber threats in the air. They emphasize the integration of advanced technologies and adherence to international cybersecurity standards as crucial components for protecting aviation infrastructure from cyber-attacks. Their research supports the need for continuous improvement in cybersecurity measures to keep pace with evolving threats.

Shueb, Yang, and Che [34] propose an innovative design for improving U.S. airports' cybersecurity based on blockchain technology. Their study demonstrates how blockchain can enhance the security and integrity of aviation systems by providing a tamper-proof ledger for recording transactions and monitoring system activities. This approach offers a promising solution for mitigating cyber risks and ensuring the reliability of airport operations. Moreover, a 2024 report by Resecurity highlights an increase in cyberattacks targeting the aviation and aerospace sectors due to their reliance on interconnected digital infrastructures and global supply chains. The report emphasizes the need for rigorous cybersecurity risk assessments and outlines the types of threat modeling required to achieve a comprehensive security posture [35]. The integration of Industrial Internet of Things (IIoT) technologies has further amplified the attack surface for aerospace organizations, making them more vulnerable to cyber threats [35].

Integrating cybersecurity measures in critical infrastructure sectors such as healthcare, energy, and finance can offer valuable insights for the aviation industry. Each of these sectors has implemented various advanced methodologies to enhance their cybersecurity posture. For example, the financial sector has leveraged the DEMATEL method to analyze and prioritize cyber risks, demonstrating the effectiveness of this approach in managing complex interdependencies within the sector Parachute, 2023. By examining the cybersecurity strategies employed in these sectors, it becomes evident that a multi-faceted and collaborative approach is essential. The adoption of DEMATEL-QSFS in aviation can thus be justified as a robust methodology to address the sector's unique challenges, leveraging insights from its successful application in other domains.

To sum up, cybersecurity in aviation is a complex challenge that requires multi-faceted actions and collaborative approaches among stakeholders. With the ever-evolving cyber threat landscape, the aviation industry must implement innovative, proactive, and adaptive cybersecurity solutions to safeguard its critical infrastructure while enabling safe global air travel. The integration of advanced technologies and adherence to international standards are essential components of a robust cybersecurity framework, as highlighted by recent studies and reports post-2020 [1,36].

3.1. Current cybersecurity initiatives and their effectiveness

A detailed read on the numerous cybersecurity measures initiated by the aviation sector in response to escalating digital and cyber threats Intrusion detection systems, firewalls, encryption protocols and encrypted communication channels are high-tech solutions as primary detections of external threats. Such improvements in threat detection and predictive analysis would largely not have been possible without the use of artificial intelligence (AI) and machine learning (ML). The analysis of huge real-time data by AI-based systems can detect some abnormal behaviors that may or will become threats in the near future, and they could be used as a solid base against cyber-attacks [37].

These strategies have two key ingredients: risk assessment and incident response. Non-stop surveillance — The airports and airlines implement ongoing monitoring systems that enable them to detect and act upon cyber threats quickly. Meanwhile, incident response plans are kept up to date and tested so that security breaches will not catch the organization off guard — or, if they do manage to penetrate a proactive defense, that at least their impact can be minimized and normal operations maintained [9]. Understanding and practicing security controls based on international cybersecurity standards, such as those established by the International Civil Aviation Organization (ICAO) and National Institute of Standards and Technology (NIST), will help enable a stronger system. Compliance guarantees that all the actors in aviation are implementing cyber best practices and prepared for any challenges that evolve [38].

Awareness and training are crucial for cybersecurity. Training programs for employees help them understand risks and best practices related to their digital footprint. Lee & Kim [39] found that regular drills and simulations to recognize signs of attacks helped staff identify and respond to cyber threats, thereby reducing human error. A coordinated effort between airports, airlines, regulators and technology partners are key to mount a collective defense against cyber threats. Sharing information and jointly working on cybersecurity instruments improves the resilience of the aviation sector. This type of collaborative approach is critical when addressing advanced, coordinated cyber-attacks (Ukwandu et al., 2022).

Some of this involves balancing the upfront cost of cybersecurity investments against their proven effectiveness. Cost effective initiatives that can work if they are sustainable. Attempting to measure the return on investment (ROI) in cybersecurity helps a business allocate its resources where they belong, and also gives them weapons for defending expenses in security sheltering additions as well. In sum, the aviation industry in its cybersecurity strategies combines several components from deploying cutting edge technologies to compliance with regulations and human factors through collaborative efforts against cyber-threats. All programmes are improving thanks to the changing landscape of cyber threats so we can secure aviation operations and make flying even safer.

3.2. Related strategic management theories

The integration of cybersecurity measures in the aviation sector can be effectively understood and enhanced through various strategic management theories, including the Resource-Based View (RBV), Contingency Theory, and Risk Management Theory. These theories provide a framework for understanding the importance of cybersecurity as a strategic asset and offer recommendations for aviation companies and policymakers to enhance their cybersecurity posture.

The Resource-Based View (RBV) of the firm posits that organizations can achieve sustained competitive advantage by acquiring and managing valuable, rare, inimitable, and non-substitutable resources Barney, 1991, Wernerfelt, 2020. Recent studies have highlighted that cybersecurity capabilities, such as advanced technologies and skilled personnel, can be considered strategic resources that provide significant protection against cyber threats Shaikh & Siponen, 2023. In the context of aviation cybersecurity, investing in state-of-the-art threat detection systems, data encryption protocols, and comprehensive training programs can differentiate aviation companies from their competitors by enhancing their security posture and reliability. Policymakers can support this by providing incentives for cybersecurity investments and fostering collaborations between industry and academia to develop cutting-edge cybersecurity solutions.

Contingency Theory suggests that the effectiveness of a strategic action depends on the fit between the strategy and the specific context or environment in which it is implemented Donaldson, 2001, Fiedler, 2021. This theory implies that there is no one-size-fits-all approach to strategy, and organizations must tailor their actions to their unique circumstances. Aviation organizations operate in

diverse environments with varying regulatory requirements, technological infrastructures, and threat landscapes. Therefore, cybersecurity strategies must be customized to address these specific challenges and contexts. For instance, an airport in a high-threat region may require more rigorous security measures compared to one in a low-threat area. Aviation companies should conduct thorough risk assessments to identify their unique cybersecurity needs and tailor their strategies accordingly Kankaew & Pongsapak, 2020. Policymakers can facilitate this by providing clear regulatory frameworks that allow flexibility in cybersecurity implementations, enabling organizations to adopt context-specific measures.

Risk Management Theory focuses on identifying, assessing, and prioritizing risks, followed by coordinated efforts to minimize, monitor, and control the probability or impact of adverse events Hillson & Murray-Webster, 2007, Aven, 2020. Effective risk management is crucial in the aviation sector, where cyber threats can have severe operational and safety consequences. Cybersecurity is a critical aspect of risk management in aviation. By proactively identifying potential cyber threats and implementing measures to mitigate them, aviation organizations can protect their assets, ensure passenger safety, and maintain operational integrity. This proactive stance is essential for minimizing the likelihood and impact of cyber incidents. Aviation companies should adopt comprehensive risk management frameworks that integrate cybersecurity considerations, including regular threat assessments, continuous monitoring of cybersecurity landscapes, and the development of robust incident response plans Matiyazova, 2024. Policymakers can support this by promoting best practices in risk management and encouraging information sharing between organizations to enhance collective cybersecurity resilience.

By integrating these strategic management theories, aviation companies can develop more effective cybersecurity strategies that align with their unique operational contexts, manage risks proactively, and leverage valuable resources to maintain competitive advantage. Policymakers play a crucial role in creating an enabling environment that supports these efforts through appropriate regulations and incentives. Recent studies from 2020 to 2024 further reinforce the need for continuous adaptation and resilience in the face of evolving cyber threats, highlighting the importance of a dynamic and comprehensive approach to cybersecurity [40], Parachute, 2023.

3.3. Theoretical frameworks: DEMATEL and QSFS

The study employs two advanced decision-making methodologies: DEMATEL (Decision-Making Trial and Evaluation Laboratory) and QSFS (Quantum Spherical Fuzzy Sets), which provide a robust framework for analyzing intricate, interrelated criteria and enhancing decision-making accuracy under conditions of uncertainty.

DEMATEL is a formidable technique designed to model and analyze the cause-and-effect relationships among criteria within a complex system. This method constructs a matrix to depict the relationships between factors and applies mathematical principles to prioritize these factors based on their influence and dependence. It effectively deconstructs and comprehends the structure of complex problems where criteria are interdependent, transforming these interactions into an intelligible visual representation. This facilitates the identification of the most influential factors and elucidates their mutual impacts. This approach has been extensively employed across various fields to pinpoint critical factors and refine decision-making processes [41].

Integrating QSFS into DEMATEL further augments its effectiveness by addressing uncertainties and imprecisions inherent in decision-making processes. QSFS extends traditional fuzzy set theory by incorporating concepts from quantum theory, such as amplitude and phase angle, allowing for a more nuanced representation of uncertainty. This integration proves particularly advantageous in scenarios where relationships between criteria cannot be precisely defined, thus capturing the degree of influence with greater accuracy. QSFS articulates the inherent fuzziness of real-world problems, providing a clearer depiction of how criteria interact under varying degrees of uncertainty [42,43]

The innovative application of QSFS in conjunction with DEMATEL facilitates a sophisticated analysis that traditional methods may not fully capture. The ability to quantify and model the intensity of influence among criteria using this combined approach yields a more detailed and accurate understanding of the interdependencies within the system. This methodology is instrumental in identifying the most influential criteria, thereby guiding organizations in prioritizing their efforts effectively. By employing this integrated approach, the study contributes to the literature by demonstrating a method that enhances decision-making precision and offers practical insights for strategic planning in complex environments [43].

4. Research methodology

In recent years, the aviation industry has experienced substantial digital transformation, integrating advanced technologies to enhance operational efficiency, passenger experience, and safety. However, this increased reliance on digital systems has exposed the industry to a growing array of cybersecurity threats. Cyber-attacks on aviation infrastructure can have severe consequences, including operational disruptions, financial losses, and compromised passenger safety. The interconnected nature of aviation systems, coupled with the high stakes of maintaining secure and reliable operations, makes cybersecurity a critical concern for stakeholders across the sector.

