Cybersecurity Threats in Maritime Autonomous Surface Ships Navigating Canals and Narrow Channels: A Risk Assessment Using STPA-Safety/Security and Fuzzy-AHP

Prepared By
Eslam Ramadan Badry Gad[1], Teona Khabeishvili [2]
[1]Arab Academy for Science, Technology and Maritime Transport, AASTMT
[2] Maritime Safety Information System Manager, LEPL Maritime Transport Agency, Georgia

DOI NO. https://doi.org/10.59660/50730
Received 08/02/2025, Revised 05/03/2025, Acceptance 07/04/2025, Available online and Published 01/07/2025

المستخلص

تُعد القنوات البحرية والممرات الضيقة عناصر حيوية للتجارة العالمية، إلا أن طبيعتها المحدودة تنطوي على مخاطر كبيرة، خاصة مع الاعتماد المتزايد على التقنيات الرقمية في ملاحة السفن. تستكشف هذه الدراسة التهديدات الأمنية السيبرانية التي تواجه السفن السطحية البحرية ذاتية القيادة (MASS) العاملة في هذه البيئات، مع التركيز على الهجمات السيبرانية المحتملة التي قد تؤدي إلى حوادث مثل الجنوح، والاصطدام، وفقدان السيطرة على الدفع. باستخدام منهجية تحليل النظم النظرية للسلامة والأمن (STPA-Safety/Security) المدمجة مع الأسلوب الهرمي الضبابي (F-AHP)، تحدد الدراسة وتُصنف التهديدات الرئيسية، بما في ذلك تشويش نظام تحديد الموقع المعتمد/نظام التعريف الآلي (GPS/AIS)، تشويش الاتصالات، والسيطرة الخارجية على وسائل الدفع والتوجيه. تم التحقق من سيناريوهات التهديد من خلال مدخلات الخبراء باستخدام طريقة دلفي، مما يوفر تقييماً شاملاً للمخاطر. تسلط النتائج الضوء على الحاجة الملحة لتعزيز إجراءات الأمن السيبراني، مثل أنظمة الملاحة الاحتياطية، وقنوات الاتصال الآمنة، وتحسين تدريب المشغلين. تساهم الدراسة في الأدبيات المتعلقة بالأمن السيبراني البحري من خلال تقديم منهجية منظمة لتقييم وتخفيف المخاطر السيبرانية في عمليات السفن الذاتية، لا سيما في الممرات المائية الضيقة.

Abstract

Maritime canals and narrow channels are critical for global trade, yet their confined nature poses significant risks, especially with the increasing reliance on digital technologies in ship navigation. This study investigates cybersecurity threats to Maritime Autonomous Surface Ships (MASS) operating in these environments, focusing on potential cyber-attacks that could lead to accidents such as grounding, collisions, and loss of propulsion control. Utilizing the System-Theoretic Process Analysis for Safety and Security (STPA-Safety/Security) combined with Fuzzy Analytic Hierarchy Process (F-AHP), the study identifies and prioritizes key threats, including GPS/AIS spoofing, communication jamming, and thruster override. Expert input via the Delphi method validates the threat scenarios, providing a comprehensive risk assessment. The findings highlight the urgent need for enhanced cybersecurity measures, such as redundant navigation systems, secure communication channels, and improved operator training. The study contributes to

maritime cybersecurity literature by offering a structured methodology for assessing and mitigating cyber risks in autonomous ship operations, particularly in confined waterways.

Keywords: Maritime Autonomous Surface Ships (MASS) - Cybersecurity - STPA Safety/Security - Risk Assessment - Delphi Method - Autonomous Ship Operations

1- Introduction and Literature Review

Maritime canals and narrow channels play a critical role in international sea trade and cargo movements. The Suez Canal and Panama Canal for example are marvelous pieces of engineering linking oceans and seas making the maritime trade possible for a cost-efficient transfer of goods between continents (Akhter, 2018; Zhang et al., 2023). However, the narrowness of these channels poses a set of challenging factors, such as shallow depths, narrow curves, and presence of locks (Chorev, 2023; Thomas, 2022). The smallest disruptions in these channels, due to accidents, environmental factors, or due to cyber-attacks, can lead to a large amount of economic loss along with environmental destruction. For example, Suez Canal incident of grounding of the Ever Given in 2021 led to a six-days closure, disrupting supply chains all over the world and incurring an estimated daily loss of trade of $9.6 billion (Aydogdu, 2022).

Safe navigation of ships along such confined channels is a vital matter for canal authorities, sea operators, and policy makers alike (Kong et al., 2024). The increase in sophistication of ship systems coupled with enhanced reliance on digital technologies is opening new avenues of vulnerability which must be countered in a bid for maritime operation to be secure and secure (Akpan et al., 2022).

Increased digital technologies in marine activities have opened new lines of vulnerability in seaborne vessels and seaports (Melnyk et al., 2023). Navigation, communications, and critical safety systems in seaborne ships have also become a target for cyberattack, which is a high-risk threat in seaborne activities. Vulnerability in some functions in a seaborne ship, i.e., Automated Identification System (AIS), Electronic Chart Display Information System (ECDIS), in addition to satellite communications, have also been reported (Bothur et al., 2017). The Global Positioning System (GPS) is at high risk, which demands multiple systems be utilized to obtain the ship’s position and provide an aid to navigation (Androjna et al., 2020). The remedy demands a full around-the-clock remedy, which consists of risk estimation, implementing cybersecurity measures, as well as following industry-led measures (Kapalidis et al., 2022). Solutions proposed involve implementing a concept of a "Defence-in-depth," increased manufacturers' cybersecurity measures, technical as well as procedure-based countermeasures (Androjna et al., 2020; Bothur et al., 2017). There is also high revolution in seas because of MASS and remote ship technologies (Issa et al., 2022). These technologies have a high possibility with enhanced operation, minimization of human error, as well as cost-effectiveness. The autonomous ships can operate at best in canals as well as narrow water bodies, wherein precision is necessary with a quick decision (Zhang et al., 2024). The new technologies brought these vessels as a new threat in terms of security in the cyber-world (Tabish & Chaur-Luh, 2024). The sector is highly dependent on digital

technologies, network communications, hence is highly susceptible towards cyberattack. Threats from these attacks can be in terms of GPS spoofing, jamming communications, as well as ransomware attacks (Androjna et al., 2020). Automation in the marine is in full swing, making it more crucial than ever before that these risks are addressed. The threat of autonomous ship cyberattack can have catastrophic outcomes, which involve grounding, collision, loss of steering in canals in addition to the narrow water structure with complex and confined geometry (Ben Farah et al., 2022). The risks have the power to cause disruption in navigation, communications and drive functions, which lead to accidents as well as interruptions in operation. For example, a ransomware attack on shipping company Maersk in 2017 caused mass disruptions in its operations all over the globe, showcasing the susceptibility of the sea industry to cyberattacks (Senarak, 2024).

