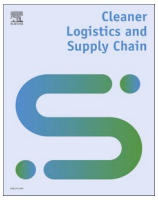
Cleaner Logistics and Supply Chain 9 (2023) 100126

Contents lists available at ScienceDirect

Cleaner Logistics and Supply Chain

journal homepage: www.journals.elsevier.com/cleaner-logistics-and-supply-chain



# Assessing the resilience of sustainable autonomous shipping: New methodology, challenges, opportunities

Kay Fjørtoft [a], Seyed Parsa Parvasi [b,*], Dag Atle Nesheim [a], Lars Andreas Lien Wennerberg [a], Odd Erik Mørkrid [a], Harilaos N. Psaraftis [b]

[a] SINTEF Ocean, Trondheim, Norway
[b] Department of Technology, Management and Economics, Technical University of Denmark, 2800 Kgs Lyngby, Denmark

ARTICLE INFO

*Keywords:*
Sustainable autonomous shipping
Maritime transportation
Resilience
Bow-tie method
Digitalization

ABSTRACT

This paper introduces a resilience assessment methodology for sustainable autonomous maritime transport networks developed by the European project entitled "Advanced, Efficient, and Green Intermodal Systems" (AEGIS). This problem being addressed in this paper concerns the investigation of threats, incidents, and risks in an autonomous- and sustainable shipping context, and the research question is the development of both preventive measures and reactive actions to maintain an acceptable level of operational constraints. The paper's methodology aids in designing sustainable logistics systems for highly automated waterborne transport, identifying threats and barriers to mitigate event consequences, thereby facilitating a seamless green transition. To examine the usability, this methodology is applied in a case study for cargo transportation, where we in this paper consider the maritime corridor between Trondheim and Rotterdam. The findings encompass the spectrum of possible actions to prevent and mitigate unwanted events and enhance resilience and flexibility. This can be used as a tool to respond to unwanted threats, enhance safety, and introduce new strategies. These results are deemed important as resilience is one of the prerequisites for the development of a sustainable transport system. This is true both for the companies that are engaged in the operation of such systems and for policymakers.

## 1. Introduction and background

These days, reducing greenhouse gases (GHG) is an important concern due to increased energy use (Park et al., 2022). The transportation industry is a significant source of these gases and its rate of becoming sustainable in terms of the environment is slower compared to other sectors (Deshmukh et al., 2023). While the transportation sector remains a significant contributor to global greenhouse gas (GHG) emissions (OECD, 2022), the movement of goods and passengers by sea stands out as a recognized and sustainable approach to maintaining a balanced global trade, distinguishing itself from other transportation modes (Fjørtoft and Mørkrid, 2021). Hence, the European Union's maritime transport policy (European Communities, 2009) and the European Green Deal (European Commission, 2019) both understand the importance of water-based transportation in promoting sustainability in Europe. To make the environment more sustainable and reduce our environmental impact, the EU seeks to shift 30 % of road freight to waterborne and rail transport by 2030 and more than 50 % by 2050 (European Commission, 2011). This will increase the importance of the need to pay attention to issues related to the resilience of this transportation method. Indeed, if maritime transport were to stop, it would have severe consequences for everyone (UNCTAD, 2020). The incident involving the MV Ever Given, a large ship carrying over 20,000 TEU (twenty-foot equivalent unit), getting stuck in the Suez Canal in March 2021 highlighted weaknesses in maritime trade and had an impact on trade between Asia and Europe. As a result, many ships had to take a much longer route around the coast of Africa, adding two weeks to their journey. The accident not only affected ship navigation but also created significant challenges for the ports on both ends. All the ships arrived at the destination ports at the same time, causing congestion and placing demands on the terminal's cargo handling equipment and logistics. Many shops run out of goods, which resulted in higher prices and an unforeseen problem to serve the customers. Industry actors were also missing components used in their production. This accident demonstrated the vulnerability of the maritime transport system and emphasized the importance of being resilient in this sector. Alternatively, the

* Corresponding author.
*E-mail address:* paparv@dtu.dk (S.P. Parvasi).

https://doi.org/10.1016/j.clscn.2023.100126
Received 20 October 2023; Received in revised form 27 November 2023; Accepted 28 November 2023
Available online 30 November 2023

emergence of innovative technologies such as autonomous ships will bring about a transformation in resiliency in maritime transport. In order to effectively address emerging risks, unfamiliar situations, and various types of incidents, it is imperative for planning and management to adopt proactive measures. Traditional indicators alone are no longer sufficient, necessitating the incorporation of new foresight indicators that can effectively handle both predicted and unexpected events (Stene, 2020).

In the context of the above background, the purpose of this research is to explore the critical role of resilience in autonomous shipping systems. Resilience is defined as the ability to prevent events that may lead to disruption, or, should this prove impossible, quickly recover once such events cannot be prevented. The importance of this research lies in the increasing implementation of sustainable automation in vessels and maritime infrastructure, including ports and terminals. While these advancements promise efficiency and sustainability, they also introduce new risks. It is crucial to understand how different stakeholders and systems are interconnected in the operation of Maritime Autonomous Surface Ships (MASS) and how the risk landscape is shaped by technological and human factors. To achieve this purpose, a comprehensive understanding of potential events and threats within the transport chain and system, as well as to identify barriers and plan appropriate actions in the event of disruptions are needed. This paper seeks to make a meaningful contribution to the maritime transport sector by conducting a thorough analysis of risks within the autonomous ship chain, considering different sources of threats (such as human and technological factors), and also investigating possible measures to prevent and/or mitigate these risks. The objective is to prepare for unexpected situations and enhance the resilience of autonomous shipping in the maritime sector.

Understanding resilience means being able to maintain the essential functions of a system before, during, and after changes in the operating environment. Woods (2015) identifies four common uses of resilience: (1) bouncing back and returning to a stable state (rebound), (2) being strong and able to withstand challenges (robustness), (3) being flexible and adaptable when unexpected events occur (opposite of brittleness), and (4) having network structures that can adapt to future changes (network architecture). It is worth mentioning that, intentionally, Woods' third definition does not consider because it pertains more to the operational performance of the system rather than its safety. The method that can be used to evaluate resilience based on these concepts is the bow-tie diagram method which includes preventive barriers, reactive barriers, to be used to prevent unforeseen events and minimize consequences if an event occur. So that, firstly, the notion of rebounding actions is linked to reactive barriers. Secondly, robustness is related to preventive barriers, aiming to minimize the occurrence of unwanted events. The idea behind robustness is that a highly robust system should effectively prevent such events from happening. Thirdly, the capacity to adapt to future events is connected to unforeseen events (Hollnagel, 2019).

The methodological framework described above strongly aligns with the so-called Formal Safety Assessment (FSA) framework used by the International Maritime Organization (IMO) to evaluate risk in maritime activities and determine the best course of action to reduce risk (IMO, 2021). The FSA is typically used to address maritime safety issues (Psaraftis, 2012), and it has also been expanded to address environmental concerns (Psaraftis, 2008). Indeed, the stages of hazard identification, risk assessment, risk control options, cost-benefit assessment, and recommendation for decision-making are five stages specifically suggested by the IMO's Guidelines on the application of FSA (Fig. 1).

From another point of view, resilience also encompasses both design vulnerabilities, disasters, and external attacks, with the vulnerability being a weakness and attacks being purposeful actions performed by attackers (Evensen, 2020). Due to the importance of this issue, various research has been done on each of the dimensions of risks and even the combination of these in the resilience literature in maritime transportation (Gu and Liu, 2023). Omer et al. (2012) explored strategies to enhance resiliency in maritime transportation systems (MTS) by reducing vulnerability and increasing adaptive capacity to mitigate the impact of disruptions on ports and goods movement. The study applied