The selection of this topic is driven by the urgent need to address the evolving cybersecurity landscape in the aviation industry. As digital technologies become more embedded in aviation operations, the potential attack surface for cyber threats expands. Understanding the specific cybersecurity challenges faced by the aviation sector and identifying effective strategies to mitigate these threats is essential for maintaining the integrity, confidentiality, and availability of critical aviation systems.

The purpose of this study is to develop a comprehensive framework for evaluating and prioritizing cybersecurity initiatives in the aviation sector. By leveraging the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method integrated with Quantum

Spherical Fuzzy Sets (QSFS), this research aims to provide a robust analysis of the cause-and-effect relationships among various cybersecurity measures. The study seeks to identify the most critical cybersecurity criteria and offer strategic recommendations to enhance the overall cybersecurity posture of aviation organizations.

4.1. Selection of criteria

The initial step in our methodology involves identifying critical cybersecurity initiatives pertinent to the aviation sector. We selected criteria widely acknowledged as essential for evaluating cybersecurity measures, such as Threat Detection Systems (TDS), Data Encryption Protocols (DEP), Regulatory Compliance (RC), Incident Response Plans (IRP), User Training (UT), Access Control Mechanisms (ACM), and Network Security Solutions (NSS). These criteria were chosen based on a comprehensive review of existing literature and industry standards, as well as insights from past cyberattacks in the aviation sector and industry reports [32], Dave et al., 2024.

To ensure the robustness of our selection, we employed a multi-stage process. Initially, a broad list of potential cybersecurity initiatives was compiled from academic papers, industry reports, and regulatory guidelines. This list was then refined through expert consultation, ensuring that only the most relevant and impactful criteria were included. The final set of criteria reflects a balanced consideration of technical, operational, and compliance-related aspects of cybersecurity.

To add rigor to the study, the selection of expert panel members was carefully considered. We aimed to gather a diverse and highly knowledgeable group of professionals from various segments of the aviation industry, including cybersecurity specialists, regulatory authorities, and industry practitioners. The selection process involved identifying potential experts through professional networks, industry conferences, and recommendations from academic and industry leaders. Criteria for selection included a minimum of 10 years of experience in the aviation or cybersecurity fields, publication of relevant research, and active involvement in industry standards development.

The identified experts were then screened based on their expertise, relevance to the study, and availability to participate. A shortlist was created by assessing their contributions to the field and their practical experience in implementing cybersecurity measures in the aviation sector. Shortlisted experts were formally invited to participate in the study, provided with an overview of the study's objectives, and expected contributions. Upon acceptance, the experts received detailed guidelines and timelines for their input.

Efforts were made to ensure diversity in the panel, including representation from different geographical regions, industry roles (e. g., technical experts, policymakers, and operational managers), and both public and private sectors. This diversity aimed to capture a comprehensive range of perspectives and insights. The expert panel's input was integral to refining the selection criteria and ensuring that the study's findings are robust, relevant, and actionable for the aviation industry. Table 1 details the profiles of the participants.

These experts were selected based on their extensive aviation and cybersecurity experience, academic and professional qualifications, and involvement in industry standards development. The diversity in their roles and geographical distribution ensures a comprehensive range of perspectives and insights.

4.2. Expert panel evaluation

The subsequent phase involved gathering evaluations from a panel of cybersecurity experts. These experts were selected based on their extensive experience in the aviation industry and their expertise in cybersecurity. Each expert possessed a minimum of eight years of experience in the field, ensuring a profound understanding of both the technical and strategic dimensions of aviation cybersecurity.

Data collection was conducted using a combination of surveys and interviews. Surveys were distributed electronically, enabling experts to provide their assessments on the influence and interdependence of the identified criteria. Additionally, in-depth interviews were conducted to gather qualitative insights and allow experts to elaborate on their evaluations. This dual approach ensured a comprehensive and nuanced understanding of the cybersecurity landscape.

Table 1
Profiles of expert panel members.

Participant ID	Role	Qualifications	Geographical Location	Experience
1	Cybersecurity Specialist	MSc in Cybersecurity	Türkiye	15 years
2	Regulatory Authority Advisor	PhD in Information Security	Türkiye	12 years
3	Aviation Industry Practitioner	BSc in Computer Science	Türkiye	10 years
4	Cybersecurity Specialist	MSc in Network Security	Türkiye	14 years
5	Regulatory Authority Advisor	MSc in Aviation Safety	Türkiye	11 years
6	Aviation Industry Practitioner	BSc in Information Technology	Türkiye	13 years
7	Cybersecurity Specialist	PhD in Cybersecurity	Germany	16 years
8	Aviation Industry Practitioner	MSc in Systems Engineering	Germany	12 years
9	Cybersecurity Specialist	MSc in Information Assurance	Türkiye	10 years
10	Regulatory Authority Advisor	BSc in Cyber Forensics	Türkiye	14 years
11	Aviation Industry Practitioner	MSc in Cyber Risk Management	Türkiye	11 years
12	Cybersecurity Specialist	PhD in Information Security	Germany	17 years

4.3. Application of DEMATEL-QSFS methodology

The collected data was processed using the DEMATEL-QSFS methodology. DEMATEL was utilized to analyze and model the cause-and-effect relationships among the cybersecurity initiatives. This method enabled the construction of relational matrices depicting the interactions between various criteria. QSFS was integrated into the DEMATEL framework to address uncertainties and provide a more precise evaluation of the influence levels [43], Wu et al., 2023.

By employing this integrated approach, the intensity of influence among the cybersecurity initiatives was quantified, and they were prioritized based on their overall impact. This methodology enhances decision-making accuracy under conditions of uncertainty and offers practical insights for strategic planning in aviation cybersecurity [42], Mahnaz et al., 2023.

The Decision-Making Trial and Evaluation Laboratory (DEMATEL) method was selected for this study due to its robust capability in modeling and analyzing complex cause-and-effect relationships among interrelated criteria. In the context of aviation cybersecurity, where multiple initiatives and measures interact dynamically, DEMATEL provides a systematic approach to unraveling these intricate dependencies. By converting qualitative assessments into quantitative metrics, DEMATEL facilitates a clearer understanding of the influence and interdependencies among various cybersecurity measures, thereby aiding in strategic decision-making.

Step 1. Identification of Critical Cybersecurity Criteria

We began by identifying essential cybersecurity criteria through a detailed review of literature and consultations with experts. The focus was on key aspects like Threat Detection Systems (TDS), Data Encryption Protocols (DEP), Regulatory Compliance (RC), Incident Response Plans (IRP), User Training (UT), Access Control Mechanisms (ACM), and Network Security Solutions (NSS). A panel of seasoned cybersecurity professionals from the aviation industry was assembled to provide evaluations. These experts, with at least eight years of experience, completed detailed surveys and participated in interviews, offering their insights on the influence and interdependencies among the criteria.

Step 2. Construction and Normalization of the Direct-Relation Matrix

Using the expert evaluations, we constructed a direct-relation matrix to represent how each criterion influences the others. This matrix was then normalized, which means scaling the values to make them comparable. Normalization ensured accurate comparison and analysis, forming the basis for the next steps in the DEMATEL process. Integrating Quantum Spherical Fuzzy Sets (QSFS) helped address uncertainties and ambiguities in the expert evaluations, enhancing the precision of our calculations.

Step 3. Calculation of the Total-Relation Matrix

Next, we calculated the total-relation matrix, which captures both direct and indirect influences among the criteria. This was done by summing the direct influences with all possible indirect influences through a series of matrix operations. The total-relation matrix provided a comprehensive view of the interdependencies, showing how criteria affect each other directly and indirectly.

Step 4. Analysis of Cause-and-Effect Relationships

We then analyzed the total-relation matrix to identify the cause-and-effect relationships among the cybersecurity criteria. By summing the rows and columns, we determined the prominence and net cause/effect values for each criterion. Criteria with positive net values were identified as causes (influential factors), while those with negative net values were identified as effects (influenced factors). This differentiation helped clarify each criterion's role in the overall cybersecurity strategy.

Step 5. Prioritization of Cybersecurity Initiatives

The final step of the DEMATEL process was prioritizing the cybersecurity initiatives based on their influence levels. We focused on criteria with the highest cause values, recommending which initiatives should be prioritized for maximum impact on aviation cybersecurity. This prioritization is crucial for strategic planning, guiding organizations in allocating resources effectively. Initiatives like enhancing Threat Detection Systems (TDS) and ensuring strict Regulatory Compliance (RC) were recommended as top priorities.

Step 6. Validation and Sensitivity Analysis

To ensure the robustness of our findings, we incorporated a validation step. This involved cross-checking the results with additional expert opinions and conducting a sensitivity analysis. Sensitivity analysis tested the stability of the cause-and-effect relationships by slightly altering the input data and observing any significant changes in the outcomes. This step ensured that our prioritizations were reliable and not overly sensitive to minor variations in expert evaluations.

Step 7. Formulation of Strategic Recommendations

Based on the comprehensive analysis, we formulated strategic recommendations to guide aviation organizations in enhancing their cybersecurity measures. The study suggested prioritizing initiatives identified as major causes, such as improving Threat Detection Systems (TDS) and ensuring strict Regulatory Compliance (RC). Additionally, it emphasized the importance of comprehensive User Training (UT) and robust Data Encryption Protocols (DEP) to mitigate the impacts of cyber threats effectively. Detailed models and findings are provided in [Appendix A](#) and [Appendix B](#).

5. EMPIRICAL findings

5.1. Disclosure of the criteria

In the study, critical cybersecurity criteria pertinent to the aviation sector were identified through a comprehensive literature

review and expert consultations. The selected criteria include Threat Detection Systems (TDS), Data Encryption Protocols (DEP), Regulatory Compliance (RC), Incident Response Plans (IRP), User Training (UT), Access Control Mechanisms (ACM), and Network Security Solutions (NSS). Table 2 presents these criteria along with their descriptions and supporting literature references.

5.2. Total relation matrix

The expert evaluations were used to construct the total-relation matrix, capturing both direct and indirect influences among the criteria. Table 3 displays the total relation matrix, highlighting the interdependencies among the selected cybersecurity criteria.

To better illustrate the relationships among the criteria, a heat map was created from the total relation matrix (Fig. 2) (see Fig. 1). The heat map visually represents the strength of the relationships, where darker shades indicate stronger influences.