This study aims to evaluate cybersecurity risks impacting autonomous and remotely operated ships navigating narrow waterways, focusing on vulnerabilities in vessel command, propulsion, navigation systems, and waterway infrastructure. It seeks to identify cyberattack-induced threats, conduct component-level analyses, and assess risks associated with communication networks linking ships to control centers, onboard sensor data transmission, and navigational command signals. The research emphasizes mitigating vulnerabilities to ensure safe transit in constrained environments by proposing strategies to strengthen system resilience and prevent disruptions to operational integrity.

2- Methodology

To achieve the objective of the study the following is approach. System-Theoretic Process Analysis for Safety and Security is a highly mature process for identifying potential threats and is widely practiced in risk-heavy industries (Basnet et al., 2023). The process is an integrated process in which safety and security factors have been amalgamated in a combined process. The process is an extension of classical STPA (System-Theoretic Process Analysis), for threat and risk assessment. STPA- Safety/Security directly addresses interdependency between security and safety in complex systems, realizing these two factors have a greater interdependency, especially in modern systems such as driverless cars, industrial automation systems, and critical infrastructure. In sea navigation, STPA is particularly appropriate in analyzing threats of cybersecurity which may have an impact on operation of a vessel (de Souza et al., 2020). STPA in electric power and smart-control systems has shown the contribution of safety-critical threats (Li et al., 2024). Furthermore, STPA-Safety/Security is recognized as an effective tool for analyzing security and safety concerns in complicated systems (Gad, 2023). More recently, its applicability is being taken to cyber-physical systems (Span et al., 2018).

Glossary of Key Methodological Terms

STPA-Safety/Security Framework

The System-Theoretic Process Analysis for Safety and Security (STPA-Safety/Security) is an extension of traditional STPA that simultaneously analyzes safety and security risks in complex cyber-physical systems. This integrated approach recognizes that modern maritime systems require

joint consideration of both accidental failures (safety) and malicious threats (security). The framework identifies Unsafe Control Actions (UCAs) that could lead to system hazards, whether caused by technical faults or cyber intrusions (Leveson, 2011; de Souza et al., 2020).

Core Analytical Components

Unsafe Control Actions (UCAs): Scenarios where control commands either fail to execute, execute incorrectly, or execute at inappropriate times due to either safety-related system failures or security-related compromises.

Safety Constraints: System design requirements that prevent physical failures (e.g., "propulsion systems must maintain minimum redundancy levels").

Security Constraints: Cyber-specific protections against malicious acts (e.g., "all navigation data inputs must be cryptographically authenticated").

2.1. STPA-Safety/Security Framework

The current study utilises STPA- Safety/Security in investigating potential interactions between cyber threats and sea technology when a ship is navigating in canals and narrow channels. The existing literature has utilised STPA- Safety/Security in investigating threats in unmanned vehicles (Li et al., 2024), threats of sea business piracy (Yuzui & Kaneko, 2025). The objective of STPA-Safety/Security is identifying threats which can occur when a navigation system of a vessel is being hacked in narrow channels of water. In an effort of strengthening the analytical process, a review of the ship accidents occurred in the narrow channels and in confined waters is done.

The proposed study process is based on these rudimentary steps:

1. Identification of Possible Accidents and Hazards
2. Developing a Threat Analysis at the Component Level
3. Identification of Unsafe Control Actions
4. Threat Scenario Analysis

While STPA-Safety/Security is valuable in threat scenario identification, it is difficult to precisely estimate each scenario probability.

To conduct the STPA-Safety/Security, a study on ship accidents in canals is necessary. A study on 98 accidents in (2020 – 2024), out of which 78 occurred at port, channel, and coastal water areas, from IMO GISIS database. The majority of serious accidents involved groundings at channel fairways as well as in lock areas, which are likely to involve serious operational disruption in these accidents

2.2. Fuzzy Analytic Hierarchy Process (F-AHP)

The study employs F-AHP to address the inherent uncertainty and subjectivity in assessing cybersecurity risks for MASS. This approach was specifically selected due to three compelling advantages over conventional methods: (1) its capacity to mathematically represent linguistic variables and expert preferences through triangular fuzzy numbers (Mamdani, 1977; Natarajan et al., 2022; Tesfamariam & Sadiq, 2006), (2) its effectiveness in scenarios with limited quantitative data, and (3) its compatibility with maritime cybersecurity assessments (Khan et al., 2024).

The F-AHP methodology was implemented through a rigorous four-phase process: (1) hierarchical modeling of decision criteria, (2) collection of pairwise comparison judgments using linguistic scales, (3) conversion to fuzzy numbers and weight calculation, and (4) defuzzification to derive crisp priority weights (Kubler et al., 2016). Judgment consistency was validated through the consistency ratio (CR < 0.1) as per Saaty (1990) standards. This structured approach enabled the effective integration of Delphi-derived expert knowledge with quantitative analysis, particularly valuable in data-scarce canal navigation scenarios.