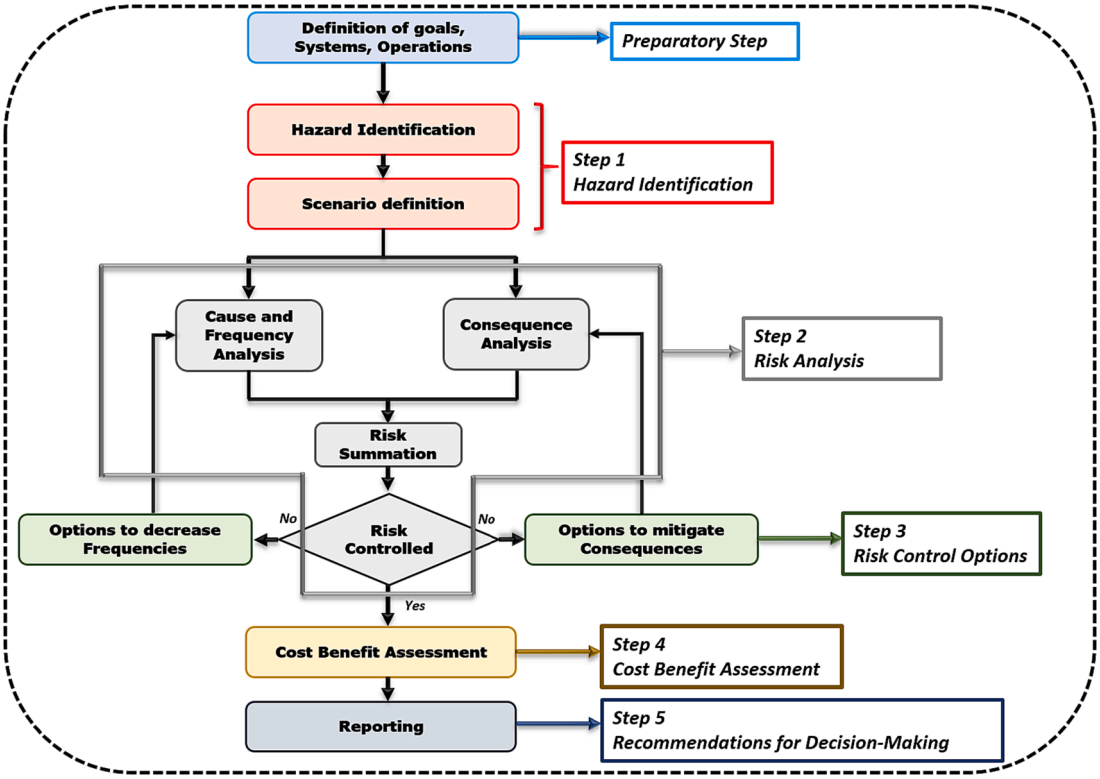



**Fig. 1.** FSA Flowchart. Source: IACS.

the networked infrastructure resiliency assessment framework, including network modeling and optimization techniques, to evaluate the impact of schemes such as diversity, collaboration, and resource allocation on key resiliency metrics, including tonnage, time, and cost resiliency. These efforts sought to improve MTS's ability to bounce back and deliver goods efficiently after shocks or disruptions. Koimtzoglou et al. (2022) introduced the new smart risk assessment platform (SRAP), designed to aid ship masters and their bridge command teams in assessing risks during emergency situations, particularly during ship evacuations. SRAP employed Bayesian networks to dynamically assess safety risks at different stages of the evacuation process, and a case study demonstrates how factors like injuries, congestion, and ship system functionality impact the decision-making process. Verschuur et al. (2020) by examining real data that port disruptions caused by natural disasters found that that disruptions have a median duration of six days, often affect multiple ports simultaneously, and are influenced by the severity of the event. The study challenges some modeling assumptions, as it finds limited substitution between ports during short-term disruptions and highlights that production recapture occurs in many cases, providing valuable insights for future modeling studies to better understand port and maritime network resilience. In terms of policy and regulation, Zavitsas et al. (2018) explored the interplay between maritime security and environmental regulations in the context of supply chain vulnerability and emissions. It establishes a framework that considers the impact of Emission Control Areas, analyzing various abatement options, disruption intensities, fuel pricing, and regulatory strategies. The research sought to help policymakers with tools to manage both environmental and resilience legislation in maritime supply chains, optimizing performance and reducing exposure to costly disruptions. Dui et al. (2021) highlighted the critical importance of resilience in maritime transportation systems, especially in the face of political and natural disruptions. It proposed a new method to optimize the resilience management of ports and routes after such disruptions and introduced an optimal resilience model. The study employed the Copeland method to rank the importance of ports and routes comprehensively and explores restoration priorities for interrupted ports and routes, aiming to minimize residual resilience and enhance the system's ability to handle interruptions.

Another important issue in maritime resilience is cyber-attacks, which is known as a major weakness in computers and networks. Attackers carry out these attacks to manipulate, harm, access without permission, or disrupt networks, computer systems, and smart devices (Tunggal, 2020). This concern would be of more crucial importance in autonomous systems. Indeed, the rise of digital transformation and real-time data exchange introduces the risk of increased fragility. For instance, studies focusing on the cyber resilience of ship information systems suggest that the widespread use of remote-controlled autonomous technology in modern ships may lead to a surge in novel cyber-attacks globally (Onishchenko et al., 2022). Kanwal et al. (2022) evaluated the relationship between critical dimensions affecting cybersecurity performance in the maritime industry, highlighting the influence of regulations on company procedures, shipboard systems readiness, training and awareness, and monitoring. The paper suggested that strengthening training and awareness can positively impact the cybersecurity performance of ships. Dagdilelis et al. (2022) focused on cyber-resilience in autonomous marine vessel navigation, addressing sensor fusion, abnormal behavior diagnosis, and change detection. It introduced a two-stage estimator for diagnosing and mitigating sensor signals during coastal navigation, using a likelihood field approach to extract shoreline and buoy features. The study showed the ability to detect and isolate attempts to compromise position measurements, offering a new approach for high-level data processing and demonstrating the detection of deviations from nominal behavior under attack or when defects occur in navigation sensors.

On the other hand, it can be seen that resilience approaches in autonomous systems are influenced by various factors, including effective communication and collaboration between humans and technology. Resilience, within a socio-technical system involving humans, technology, and organizations, refers to the ability to sustain operations and achieve system goals under diverse conditions, including unexpected events (Schröder-Hinrichs et al., 2016). In addition, the autonomous shipping system involves external stakeholders, including traffic centers, vessel traffic services, ports, terminal operators, and governmental support centers, among others, all of whom play essential roles within the operational chain. Each stakeholder has specific tasks and responsibilities contributing to the overall functioning of the system. The risk level associated with the operation is a comprehensive assessment of all risks arising from technological factors and human engagement. To describe better, Fig. 2 demonstrates the transportation chain in autonomous vessels and how different stakeholders are related in this chain. Therefore, it is crucial to integrate resilience into autonomous systems by addressing human, operational and technological limitations, as well as assessing safety and criticality. This includes considering risk elements that can be both technological and operational in nature. While certain risk categories in autonomous shipping may be similar to those in conventional shipping, the introduction of autonomy brings about new and yet unknown risks. However, it is anticipated that automation will have a positive impact and contribute to a reduction in overall accidents compared to conventional shipping (Hoem et al., 2021). Abaei et al. (2022) addressed the significant impact of digitalization and automation on the maritime transportation industry and emphasized the importance of assessing unattended engine rooms' performance and resilience in autonomous vessels. It presents a machine learning-based model that predicts the engine room's performance and estimates the duration it can operate without human intervention. The model employs techniques such as Random Process Trees, Hierarchical Bayesian Inference, and probabilistic Bayesian Networks to evaluate the system's reliability and resilience. The study offered valuable insights into understanding and predicting untoward events in unattended engine rooms and demonstrated the model's application with a real case study involving a merchant vessel in European waters. Fjørtoft and Holte (2022) addressed the potential of autonomous ferries in revolutionizing passenger transport, offering flexible, unmanned services for coastal cities and inland waterways. However, it emphasized the need to develop new safety solutions to replace the roles of onboard safety crews, as current rules and regulations require. The paper introduced the concept of operational envelopes as a way to enhance safety and resilience in autonomous ferry operations, highlighting the importance of balancing the focus on safe navigation with the development of comprehensive safety systems and processes. Mallam et al. (2020) investigated the evolving role of humans within complex socio-technical systems, particularly in the context of autonomous technologies in maritime operations. The research was extracted from interviews with Subject-Matter Experts from both industry and academia and identified four primary themes: Trust, Awareness and Understanding, Control, and Training and Organization of Work. Additionally, a fifth theme, Practical Implementation Considerations, emerged, covering various aspects related to the real-world implementation of autonomous ships. The study offered insights into the human element issues that are crucial for the organization and deployment of autonomous maritime operations. In following, Veitch and Alsos (2022) reviewed the role of human supervision and control in the context of autonomous ships, addressing key questions related to their adoption, safety concerns, and design challenges. The findings revealed that human operators play a significant role in ensuring the safety of autonomous ships, with specific risk assessment tools being commonly employed. Additionally, the emergence of shore control center operators highlighted the need for new competencies and training in the field. The study emphasized the growing importance of human-AI interaction design and the importance of interdisciplinary efforts to balance productivity with safety, address technical limitations, and manage the interaction between machine task autonomy and human supervisory control in the context of autonomous

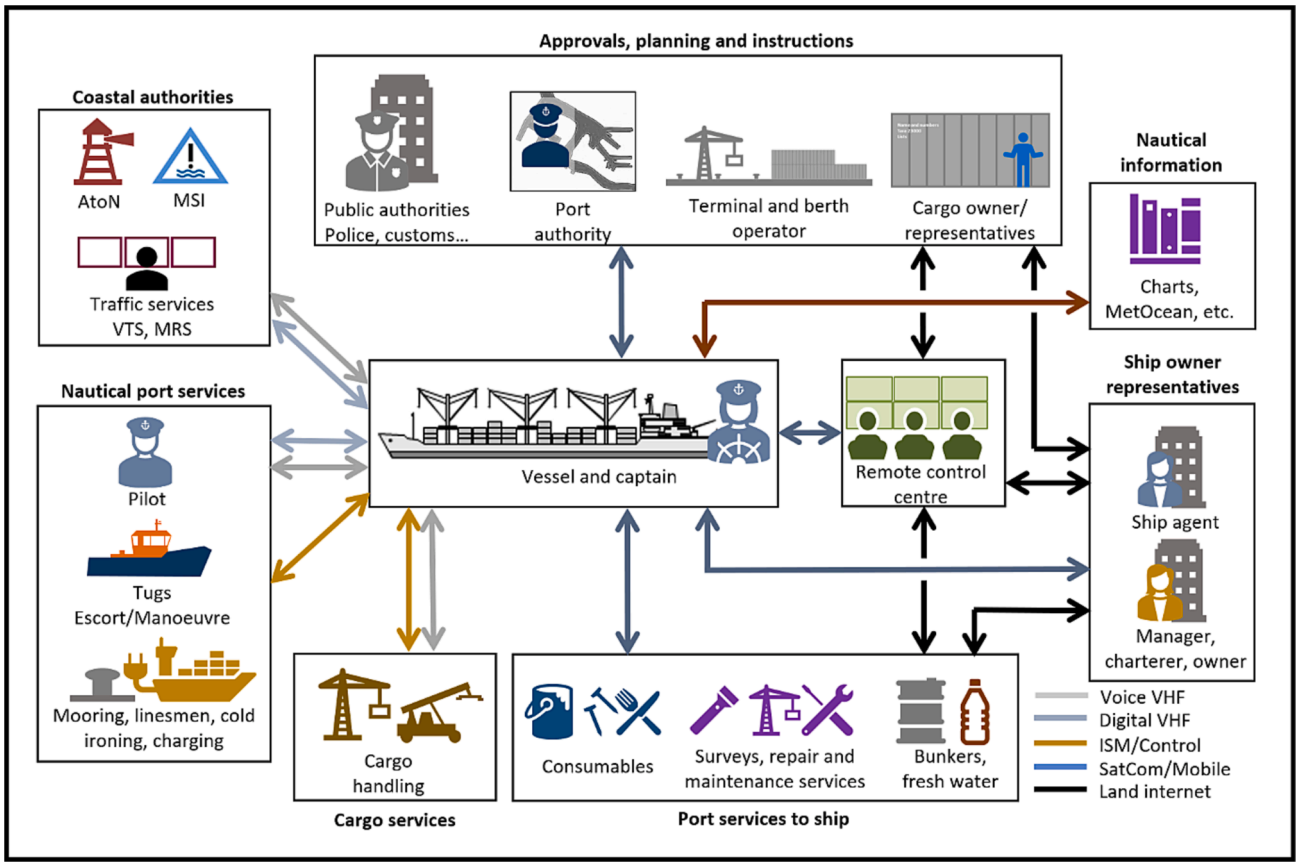



**Fig. 2.** The entire maritime transportation system.

shipping.

Besides academic research, several EU projects like Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) have run and focused on ensuring the safety and security of autonomous and large merchant ships, considering both human and technological aspects (MUNIN, 2016). In terms of technological issues, building robustness, redundancy, and options for recovery are important (Hollnagel, 2019). Operational knowledge plays a significant role, particularly when transitioning from a sea-based to a shore-based captain for MASS operations. The shore captain's responsibility may involve navigating multiple vessels simultaneously, requiring expertise beyond conventional navigation. Zhou et al. (2019) have examined resilience in sea transport, aiming to enhance safety through comprehensive risk assessment at both theoretical and operational levels, considering the unique characteristics of water transport. It is essential to recognize that while the MASS automation system is designed to make independent decisions, there may be situations where human intervention and expertise are necessary. In addition, achieving resilience necessitates the integration of plans across the value chain, encompassing various planning stages and geographical areas.