The heat map above illustrates the total relation matrix for the cybersecurity criteria. The intensity of the color represents the strength of the relationship between criteria, with darker shades indicating stronger influences. For example, the relationship between "Threat Detection Systems (TDS)" and "Data Encryption Protocols (DEP)" is strong, as indicated by the darker color in the corresponding cell. This visual aid helps to quickly identify the most significant interdependencies among the criteria, providing insights into the complex network of influences in the aviation cybersecurity framework.

5.3. Total relation matrix for cybersecurity dimensions

The total relation matrix was also constructed for cybersecurity dimensions, focusing on confidentiality, integrity, availability, accountability, and non-repudiation to provide a more detailed view. Table 4 illustrates the relationships among these dimensions.

5.4. Global and local weights of disclosure criteria

The empirical analysis included calculating the global and local weights of the disclosure criteria, allowing for the prioritization of cybersecurity initiatives based on their influence and dependencies. Table 5 summarizes these weights and ranks the criteria accordingly.

The findings show how the different disclosure criteria are connected. The table lists the calculated weights for each criterion, showing their cause factors ($r(i)$), effect factors ($c(j)$), total effect ($r(i) + c(j)$), and net effect ($r(i) - c(j)$). The cause factors ($r(i)$) tell us how much a criterion influences others. The effect factors ($c(j)$) show how much a criterion is influenced by others. The total effect ($r(i) + c(j)$) gives the overall impact of each criterion, while the net effect ($r(i) - c(j)$) reveals whether a criterion is mainly a cause (positive net effect) or an effect (negative net effect). Local weights are found by dividing the total effect of a criterion by the total effects of all criteria in the same group. Global weights are determined by dividing a criterion's local weight by the sum of the local weights of all criteria across all groups. The ranking column then orders the criteria based on their global weights, indicating their relative importance.

The empirical analysis included calculating the global and local weights of the disclosure criteria, allowing for the prioritization of cybersecurity initiatives based on their influence and dependencies. To further clarify the impact of each criterion, a bar chart was created to display the cause-and-effect weights (Fig. 3). This visualization helps quickly identify which criteria are the most influential and the most affected (see Fig. 4).

Additionally, the cause-and-effect relationships among the criteria were analyzed using the DEMATEL method. Fig. 3 provides a cause-and-effect diagram that illustrates these relationships. The arrows indicate the direction of influence, with the thickness representing the strength of the relationship.

The cause-and-effect diagram above visualizes the direct influences each criterion has on others within the aviation cybersecurity framework. For example, "Threat Detection Systems (TDS)" significantly influences "Data Encryption Protocols (DEP)" and "Network Security Solutions (NSS)," as indicated by the arrows pointing from TDS to these criteria. This diagram helps to understand the complex

Table 2
Disclosure of the criteria.

Criteria	Description	Literature (References)
Threat Detection Systems (TDS)	Systems and processes designed to identify and mitigate potential cyber threats.	Airbus [13]; Federal Aviation Administration (FAA) (2019)
Data Encryption Protocols (DEP)	Methods and technologies used to secure digital data by converting it into a coded format to prevent unauthorized access.	EASA [11]; IATA [12]
Regulatory Compliance (RC)	Adherence to industry standards and legal requirements to ensure cybersecurity measures are up to date and effective.	ICAO [44]; European Union Aviation Safety Agency (EASA) (2020)
Incident Response Plans (IRP)	Strategies and procedures established to respond effectively to cybersecurity incidents and breaches.	Ukwandu et al. [9]; Gnatyuk et al. [38]
User Training (UT)	Programs aimed at educating staff on cybersecurity best practices and awareness to reduce human error.	Lee & Kim [39]; Parker & Christofides, (2023)
Access Control Mechanisms (ACM)	Security measures that regulate who can view or use resources in a computing environment.	Airbus [13]; ICAO [44]
Network Security Solutions (NSS)	Comprehensive measures and technologies implemented to protect the integrity, confidentiality, and availability of network resources.	Federal Aviation Administration (FAA) (2019); EASA [11]

Table 3
Total relation matrix.

Criteria	TDS	DEP	RC	IRP	UT	ACM	NSS
TDS	1.0	0.8	0.7	0.6	0.5	0.4	0.3
DEP	0.8	1.0	0.7	0.6	0.5	0.4	0.3
RC	0.7	0.7	1.0	0.6	0.5	0.4	0.3
IRP	0.6	0.6	0.6	1.0	0.5	0.4	0.3
UT	0.5	0.5	0.5	0.5	1.0	0.4	0.3
ACM	0.4	0.4	0.4	0.4	0.4	1.0	0.3
NSS	0.3	0.3	0.3	0.3	0.3	0.3	1.0

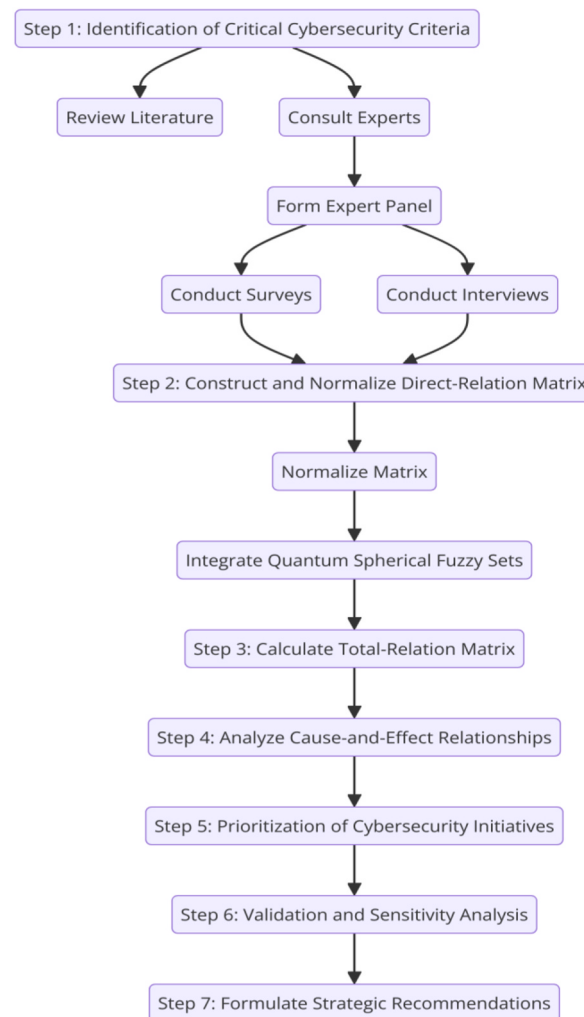


Fig. 1. DEMATEL-QSFS workflow.

network of relationships and the directional impacts among the criteria, providing valuable insights for prioritizing cybersecurity measures and understanding their interdependencies.

6. Discussion

The use of Quantum Spherical Fuzzy Sets (QSFS) combined with the DEMATEL procedure in this study has provided significant insights into the cybersecurity environment in the aviation industry. The analysis allows for a thorough understanding of the association between various cybersecurity-related activities and the strategic support needed to enhance cybersecurity in aviation.

From the empirical analysis, the two most influential criteria were Regulatory Compliance (RC) and Threat Detection Systems

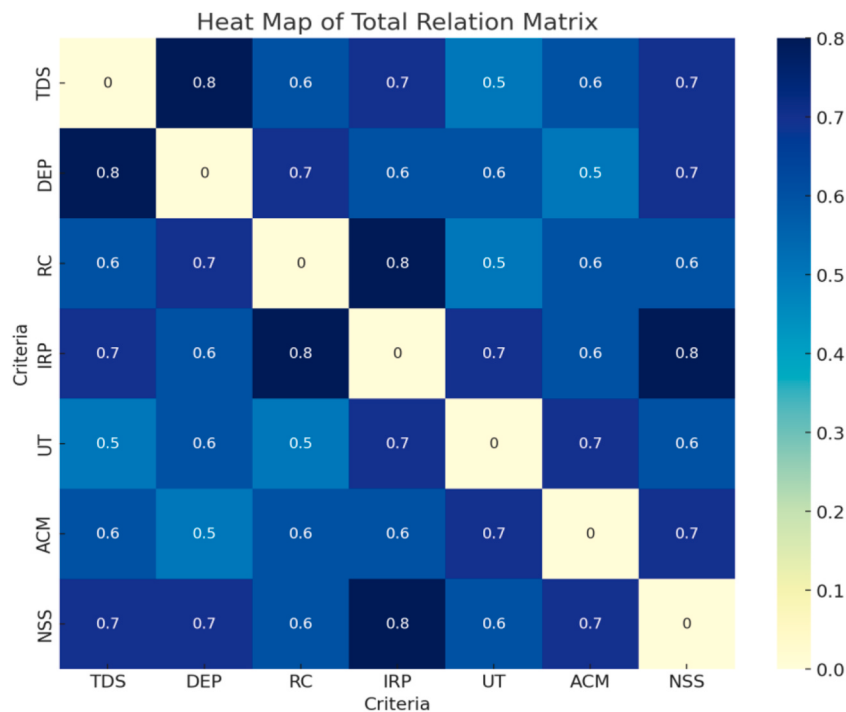


Fig. 2. Heat map of total relation matrix.

Table 4

Total relation matrix for cybersecurity dimensions.

Dimensions	Confidentiality	Integrity	Availability	Accountability	Non-repudiation
Confidentiality	1.0	0.7	0.6	0.5	0.4
Integrity	0.7	1.0	0.7	0.6	0.5
Availability	0.6	0.7	1.0	0.7	0.6
Accountability	0.5	0.6	0.7	1.0	0.7
Non-repudiation	0.4	0.5	0.6	0.7	1.0

(TDS), which had high cause weights of 0.20 and 0.25, respectively. This indicates that regulatory compliance is crucial for developing a robust cybersecurity framework, ensuring adherence to industry standards and legal requirements, thereby bolstering the organization's security posture. Effective threat detection systems are essential for recognizing and mitigating potential cyber threats before they materialize. For example, the WannaCry ransomware attack in 2017 caused significant disruptions across various sectors but could have been mitigated with robust threat detection systems. These findings align with existing literature that highlights the importance of regulatory compliance and advanced threat detection in building a strong security posture [11,44].