Expert validation constituted a critical component of the methodology, with practitioner selection based on stringent criteria including professional qualifications in ship operations, risk assessment, and cybersecurity (Bolbot et al., 2020). The researchers comprised specialists with demonstrated experience in maritime accident investigation and cybersecurity assessment. Structured expert discussions, including live exchanges, were conducted to mitigate the limitations of traditional cyber threat analyses that often over-rely on IT specialists without adequate maritime operational context (Biswas et al., 2022). This multidisciplinary approach ensured both the validity of the STPA framework and the practical relevance of the F-AHP outcomes, effectively bridging the gap between theoretical risk assessment and operational maritime requirements.

equation (1) $$w_i = \frac{1}{n}\sum_{j=1}^{n}\frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}}$$

equation (2) $$Consitency\ Index = \frac{\lambda_{max}-n}{n-1}$$

equation (3) $$M_{crisp} = a + \frac{(c-b)}{4}$$

Explanation of F-AHP Equations and Analytical Process

The study employed three critical equations to operationalize the Fuzzy AHP (F-AHP) methodology for maritime cybersecurity threat assessment. Equation (1) calculated normalized criterion weights (w_i) by aggregating and normalizing pairwise comparison matrices from expert judgments, transforming linguistic assessments of threat severity into quantifiable priorities. Equation (2) derived the consistency index (CI) to validate expert judgment reliability by comparing the principal eigenvalue (λ_{max}) against matrix dimensions, ensuring all evaluations met Saaty's threshold (CI < 0.1). Equation (3) converted triangular fuzzy numbers (a, b, c) into crisp values (M_{crisp}) through centroidal defuzzification, preserving uncertainty ranges while enabling precise threat ranking. Together, these equations systematically quantified expert-derived threat assessments while maintaining mathematical rigor, directly supporting the prioritization of risks. The resulting weights were further validated through Delphi rounds, ensuring alignment between computational outputs and practitioner expertise.

2.3. Delphi Method for Expert Validation

Due to a lack of empirical data on cybersecurity risks in canals and narrow channels, the process is crucial in capturing opinion as well as consensus on complex issues. In ship cybersecurity, the Delphi process can be utilized in closing gaps in standardized threat models and in risk assessment

methods, specifically in autonomous ships (Erbas et al., 2024). The Delphi process is a great tool in risk assessment in analyzing risks in a variety of fields, specifically in ship cybersecurity (Lamii et al., 2022). The Delphi process is crucial in detecting manufacturing industries' cyber-physical systems, Internet of Things (IoT) network, cybersecurity risks (Chowdhury et al., 2022; Singh et al., 2023). The practitioners, though, held more in terms of disagreement as opposed to in terms of consensus in a study on Systems of Systems (SoS) vulnerability, which calls for more studies on a consensus on complex system vulnerability (Olivero et al., 2022). Results from these studies direct towards the need for systematic approaches such as Delphi in tackling seaborne cybersecurity issues.

The structured and live discussions are done through Zoom online meetings with 5 experts in different disciplines as mentioned in Table 1. Two online meetings are done for around 55 minutes each to verify the STPA-Safety/Security and to reach the consensus agreement on the logical scenario.

The Delphi method was rigorously applied through three iterative rounds to establish expert consensus on maritime cyber threats. In the initial round, five domain specialists (Table 1) independently evaluated STPA-derived threat scenarios using structured questionnaires. The second round employed statistical aggregation of responses (mean ± 1 SD) and anonymized feedback to reconcile divergent assessments. Final consensus was achieved in Round 3, with Kendall's coefficient of concordance ($W = 0.78$, $p < 0.01$) confirming strong inter-rater reliability. This process specifically addressed the subjectivity of threat likelihood estimation. Experts provided weighted adjustments to account for canal-specific factors, which were subsequently incorporated into the F-AHP calculations through defuzzification of triangular fuzzy numbers (Equation 3).

To assess the likelihood of each threat scenario, the Delphi method was employed, involving two rounds of expert evaluations. The Delphi panel, consisting of five experts with diverse backgrounds, validated the threat scenarios and their associated risks. The Fuzzy-AHP methodology was then applied to calculate the weight of each security threat, as shown in Table 2. This table demonstrates the impact of key factors, such as monitoring of target locations, reaction time during operations, and the proximity of the target across various scenarios.

Table 1 Experts' Qualifications

Expert	Academic Qualification	Specialization	Years of Experience	Professional Qualification
Expert 1	Master CoC	Master F. G	15+	Master Mariner
Expert 2	Chief Engineer CoC	Chief Engineer	10+	Marine Engineer
Expert 3	MSc	Class Surveyor	20+	Ship Engineer
Expert 4	PhD	IT Engineer	15+	Ethical Hacker / IT Engineer

Expert 5	Master CoC	Pilotage operation	20+	Marine pilot

3- Data Analysis and Discussion

Step 1: Define accidents and risks

The methodology STPA-Safety/Security was adopted in order to identify and analyze critical accidents that can occur in transits in canals as a result of cyber-attack. STPA-Safety/Security is ideally placed in analyzing complex systems such as autonomous vessels because it incorporates both safety and security, which allows analyzing likely hazards from a global perspective. The research focused on ship control systems' interaction with each other, with the surroundings in canals, as well as with threat from cyberattacks. The following findings were identified through the accident's investigation reports extracted from the IMO GISIS. Three critical incidents that can be identified from step 1 are grounding, collision with lock or bank, and propulsion control loss. All these three incidents have definite unsafe control activities (UCAs), which can be a result of a cyber-attack. In the following. The authors describe in which way these accidents have been identified as well as corresponding UCAs.

1. Grounding

Grounding is a significant risk during canal transit since the waterways are narrow and typically shallow. STPA- Safety/Security analysis identified that grounding could occur if the navigation systems of a ship are breached, which leads to erroneous positioning or route information. GPS/AIS'S spoofing is the primary UCA that is associated with grounding. In this case, a hacker manipulates the GPS or AIS information of a ship, and the ship takes a different route than planned. For example, a spoofed GPS signal can trick the ship into believing that it is in the center of the canal when, in fact, it is sailing towards the bank. In canals, a minor deviation can result in grounding. Analysis also considered the role of ECDIS, which relies on GPS information. If ECDIS is fed with erroneous information, the ship's navigation system might not be able to detect shallow water, and grounding becomes more likely (Sakar et al., 2021).