Given the study of literature review in autonomous ships and the critical role of resilience in this type of transport system, there is a pressing need for research to develop a comprehensive framework aimed at identifying potential threats and outlining strategies to address them both before and after threats. This study seeks to add a valuable contribution to the existing literature by introducing a new methodology inspired by the bow-tie approach for evaluating vulnerabilities in autonomous maritime transport. Indeed, this study is under the EU project named Advanced, Efficient and Green Intermodal Systems (AEGIS), funded under Horizon 2020, and has been implemented in Europe (AEGIS, 2023). In brief, the objective of the AEGIS project is to establish an advanced and environmentally sustainable waterborne transport system within Europe. By utilizing cleaner fuel engines, such as batteries and methanol, this system aims to implement innovations from the Connected and Automated Transport (CAT) domain to advance a maritime logistics system for the future. By aligning with the European Commission's strategic direction of shifting from road transport to more sustainable alternatives such as waterborne and rail transportation, the project aims to contribute to the reduction of greenhouse gas (GHG) emissions (European Commission, 2011). Additionally, the AEGIS project seeks to improve the efficiency of the transport system through the introduction of smaller vessels, which would result in increased frequency, varying speeds, reduced terminal costs, and shorter port times. The implementation of remotely controlled vessels also enables centralized control from a dedicated control center, further enhancing operational capabilities (Krause et al., 2022).

In particular, this paper, which uses the three-year results of the AEGIS project, focuses on implementing resilience in the sustainable autonomous shipping system. To fill the research gap in identifying and categorizing the novel risks in autonomous shipping transport, we describe a set of vulnerabilities in different levels of threat sources named human, organizational, and operational sources, technological sources, and external. Following the identification of threats, comprehensive measures are introduced to both mitigate the likelihood of these threats occurring and minimize their impact in the event of an incident.

The remaining sections of this paper are organized as follows: Section 2 presents the real case study that serves as the foundation for our examination. In Section 3, we describe our methodology. In Section 4, we introduce threat sources and then how to mitigate those threats described in Section 5. Section 6, we implement our proposed methodology as a real example. Finally, in Sections 7, we present a discussion and the paper's conclusions based on our findings.

## 2. A case study of short-sea shipping corridor from west coast of Norway to Rotterdam in the Netherlands

This case study in the AEGIS project is led by the Norwegian shipping company North Sea Container Line (NCL), along with the inter-municipal port of Trondheim and the research company SINTEF Ocean Company. Grieg Connect contributes with software experience as a provider for ports, terminals and maritime transport stakeholders, and DFDS have contributed with valuable comments from other corridors, as a supporting contributor to the Use Case. The case focuses on moving cargo from the biggest port in Europe (Rotterdam) to smaller places along the west coast of Norway. NCL uses a Load-on, Load-off (LoLo) service and currently operates four container vessels with a capacity of about 1000 TEUs each, vessels that are about 10,000 Gross tonnage. NCL is about to renew its fleet and have two new vessels in production to be launched in 2024, with a capacity of about 1300 TEU each, that will be sailing on methanol and use battery energy in the ports. The ambition is to replace three of their current, diesel-powered ships. Since the size of the vessel is increasing, it will be necessary to rethink the logistics. It is likely that they will serve fewer terminals with the mother vessel, which requires the new need for smaller vessels, with the ambition to be autonomous at the end, to feed the main ports along their chain. It takes about one extra sailing day to visit a port in the inner Trondheim fjord compared to having a turnaround on the island Hitra, located at the start of the fjord. This also means the capacity utilization will increase on the new vessels. The use case is used as a study case for the implementation of a methodology to assess the resilience of autonomous shipping. The use case planned for the use of small unmanned and preferably autonomous and electric vessels to transport the cargo to the connection points at the port of Hitra before the mother vessel was transporting it to the continental destination in Rotterdam. This case study explores the entire container transport process along the Norwegian coast, aiming to identify opportunities for enhanced collaboration among transport operators to offer more user-focused services.

The AEGIS transport system, illustrated in Fig. 3, will comprise mother and daughter vessels exchanging cargo at a transshipment terminal (port of Hitra). It will be divided into two main segments, as outlined below:

1. The transport between Rotterdam in the Netherlands and Hitra Kysthavn in Norway (Fig. 4 as region 1).

2. The transport within the Trondheim Fjord region in Norway (Fig. 4 as region 2).

Indeed, the AEGIS concept involves a different operating approach than the current practice. The core idea is to deploy one or more mother vessels to travel between Rotterdam and Norway, carrying substantial cargo volumes and incorporating a higher level of automation to benefit from economies of scale, and use of sustainable alternatives. As these mother vessels navigate along Norway's west coast, a fleet of daughter vessels can handle cargo transportation between a designated set of regional ports and the mother vessel. Although our project focuses on the Trondheim fjord, it's essential to note that this concept can be adapted for other corridors in Europe and even in various regions worldwide.

To enhance operational efficiency, this route has been divided into four distinct sub-routes, as shown at the bottom of Fig. 4. It is expected that some of the smaller terminals along the route may need to adopt self-service capabilities. Consequently, the autonomy level of the daughter vessel must allow for moving containers from the quayside onto the vessel without requiring human involvement at the quayside. Thus, a specialized daughter vessel with appropriate gear is necessary to handle containers at any terminal within the fjord.

To sum up, the mother-daughter concept emerged as a viable solution for this use case, with Hitra chosen as the hub for transshipment between the mother and daughter vessels.

Regarding ship specifications, for the mother vessels, we considered new short-sea shipping vessels capable of carrying around 1100 TEU (twenty-foot equivalent units) from Rotterdam to the Trondheim region. These conceptual ships would feature a hybrid propulsion system using methanol and batteries, with methanol being the primary fuel. Transitioning to this clean fuel system for autonomous ships in this region, as opposed to conventional ships that rely on diesel fuel, will significantly reduce carbon emissions.

As for the daughter vessel, we envisioned a self-propelled shuttle, fully electric with zero carbon emission, with a capacity of approximately 60 TEU. In this instance, two ships operate within the Trondheim fjord, collecting cargo from various smaller ports or industry sites.

Information on the design of these autonomous ships with eco-friendly fuels is presented by Krause et al. (2022). In addition, Zis et al. (2023) have performed a preliminary cost benefit analysis of the AEGIS system.

## 3. The AEGIS resilience methodology

To assess the reliability of a logistic chain, we consider various operations involving different stakeholders in transportation. We also consider different threats, unwanted events, potential consequences, and measures to reduce their likelihood or impact. Bow-tie diagrams are then used to visualize these probabilities and consequences, which affect the resilience of the logistic chain. The bow-tie method is a structured approach for identifying and visualizing safety-related barriers and measures, both for preventing and reacting to unwanted events. Fig. 5 shows the bow-tie diagram with sources of threats on the left side, the top event in the middle, and possible consequences on the right side. Arrows represent the connection between threats, the top event, and its consequences. Barriers or measures in green are used to reduce the likelihood of the top event and unwanted consequences in orange.

To assess resilience, one must first consider the operations that want to be evaluated before identifying potential unwanted events, associated threats, preventive mitigation measures, and potential consequences with reactive mitigation measures. In logistics chains, there are various ways to assess the overall resilience of transporting goods from origin to destination. Often, cargo owners are primarily concerned with this aspect.

There are two main reasons for using this framework in the case study. First, it helps assess the reliability of the operational, physical, and/or digital processes that make up the logistic chain. Second, it helps identify threats, measures and barriers to improve resilience, which can be implemented by individual stakeholders in the logistic chain.

The methodology is considered generic and valuable for developing solutions beyond the project's primary focus of dealing with abnormal events. It consists of six steps (See Fig. 6):

**Step 1:** Describe different impact categories to define the analysis focus. An impact category is potential that can be suffered when an event occurs (step 2). It can be a category that goes to "humans", that