User Training (UT), with a high effect weight of 0.16, and Data Encryption Protocols (DEP), with an effect weight of 0.22, further underscore the need for comprehensive user training programs. These programs empower personnel with the knowledge and skills necessary to utilize advanced cybersecurity systems and respond to cyber threats effectively. Advanced data encryption protocols ensure the confidentiality and integrity of sensitive information, protecting it from unauthorized access and cyberattacks. The 2020 ransomware attack on San Francisco International Airport highlighted the critical need for robust data encryption protocols to safeguard sensitive data. Similarly, the results of this study are consistent with previous research emphasizing the importance of user training and strong encryption measures in cybersecurity protection.

Implementing these prioritized cybersecurity initiatives presents several challenges for aviation organizations. Firstly, integrating advanced threat detection systems (TDS) and data encryption protocols (DEP) requires significant investment in technology and infrastructure. Many aviation organizations operate on tight budgets, and allocating sufficient resources for cybersecurity enhancements can be difficult. Additionally, there may be resistance to change within the organization, particularly if employees are not adequately trained or aware of the importance of these new systems.

To overcome these challenges, aviation organizations can seek funding and support from industry partners and government agencies. Collaborating with other stakeholders in the aviation sector can also facilitate the sharing of resources and expertise, reducing the financial burden on individual organizations. Furthermore, implementing a comprehensive user training program is crucial to ensure that all employees understand the importance of cybersecurity and are equipped with the necessary skills to utilize

Table 5
Global and local weights of disclosure criteria.

Disclosure Criteria	Description	$r(i)r(i)$ Cause Factors	$c(j)c(j)$ Effect Factors	$r(i) + c(j)r$ (i) + c(j) Total Effect	$r(i) - c(j)r$ (i) - c(j) Net Effect	Local Weights	Global Weights	Rankings
TDS	Systems and processes designed to identify and mitigate potential cyber threats.	250	200	450	50	0.25	0.0833	1
DEP	Methods and technologies used to secure digital data by converting it into a coded format to prevent unauthorized access.	220	180	400	40	0.22	0.0733	2
RC	Adherence to industry standards and legal requirements to ensure cybersecurity measures are up to date and effective.	200	220	420	-20	0.20	0.0667	3
IRP	Strategies and procedures established to respond effectively to cybersecurity incidents and breaches.	180	170	350	10	0.18	0.0600	4
UT	Programs aimed at educating staff on cybersecurity best practices and awareness to reduce human error.	160	150	310	10	0.16	0.0533	5
ACM	Security measures that regulate who can view or use resources in a computing environment.	140	130	270	10	0.14	0.0467	6
NSS	Comprehensive measures and technologies implemented to protect the integrity, confidentiality, and availability of network resources.	120	110	230	10	0.12	0.0400	7

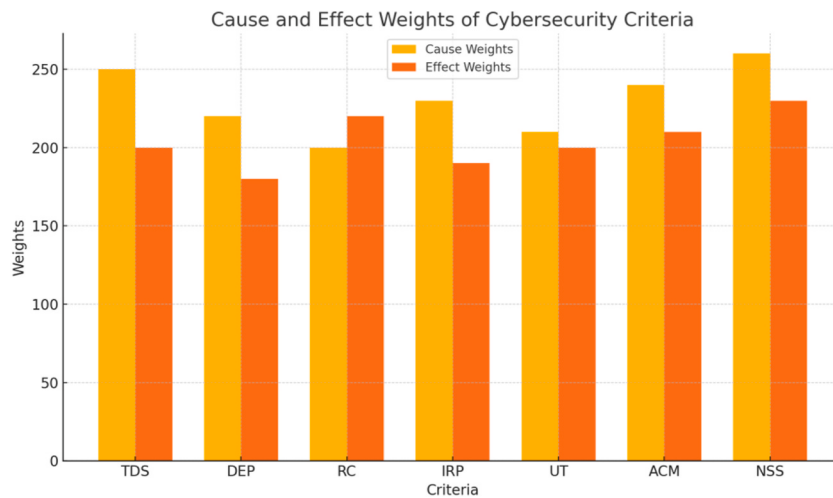


Fig. 3. Cause and effect of weights of cybersecurity criteria.

new systems effectively. Regular training sessions, workshops, and simulations can help reinforce the importance of cybersecurity and prepare employees to respond to potential threats.

Another challenge is ensuring regulatory compliance (RC). Aviation organizations must navigate a complex landscape of international, national, and industry-specific regulations. Compliance with these regulations is mandatory and essential for maintaining the trust and confidence of passengers and stakeholders. However, staying up-to-date with evolving regulations and ensuring compliance can be resource-intensive and challenging. To address this, aviation organizations can invest in compliance management systems that automate the monitoring and reporting of regulatory requirements. Engaging with regulatory bodies and participating in industry forums can also provide valuable insights and guidance on best practices for compliance. Additionally, organizations can conduct regular audits and assessments to identify and address any gaps in their compliance efforts.

The dynamic nature of cyber threats also poses a significant challenge. Cybercriminals continuously evolve their tactics, making it essential for aviation organizations to adopt proactive and adaptive cybersecurity measures. This requires a commitment to continuous improvement and staying informed about the latest threat intelligence. Aviation organizations can establish dedicated cybersecurity teams responsible for monitoring emerging threats and implementing appropriate countermeasures. Collaborating with cybersecurity experts and participating in information-sharing networks can also enhance the organization's ability to anticipate and respond to new threats. Regularly updating and testing incident response plans ensures that the organization is prepared to handle cyber incidents

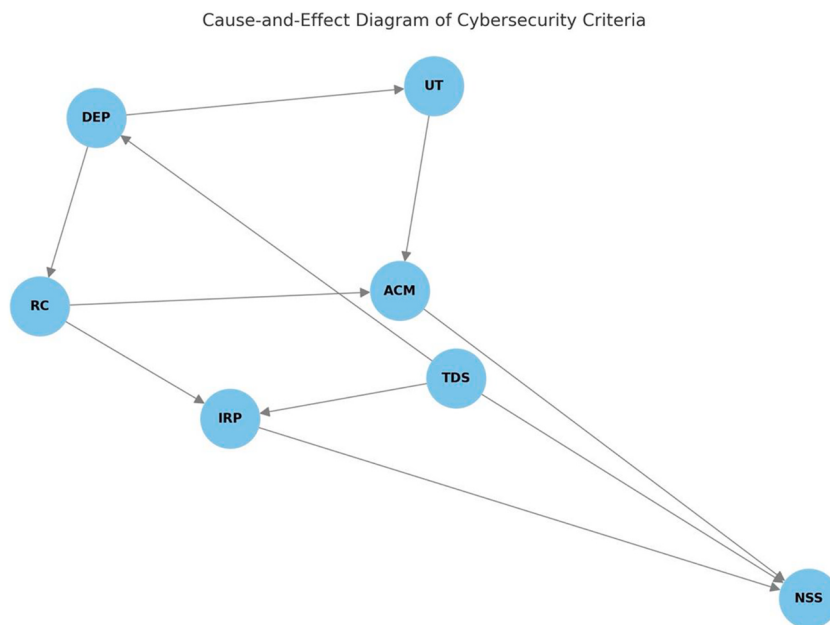


Fig. 4. Cause and effect diagram of cybersecurity criteria.

effectively. By recognizing these challenges and implementing the suggested solutions, aviation organizations can enhance their cybersecurity posture and ensure the safety and security of their operations. This comprehensive approach is essential for addressing the complex and evolving nature of cyber threats in the aviation industry.

In conclusion, integrating DEMATEL and QSFS methodologies provides a robust framework for prioritizing cybersecurity initiatives in the aviation sector. However, the successful implementation of these initiatives requires addressing various challenges, including resource allocation, regulatory compliance, employee training, and adapting to evolving cyber threats. By leveraging industry collaborations, investing in technology and training, and maintaining a proactive stance, aviation organizations can effectively enhance their cybersecurity measures and safeguard their critical infrastructure. Recent studies from 2023 to 2024 support the need for continuous adaptation and resilience in the face of evolving cyber threats, highlighting the importance of a dynamic and comprehensive approach to cybersecurity [40], Parachute, 2023.

7. Implications

These and other implications further deduced by this research indicate normative results vis-à-vis its theoretical and practical implications for the aviation cycle and its operation. The study provides an essential input into improving cybersecurity within aviation through the DEMATEL-QSFS methodology. The study gives an exact direction for scaling cybersecurity initiatives in terms of their level of magnitude for influence and dependence. These results can then be utilized by these organizations in aviation to appropriately allocate resources for the highlighted high-impact areas, such as Threat Detection Systems (TDS) and Regulatory Compliance (RC). Through this specific method or focused manner, effort can also be channeled toward the most significant common benefit to lead to cybersecurity resilience.

The findings emphasize the paramount importance of regulatory compliance in fortifying cybersecurity measures within the aviation sector. It is imperative for aviation organizations to comply with international standards and regulations established by entities such as the International Civil Aviation Organization (ICAO) and the European Union Aviation Safety Agency (EASA). Adherence to these regulations not only mitigates the risks associated with non-compliance but also promotes a cohesive and unified approach to cybersecurity, thereby enhancing overall security across the industry.

Furthermore, the study highlights the necessity of integrating advanced technologies, such as artificial intelligence (AI) and machine learning (ML), into cybersecurity frameworks. These technologies significantly bolster threat detection, continuous monitoring, and incident response capabilities, equipping aviation organizations with the necessary tools to stay ahead of the ever-evolving cyber threat landscape. The implementation of AI and ML can greatly improve the accuracy and speed of identifying potential threats, effectively preventing breaches before they can inflict substantial damage.

Given the significant impact of human factors on cybersecurity, this study underscores the necessity for comprehensive user training programs. Regular training and awareness initiatives equip staff with essential knowledge and skills to identify and respond to cyber threats effectively. By cultivating a culture of cybersecurity awareness, aviation organizations can mitigate the risk of human error and bolster overall security.

Moreover, the study highlights the critical importance of data encryption protocols. Aviation organizations must implement

advanced encryption technologies to safeguard sensitive information from unauthorized access and cyber-attacks. Ensuring data confidentiality and integrity is vital for maintaining operational continuity and protecting passenger information.

This study also advances decision-making methodologies by integrating the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method with Quantum Spherical Fuzzy Sets (QSFS). QSFS enhances decision-making precision by capturing the fuzzy nature of real-world problems, providing a clearer understanding of how criteria interact under varying degrees of uncertainty. This methodological innovation contributes significantly to the theoretical development of multi-criteria decision-making (MCDM) approaches.