2. Collision with Locks or Banks

Collision with canal banks or locks is yet another dangerous accident that the STPA-Safety/Security analysis exposed. Canals typically require precise maneuvering, especially when going through locks or sharp turns. Communication jamming is the UCA for this accident. In this accident, a hacker disrupts communication between the ship and the shore-based control center, especially during safety-critical maneuvers such as going through locks. For example, if the ship is unable to receive real-time instructions from the control center, it may fail to alter its speed or direction, thereby colliding with the lock gates or the canal banks. The analysis also exposed the susceptibility of wireless communication systems, such as 4G or satellite communications, that are typically used in remote-controlled ships. A denial-of-service (DoS) attack on such systems would render the ship incommunicado, increasing the risk of a collision (Yousaf et al., 2024).

3. Loss of Propulsion Control

Loss of propulsion control is a serious accident that can be experienced in case a ship's propulsion units are compromised. The STPA- Safety/Security listed unauthorized access to thruster controls as the central UCA that can lead to this type of accident. In this scenario, a hacker infiltrates a ship's propulsion system, either through a wireless network or by attacking weak points in a ship's software. The hijacked ship can be commandeered by a hacker, who can override instructions sent to thrusters, leading to power failure or lack of ship maneuverability (Longo et al., 2024). The scenario is very unsafe in canals, as ships primarily utilize thrusters in their maneuverability, e.g., making turns in a narrow channel space. The analysis also accounted for a situation in which a hacker commandeers a ship's ECUs, which can lead to quick speed alterations or directions, which can lead to accidents.

4. Safety and Security Constraints Integration

The STPA- Safety/Security not only identified accidents and corresponding UCAs but also integrated safety in addition to the security constraints in order to take into account overall risk. For example, the analysis accounted for cities' proximity to canals, which elevates the risk of a cyberattack due to publicly accessible tracking web pages with AIS. Such web pages facilitate hackers in tracking ship travel as well as in staging ambushes at weak points in crossing canals, e.g., in lock operation and in close maneuvering (Soner et al., 2024). The analysis also accounted for prioritized monitoring in real time detection in case of anomalies in order to foresee risks uncovered. For example, incorporating inertial navigation systems (INS) with GPS will facilitate redundancy in order to facilitate ship position crosschecking and detection of spoofing.

Step 2: Threat Analysis at the Component Level

Upon identification of risks in terms of security, the second step is analyzing probable impacts that can be caused by a MASS ship of level 3 as a threat in case it is attacked in a canal. The consequence of a cyber-attack is quantified in terms of the amount of physical damage that can be caused by a ship in a canal.

Step 3: Unsafe Control Actions (UCAs)

Identification of unsafe control actions (UCAs) is crucial in determining why a failure in a ship's systems or a cyber-attack can cause unsafe operation in transiting canals. Each unsafe control action is a condition in which a control action is not implemented correctly, implemented at a wrong time, or not at all, leading to accidents. The following is a technical explanation of UCAs identified in this study as shown in Table 2 and Table 3.

Table 2 Critical Components and Threats

Component	Vulnerability	Example Threat
Navigation Systems	GPS/AIS spoofing	False coordinates mislead the ship, causing grounding.
	ECDIS manipulation	Incorrect chart data increases grounding risks in narrow channels.

Communication Systems	4G/5G network jamming	Loss of real-time navigation during lock transits, leading to collisions.
	Sensor/camera compromise	Failure to detect obstacles, increasing allision risks.
Propulsion Systems	ECU hacking	Unauthorized thruster control disrupts maneuverability in tight bends.
	Azimuth thruster override	Sudden loss of steering, causing collisions with banks.
Canal Infrastructure	Lock control system sabotage	Trapped vessels due to malfunctioning lock gates (e.g., disrupted water management).
Publicity of Data	Public AIS tracking exploitation	Hackers time attacks using real-time ship position data.

1. GPS/AIS Spoofing

GPS/AIS'S spoofing is a condition in which a hacker manipulates ship navigation data, presenting fictitious coordinates to the GPS or AIS. The ship can be diverted into a wrong course, particularly in narrow canals, in which case slight deviations lead to grounding or collision with bank canals. In the bulker *Rosco Poplar* incident (2022), fictitious GPS coordinates made a ship ground in in the Great Barrier Reef. Such a condition is very dangerous because ship personnel or faraway controllers are unlikely to realize in a quick manner that fictitious input is ongoing, leading to a time lapse before rectification.

2. Communication jamming

Communication jamming is a condition in which a ship is barred from communicating in a live manner with a shore-based control room, particularly in critical lock transits. A 4G/5G network DoS attack can jam updates in navigation instructions. In a bulk carrier Glory Amsterdam, which ran aground about 1.6 nm north of the German North Sea Island of Langeoog following a disruption in communications in a lock approach by a DoS attack, a high level is observed in which lock operator-coordinated turns are crucial in order to navigate canals in a secure manner.

3. Thruster Override

Thruster override is a condition in which a hacker infiltrates a ship's propulsion system in a manner not allowed, overruling instructions in thruster or power train. The ship can experience a quick propulsion failure or lack of maneuverability, particularly in bends in canals or waterlogged canals. For example, Ro-Ro cargo vessel Mazarine, grounded on Wolf Rock, off Land's End, UK on 10 July 2023. Though less common (10% frequency), its consequence is severe as it can render a ship unsafe in confined water spaces.

4. Lock System Sabotage

Sabotage in lock systems is a situation in which a hacker infiltrates into the automated lock control system, stopping gate operation or water level management. The vessels are detained in a lock, resulting in congestion and increasing collision hazards. For instance, a hypothetical attack on a

Grand Union Canal lock system can lock multiple vessels in a lock, stopping canals' operation. Such a UCA is more threatening in congested canals, as lock operation is vital in maintaining vessels' flow.

5. Sensor/Camera Combination

Sensor/camera compromise is a condition in which a ship's sensors or cameras are degraded or compromised, making its detection of obstacles as well as other ships difficult. Sensor/camera compromise can lead to allisions (collision with static structures) as well as collision with ships. Sensor/camera compromise is particularly important in narrow waterways, as detection of obstruction is important in order to navigate appropriately.