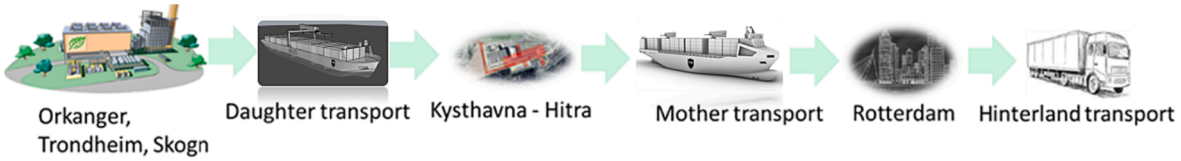



**Fig. 3.** The AEGIS transport systems.

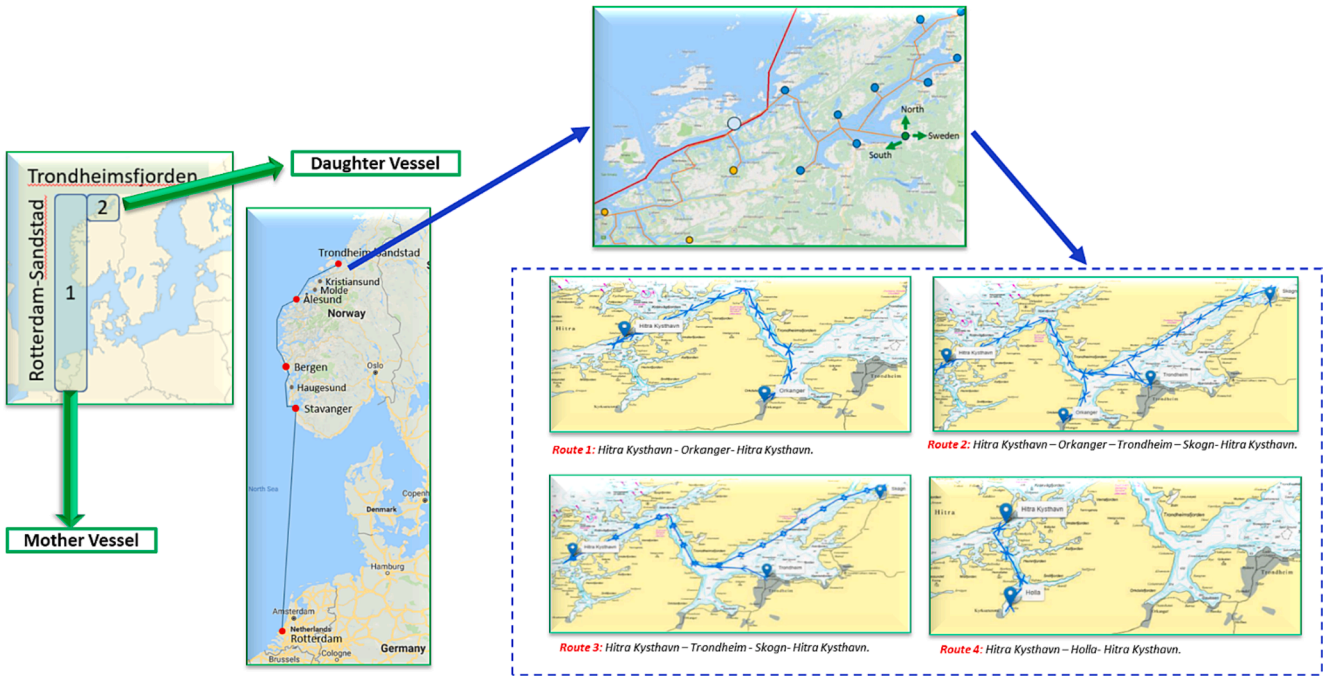



**Fig. 4.** Short-sea connection to Norway and Local distribution in Trondheim Fjord.

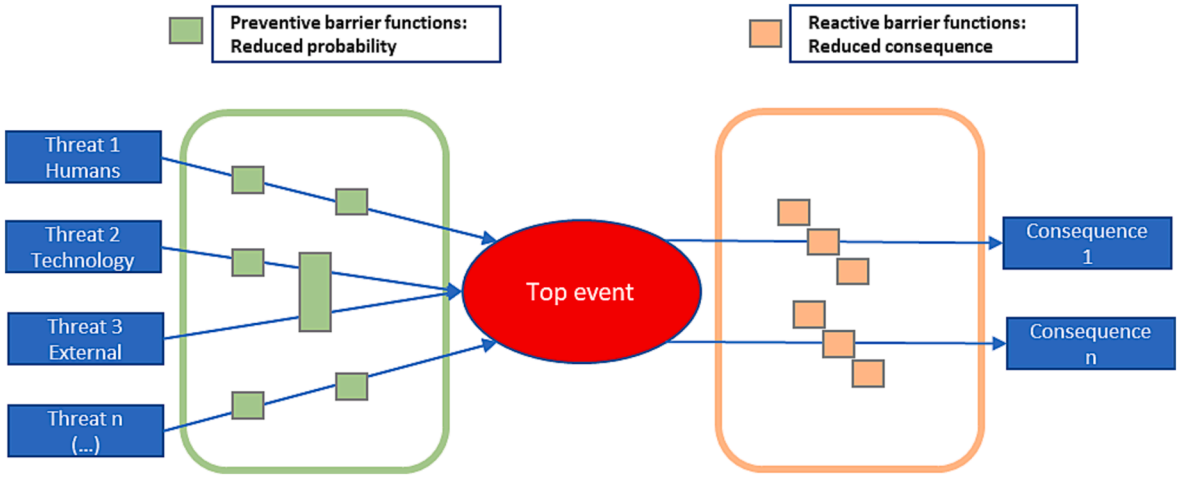



**Fig. 5.** Generic bow-tie diagram.

can be a safety-related issue, or it can be a category pointing to "reputation" that are more concerned to the transport service quality. When working with the methodology it is important to firstly decide what category to focus on, to limit the scope. The list of categories in our example can be changed; the examples listed are based on the categories from the use case described above.

**Step 2:** Identify various top events related to the consequences identified in step 1, forming the basis for further analyses. This step is to identify possible events that can happen, that are related to the impact categories. A top event to "human" can be an injured person, while a top event to "reputation" can be damage to cargo or time deviation to transport.

**Step 3:** Use workshops to identify relevant sources of threats that can trigger the selected top events in the bow-tie diagram. The methodology has suggested a list of possible threats that might be of relevance to a top event. It is organized in humans, organizational and operational oriented, regards technology, and to external threats that often are threats that are hard to prevent and are outside the control of an operator.

**Step 4:** Link the most critical sources of threats to possible preventive barriers and measures, forming the structure for developing preventive measures. The methodology has identified a set of possible preventive barriers to be used when doing the studies, that can be used as it is or can be replaced with new barriers suggested within a case study. The meaning is to prevent a top event from happening.

**Step 5:** Identify possible reactive barriers and describe potential consequences if these barriers fail, based on the top event that occurs. These reactive barriers mission is to reduce the consequences of an event after the event has occurred. This is also to think about potential resilience activities to be launched. If an "injured person" was the top event, then medical treatment or support from a medical center to handle the situation could be planned for. If loss of reputation was the event, the use of media or professionals to be the contact person to the media or to the customers could be the reactive barrier to be used. Also, price reduction is a possible reactive barrier regarding loss of reputation.

**Step 6:** Identify the worst possible consequences of a top event. This step must be aligned with step 1, the impact group selected for the use

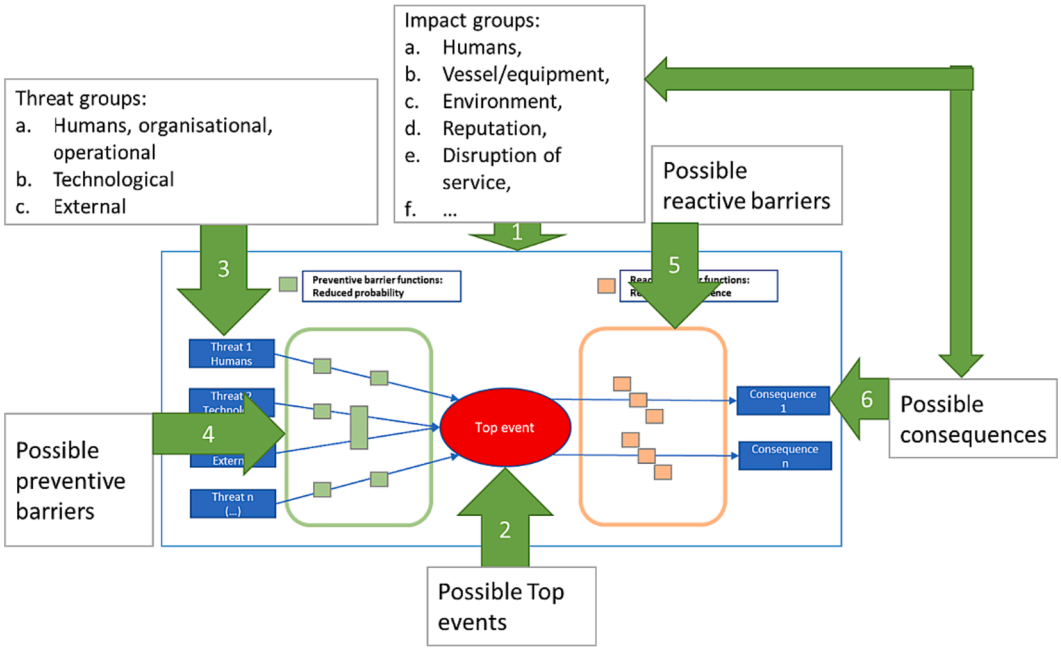



**Fig. 6.** Steps in the AEGIS Resilience methodology.

case. It is important to prepare for the worst possible consequences, that in the example above could be an injured person can lose its life, or loss of reputation could lead to loss of customers.

The steps described above can be illustrated as shown in Fig. 6.

Workshops organized by AEGIS Use-cases helped develop the framework, and visualization techniques aided in identifying relevant threats and top events following the AEGIS use cases. The results, along with discussions with project partners, formed the basis for the framework.

It's worth mentioning that while there is no direct one-to-one mapping between the steps of the AEGIS method and FSA, there is a clear equivalence between Steps 1 and 2 of FSA and Steps 1, 2, and 3 of the AEGIS approach. Step 3 of FSA corresponds to Steps 4 and 5 of the AEGIS approach. AEGIS excludes FSA Steps 4 and 5 (Cost Benefit Assessment and Recommendations for Decision Making), but these can follow the resilience assessment using its results.

In the rest of this section, each step of the AEGIS methodology will be explained in more detail.

### 3.1. Step 1: Identification of impact categories

Selecting relevant impact categories for a case study is crucial for identifying appropriate top events and maintaining a consistent analysis. The impact categories include human/people, technology, equipment, infrastructure, environment, reputation, and disruption of services (Table 1). "Disruption of services" is of primary interest in AEGIS use cases, but assessing the impact of introducing automation or autonomy is also relevant. It is also important to mention that the following tables are only examples, the use case studies must define its own definition and limitations such that the value will of a study will be higher.

### 3.2. Step 2: Selection of top events

Through workshops, industry input, and available literature, the project identifies critical events to ensure sufficient logistics performance, including operational safety within the transport chain. The prioritization of top events in Table 2 is based on the real case study and the project group's experiences, primarily focusing on inland waterways transport, short-sea shipping operations, and terminal activities. When using the framework for other cases or focus areas, other top events not listed may be more relevant. The column to the left in Table 2 is related to the case study described above and can be deleted. The purpose of our study was to structure the event following the main transport corridors from a transport from Trondheim to Rotterdam. The list of top events is selected from the framework, but it is important to say that the list can be longer and include new top event types.

Step 6 can be addressed in conjunction with steps 1 and 2. The consequences will depend on the selected top events to be examined. Reactive barriers are utilized to mitigate the consequences, which is an integral part of the work in step 5.