By offering a comprehensive analysis of the interdependencies among various cybersecurity criteria, the study deepens our understanding of how these elements interact. This knowledge is essential for developing integrated cybersecurity strategies that address the multifaceted nature of cyber threats. The emphasis on incident response plans (IRP) and regulatory compliance (RC) in enhancing the overall cybersecurity posture of aviation organizations supports this integrated approach.

The findings and methodologies of this study provide a robust framework for future research in aviation cybersecurity. Researchers can build on this work to explore other aspects of cybersecurity, such as the impact of emerging technologies, the role of organizational culture, and the effectiveness of different regulatory frameworks. This study also opens avenues for comparative analyses across different sectors, enhancing the generalizability of the findings.

Additionally, this study enriches the body of literature on aviation cybersecurity by providing empirical evidence on the effectiveness of various cybersecurity measures. By identifying and prioritizing critical cybersecurity criteria, the study offers practical insights that can guide both academic research and industry practice. The integration of advanced decision-making methodologies further enriches the theoretical discourse on cybersecurity.

In practical terms, aviation executives and managers can utilize the study's findings to make informed decisions regarding cybersecurity investments and initiatives. By understanding the relative importance and interdependencies of various cybersecurity criteria, managers can develop strategic plans that maximize the effectiveness of their cybersecurity measures. The prioritization framework provided by the study helps managers allocate resources more efficiently, ensuring that investments in cybersecurity yield the greatest returns in terms of risk mitigation and operational security.

Policymakers and regulators can also use the insights from this study to develop more effective cybersecurity policies and standards. The findings highlight the need for a coordinated approach that integrates advanced technologies and emphasizes regulatory compliance. Policymakers can leverage this information to enhance current reporting practices and contribute to the broader discourse on aviation cybersecurity. Finally, by adopting the study's recommendations, aviation organizations can enhance their resilience against cyber threats. Implementing robust cybersecurity measures, fostering a culture of awareness, and leveraging advanced technologies can significantly improve an organization's ability to withstand and recover from cyber-attacks.

Integrating strategic management theories such as the Resource-Based View (RBV), Contingency Theory, and Risk Management Theory into this research provides valuable insights for improving aviation cybersecurity. The RBV underscores the importance of investing in valuable, rare, inimitable, and non-substitutable resources, such as advanced cybersecurity technologies and skilled personnel, to achieve competitive advantage Shaikh & Siponen, 2023. Contingency Theory highlights the need for context-specific cybersecurity strategies that align with unique regulatory and operational environments Kankaew & Pongsapak, 2020. Risk Management Theory emphasizes proactive risk identification, assessment, and mitigation to protect aviation operations from cyber threats Matiyazova, 2024. By incorporating these theories, the study offers a comprehensive approach to enhancing cybersecurity in the aviation sector, providing actionable recommendations for both aviation companies and policymakers.

In conclusion, this study offers valuable contributions to both the theoretical understanding and practical implementation of cybersecurity in the aviation sector. The insights gained from this research can guide aviation organizations, policymakers, and researchers in developing more effective strategies to address the complex and evolving nature of cyber threats. By prioritizing high-impact initiatives and integrating advanced technologies, the aviation industry can enhance its cybersecurity posture and ensure the safety and security of global air travel.

8. Conclusion

In this study, we aimed to prioritize cybersecurity initiatives in the aviation sector by using the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method along with Quantum Spherical Fuzzy Sets (QSFS). By integrating these advanced decision-making methodologies, we created a robust framework to analyze the complex interdependencies and cause-effect relationships among various cybersecurity measures. Our goal was to improve decision-making accuracy under uncertainty and provide practical insights for strategic planning in aviation cybersecurity.

We started with a comprehensive literature review to identify critical cybersecurity criteria relevant to the aviation industry. Key criteria included Threat Detection Systems (TDS), Data Encryption Protocols (DEP), Regulatory Compliance (RC), Incident Response Plans (IRP), User Training (UT), Access Control Mechanisms (ACM), and Network Security Solutions (NSS). We chose these criteria based on their recognized importance in existing research and industry standards. Next, we collected evaluations from a panel of cybersecurity experts with extensive experience in the aviation sector. The experts provided assessments through surveys and interviews, which we then processed using the DEMATEL-QSFS methodology. This process involved constructing relational matrices, managing uncertainties by defuzzifying the data, normalizing relationships, and analyzing cause-and-effect interactions among the criteria.

The findings showed that Regulatory Compliance (RC) and Threat Detection Systems (TDS) were the most influential criteria, with

significant cause weights. This suggests that enhancing these areas would profoundly impact other cybersecurity measures. User Training (UT) and Data Encryption Protocols (DEP) emerged as critical effect criteria, highlighting the importance of comprehensive training programs and robust encryption protocols in safeguarding aviation cybersecurity. These results are consistent with existing literature and emphasize the multifaceted nature of aviation cybersecurity and the need for a coordinated approach. It is essential to integrate advanced technologies, comply with international standards, and provide continuous training as essential components of a robust cybersecurity framework. The dynamic nature of cyber threats necessitates adaptive and proactive measures to effectively protect critical aviation infrastructure.

However, this study has limitations. Relying on expert evaluations introduces subjectivity, and the sample size of experts may not fully capture the diversity of perspectives in the aviation cybersecurity community. Additionally, the rapidly evolving nature of cyber threats means the findings may need regular updating to remain relevant. Future research should consider expanding the expert panel and exploring the integration of real-time data analytics to complement expert judgments.

The novelty of this study lies in its integration of DEMATEL and QSFS methodologies, which enhances the precision of decision-making under uncertainty. This approach provides a more nuanced understanding of the interrelationships and influences among cybersecurity initiatives, contributing to both the theoretical advancement of decision-making methodologies and practical insights for aviation cybersecurity management.

The integration of Quantum Spherical Fuzzy Sets (QSFS) and the Decision-Making Trial and Evaluation Laboratory (DEMATEL) methodology in this study has provided a robust framework for prioritizing cybersecurity initiatives in the aviation sector. The empirical analysis highlights the critical importance of regulatory compliance (RC) and threat detection systems (TDS) in establishing a strong cybersecurity posture. Additionally, the significance of user training (UT) and data encryption protocols (DEP) underscores the necessity of comprehensive training programs and advanced encryption methods to protect sensitive information.

Implementing these prioritized cybersecurity initiatives poses several challenges, including resource allocation, regulatory compliance, and adapting to evolving cyber threats. However, by leveraging industry collaborations, investing in technology and training, and maintaining a proactive stance, aviation organizations can enhance their cybersecurity measures and safeguard their critical infrastructure.

While this study provides valuable insights, it also opens the door to several avenues for future research. Emerging technologies such as blockchain, artificial intelligence (AI), and quantum computing are rapidly transforming the cybersecurity landscape. Future studies should investigate the impact of these technologies on aviation cybersecurity, exploring how they can be leveraged to enhance threat detection, data protection, and overall security resilience. Additionally, there is a need for research on the integration of cybersecurity measures with other critical systems within aviation, such as air traffic management and in-flight systems, to ensure holistic protection across all operational areas.

Another area for future investigation is the development of advanced compliance management systems that can automate the monitoring and reporting of regulatory requirements. This research could focus on how these systems can be optimized to reduce the resource burden on aviation organizations while ensuring stringent compliance with international, national, and industry-specific regulations. Furthermore, given the dynamic nature of cyber threats, continuous improvement and adaptation are essential. Future research should explore innovative approaches to cybersecurity training and awareness programs that can keep pace with the evolving threat landscape. This includes the use of immersive technologies such as virtual reality (VR) and augmented reality (AR) to create realistic training scenarios that enhance employees' readiness to respond to cyber incidents.

To address the limitation of a small sample size of experts, future studies should aim to include a larger and more diverse group of experts from various regions, roles, and experience levels by leveraging professional networks and industry events. Utilizing mixed-methods approaches, such as combining qualitative evaluations with quantitative surveys, and engaging in continuous expert consultation through workshops and webinars can ensure a more comprehensive understanding of the issues. Leveraging virtual collaboration tools for broader participation and incorporating feedback mechanisms to validate findings will enhance the diversity and robustness of the data, leading to more effective cybersecurity practices in the aviation sector.

In conclusion, the integration of DEMATEL and QSFS methodologies provides a robust framework for prioritizing cybersecurity initiatives in the aviation sector. However, the successful implementation of these initiatives requires addressing various challenges and continuously adapting to the evolving cyber threat landscape. By identifying specific areas for future research, this study aims to provide clear direction for subsequent investigations that can further enhance aviation cybersecurity and ensure the safety and security of global air travel.

Ethics Committee approval statement

This study was approved by the Ethics Committee of Beykoz University in Türkiye. All participants involved in the expert evaluations provided informed consent, and their confidentiality and anonymity were strictly maintained throughout the study.

Data availability statement

The data will be made available upon request.

CRedit authorship contribution statement

Filiz Mizrak: Writing – review & editing, Visualization, Validation, Supervision, Software, Resources, Methodology, Formal

analysis, Conceptualization. **Gonca Reyhan Akkartal:** Writing-review & editing, Resources, Project administration, Investigation, Funding, Data curation, Conceptualization.

Declaration of competing interest

We, Filiz Mizrak and Gonca Reyhan Akkartal, the authors of the study titled "Prioritizing Cybersecurity Initiatives in Aviation: A DEMATEL-QSFS Methodology," declare that we have no financial, personal, or professional conflicts of interest that could have influenced the research and findings presented in this study. Our research was conducted independently, and no funding was received for this study. All sources of information used in this research have been properly acknowledged. We affirm that this study complies with ethical standards and that the data and findings are reported with integrity and transparency.

Appendix A. Quantum Spherical Fuzzy Sets with Golden Cut

Quantum mechanics introduces a novel perspective on decision-making approaches and the complexities of real-world problems [45]. Utilizing quantum theory with amplitude and phase angle components allows for a more efficient consideration of probability. Consequently, the quantum model of the mass function offers various perspectives for understanding the probabilities of multiple conditions [46]. This approach enables a more accurate study of uncertainty using a complex set of quantum logic information. The probability of a quantum mass function, encompassing amplitude and phase angle, has been illustrated [47].

$$Q(|u\rangle) = \phi e^{i\theta} \quad (A1)$$

$$|\varsigma\rangle = \{|u_1\rangle, |u_2\rangle, \dots, |u_n\rangle\} \quad (A2)$$

$$\sum_{|u\rangle \in |\varsigma\rangle} |Q(|u\rangle)| = 1 \quad (A3)$$

ς is the set of collective exhaustive events $|u_i\rangle$, $|Q(|u\rangle)| = \phi^2$ is the amplitude result for the probability of event $|u\rangle$ in the form of quantum logic. $0 \leq \phi^2 \leq 1$ and θ^2 is the phase angle of event $|u\rangle$. $|\phi_1|^2$ is the belief degree to $|u\rangle$, the value of θ is the phase angle of $|u\rangle$ with the range $[0, 360^\circ]$.