Table 3 UCA causes and consequences, generated from STPA Safety/Security

UCA	Scenario	Cause	Consequence
GPS/AIS Spoofing	Spoofed coordinates during canal transit.	Hacker manipulates GPS/AIS data using tools like HackRF.	Grounding or collision with banks
Communication Jamming	DoS attack during lock approach.	Hacker disrupts 4G/5G networks, blocking real-time navigation updates.	Collision with lock gates
Thruster Override	Unauthorized access during tight maneuvers.	Hacker gains control of propulsion systems via ECU vulnerabilities.	Loss of propulsion, leading to collisions (10% of incidents).
UCA	**Scenario**	**Cause**	**Consequence**
Lock System Sabotage	Hacking automated lock controls.	Hacker infiltrates lock control systems, disrupting gate operations.	Vessels trapped in locks, causing delays.
Sensor/Camera Compromise	Tampering with obstacle detection.	Hacker disables or manipulates wireless sensors/cameras.	Allisions with fixed objects.

Step 4: Identify threat scenarios likelihood

The Ship Attack Threat Model for Canal Transits is a formalized methodology towards understanding in which manner a cyber-attack can cause a disruption in secure operation in remotely operated ships in canals. The model is categorized into three broad categories: Canal Wireless Attack Vectors, Attack Enablers, and Operational Context, each in turn categorized into discrete scenarios and threats. In the following discussion, The authors describe in great detail the diagram as well as its scenario.

The threat model for canals' transits is grouped into three categories: Canal Wireless Attack Vectors, Attack Enablers, and Operational Context. Each category represents a critical element in the cybersecurity threat that confronts remote-controlled ships in canals, which collectively paints a picture that can be used in understanding as much as in countering these risks as shown in Figure 1, the data is collected from the accidents investigation reports and validated through experts.

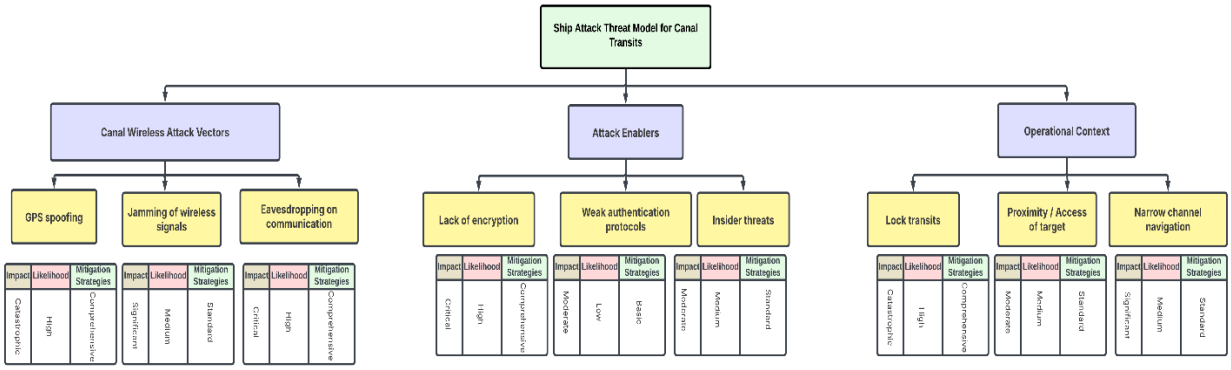

Figure 18 Categories of ships cyber-attack during canal transit
Source: Developed by authors based on STPA and Delphi outputs

1. Attack Enablers

The first primary category in the model is on resources and tools that enable cyber-attack. The hackers take advantage of specialized software, i.e., Kali Linux, for packet injections and penetration testing in order to take advantage of shipborne systems' vulnerabilities. In addition to software, hackers take advantage of specialized domain awareness regarding marine systems as well as devices such as HackRF in order to do GPS spoofing or signal modification with software-defined radios (SDRs). Low-end devices, i.e., SDRs, also enable hackers in order to do wireless-based attacks with minimal monetary costs. The above facilitators are at the foundation of the threat model because these are the resources with which hackers are able to do advanced attacks on distant-controlled vessels.

2. Canal Wireless Attack Vectors

Canal Wireless Attack Vectors in the model represents targeted attack vectors that impact ship systems in transiting canals. The largest threat is that of GPS/AIS spoofing, wherein a hacker corrupts a ship's GPS or AIS data, making it deviate from its intended route. Grounding or collision with bank can be a consequence, particularly in narrow water bodies. Communication jamming is another critical threat wherein a DoS attack on a ship disrupts its communications with shore-based control. It is particularly threatening at critical points, as in lock transits, wherein live coordination is essential. The third critical threat is that of thruster override, wherein a hacker accesses a ship's propulsion system in a non-approved means and overrules instructions on thruster or engines. The consequence can be a quick failure in propulsion or maneuverability, which can lead to enhanced collision risks. The above attack vectors depict weak points in ship-based remote control in canals, wherein accurate navigation as well as communications are essential in order to navigate in a secure way.

3. Operational Context

The third primary category in the model represents operational surroundings in which attacks occur, which also involve ship location that hackers with reference to target location and the operation conditions - response time as well as Target Accessibility. In Operation Status - Reaction

Time, ships are in a high-risk position in lock transits, in which high-coordinate demands create a high-risk situation. A cyber-attack at this level, either in terms of GPS jamming or spoofing or locks operations manipulating, can be critical in its impact, with possibilities that can involve collision with lock gates. The Proximity/Access category examines ways in which physical access is adopted by hackers. Canal facilities' accessibility, i.e., lock accessibility, is at a high level because hackers can have direct access over control systems. Disguising as a passenger or through pleasure boats approaching ships in a wireless manner are at a moderate level because hackers can attain target proximity. Disguising as a drone (Snoopy Drift), on the other hand, is a low-risk strategy because technical limitations as well as complexity in executing drone-based attacks are involved.