**Table 1**
Impact categories.

| Impact categories | Description |
|---|---|
| *Humans* | The risk involves the potential loss of human lives or injuries to people within the transport chain. These individuals include passengers, workers on vessels and terminals, crew members, drivers, logistics personnel, and anyone else who encounters the transport operations. Different severity levels, such as loss of multiple lives or minor injuries, can be considered. |
| *Vessel, equipment, and infrastructure* | The risk involves potential loss or damage to vessel and terminal equipment. It can be measured through expected loss of monetary value, grading losses facilitating comparison of consequences from different threats. |
| *Environment* | The risk involves incidents damaging the environment (e.g., road users, vessels, quays) or through discharges. It can be expressed in monetary terms based on the expected damage or destruction. |
| *Reputation* | The risk involves incidents negatively affecting the operator's reputation and/or autonomous ship operations. The severity of impact categories (human, vessel, infrastructure, environment) influences the risk. |
| *Disruption of Service* | Any disruption of the transport chain, whether caused by technical failures, operational or administrative issues, or external factors like bad weather leading to deviations, can result in unexpected delays, damage to, or loss of cargo. |

**Table 2**
Top event.

| Relevance for (node/leg) | Top event | Typical reasons for the event |
|---|---|---|
| *Pickup location* | 1.1 Cargo delays (cargo not ready for pickup) | Manufacturer/vendor/ production delay; Traffic jam to pick up location; paperwork not ready |
| | 1.2 Load unit not available (the cargo has nowhere to be put) | Amount of cargo exceeds transport capacity |
| | 1.3 Loading equipment not available | Equipment failure or malfunction; Equipment faulty maintenance; Equipment busy with other loading tasks |
| | 1.4 Freight documents/ Clearance not ready | Delay of administrative/ customs procedures |
| *Pre-carriage* | 2.1 Loading equipment not available | Equipment failure or malfunction; Equipment faulty maintenance; Equipment busy with other loading tasks |
| | 2.2 Freight documents/ Clearance not ready | Delay of administrative/ customs procedures |
| | 2.3 Failure navigation/ berthing/mooring equipment/sensor | Failure of equipment |
| | 2.4 Transport means not ready for loading | Failure of vehicle; vehicle busy with other tasks |
| | 2.5 Energy for transport means not available | Exogenous energy crisis; shortage of energy |
| *Transhipment Terminal* | 3.1 Cargo not ready for discharge or loading (e.g., delayed arrival of precarriage) | Traffic jam outside the terminal; port congestion |
| | 3.2 Loading equipment not available | Equipment failure or malfunction; Equipment faulty maintenance; Equipment busy with other loading tasks; Automation System failure |
| | 3.3 Freight documents/ Clearance not ready | Delay of administrative/ customs procedures |
| | 3.4 Failure navigation / berthing /mooring equipment/sensor | Failure of equipment |
| | 3.5 Transport means not ready for loading | Failure of vehicle; vehicle busy with other tasks |
| | 3.6 Delays on transport means for main carriage | Traffic jam outside the terminal; port congestion |
| | 3.7 Energy for transport means not available | Exogenous energy crisis; shortage of energy |
| | 3.8 Storage infrastructure not available | Storage capacity exceeded |
| | 3.9 Failure in interaction between technologies for collaboration | Poorly designed interface; failure or malfunction of a component |
| | 3.10 Failure in communication | Failure of communication equipment |
| | 3.11 Failure in data integrity | Cyber-security breach |
| *Main carriage* | 4.1 Cargo not ready for discharge or loading | Traffic jam outside the terminal; port congestion |
| | 4.2 Loading equipment not available | Equipment failure or malfunction; Equipment faulty maintenance; Equipment busy with other loading tasks |
| | 4.3 Freight documents/ Clearance not ready | Delay of administrative/ customs procedures |
| | 4.4 Failure navigation/ berthing/mooring equipment/sensor | Failure of equipment<br>No berth available |
| | 4.5 Transport means not ready for loading | Failure of vehicle; vehicle busy with other tasks<br>Slow cargo operation<br>Bad weather<br>Lack of pilotage into port<br>Late arrival vessel |
| | 4.6 Energy for transport means not available | Exogenous energy crisis; shortage of energy |
| *Terminal* | 5.1 Cargo delays (cargo not ready for pickup) | Traffic jam outside the terminal; port congestion; loading equipment busy with other tasks<br>Lack of labor<br>Crane breakdown |
| | 5.2 Load unit not available (the cargo has nowhere to be put) | Amount of cargo exceeds transport capacity |
| | 5.3 Loading equipment not available | Equipment failure or malfunction; equipment faulty maintenance; equipment busy with other loading tasks; Automation system failure |
| | 5.4 Freight documents/ Clearance not ready | Delay of administrative/ customs procedures |
| | 5.5 Terminal shutdown | Personnel strike |
| *On carriage* | 6.1 Cargo not ready for discharge or loading | Traffic jam outside the terminal; port congestion |
| | 6.2 Loading equipment not available | Equipment failure or malfunction; Equipment faulty maintenance; Equipment busy with other loading tasks |
| | 6.3 Freight documents/ Clearance not ready | Delay of administrative/ customs procedures |
| | 6.4 Cargo and load unit damage | Damage due to bad weather/ accident/theft/vandalism |
| | 6.5 Transport means not ready for loading | Failure of vehicle; vehicle busy with other tasks |
| | 6.6 Energy for transport means not available | Exogenous energy crisis; shortage of energy |
| *Drop-off location* | 7.1 Cargo and load unit damage | Damage due to bad weather/ accident/theft/vandalism |
| | 7.2 Cargo not ready for discharge or loading | Traffic jam outside the terminal; port congestion |

### 3.3. Step 3: Selection of threats sources

Step 3 involves identifying threat sources based on defined top events, grouped into three main categories (Table 3); A) Human, organizational, and operational threats, B) Technological threats, and C) External threats. These threat sources have various subgroups, aiding in a more specific and detailed analysis.

Groups A and B of threat sources are controllable through design, procedures, etc. Also, group C of threat sources involves uncontrollable threats like environmental forces: waves, wind, currents, tides, and river water levels. As for the previous step, this list can be tailored different to meet other top events.

Table 3 shows various subgroups, some focusing on operational conditions and others on technology. This helps identify relevant threats for a selected event. Adaptation of the threat sources is crucial for the analysis scenario, connecting top events, user cases, and consequences.

**Table 3**
Sources of threats.

| # | Sources of threats |
|---|---|
| **Human, organizational, and operational sources of threats** | |
| 1 | Terminal workers and crew, external service providers, terminal workers, operation centre |
| 2 | Collaboration, low planning quality, information exchange between parties/ ICT-systems, procedures |
| **Technological sources of threats** | |
| 3 | Communication, remote operation, cyber attacks |
| 4 | Navigation and steering system, geotagging, geofencing |
| 5 | Vessels, Crane, Port equipment and resources |
| **External sources of threats** | |
| 6 | Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc. |
| 7 | Other external factors (e.g., other ship traffic, construction work) |

These identified sources form the basis for step 4.

### 3.4. Step 4: Identification of preventive barriers and measures

Step 4 involves identifying preventive barriers and measures (probability reduction) on the left side of top event in the bow-tie diagram. The diagram serves as an effective tool for communication and facilitates productive discussions. The goal is to establish an overview of relevant barriers and measures based on critical threat sources identified in step 3. Critical sources of threats are those with high probability of occurrence and the highest undesired consequences. The work is carried out as follows:

- Define the area of interest (refer to Table 3).
- Identify and select threats to investigate.
- Identify and select preventive barriers.

Section 5 provides a detailed description of possible preventive barriers and measures. These are adapted to the case study and threat scenarios being analyzed (top events). It's important to note that the design criteria for barriers and measures, such as RRF (risk reducing factor) and SIL (Safety Integrity Level), are also described, focusing on the effectiveness, safety, reliability, and quality of the measures.

### 3.5. Step 5: Identification of reactive barriers and measures

Step 5 complements step 4, selecting reactive barriers and measures to protect against undesirable consequences if a top event occurs (e.g., crane failure). These reactive barriers are on the right side of the bow-tie chart. The process is like step 4, using main threat categories to document the connection between sources, threats, and consequence-reducing measures.

### 3.6. Step 6: Identify possible consequences

"Reactive barriers" mitigate unwanted top events, and "Consequence" reveals potential outcomes if barriers fail. There is a strong connection between the top events defined in Step 1 and the consequences identified, representing the worst-case scenario if it will not be possible to stop the escalation of a top event.

## 4. Identification of threat sources

This section provides useful guidance for identifying relevant threats to transport resilience. It is a starting point for probability-reducing measures and barriers. It should be noted that threats will vary depending on specific user cases, such as route length, location, speed range, degree of autonomy, and technology used.

### 4.1. Human, organizational, and operational sources of threats

As can be seen in Table 3, the subgroups of this kind of threat are as below:

(1) Terminal workers and crew, external service providers, terminal workers, operation center.

(2) Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures.

The first subgroup focuses on threats resulting from human limitations or errors, incorrect procedures, or organizational limitations (Table 4). These threats can occur during vessel crossings, boarding and disembarking, and loading or unloading at terminals.

The "collaboration" subgroup addresses threats related to communication and coordination between people, workers, drivers, providers, and operators across different organizations (e.g., between vessels, control centers, and terminal workers). Effective communication is crucial, like for external service providers communicating with operators of unmanned vessels. Collaboration is also essential in managing undesirable events and following appropriate procedures. These procedures should clearly define responsibilities for various actions/incidents and establish the division of responsibilities among the actors in the transport system. Overall, the threats in this subgroup are associated with deficiencies, uncoordinated situational awareness, and an inability to coordinate interactions among the involved actors (Table 5).

**Table 4**
Threats sources passengers, crew, and terminal workers.

| # | Threats sources terminal workers and crew, external service providers, operation centre |
|---|---|
| 1 | Crew and terminal workers with unforeseen medical needs (cardiac arrest, malaise, seizures, and loss of consciousness, etc.). |
| 2 | Crew and terminal with unintentional or erratic behaviour – acting out and/or under the influence of drugs. |
| 3 | Crew and terminal workers with inadequate ability to handle. |
| 4 | Crew, drivers, and terminal workers in shock and/or with an irrational reaction pattern (e.g., in the event of an accident, stress). |
| 5 | Accidents within the transport systems, as example crew falls into the water at the quay side ("Man overboard" observed and not observed). |
| 6 | Crushing injuries for crew and terminal workers (especially boarding and alighting). |
| 7 | Lack of control over the number of people at the terminal area or on board the loading zone at a vessel. |
| 8 | Stress due to low staffing, crews/terminal workers have too many tasks that must be handled in parallel. |
| 9 | Lack of control over what crew/workers carry on board which can be threat source. |
| 10 | Lack of competence (for example in control centres, medical expertise, technical expertise). |
| 11 | Insufficient information for training of operators and crew (vessel, ROC, terminal, drivers, …). |
| 12 | Inadequate procedures and liability maps. |
| 13 | Use of open fire on board or at the terminal (incl. Smoking). |
| 14 | Language problem between the involved stakeholders and workers |
| 15 | Lack of procedural understanding in cargo operation |
| 16 | Lack of common situational awareness of the operation |
| 17 | Poor planning quality or operational knowledge |
| 18 | The ability to stop loading or transport operations (access to control/operation system or contact with operational staff) |
| 19 | External service providers are not receiving authority to do maintenance work |
| 20 | External service providers are not familiar with the safety or operational instructions to perform their work |

### 4.2. Technological sources of threats

According to Table 3, the technology threat source group comprises three subgroups (communication and technical, navigation, and vessels)

**Table 5**
Threats sources collaboration low planning quality, information exchange between parties/ICT-systems, procedures.

| # | Threats sources collaboration low planning quality, information exchange between parties/ICT-systems, procedures |
|---|---|
| 1 | Uncoordinated interaction between control centre, autonomous vessel, and with terminal services. |
| 2 | Loss of control centre capability to remotely assist autonomous operations (vessels, cranes, etc). |
| 3 | Inadequate and poorly rooted planning procedures for cargo handling |
| 4 | Limited opportunity to assist loading operations from a ROC, or from stakeholders involved in a loading process. |
| 5 | Language and cultural barriers between control centres and workers (non-English-speaking workers). |
| 6 | Different situational understanding between vessel and control centre. |
| 7 | Lack of collaboration possibilities between workers and operation centre, and with the stakeholders involved in the transport system. |
| 8 | Overloaded role for remaining staff in safety–critical operations. |
| 9 | Lack of interaction between crew, terminal workers, port authorities. |
| 10 | Lack of procedures for handling deviation/damage management (time, resources, equipment, damages, …) |
| 11 | Lack of documentation for cargo/load units to be transported (clearance, safety, insurance, etc) |

that are vital for safe vessel navigation and effective monitoring, operation, and control from a control center.