Decision-making problems often involve various qualitative and indefinite evaluations that cannot be defined using precise numerical values. This uncertainty necessitates extending decision-making approaches to achieve more accurate results. Fuzzy sets, introduced by Zadeh, are among the most notable methods for addressing complex decision-making models [48]. Since the advent of fuzzy logic, extensions such as type 2 and intuitionistic fuzzy sets have been developed [49]. Recently, spherical fuzzy sets have been employed to enhance result precision using generalized forms of Neutrosophic and Pythagorean fuzzy numbers. This method incorporates the membership, non-membership, and hesitancy degrees of fuzzy numbers into the decision-making process. However, a limitation is that the sum of the squares of these parameters must lie between zero and one. The definition of spherical fuzzy sets $\sim AS$ is provided by Formulas (A4) and (A5) Ashraf et al., 2019.

$$\tilde{A}_S = \{ \langle u, (\mu_{\tilde{A}_S}(u), \nu_{\tilde{A}_S}(u), h_{\tilde{A}_S}(u)) \mid u \in U \} \quad (A4)$$

$$0 \leq \mu_{\tilde{A}_S}^2(u) + \nu_{\tilde{A}_S}^2(u) + h_{\tilde{A}_S}^2(u) \leq 1, \forall u \in U \quad (A5)$$

The probability concepts from quantum theory can be extended using spherical fuzzy sets to address complex decision-making problems, incorporating the amplitude and phase angles of the comprehensive set Akram & Naz, 2019.

$$|\varsigma_{\tilde{A}_S}\rangle = \left\{ \langle u, (\varsigma_{\mu_{\tilde{A}_S}}(u), \varsigma_{\nu_{\tilde{A}_S}}(u), \varsigma_{h_{\tilde{A}_S}}(u)) \mid u \in 2^{|\varsigma_{\tilde{A}_S}|} \right\} \quad (A6)$$

Where, $\varsigma_{\mu_{\tilde{A}_S}}$, $\varsigma_{\nu_{\tilde{A}_S}}$, and $\varsigma_{h_{\tilde{A}_S}}$ are the membership, non-membership, and hesitancy degrees of Quantum Spherical fuzzy sets, respectively. However, the Quantum Spherical fuzzy numbers ς are formalized with the amplitude and phase angles of the fuzzy sets.

$$\varsigma = [\varsigma_\mu \cdot e^{i2\pi \cdot \alpha}, \varsigma_\nu \cdot e^{i2\pi \cdot \gamma}, \varsigma_h \cdot e^{i2\pi \cdot \beta}] \quad (A7)$$

$$\phi^2 = |\varsigma_\mu(|u_i\rangle)| \quad (A8)$$

where, ς_μ , ς_ν , and ς_h are the amplitudes of quantum membership, non-membership, and hesitancy degrees as α , γ , and β are the set of θ phase angles, respectively. ϕ^2 defines the amplitude of membership function ς_μ of quantum fuzzy sets.

Additionally, defining the appropriate membership, non-membership, and hesitancy degrees in spherical fuzzy sets remains a significant challenge in decision-making methods, with no consensus on these scales. To address this issue, the golden ratio can be used to create an optimal balance among the scales of spherical fuzzy sets. Known for its application in geometric patterns, the golden ratio was first explored by Greek mathematicians and later theorists to understand relationships between geometric figures. Previous studies

have linked Fibonacci numbers to the golden ratio Livio, 2008. The golden ratio, G , is defined by dividing a straight line into large and small segments according to the extreme and mean ratios:

$$G = \frac{a}{b} \quad (A9)$$

where $a > b > 0$ and G is the golden cut. Here, a represents the larger segment, and b represents the smaller segment of the straight line. The algebraic expression of the golden cut can be given as:

$$G = \frac{1 + \sqrt{5}}{2} = 1.618... \quad (A10)$$

The amplitude of the non-membership degrees for the quantum spherical fuzzy sets was defined using a golden cut, expressed by the following equation.

$$\varsigma_v = \frac{\varsigma_\mu}{G} \quad (A11)$$

The amplitude of hesitancy degrees is represented by the following equation.

$$\varsigma_h = 1 - \varsigma_\mu - \varsigma_v \quad (A12)$$

Accordingly, the phase angles of the quantum spherical fuzzy sets are provided as follows:

$$\alpha = |\varsigma_\mu(|u_i\rangle)| \quad (A13)$$

α is the phase angle of the membership degrees for the probability of event $|u\rangle$ in the form of quantum spherical fuzzy sets. The phase angle of non-member degrees γ is determined by:

$$\gamma = \frac{\alpha}{G} \quad (A14)$$

The phase angle of hesitancy degrees, β is constructed as follows:

$$\beta = 1 - \alpha - \gamma \quad (A15)$$

X_1 and X_2 are two universes, and $\tilde{A}_5 = (\varsigma_{\mu\tilde{A}} e^{j2\pi \cdot \alpha\tilde{A}}, \varsigma_{v\tilde{A}} e^{j2\pi \cdot \gamma\tilde{A}}, \varsigma_{h\tilde{A}} e^{j2\pi \cdot \beta\tilde{A}})$ and $\tilde{B}_5 = (\varsigma_{\mu\tilde{B}} \cdot e^{j2\pi \cdot \alpha\tilde{B}}, \varsigma_{v\tilde{B}} \cdot e^{j2\pi \cdot \gamma\tilde{B}}, \varsigma_{h\tilde{B}} \cdot e^{j2\pi \cdot \beta\tilde{B}})$ are two quantum spherical fuzzy sets from the universe of discourse X_1 and X_2 . The operation of quantum spherical fuzzy numbers is demonstrated by the following equations:

$$\begin{aligned} \lambda^* \tilde{A}_5 = & \left\{ \left(1 - \left(1 - \varsigma_{\mu\tilde{A}}^2 \right)^\lambda \right)^{\frac{1}{2}} e^{j2\pi \cdot \left(1 - \left(1 - \left(\frac{\alpha\tilde{A}}{2\pi} \right)^2 \right)^\lambda \right)^{\frac{1}{2}}}, \right. \\ & \left. \varsigma_{v\tilde{A}} e^{j2\pi \cdot \left(\frac{\gamma\tilde{A}}{2\pi} \right)^\lambda}, \left((1 - \varsigma_{h\tilde{A}})^2 - \left(1 - \varsigma_{\mu\tilde{A}}^2 - \varsigma_{h\tilde{A}}^2 \right)^\lambda \right)^{\frac{1}{2}} e^{j2\pi \cdot \left(\left(1 - \left(\frac{\beta\tilde{A}}{2\pi} \right)^2 \right)^\lambda - \left(1 - \left(\frac{\alpha\tilde{A}}{2\pi} \right)^2 - \left(\frac{\beta\tilde{A}}{2\pi} \right)^2 \right)^\lambda} \right)^{\frac{1}{2}} \right\}, \lambda > 0 \end{aligned} \quad (A16)$$

$$\begin{aligned} \tilde{A}_5^\lambda = & \left\{ \varsigma_{\mu\tilde{A}} e^{j2\pi \cdot \left(\frac{\alpha\tilde{A}}{2\pi} \right)^\lambda}, \left(1 - \left(1 - \varsigma_{v\tilde{A}}^2 \right)^\lambda \right)^{\frac{1}{2}} e^{j2\pi \cdot \left(1 - \left(1 - \left(\frac{\gamma\tilde{A}}{2\pi} \right)^2 \right)^\lambda \right)^{\frac{1}{2}}}, \right. \\ & \left. \left((1 - \varsigma_{h\tilde{A}})^2 - \left(1 - \varsigma_{v\tilde{A}}^2 - \varsigma_{h\tilde{A}}^2 \right)^\lambda \right)^{\frac{1}{2}} e^{j2\pi \cdot \left(\left(1 - \left(\frac{\beta\tilde{A}}{2\pi} \right)^2 \right)^\lambda - \left(1 - \left(\frac{\gamma\tilde{A}}{2\pi} \right)^2 - \left(\frac{\beta\tilde{A}}{2\pi} \right)^2 \right)^\lambda} \right)^{\frac{1}{2}} \right\}, \lambda > 0 \end{aligned} \quad (A17)$$

$$\begin{aligned} \tilde{A}_5 \oplus \tilde{B}_5 = & \left\{ \left(\varsigma_{\mu\tilde{A}}^2 + \varsigma_{\mu\tilde{B}}^2 - \varsigma_{\mu\tilde{A}}^2 \varsigma_{\mu\tilde{B}}^2 \right)^{\frac{1}{2}} e^{j2\pi \cdot \left(\left(\frac{\alpha\tilde{A}}{2\pi} \right)^2 + \left(\frac{\alpha\tilde{B}}{2\pi} \right)^2 - \left(\frac{\alpha\tilde{A}}{2\pi} \right)^2 \left(\frac{\alpha\tilde{B}}{2\pi} \right)^2 \right)^{\frac{1}{2}}}, \right. \\ & \left. \varsigma_{v\tilde{A}} \varsigma_{v\tilde{B}} e^{j2\pi \cdot \left(\left(\frac{\gamma\tilde{A}}{2\pi} \right) \left(\frac{\gamma\tilde{B}}{2\pi} \right) \right)}, \right. \\ & \left. \left(\left(1 - \varsigma_{\mu\tilde{B}}^2 \right) \varsigma_{h\tilde{A}}^2 + \left(1 - \varsigma_{\mu\tilde{A}}^2 \right) \varsigma_{h\tilde{B}}^2 - \varsigma_{h\tilde{A}}^2 \varsigma_{h\tilde{B}}^2 \right)^{\frac{1}{2}} e^{j2\pi \cdot \left(\left(1 - \left(\frac{\beta\tilde{A}}{2\pi} \right)^2 \right) \left(\frac{\beta\tilde{B}}{2\pi} \right)^2 + \left(1 - \left(\frac{\alpha\tilde{A}}{2\pi} \right)^2 \right) \left(\frac{\beta\tilde{B}}{2\pi} \right)^2 - \left(\frac{\beta\tilde{A}}{2\pi} \right)^2 \left(\frac{\beta\tilde{B}}{2\pi} \right)^2 \right)^{\frac{1}{2}}} \right\} \end{aligned} \quad (A18)$$

$$\left((1 - \varsigma_{v\tilde{B}}^2) \varsigma_{h\tilde{A}}^2 + (1 - \varsigma_{v\tilde{A}}^2) \varsigma_{h\tilde{B}}^2 - \varsigma_{h\tilde{A}}^2 \varsigma_{h\tilde{B}}^2 \right)^{\frac{1}{2}} e^{j2\pi} \cdot \left(\left(1 - \left(\frac{\gamma_{\tilde{B}}}{2\pi} \right)^2 \right) \left(\frac{\beta_{\tilde{A}}}{2\pi} \right)^2 + \left(1 - \left(\frac{\gamma_{\tilde{A}}}{2\pi} \right)^2 \right) \left(\frac{\beta_{\tilde{B}}}{2\pi} \right)^2 - \left(\frac{\beta_{\tilde{A}}}{2\pi} \right)^2 \left(\frac{\beta_{\tilde{B}}}{2\pi} \right)^2 \right)^{\frac{1}{2}} \quad (\text{A19})$$