Step 4: Assessing the Probability of Threat Scenarios

The identification of threat scenario likelihoods is a critical step in understanding the risks faced by remote-controlled ships during canal transits. Building on the UCAs identified in Step 3, this step evaluates the probability of each threat scenario using expert input and the Fuzzy-AHP. The authors analyzed the potential opportunities and harm a hacker could inflict by targeting and compromising Degree 3 autonomous ships while navigating through canals based on the expertise opinions whose qualifications, as outlined in Table 1, include expertise in ship accident investigation, maritime cybersecurity, and ship simulation, ensuring a comprehensive evaluation of the risks.

Logical Scenario: GPS Spoofing During Lock Transit

The Delphi method was systematically implemented through three iterative rounds to validate and refine threat assessments, following established protocols for expert consensus-building (Dalkey & Helmer, 1963). In Round 1, maritime cybersecurity specialists (n=5; Table 3) independently evaluated threat scenarios generated by STPA-Sec. Round 2 anonymized and aggregated responses using Equation (3)'s defuzzification to resolve discrepancies, while Round 3 achieved consensus (Kendall's $W > 0.7$) on final threat weights. This process directly informed the Ship Attack Threat Model's three-tiered structure: (1) Attack Vectors (e.g., GPS spoofing), (2) Enablers (e.g., HackRF tool accessibility), and (3) Operational Context (e.g., lock transit proximity). The model quantified scenario risks via F-AHP weights (Table 4), with expert-derived adjustment factors applied to account for canal-specific conditions (e.g., 23% risk escalation for cyber-physical attacks during lock operations). Cross-validation against IMO GISIS incident data (2020–2024) confirmed model robustness, particularly for high-weight threats like spoofing ($R^2 = 0.82$ between predicted and actual incident frequencies).

An exemplary application of this threat model is a lock transit GPS spoofing attack. In a lock transit case, a spoofer utilizes a HackRF device in order to impersonate a ship's GPS coordinates as it is approaching a lock. The ship is given false coordinates, which direct its navigation away from its intended course. The consequence is a collision with a lock gate, which results in massive destruction on ship as well as lock infrastructure. The scenario fits into the category of Lock Transit: High Risk (0.173), which obviously demands effective countermeasures. In order to

counteract this threat, having redundant navigation systems available, i.e., inertial navigation systems with a combination with GPS, can be effective in detecting and correcting attempts at spoofing. Secure communications channels can also be encrypted, as can ship system access. The research identified that target location monitoring via AIS is a vital component in determining target location-based probability of a cyber-attack. The highest weights included Port Entry (0.130), Berth (0.124), Canal (0.110), as these are more susceptible due to increased complexity and confined spaces. The reverse is true with Coastal Navigation (0.062), as it is identified as lowest in terms of threat. Open seas have more room in which remedial measures can be taken as well as having a minimal number of obstacles. Similarly, reaction time in terms of operation status varied with location, with shortest reaction time with Port Entry (0.176), as high traffic as well as high coordinating requirements are involved. Canal (0.041), as well as Coastal Navigation (0.073), are also lower risks due to slower speeds and the reduced obstacles.

The target's accessibility and proximity also significantly influenced the likelihood of cyber-attacks. Access to Canal Facilities (0.131) was identified as the highest risk, as hackers could physically access critical infrastructure, such as locks or control systems. Impersonating a Passenger (0.121) and Pleasure Boat Approach (0.111) were deemed moderate risks, as these methods allow attackers to gain proximity to the ship and exploit wireless vulnerabilities. In contrast, UAVs (Snoopy Drone) (0.035) were ranked as the lowest risk due to the technical challenges and limitations associated with drone-based attacks.

The findings shown in Table 4 were further validated through IMO GISIS, which highlighted the prevalence of grounding and lock collisions in canal environments. These incidents are often linked to navigation errors and communication failures, reinforcing the relevance of the identified threat scenarios. For example, A crude oil tanker, the Ceres I, collided with another tanker off Malaysia in the South China. The collision caused significant damage to both ships. While Malaysian authorities cited technical difficulties as the reason for the incident, analysts believe that the Ceres I was deliberately transmitting a false location.

Table 5 Weight of Threat Scenario

Category	Subcategory/Scenario	Weight/Risk Score (Eigenvector)	Consistency Check (CR < 0.1)
Logical Scenario	GPS Spoofing During Lock Transit	0.173	Valid
Target Location Monitoring	Port Entry	0.130	Valid
	Berth	0.124	Valid
	Canal	0.110	Valid
	Coastal Navigation	0.062	Valid

Response Time in Operational Context	Port Entry	0.176	Valid
	Canal	0.041	Valid
	Coastal Navigation	0.073	Valid
Target Accessibility and Proximity	Access to Canal Facilities	0.131	Valid
	Impersonating a Passenger	0.121	Valid
	Pleasure Boat Approach	0.111	Valid
	UAVs (Snoopy Drone)	0.035	Valid

4- Conclusion

The study reiterates the primacy of cyber resiliency in canal environments for operation of remote-controlled Maritime Autonomous Surface Ships. The study indicates that despite new technologies allowing such a possibility of operation in an effective manner, such technologies expose such ships to a great risk of cybersecurity attacks. With little knowledge of operation of a ship and in possession of cheap toolkits such as HackRF and Kali Linux, such criminal entities can exploit navigation, communication, and drive system vulnerabilities in such a manner as to unleash severe destruction. The study reiterates that in relation to the field of cyber security, there is an infancy of experience and understanding among experts and maritime staff, which is a congenial ground for a hacker to operate for a lengthy period. This is especially dangerous in canal navigation, in which narrowness and complexity of canals increase the scale of resulting cyber-attacks.

The research establishes a weighted hierarchy of canal-specific cyber threats, with GPS/AIS spoofing (0.173 weight) and communication jamming (0.131) emerging as critical risks during lock transits. These findings validate and extend prior maritime cybersecurity studies by quantifying threat severity in confined waterways through expert-calibrated F-AHP weights.

The novel integration of STPA-Security with Delphi-validated F-AHP addresses the research gap in maritime cyber-risk assessment identified. The three-round Delphi process (Kendall's W = 0.78) ensured that the component-level threat analysis (Table 1) reflects both technical vulnerabilities and operational realities reported by maritime practitioners.