The "Communication and technical" subgroup encompasses threats related to communication problems, loss of communication, and deliberate actions to compromise communication and technical systems, emphasizing the need to identify critical sensors and assess potential backup or redundant systems. For instance, errors in charging infrastructure can limit a vessel's energy supply, potentially leading to a top event (Table 6).

The second subgroup focuses on functional hazards during navigation and manoeuvring, as these threats are crucial to address, impacting the vessel's safe navigation and maneuverability (Table 7). Finally, the last subgroup focuses on threats or damages on vessels, resources or infrastructure that can disrupt the performance (Table 8).

### 4.3. External sources of threats

External sources of threats have two subgroups:

1. Threat sources related to weather, closure of parts of the route (sea-leg, terminal, gate, etc.), tide and low water, strikes, etc., are of operational and technical nature. These provide input for design requirements that need to be met (Table 9).

2. Threat sources for other external factors encompass threats that are often beyond the vessel's control, such as uncontrollable threats (Table 10).

## 5. Measures to enhance resiliency

The main purpose of this section is to deal with the measures before and after the occurrence of the threats stated in the previous section in order to strengthen the system's resilience. It is worth mentioning that these measures are categorized based on the nature of threats (humans, organizational and operational, technological and external). This chapter summarizes some barriers and measures identified by the project in light of the AEGIS project's defined case study.

### 5.1. Preventive and probability-reducing measures

According to the categories of threats presented, Tables 11-13 section state the measures that can prevent its occurrence and reduce its probability. Also, Fig. 7 shows that a preventive barrier can be related to a specific threat source or have a function against several.

### 5.2. Reactive and impact-reducing measures

This subsection provides an overview of the reactive barriers and measures that the project has identified. The aim is to suggest appropriate barriers and measures that can mitigate or eliminate any unfavorable outcomes following top events (Fig. 8). Tables 14-16 list the measures based on the categories of threats, like preventive and probability-reducing measures.

**Table 6**
Threat sources communication, remote operation, cyber attacks.

| # | Threats sources communication, remote operation, cyber attacks |
|---|---|
| 1 | Loss of communication between vessel/terminal/crane and control centre. |
| 2 | Errors on data and sensors (e.g., for fire detection, water intrusion, geofencing of cargo, temperature sensors, etc). |
| 3 | Lack of access to data for establishing situational awareness (for the ship's autonomy system and control centre). |
| 4 | Error on charging- and energy infrastructure. |
| 5 | Loss of communication for remote operation of equipment or vessel |
| 6 | Lack of knowledge regarding various on-board systems, terminal systems, operation systems and their capacities, and how they can be operated. |
| 7 | Lack of understanding of available land-based communication and technical infrastructure. |
| 8 | Loss of possibilities to communicate between involved ICT-systems (different management, owners, stakeholders, etc) |
| 9 | Error and downtime at the control centre. |
| 10 | Cyber-attacks or Computer attacks aimed at sensors and control system at the vessels, terminals, or control centres. |
| 11 | Loss of possibilities for situational awareness because of technical failures (CCTV, Communication, Navigation, Observation) |

**Table 7**
Threats sources navigation and steering system, geotagging, geofencing.

| # | Threats sources navigation and steering system, geotagging, geofencing |
|---|---|
| 1 | Loss of navigation sensors or digital signals for navigation, steering or status |
| 2 | Machinery failure (i.e., reduced propulsion on a vessel). |
| 3 | Incomplete situational awareness (e.g., lack of understanding of traffic picture in operating area). |
| 4 | Lack of detection of objects in fairway (e.g., paddlers, leisure boats), or objects at a terminal. |
| 5 | Fault in / Insufficient dynamic positioning system on vessel, terminal, or crane |
| 6 | Loss of geotagging/cargo mark for loading or unloading operations |
| 7 | Non-compliance with ColReg. |
| 8 | Loss of possibilities of geofencing areas |
| 9 | Loss of sensors due to failures or low battery percentage |
| 10 | Loss of opportunities of remote operation |

**Table 8**
Threats sources vessel, crane, port equipment and resources.

| # | Threats sources vessel, crane, port equipment and resources |
|---|---|
| 1 | Not detected water intrusion, leaks, and damage to the vessel |
| 2 | Control systems and equipment is damaged and cannot be used |
| 3 | Fire and / or smoke development in: engine room / battery room / lounge / control systems / cargo or other technological installations. |
| 4 | Failure in secure connection/interaction between vessel/resources and sensors in the infrastructure |
| 5 | Lack of standardisation such that vessel cannot use port infrastructure (i.e., energy loading point in infrastructure is not tailored to vessel position) |
| 6 | Lost opportunity for remote control of sensors, cranes, water doors and hatches. |
| 7 | Lack of detection of objects in fairways (e.g., fog and rain negatively affects sensors / camera). |
| 8 | Insufficient energy capacity on the vessel for loading activities, or for sailing. |
| 9 | Insufficient information sharing between systems and organisations |
| 10 | Loading system break down or failure |
| 11 | Crane Valve leakage |

**Table 9**
Threats sources Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water.

| # | Threats sources Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, etc. |
|---|---|
| 1 | Operation is initiated at the wrong time (premature start of docking/crane operations vs. late start). |
| 2 | Lack of understanding of the time consumption regards operation. |
| 3 | Crushing injuries/damages when launching container operations, loading, and unloading containers from cargo deck at vessel or terminal. |
| 4 | Improper use of equipment. |
| 5 | Lack of information/instructions from the control centre, terminal workers, or crew regards operation. |
| 6 | Lack of understanding of (or overview of) the need to assist technology during a critical incident or operation (Operational Envelope) |
| 7 | Lack of coordination of an operation (e.g., between terminal workers and control centre, but also where external services/providers are involved). |
| 8 | Lack of control of equipment. For example, if somethings falls into a not controlled area, there may be a need to navigate crane or vessel to achieve operation capabilities. |
| 9 | Wind or other MetHyd-forces makes it difficult to perform loading activities |
| 10 | The vessel have difficulties to be served due to not tailored infrastructure (i.e., the tide water makes the distance between terminal and vessel too big) |
| 11 | The terminal is not ready for the vessel |
| 12 | The vessel cannot be sailed into port because bad weather |
| 13 | The vessel cannot be sailed into port because of no pilotage available |
| 14 | The vessel cannot be served because of lack of terminal resources (workers, crane, terminal tractors, etc) |

**Table 10**
Threats sources other external factors.

| # | Threats sources other external factors |
|---|---|
| 1 | Handling a safety–critical operations in severe weather (e.g., strong winds, large waves, fog, darkness). |
| 2 | Insufficient ability to assist externally vessels. |
| 3 | Loss of possibility of solving conflicts or damages. |
| 4 | Technical or human faults reduce the possibility of assisting incidents. |
| 5 | Lack of opportunity to contact other stakeholders in a distress situation. |
| 6 | Terror or wilful execution with malicious intent (cyber-attacks, etc.). |
| 7 | Insufficient capabilities to fix damaged cargo, equipment, or load units |

## 6. Implementation of the AEGIS methodology on an example

In this section, we implement the AEGIS methodology on an example where we focus on the consequence of "Transport means not ready for loading" and link it to the use case transport of cargo from the Trondheim region to Rotterdam, following the route described in Section 2. The aim is to assess the practical capabilities of the proposed methodology in that transport route. Hence, special attention is given to ensuring ease of use, involving industry stakeholders, and making the methodology comprehensive. All of this seeks to promote the adoption of new technologies, such as sustainable autonomous systems that can effectively reduce GHG emissions in transportation.

The following sequence outlines the process of recognizing and selecting pertinent threats, and preventative and reactive measures, all aimed at the ultimate objective of restoring functionality to the transportation service.

### 6.1. Step 1: Identification of impact categories

As an impact category, this example is related to the Reputation, or rather loss of Reputation (Table 1). This is a likely impact when introducing autonomy into the transport system. The technology is still immature and needs to be tested thoroughly. It can be a challenge to be the pioneer to start using it and thereby be vulnerable to failures that can lead to loss of Reputation. In our case, we selected this category and worked out a scenario that is of high value when planning for transport.

### 6.2. Step 2: Selection of top events

The top event in this example is relevant to the main carriage that, as indicated in Table 2 (transport means not ready for loading -Late arrival vessel). The case study was working with the entire transport from Trondheim to Rotterdam, but to better understand the approaches in this paper, we selected the transshipment terminal in Hitra and two possible top events for further studies, 3.1 and 3.2.