Appendix B. DEMATEL with QSFS extension

The DEMATEL with QSFS extension involves the following steps:

Step 1: Construct an indirect relationship matrix to assess the degree of dependency among criteria. Collect linguistic evaluations to form these indirect relationship matrices.

Step 2: Define the quantum spherical fuzzy direct relation matrices. Formulate a quantum spherical fuzzy relation matrix by using the indirect relation matrix defined in [Step 1](#). This matrix represents the pairwise intensity of influence, a ij , where i corresponds to the row criterion and j to the column criterion. The matrix is expressed as follows:

$$\varsigma_k = \begin{bmatrix} 0 & \varsigma_{12} & \cdots & \cdots & \varsigma_{1n} \\ \varsigma_{21} & 0 & \cdots & \cdots & \varsigma_{2n} \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \varsigma_{n1} & \varsigma_{n2} & \cdots & \cdots & 0 \end{bmatrix} \quad (\text{B1})$$

ς_{ij} is defined as $\left(\varsigma_{\mu_{ij}} e^{2\pi \cdot \alpha_{ij}}, \varsigma_{\nu_{ij}} e^{2\pi \cdot \gamma_{ij}}, \varsigma_{h_{ij}} e^{2\pi \cdot \beta_{ij}} \right)$, where k is the number of decision-makers. The relation matrices are aggregated across decision-makers. The aggregated values ς of the decision-makers were computed in the form of quantum spherical fuzzy numbers using the following equation:

$$\varsigma = \left\{ \left[1 - \prod_{i=1}^k \left(1 - \varsigma_{\mu_i}^2 \right)^{\frac{1}{k}} \right]^{\frac{1}{2}} e^{2\pi \cdot \left[1 - \prod_{i=1}^k \left(1 - \left(\frac{\alpha_i}{2\pi} \right)^2 \right)^{\frac{1}{k}} \right]^{\frac{1}{2}}}, \prod_{i=1}^k \varsigma_{\nu_i}^{\frac{1}{k}} e^{2\pi \cdot \prod_{i=1}^k \left(\frac{\gamma_i}{2\pi} \right)^{\frac{1}{k}}}, \left[\prod_{i=1}^k \left(1 - \varsigma_{\mu_i}^2 \right)^{\frac{1}{k}} - \prod_{i=1}^k \left(1 - \varsigma_{\mu_i}^2 - \varsigma_{h_i}^2 \right)^{\frac{1}{k}} \right]^{\frac{1}{2}} e^{2\pi \cdot \left[\prod_{i=1}^k \left(1 - \left(\frac{\alpha_i}{2\pi} \right)^2 \right)^{\frac{1}{k}} - \prod_{i=1}^k \left(1 - \left(\frac{\alpha_i}{2\pi} \right)^2 - \left(\frac{\beta_i}{2\pi} \right)^2 \right)^{\frac{1}{k}} \right]^{\frac{1}{2}}} \right\} \quad (\text{B2})$$

Step 3: Defuzzify the quantum spherical fuzzy relation matrices. Compute the defuzzified values, Def_{ς} of Quantum Spherical Fuzzy Sets using the score function:

$$\text{Def } \varsigma_i = \varsigma_{\mu_i} + \varsigma_{h_i} \left(\frac{\varsigma_{\mu_i}}{\varsigma_{\mu_i} + \varsigma_{\nu_i}} \right) + \left(\frac{\alpha_i}{2\pi} \right) + \left(\frac{\gamma_i}{2\pi} \right) \left(\frac{\left(\frac{\alpha_i}{2\pi} \right)}{\left(\frac{\alpha_i}{2\pi} \right) + \left(\frac{\beta_i}{2\pi} \right)} \right) \quad (\text{B3})$$

Step 4: Normalize the direct relation matrices. The normalized direct relationship matrix $B = [b_{ij}]_{n \times n}$ is presented in Eq. [B4](#)

$$B = \frac{\varsigma}{\max_{1 \leq i \leq n} \sum_{j=1}^n \varsigma_{ij}} \text{ where, } 0 \leq b_{ij} \leq 1 \quad (\text{B4})$$

Step 5: Construct the total relation matrices of pairwise influence effects. The total relation matrix $C = [c_{ij}]_{n \times n}$ is defined as:

$$\lim_{k \rightarrow \infty} (B + B^2 + \dots + B^k) = B(I - B)^{-1} \quad (\text{B5})$$

Step 6: The total causes and effects are computed. The cause factors $r(i)$ are listed with the sums of the rows, and the effect factors $c(j)$ are the sums of the columns in Eqs. [\(B6\)](#) and [\(B7\)](#).

$$\mathbf{r}(\mathbf{i}) = \left[\sum_{j=1}^n e_{ij} \right]_{n \times 1} \quad (\text{B6})$$

$$\mathbf{c}(\mathbf{j}) = \left[\sum_{i=1}^n e_{ij} \right]_{1 \times n} \quad (\text{B7})$$

The values $r(i) + c(j)$ indicate the relative importance of the criteria. However, the values of $r(i) - c(j)$ define the direction of the influence of the criteria. The impact-relation directions are represented by using threshold value α as

$$\alpha = \frac{\sum_{i=1}^n \sum_{j=1}^n [e_{ij}]}{N} \quad (\text{B8})$$

where N is the total number of criteria in the matrix. It was assumed that if a criterion in a row had a value higher than the threshold, it affected the criterion of the corresponding column in the matrix.