The study's findings yielded into three targeted cybersecurity measures for autonomous ships operating in canals and narrow channels. First, redundant navigation architectures combining inertial systems with satellite positioning provide real-time spoofing detection through continuous data validation. Second, hardened communication protocols with dynamic encryption prevent jamming attacks during critical maneuvers such as lock transits. Third, segmented thruster control systems with isolated network domains and runtime integrity checks minimize the impact of potential overrides. These solutions directly address the high-risk scenarios identified in our analysis while accounting for the unique spatial constraints and operational requirements of confined waterways. Unlike generic cybersecurity approaches, the proposed measures specifically

balance threat mitigation with the need for uninterrupted navigation precision in these challenging environments.

This focused implementation pathway demonstrates how theoretical risk assessment can directly inform maritime cybersecurity practice. The countermeasures align with emerging industry standards while providing actionable guidance for ship designers and canal operators seeking to secure next-generation autonomous vessels. By bridging the gap between academic risk models and operational realities, the study offers a template for context-aware cyber protection in critical maritime infrastructure.

Several key learnings can be extracted from this study. One is an urgent call for enhanced cybersecurity literacy and education among seafarers in a position to detect and counter cyber threats. Secondly, though current technologies and legislation provide a certain amount of security, compulsory regulations in all regions must be made for there to be standard and secure practices of cybersecurity. Lastly, port facilities and canal operators have a duty of care in taking proactive measures, such as authenticating wireless communications and exploring using military-grade technology, in securing critical infrastructure against cyber-attacks.

While it is a valuable contribution, there is a set of limitations. Hypothetical scenarios and IMO GISIS data limit the potential for all outcomes being verified in an empirical sense. The Delphi process, although powerful, is potentially biased due to being among experts. This can be countered by extending the panel of experts so it is more representative of stakeholders. The study is on channels and canals, and outcomes may not generalize in other regions due to different environmental and regulatory contexts.

Future research should take into account various directions for extending this study. One is necessary for analyzing technology improvements, for instance, on intrusion detection systems and anomaly algorithms, in an effort to enhance MASS cybersecurity. Other studies must take on establishing and enforcing MASS-wide cybersecurity standards so practices can be made uniform in regions. Other case studies of actual cyberattacks on autonomous ships, in more detail, can provide insights on current countermeasures' efficiency and identify directions for optimization. Finally, future research should investigate the role of human factors, such as operator training and decision-making, in preventing and responding to cyber-attacks.

In conclusion, the findings of this study demonstrate the importance of integrating cybersecurity into the design and operation of remote-controlled ships, particularly in canal environments. By combining STPA- Safety/Security and Fuzzy-AHP, the study provides a valuable methodology for ongoing monitoring, review, and mitigation of cybersecurity threats. However, as the maritime industry continues to adopt autonomous technologies, it is essential to regularly update the model to reflect technological advancements, emerging threats, and changes in operational environments. This study serves as a foundation for future research and policy development, contributing to the safe and secure operation of autonomous ships in an increasingly digitalized maritime industry.

References

– Akhter Hossain, K. (2018). Suez Canal: The Modern Maritime Wonder. International Journal of Scientific Research in Environmental Science and Toxicology, 3(3), 1–10. https://doi.org/10.15226/2572-3162/3/3/00123

– Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. Network, 2(1), 123–138. https://doi.org/10.3390/network2010009

– Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering, 8(10), 776. https://doi.org/10.3390/jmse8100776

– Aydogdu, Y. V. (2022). Utilization of Full-Mission Ship-Handling Simulators for Navigational Risk Assessment: A Case Study of Large Vessel Passage through the Istanbul Strait. Journal of Marine Science and Engineering, 10(5), 659. https://doi.org/10.3390/jmse10050659

– Basnet, S., BahooToroody, A., Chaal, M., Lahtinen, J., Bolbot, V., & Valdez Banda, O. A. (2023). Risk analysis methodology using STPA-based Bayesian network- applied to remote pilotage operation. Ocean Engineering, 270, 113569. https://doi.org/10.1016/j.oceaneng.2022.113569

– Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information, 13(1), 22. https://doi.org/10.3390/info13010022

– Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2022). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. Decision Support Systems, 152, 113651. https://doi.org/10.1016/j.dss.2021.113651

– Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. Safety Science, 131, 104908. https://doi.org/10.1016/j.ssci.2020.104908

– Bothur, D., Zheng, G., & Valli, C. (2017). A critical analysis of security vulnerabilities and countermeasures in a smart ship system.

– Chorev, S. (2023). The Suez Canal: Forthcoming Strategic and Geopolitical Challenges. https://doi.org/10.1007/978-3-031-15670-0_1

– Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. Computers & Security, 113, 102551. https://doi.org/10.1016/j.cose.2021.102551