### 6.3. Step 3: Selection of threats sources

Due to this scenario, applicable threats are drawn from the tables mentioned in Section 4, but they can also be individually identified. In simpler terms, these threats could initiate or intensify the actual top event. Main identified threats following the step 2, event 3.1 and 3.2 was identified are as shown below:

1 Threats sources terminal workers and crew, external service providers, operation centre (Table 4):

- Lack of common situational awareness of the operation (Table 4- #16)
- Poor planning quality or operational knowledge (Table 4- #17)

2 Threats sources collaboration low planning quality, information exchange between parties/ICT-systems, procedures (Table 5):

- Uncoordinated interaction between control centre, autonomous vessel, and with terminal services (Table 5- #1)
- Lack of procedures for handling deviation/damage management (time, resources, equipment, damages, …) (Table 5- #10)
- Lack of documentation for cargo/load units to be transported (clearance, safety, insurance, etc) (Table 5- #11)

**Table 11**
Preventive barriers and measures for threats associated with humans, organisational and operational.

| # | Preventive barriers |
|---|---|
| | **Terminal workers and crew, external service providers, terminal workers, operation centre** |
| 1 | Design of boarding, disembarking, loading, and unloading zones at the terminal and on board the vessel that prevents injuries (e.g., crush injuries, person in water, boarding unmanned vessels). |
| 2 | Install procedures for security personnel rejecting loads who pose a security threat. |
| 3 | Install camera/technology for monitoring cargo and technical equipment to build situational awareness at i.e., a ROC, as well as outlook from the vessel and at the terminal |
| 4 | Develop procedures/practices for allowing people access to the areas of operation |
| 5 | Develop systems for monitoring crew and guest on board |
| 6 | Develop secure infrastructure and solution for boarding (e.g., boarding at sea, boarding at terminal) |
| 7 | Eliminate the possibility of going in restricted areas. This both at a terminal and on board a vessel. Implement loading zones or "kiosk" where people are separated from cargo and cargo handling |
| 8 | Develop intelligent and self-learning systems for object detection and situation understanding (sensor fusion) to avoid conflict between humans and technology. |
| 9 | Provide technical understandable information to involved humans, staff at the ROC and at the terminal (e.g., emergency posters and information screens). |
| 10 | Develop instructions/procedures for safety clearance of crew on board, terminal workers, and personnel at the control centre. |
| 11 | Implement easy access to security clearance of load units and cargo |
| 12 | Implement E-learning or other training programs for workers and operators |
| 13 | Implement easy access to "stop"-buttons or procedures to allow workers stop an autonomous operation (the technology should than aim to achieve a Minimum Risk Condition) |
| 14 | Develop and implement shared situational awareness between involved operators and stakeholders (CCTV, ICT-systems) (could be a common interface that allows the involved to see same information and picture) |
| 15 | Implement digital twins/simulations to be used to train on an operation before executing |
| 16 | Ensure universal design, but also consider measures that exceed specified requirements. Plans and aids must be able to handle various challenges, such as unfamiliar equipment in used by the terminal workers. |
| 17 | Implement automatic sanity checks for manual data entries |
| | **Collaboration, low planning quality, information exchange between parties/ ICT-systems, procedures** |
| 18 | Procedures for detection of unforeseen events in the transport system. |
| 19 | Establish procedure descriptions with clear responsibilities, which are also used in training and exercises (e.g., who is responsible on board or at the terminal, who decides stops in operation, how and who calls for external assistance / rescue assistance. Planning must also include time for mobilization, and plan for how the understanding of the situation is communicated between the various actors). |
| 20 | Automatic counting of cargo units combined with lock system at quay facilities. |
| 21 | Guidelines and good communication with workers and external service providers, as well as with the ROC personnel. |
| 22 | Possibilities to contact involved via PA systems, information screens and emergency posters (multilingual). |
| 23 | Alarms with light/sound. |
| 24 | Design of a solution for communication between stakeholders (intuitive user interface). |
| 25 | Notification of ROC (Operation centres), responsibility and possibilities of remote operation |
| 26 | Allow humans to interact with technology and autonomous solutions |
| 27 | Integrated planning and shared information between involved in the transport system |
| 28 | Standardised information exchange when deviation, damage or not planned events happens |
| 29 | Guidelines on how humans can interact with autonomous technology |

**Table 12**
Preventive barriers and measures for threats associated with technological.

| # | Preventive barriers |
|---|---|
| **Communication, remote operation, cyber attacks** | |
| 1 | Implement redundancy in communication equipment for ensuring uninterrupted communication possibilities. |
| 2 | Implement redundant systems to avoid incorrect positioning, e.g., redundant systems, systems that predict position based on speed/steering direction and other available technical information. |
| 3 | Implement "Emergency Stop"-switch available to stop operations. |
| 4 | Implement fire walls or measures to avoid cyber attacks |
| 5 | Implement data security plan |
| 6 | Implement solutions for status monitoring of ships and systems, including technical condition measurement |
| 7 | Implement redundancy in sensors and other relevant solutions to avoid «single point of failure». |
| 8 | Implement plan for preventive maintenance of critical systems. |
| 9 | Develop procedures to transfer operational management between ROC's (in case of technical failure at a ROC etc.) |
| 10 | Develop procedures on "how to get back to normal operation" in case of technical failures happens |
| **Navigation and steering system, geotagging, geofencing** | |
| 11 | Implement redundant navigation solutions on critical technologies used for loading/unloading or transport. |
| 12 | Develop and implement MRC (minimum risk condition) barriers on critical technologies used in the transport system |
| 13 | Implement redundancy in critical sensors and steering systems to avoid «single point of failure» |
| 14 | Develop a contingency plan on possible failures on navigation and steering system, geotagging, or geofencing technology |
| 15 | Develop awareness to available local infrastructure and resources (e.g., how to build awareness based on the technology available in the infrastructure, or from humans in the area). |
| 16 | Implement geofence zones at the vessel for cargo operation, at the terminal, and for allowed navigation zones for autonomous technology. |
| 17 | Implement robust technology for object detection and situation understanding (also by sensor fusion). |
| 18 | Establish a CONOPS for the technology to avoid unwanted situations such as collision or conflict between humans and technology. |
| 19 | Implement possibility for decision support based on data from sensors in infrastructure |
| 20 | Establish machine learning and AI for improved understanding of operational behaviour (could also be used to learn the technology to operate more efficient or safer) |
| 21 | Implement solutions for automatic tracking and tracing of cargo, load units, equipment, and humans |
| 22 | Implement Internal system health monitoring |
| **Vessels, Crane, Port equipment and resources** | |
| 23 | Implement remote monitoring of technical condition on transport means and cargo handling equipment |
| 24 | Install high-sensitivity sensors and alarms for early identification of fire and smoke |
| 25 | Install lights that informs others that it is an autonomous vessel, truck, or crane |
| 26 | Implement hatch for venting harmful fumes and gases in case of fire. |
| 27 | Establish plan for preventive maintenance of technology. |
| 28 | Develop contingency plan for new transport route if deviations in original plans occurs |
| 29 | Develop plan for use of new cargo handling technology/equipment/resources if origin fails |
| 30 | Develop plan for deviation management, i.e., a priority list of cargo to be handle if the time slots do not allow to follow original plan |
| 31 | Establish procedures and/or a collaboration room between stakeholders involved in a transport system (teams or similar) to be used if deviation or damages occurs or leads to disruption in transport |

3 Threats sources vessel, crane, port equipment and resources (Table 8):

- Loading system break down or failure (Table 8- #10)
- Crane Valve leakage (Table 8- #11)

### 6.4. Step 4: Identification of preventive barriers and measures

This step shows the link between the identified sources of threats and current barriers of a preventive nature. Therefore, the preventive barriers are described as below:

**Table 13**
Preventive barriers and measures for threats associated with external.

| # | Preventive barriers |
|---|---|
| **Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc.** | |
| 1 | Develop procedures how to order assistance from external services/emergency services. In case of expected bad weather or expected deviation from planned route the ordering should be sent as soon as possible to avoid deviation. |
| 2 | Implement a new route plan in case of weather or conjunctions do not allow original plan |
| 3 | Implement awareness to technical limitations in case of unforeseen events (heavy tide water or low water in rivers, to long distance between vessel and terminal, crane limitation in range and weight, availability to energy in terminal, etc.) |
| 4 | Develop routines to build awareness on operational limitations, such as use of information from sensors in the infrastructure to plan cargo operations (i.e., use the wind sensors in a terminal to simulate the crane operations, that follows the crane restrictions). |
| 5 | Develop a contingency plan of using other services/resources/equipment in the immediate area, such as call for an ad-hoc vessels or sister vessels in case of need for assistance. |
| 6 | Implement alarms on technical equipment, with light/sound and need for human interaction if required. |
| 7 | Develop learning materials such as a video that describes the autonomous technology in use, its limitations, and how to interact (humans vs technology) |
| 8 | Develop plan for different port quay visits as an alternative if weather predictions indicate conditions outside the operational envelope |
| 9 | Implement automatic shutdown when operational conditions are exceeded |
| **Other external factors (e.g., other ship traffic, construction work)** | |
| 10 | Develop CONOPS on how to operate the vessel/technology together with other traffic |
| 11 | Implement operational envelops where the time interaction between a ROC and technology is defined |
| 12 | Develop routines that limits the operation in bad weather or unforeseen events (i.e., definition of operational limitations on technology, plan for how to operate if some sensors fails, execution of a contingency plan). |
| 13 | Develop plan for how to achieve awareness at a ROC if the sensor quality is degraded and cannot be used for remote technical operation, for example if fog, snow, darkness, heavy rain etc. makes the sensor quality below threshold for operation |
| 14 | Develop plan for operation in a degraded condition, such as sailing with reduced speed, increased safety zones, and with a higher risk factor than normal. |
| 15 | Develop routines to receive needed information on limitations in operation, e.g., information about construction work that limits the operational areas of the technology for a period of time. |

1 Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures (Table 11):

- Procedures for detection of unforeseen events in the transport system (Table 11- #18)
- Integrated planning and shared information between involved in the transport system (Table 11- #27)
- Standardised information exchange when deviation, damage or not planned events happens (Table 11- #28)
- Guidelines on how humans can interact with autonomous technology (Table 11- #29)

2 Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc. (Table 13):

- Develop procedures how to order assistance from external services/emergency services. In case of expected bad weather or expected deviation from planned route the ordering should be sent as soon as possible to avoid deviation (Table 13- #1)
- Implement a new route plan in case of weather or conjunctions do not allow original plan (Table 13- #2)

The list is only a few examples identified for the use case to prevent the top events mentioned in step 2. Other elements when introducing