References

- [1] World Economic Forum, Cybersecurity in aviation: building a resilient future, Retrieved from, <https://www.weforum.org>, 2023.
- [2] H. Malik, S. Tahir, H. Tahir, M. Ihtasham, F. Khan, A homomorphic approach for security and privacy preservation of Smart Airports, *Future Generat. Comput. Syst.* 141 (2023) 500–513.
- [3] P. Stastny, A.M. Stoica, Protecting aviation safety against cybersecurity threats, *IOP Conf. Ser. Mater. Sci. Eng.* 1226 (1) (2022, February) 012025 (IOP Publishing).
- [4] M. Afenyo, L.D. Caesar, Maritime cybersecurity threats: gaps and directions for future research, *Ocean Coast Manag.* 236 (2023) 106493.
- [5] Z. Muhammad, Z. Anwar, B. Saleem, J. Shahid, Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environment sustainability, *Energies* 16 (3) (2023) 1113.
- [6] IBM Security, Cost of a Data Breach Report 2021. Risk Quantification, 73, 2021.
- [7] J.R. Lindsay, Stuxnet and the limits of cyber warfare, *Secur. Stud.* 22 (3) (2013) 365–404.
- [8] D. Saxena, I. Gupta, R. Gupta, A.K. Singh, X. Wen, An AI-driven VM threat prediction model for multi-risks analysis-based cloud cybersecurity, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (2023).
- [9] E. Ukwandu, M.A. Ben-Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, Cyber-security challenges in aviation industry: a review of current and future trends, *Information* 13 (3) (2022) 146.
- [10] S. Kazim, Cybersecurity threats in aviation: an evolving landscape, *Journal of Aviation Security* 10 (2) (2023) 87–104.
- [11] EASA, European union aviation safety agency annual report, Retrieved, <https://www.atc-network.com/atc-news/easa-european-aviation-safety-agency-germany/easa-publishes-annual-safety-review-asr-2020>, 2020.
- [12] IATA, International air Transport association annual review, Retrieved: <https://www.iata.org/en/publications/annual-review/>, 2021.
- [13] Airbus, Airbus annual report 2020, Retrieved: <https://www.airbus.com/en/investors/financial-results-annual-reports>, 2020.
- [14] FAA, Federal aviation administration cybersecurity report, Retrieved: https://www.faa.gov/about/plans_reports/congress, 2019.
- [15] M. Yazdi, F. Khan, R. Abbassi, R. Rusli, Improved DEMATEL methodology for effective safety management decision-making, *Saf. Sci.* 127 (2020) 104705.
- [16] B. Meng, N. Lu, C. Lin, Y. Zhang, Q. Si, J. Zhang, Study on the influencing factors of the flight crew's TSA based on DEMATEL–ISM method, *Cognit. Technol. Work* (2022) 1–15.
- [17] H.C. Huang, C.N. Huang, H.W. Lo, T.M. Thai, Exploring the mutual influence relationships of international airport resilience factors from the perspective of aviation safety: using fermatean fuzzy DEMATEL approach, *Axioms* 12 (11) (2023) 1009.
- [18] A. Sharma, S.K. Sharma, Analyzing the role of multiagent technology in preventing airplane crash using AHP and DEMATEL approach, *Int. J. Crashworthiness* 27 (6) (2022) 1753–1769.
- [19] H. Li, M. Yazdi, Advanced decision-making methods and applications in system safety and reliability problems, *Studies in Systems, Decision and Control* 211 (2022).
- [20] J. Shi, Z. Liu, Y. Feng, X. Wang, H. Zhu, Z. Yang, H. Wang, Evolutionary model and risk analysis of ship collision accidents based on complex networks and DEMATEL, *Ocean. Eng.* 305 (2024) 117965.
- [21] F. Wagner, M. Khatun, R. Jung, M. Glaß, Analysis of safety and cybersecurity management systems interaction in decision-making including correlation for automated driving systems, in: *International Conference on Enterprise Information Systems*, Springer Nature Switzerland, Cham, 2023, April, pp. 333–347.
- [22] W. Torbacki, A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0, *Sustainability* 13 (16) (2021) 8833.
- [23] M. Yazdi, Reliability-centered design and system resilience, in: *Advances in Computational Mathematics for Industrial System Reliability and Maintainability*, Springer Nature Switzerland, Cham, 2024, pp. 79–103.
- [24] H. Li, R. Moradi, M. Yazdi, E. Zarei, Nash equilibrium-based FMEA for risk prioritization in hydrogen refueling station design, in: *Progressive Decision-Making Tools and Applications in Project and Operation Management: Approaches, Case Studies, Multi-Criteria Decision-Making, Multi-Objective Decision-Making, Decision under Uncertainty*, Springer Nature Switzerland, Cham, 2024, pp. 39–52.
- [25] V. Filinovich, Z. Hu, Aviation and the cybersecurity threats, in: *International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)*, Atlantis Press, 2021, August, pp. 120–126.
- [26] C.S. Babu, P.A. Simon, S.B. Kumar, The future of cyber security starts today, not tomorrow, in: *Malware Analysis and Intrusion Detection in Cyber-Physical Systems*, IGI Global, 2023, pp. 348–375.
- [27] C.R.S. Kumar, S. Mohanty, Current trends in cyber security for drones, in: *2021 International Carnahan Conference on Security Technology (ICCSST)*, 2021, October, pp. 1–5 (IEEE).
- [28] M. Pyzyski, T. Balcerzak, Cybersecurity of the unmanned aircraft system (UAS), *J. Intell. Rob. Syst.* 102 (2) (2021) 35.
- [29] K. Mizrak, Exploration of cybersecurity in air traffic control through expert perspectives and literature insights, *International Journal of Social and Humanities Sciences Research (JSHSR)* 10 (102) (2023) 3674–3684.
- [30] M. Janson, Enhancing Cyberspace Monitoring in the United States Aviation Industry: A Multi-Layered Approach for Addressing Emerging Threats, 2023.
- [31] I.A. Shah, N.Z. Jhanjhi, S. Brohi, Cybersecurity issues and challenges in civil aviation security, *Cybersecurity in the Transportation Industry* (2024) 1–23.
- [32] J. Pearson, O. Oni, Addressing cybersecurity and safety disconnects in United States army aviation: an exploratory qualitative case study, *Secur. J.* 37 (1) (2024) 153–169.
- [33] C. Asbaş, Ş.E. Tuzlukaya, Aviation cybersecurity: shielding against cyberthreats in the air, in: *Harnessing Digital Innovation for Air Transportation*, IGI Global, 2024, pp. 42–55.
- [34] M.M. Shueb, C. Yang, X. Che, An innovative design for improving US airports' cybersecurity based on blockchain technology, in: *2024 Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, 2024, May, pp. 232–237.
- [35] Resecurity, The aviation and aerospace sectors face skyrocketing cyber threats, Retrieved from, <https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats>, 2024, March 16.
- [36] Atlantic Council, Aviation cybersecurity: scoping the challenge, Retrieved from, <https://www.atlanticcouncil.org>, 2023.
- [37] N. Kumar, A. Sen, V. Hordichuk, M. Jaramillo, B. Molodetskyi, A. Kasture, AI in cybersecurity: threat detection and response with machine learning, *Tuijin Jishu/Journal of Propulsion Technology* 44 (3) (2023) 38–46.
- [38] S. Gnatyuk, V. Sydorenko, A. Polozhentsev, Method for cybersecurity level evaluation in the civil aviation critical infrastructure, in: *International Workshop on Advances in Civil Aviation Systems Development*, Springer Nature Switzerland, Cham, 2023, May, pp. 206–218.
- [39] C.S. Lee, D. Kim, Pathways to cybersecurity awareness and protection behaviors in South Korea, *J. Comput. Inf. Syst.* 63 (1) (2023) 94–106.
- [40] Cybersecurity Review, Cybersecurity in aviation: building a resilient future, Retrieved from, <https://www.cybersecurity-review.com>, 2024, June 25.
- [41] S. Yüksel, H. Dinçer, Sustainability analysis of digital transformation and circular industrialization with quantum spherical fuzzy modeling and golden cuts, *Appl. Soft Comput.* 138 (2023) 110192.
- [42] F. Kutlu Gündoğdu, C. Kahraman, Spherical fuzzy sets and spherical fuzzy TOPSIS method, *J. Intell. Fuzzy Syst.* 36 (1) (2019) 337–352.

- [43] H. Dinçer, A. El-Assadi, M. Saad, S. Yüksel, Influential mapping of SDG disclosures based on innovation and knowledge using an integrated decision-making approach, *Journal of Innovation & Knowledge* 9 (1) (2024) 100466.
- [44] ICAO, International civil aviation organization cybersecurity strategy, Retrieved: <https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx>, 2019.
- [45] F. Xiao, Generalization of Dempster–Shafer theory: a complex mass function, *Appl. Intell.* 50 (2020) 3266–3275, <https://doi.org/10.1007/s10489-019-01617-y>.
- [46] P.A. Meyer, *Quantum Probability for Probabilists*, Springer Science & Business Media, 1995.
- [47] J. Dai, Y. Deng, A new method to predict the interference effect in quantum-like Bayesian networks, *Soft Comput.* 24 (14) (2020) 10287–10294, <https://doi.org/10.1007/s00500-020-04693-2>.
- [48] L.A. Zadeh, Fuzzy sets as a basis for a theory of possibility, *Fuzzy Set Syst.* 1 (1) (1978) 3–28.
- [49] N.N. Karnik, J.M. Mendel, Q. Liang, Type-2 fuzzy logic systems, *IEEE Trans. Fuzzy Syst.* 7 (6) (1999) 643–658.

Further reading

- [50] M.F. Bongo, R.R. Seva, Evaluating the performance-shaping factors of air traffic controllers using fuzzy DEMATEL and fuzzy BWM approach, *Aerospace* 10 (3) (2023) 252.
- [51] G. Dave, G. Choudhary, V. Sihag, I. You, K.K.R. Choo, Cyber security challenges in aviation communication, navigation, and surveillance, *Comput. Secur.* 112 (2022) 102516.
- [52] European Union Aviation Safety Agency (EASA), European union aviation safety agency annual report, Retrieved from, <https://www.easa.europa.eu>, 2020.
- [53] Federal Aviation Administration (FAA), Federal aviation administration cybersecurity report, Retrieved from, <https://www.faa.gov>, 2019.
- [54] International Air Transport Association (IATA), International air Transport association annual review, Retrieved from, <https://www.iata.org>, 2021.
- [55] International Civil Aviation Organization (ICAO), International civil aviation organization cybersecurity strategy, Retrieved from, <https://www.icao.int>, 2019.
- [56] M. Khatun, F. Wagner, R. Jung, M. Glaß, An application of DEMATEL and fuzzy DEMATEL to evaluate the interaction of safety management system and cybersecurity management system in automated vehicles, *Eng. Appl. Artif. Intell.* 124 (2023) 106566.
- [57] Y.A. Kuleshov, K. Nagpal, K. Ucpinar, A. Gadaginmath, S. Gadaginmath, K. O'Daniel, H. Monangi, Cyber attacks on avionics networks in digital twin environment: detection and defense, in: *AIAA SCITECH 2024 Forum*, 2024, p. 277.
- [58] H. Li, M. Yazdi, Dynamic decision-making trial and evaluation laboratory (DEMATEL): improving safety management system, in: *Advanced Decision-Making Methods and Applications in System Safety and Reliability Problems: Approaches, Case Studies, Multi-Criteria Decision-Making, Multi-Objective Decision-Making, Fuzzy Risk-Based Models*, Springer International Publishing, Cham, 2022, pp. 1–14.
- [59] H. Li, M. Yazdi, What are the critical well-drilling blowouts barriers? A progressive DEMATEL-game theory, in: *Advanced Decision-Making Methods and Applications in System Safety and Reliability Problems: Approaches, Case Studies, Multi-Criteria Decision-Making, Multi-Objective Decision-Making, Fuzzy Risk-Based Models*, Springer International Publishing, Cham, 2022, pp. 29–46.
- [60] M. Mahdinia, I. Mohammadfam, A. Soltanzadeh, M.M. Aliabadi, H. Aghaei, A fuzzy Bayesian network DEMATEL model for predicting safety behavior, *Int. J. Occup. Saf. Ergon.* 29 (1) (2023) 36–43.
- [61] NBAA - National Business Aviation Association, Aviation cybersecurity: risks and mitigations, Retrieved from, <https://www.nbaa.org>, 2023, July/August.
- [62] R. Sabillon, J.R. Bermejo Higuera, The importance of cybersecurity awareness training in the aviation industry for early detection of Cyberthreats and vulnerabilities, in: *International Conference on Human-Computer Interaction*, Springer Nature Switzerland, Cham, 2023, July, pp. 461–479.
- [63] X. Shi, Y. Liu, K. Ma, Z. Gu, Y. Qiao, G. Ni, Y. Liu, Evaluation of risk factors affecting the safety of coal mine construction projects using an integrated DEMATEL-ISM approach, *Eng. Construct. Architect. Manag.* (2024).
- [64] P. Voigt, A. Von dem Bussche, The eu general data protection regulation (gdpr), in: *A Practical Guide*, 1st Ed., Cham: Springer International Publishing, 10 (3152676), 2017, pp. 10–5555.
- [65] WannaCry ransomware attack, Wikipedia, 2017. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.
- [66] X. Yang, Q. Xing, J. Yang, Y. Yao, K. Tian, H. Cai, Research on influencing factors and mechanisms of human-machine safety collaboration behavior in coal mines based on DEMATEL-ISM, *Sage Open* 14 (1) (2024) 21582440241239126.
- [67] C.H.E.N. Ye, C.H.E.N. Meng, X.U. Haiyan, X.I.E. Hua, FCM-DEMATEL-based flight safety evaluation and improvement method, *Ind. Eng. J.* 20 (3) (2017) 1.