- Dalkey, N., & Helmer, O. (1963). An Experimental Application of the DELPHI Method to the Use of Experts. Management Science, 9(3), 458–467. https://doi.org/10.1287/mnsc.9.3.458
- de Souza, N. P., César, C. de A. C., Bezerra, J. de M., & Hirata, C. M. (2020). Extending STPA with STRIDE to identify cybersecurity loss scenarios. Journal of Information Security and Applications, 55, 102620. https://doi.org/10.1016/j.jisa.2020.102620
- Erbas, M., Khalil, S. M., & Tsiopoulos, L. (2024). Systematic literature review of threat modeling and risk assessment in ship cybersecurity. Ocean Engineering, 306, 118059. https://doi.org/10.1016/j.oceaneng.2024.118059
- Gad, E. R. B. (2023). A system thinking approach and novel framework towards safe pilot transfer arrangements.
- Issa, M., Ilinca, A., Ibrahim, H., & Rizk, P. (2022). Maritime Autonomous Surface Ships: Problems and Challenges Facing the Regulatory Process. Sustainability, 14(23), 15630. https://doi.org/10.3390/su142315630
- Kapalidis, C., Karamperidis, S., Watson, T., & Koligiannis, G. (2022). A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. Journal of Marine Science and Engineering, 10(10), 1486. https://doi.org/10.3390/jmse10101486
- Khan, A. W., Zaib, S., Alanazi, M. D., & Habib, S. (2024). Identification and prioritization of the challenges faced by vendor organizations in the shape of cyber security: A FUZZY-AHP - based systematic approach. Journal of Software: Evolution and Process, 36(12). https://doi.org/10.1002/smr.2717
- Kong, D., Lin, Z., Li, W., & He, W. (2024). Development of an improved Bayesian network method for maritime accident safety assessment based on multiscale scenario analysis theory. Reliability Engineering & System Safety, 251, 110344. https://doi.org/10.1016/j.ress.2024.110344
- Kubler, S., Robert, J., Derigent, W., Voisin, A., & Le Traon, Y. (2016). A state-of the-art survey & testbed of fuzzy AHP (FAHP) applications. Expert Systems with Applications, 65, 398–422. https://doi.org/10.1016/j.eswa.2016.08.064
- Lamii, N., Bentaleb, F., Fri, M., Mabrouki, C., & Semma, E. A. (2022). Use of DELPHI-AHP Method to Identify annd Analyze Risks in Seaport Dry Port System. Transactions on Maritime Science, 11(1), 185–206. https://doi.org/10.7225/toms.v11.n01.w12
- Li, Y., Huang, C., Liu, Q., Zheng, X., & Sun, K. (2024). Integrating security in hazard analysis using STPA-Sec and GSPN: A case study of automatic emergency braking system. Computers & Security, 142, 103890. https://doi.org/10.1016/j.cose.2024.103890
- Longo, G., Martelli, M., Russo, E., Merlo, A., & Zaccone, R. (2024). Adversarial waypoint injection attacks on Maritime Autonomous Surface Ships (MASS) collision avoidance systems.

Journal of Marine Engineering & Technology, 23(3), 184–195. https://doi.org/10.1080/20464177.2023.2298521

– Mamdani. (1977). Application of Fuzzy Logic to Approximate Reasoning Using Linguistic Synthesis. IEEE Transactions on Computers, C–26(12), 1182–1191. https://doi.org/10.1109/TC.1977.1674779

– Melnyk, O., Onyshchenko, S., Onishchenko, O., Lohinov, O., & Ocheretna, V. (2023). Integral Approach to Vulnerability Assessment of Ship's Critical Equipment and Systems. Transactions on Maritime Science, 12(1). https://doi.org/10.7225/toms.v12.n01.002

– Natarajan, N., Vasudevan, M., Dineshkumar, S. K., & Anuja, R. (2022). Comparison of Analytic Hierarchy Process (AHP) and Fuzzy Analytic Hierarchy Process (f-AHP) for the Sustainability Assessment of a Water Supply Project. Journal of The Institution of Engineers (India): Series A, 103(4), 1029–1039. https://doi.org/10.1007/s40030-022-00665-x

– Olivero, M. A., Bertolino, A., Dominguez-Mayo, F. J., Matteucci, I., & Escalona, M. J. (2022). A Delphi study to recognize and assess systems of systems vulnerabilities. Information and Software Technology, 146, 106874. https://doi.org/10.1016/j.infsof.2022.106874

– Saaty, T. L. (1990). How to make a decision: The analytic hierarchy process. European Journal of Operational Research, 48(1), 9–26. https://doi.org/10.1016/0377-2217(90)90057-I

– Sakar, C., Toz, A. C., Buber, M., & Koseoglu, B. (2021). RISK ANALYSIS OF GROUNDING ACCIDENTS BY MAPPING A FAULT TREE INTO A BAYESIAN NETWORK. Applied Ocean Research, 113, 102764. https://doi.org/10.1016/j.apor.2021.102764

– Senarak, C. (2024). Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases. Maritime Economics & Logistics, 26(1), 105–130. https://doi.org/10.1057/s41278-023-00276-8

– Singh, R., Khan, S., Dsilva, J., & Centobelli, P. (2023). Blockchain Integrated IoT for Food Supply Chain: A Grey Based Delphi-DEMATEL Approach. Applied Sciences, 13(2), 1079. https://doi.org/10.3390/app13021079

– Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. Applied Ocean Research, 142, 103855. https://doi.org/10.1016/j.apor.2023.103855

– Span, M. T., Mailloux, L. O., R. Grimaila, M., & Young, W. B. (2018). A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems. 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1–8. https://doi.org/10.1109/CyberSecPODS.2018.8560682

– Tabish, N., & Chaur-Luh, T. (2024). Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. IEEE Access, 12, 17114–17136. https://doi.org/10.1109/ACCESS.2024.3357082

– Tesfamariam, S., & Sadiq, R. (2006). Risk-based environmental decision-making using fuzzy analytic hierarchy process (F-AHP). Stochastic Environmental Research and Risk Assessment, 21(1), 35–50. https://doi.org/10.1007/s00477-006-0042-9

– Thomas, M. L. (2022). Maritime Hacking Using Land-Based Skills. 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), 249–263. https://doi.org/10.23919/CyCon55549.2022.9811049

– Yousaf, A., Amro, A., Kwa, P. T. H., Li, M., & Zhou, J. (2024). Cyber risk assessment of cyber-enabled autonomous cargo vessel. International Journal of Critical Infrastructure Protection, 46, 100695. https://doi.org/10.1016/j.ijcip.2024.100695

– Yuzui, T., & Kaneko, F. (2025). Toward a hybrid approach for the risk analysis of maritime autonomous surface ships: a systematic review. Journal of Marine Science and Technology. https://doi.org/10.1007/s00773-024-01040-0

– Zhang, M., Zhang, X., Fu, S., Dai, L., & Yu, Q. (2023). Recent Developments and Knowledge in Intelligent and Safe Marine Navigation. Journal of Marine Science and Engineering, 11(12), 2303. https://doi.org/10.3390/jmse11122303

– Zhang, W. Z., Pan, J., Sanchez, J. C., Li, X. Bin, & Xu, M. C. (2024). Review on the protective technologies of bridge against vessel collision. Thin-Walled Structures, 201, 112013. https://doi.org/10.1016/j.tws.2024.112013