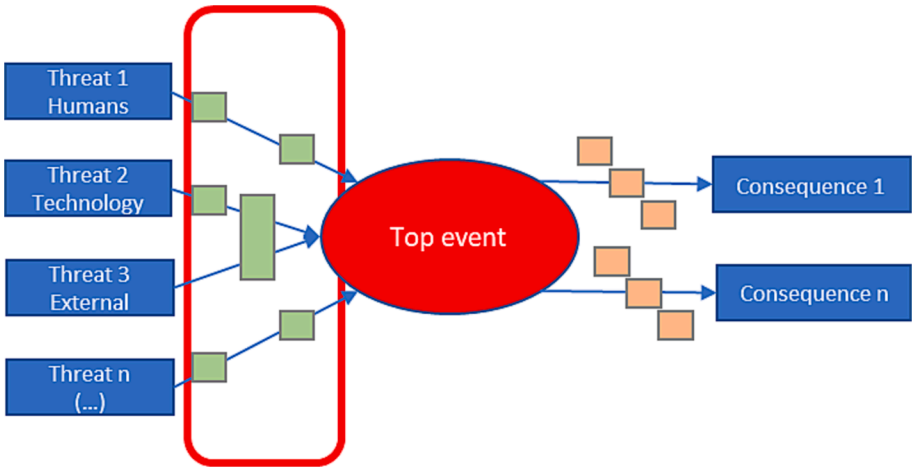



**Fig. 7.** Preventive barriers for reduction of probability.

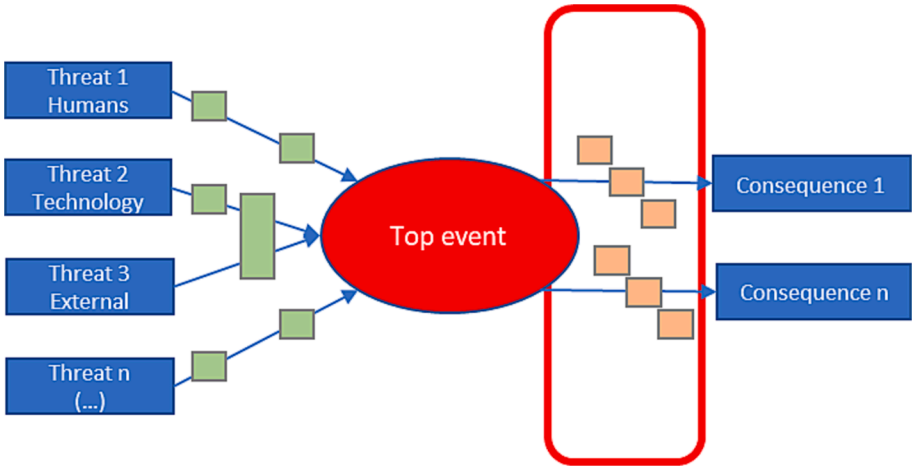



**Fig. 8.** Reactive barriers for consequence reduction.

more autonomy to the transshipment terminal could be to focus on the following:

1 Language problem between the involved stakeholders and workers:

- Provide technical understandable information to involved humans, staff at the ROC and at the terminal (e.g., emergency posters and information screens) (Table 11- #9)
- Implement E-learning or other training programs for workers and operators (Table 11- #12)

2 Lack of documentation for cargo/load units to be transported (clearance, safety, insurance, etc):

- Automatic counting of cargo units combined with lock system at quay facilities. (Table 11- #20)
- Integrated planning and shared information between involved in the transport system (Table 11- #27)
- Standardised information exchange when deviation, damage or not planned events happens (Table 11- #28)

3 Loss of navigation sensors or digital signals for navigation, steering or status:

- Implement redundant navigation solutions on critical technologies used for loading/unloading or transport (Table 12- #11)
- Develop awareness to available local infrastructure and resources (e.g., how to build awareness based on the technology available in the infrastructure, or from humans in the area) (Table 12- #15)
- Implement possibility for decision support based on data from sensors in infrastructure (Table 12- #19)

4 The vessel cannot be sailed into port because bad weather:

- Implement a new route plan in case of weather or conjunctions do not allow original plan (Table 13- #2)
- Implement awareness to technical limitations in case of unforeseen events (heavy tide water or low water in rivers, to long distance between vessel and terminal, crane limitation in range and weight, availability to energy in terminal, etc.) (Table 13- #3)
- Develop a contingency plan of using other services/resources/equipment in the immediate area, such as call for an ad-hoc vessels or sister vessels in case of need for assistance (Table 13- #5)
- Develop plan for different port quay visits as an alternative if weather predictions indicate conditions outside the operational envelope (Table 13- #8)

### *6.5. Steps 5 and 6: Identification of reactive barriers and measures, and consequences*

At this stage, the top event has occurred, and our task is to find potential reactive measures to minimize the consequences of a delayed

**Table 14**
Reactive barriers and measures for threats associated with humans, organisational and operational.

| # | Reactive barriers |
|---|---|
| | **Terminal workers and crew, external service providers, terminal workers, operation centre** |
| 1 | **Effective coordination of salvage situation:** Execute procedures for how the control centre and workers/providers/service personnel should be able to assist and support technology to give qualified awareness/support regards a situation. This includes the possible use of a contact person/site manager that can provide support, that are familiarised with the equipment/vessel as well as with the infrastructure. |
| 2 | **Effectuate correct use of equipment**: Follow instructions on how to operate the technology, guidelines must be followed to ensure best possible use of equipment/resources. This will consider limitations, to be used to mitigate consequences. |
| 3 | **Effectuate effective cargo handling:** Call for extra loading resources (workers, technology). |
| 4 | **Effectuate deviation management:** Inform and discuss challenges with cargo owners to decide new plan for execution. This will follow a contingency plan, or a priority list. |
| 5 | **Get control of number of people in a zone:** Get information from sensors that provides a quick overview of whom is working in an area, where they are located and how to communicate with them to avoid unwanted situations. |
| 6 | **Effectuate treatment of injuries to humans:** Use first aid equipment for treatment of injuries to humans. Injuries can occur at the terminal, during loading activities or as a medical condition to humans etc. The access to the first aid materials must be efficient. In case of serious injuries, call for medical expertise could be required, a "hot line" should be planned for. Also, use of TeleMed for treatment must be an option. |
| 7 | **Effectuate warning to workers:** In case of an accident or a situation that requires information to workers or humans in an area, clear procedures for information sharing and possible way of broadcasting the information should be effectuated. This must be correlated with available technology at site, sometimes a text message to the workers is fine, sometimes execution of alarms or use of PA for voice messages is preferable. |
| | **Collaboration, low planning quality, information exchange between parties/ ICT-systems, procedures** |
| 8 | **Execution of procedures:** Use existing procedures to contact involved stakeholders in case of an incident. The way of collaboration between the involved must be predefined, where also required information for situational awareness should be in place and agreed upon. |
| 9 | **Effectuate call for assistance in case of an incident requiring external assistance**: Follow defined procedures in case of an incident. The routines and procedures should be known and should also be part of a training program. |
| 10 | **Effectuate effective assistance to terminal and crew workers:** The procedures for interaction between the control centre and the transport means/ loading equipment should be followed/effectuated. These procedures will include working orders and information, as well as instructions how to handle an event. The training aspect should address adverse events, such as how to guide the humans during an unwanted event. |
| 11 | **Effectuate interaction with other traffic:** Follow procedures and plans for interaction with other traffic, as for example if the means are an autonomous vessel, then other traffic should know how to exchange information with the ROC/vessel. There will be cases where ColReg (vessel regulations) cannot be followed. It is important that the interaction with other traffic can solve a possible conflict, it is especially important when a top event occurs, the barriers will be to make the interaction as efficient as possible to minimise conflict with other traffic. |
| 12 | **Use mapped list of possible assistance from external/workers/crew/ terminal workers:** A list with people to be contacted in case of an event should be available. The people can assist to achieve site awareness and be a connection point with the ROC when handling the event. |
| 13 | **Effectuate interaction with service providers:** Use existing procedures on how to interact with externals, which means; with tug and port operators, with traffic management, with cargo owners, with agents and stevedores, with the technology at the vessel in interaction with the terminal systems. Each contact point might have a different way for interaction. |

ship arrival. We are using the same approach as previously described, but the barrier ambition will be to minimize the consequences of an event.

Following consequences and possible reactive barriers have been identified, that was of high importance regards the case study mentioned:

1 The customer stop using the service:

**Table 15**
Reactive barriers and measures for threats associated with technological.

| # | Reactive barriers |
|---|---|
| | **Communication, remote operation, cyber attacks** |
| 1 | **Effectuate assistance from the control centre:** Initiate and start remote control assistance by following procedures. This can be assistance with navigation, evacuation, operation of technology, support terminal workers and crew, and for managing an incident, etc. |
| 2 | **Get and exchange shared situational awareness:** Get data from sensors and from observation to be used for decision support. The information should be shared with predefined stakeholders, in an agreed format. Early warnings from alarms should be noted and measures should be executed to combat situation. |
| 3 | **Initiate redundant solutions for critical systems:** Parts of the security system can be knocked out or disabled, either by errors, damages, mistake or by proven actions. It is important to start initialising backup or redundant solutions if required. For example, if the vessel's camera fails, how can awareness from another source/technology be sent/conveyed to the control centre? |
| 4 | **Effectuate remote control of critical equipment:** The control centre should remotely operate critical equipment, such as being able to trigger fire extinguishing systems or initiate redundant technologies available. |
| 5 | **Initiate the use of other communication channels if main fails:** Start using back-up communication system if main solutions go down. |
| 6 | **Allow involvement of external assistance by providing access to the technology:** In this, there are opportunities in providing access to, for example, the vessel's PA system to salvage agencies, which can then provide direct information to humans nearby during an incident or as a mechanism to report an unwanted situation during an operation. |
| 7 | **Shut down in case of cyber-attacks:** In case of cyber-attacks or terrorism the systems should be shut down as soon as possible. There must exist procedures to be followed as well as back-up plans how to operate without the system. |
| | **Navigation and steering system, geotagging, geofencing** |
| 8 | **Effectuate error correction of the ship's or terminal navigation system:** In case of the digital navigation systems fails (position system, sensors in the infrastructure, etc.) the ROC must navigate the vessel in to port/quay remotely by use of cameras or available sensors. |
| 9 | **Send notification to other traffic:** In case of an unwanted situation that might be a hindrance for the surrounding traffic, a notification of vessel condition should be notified and sent to the traffic centre with contact information to the ROC. |
| 10 | **Send notification of deviations according to plan:** Inform deviation to relevant stakeholders and start preparing deviation management, that can be to order for extra services in the loading/unloading of a vessel to minimise the consequences. |
| 11 | **Effectuate *incident navigation guidelines:*** Prepare guidelines for handling the autonomous equipment, e.g., vessel, in the event of a collision or grounding. |
| 12 | **Initialise Minimum Risk Condition:** In case of an uncontrollable event, either the technology or the ROC should launch the MRC procedures/safe state. |
| 13 | **Start identifying cargo or vessel position:** In case the cargo identification is wrong, the sensors indicates errors, or the cargo position is not according to plan, the operators should start the process of identifying where missing cargo is located and start the processes of achieving control to minimise the consequences. |
| 14 | **Start geofencing areas of interest:** In case there are obstacles or humans in a geofenced area, for example an autonomous loading area, the operators or the technology should stop operation until the area is cleared for autonomous operations. |
| 15 | **Error in technological navigation or operation:** In case the technology is doing abnormal operations either the ROC or the humans involved should stop the operation by either press the stop button or by having an interface that can be used. |
| | **Vessels, Crane, Port equipment and resources** |
| 16 | **Get and share situational understanding of incidents/accidents:** Initiate procedures to achieve situational awareness of an incident/accident to be used for decision support. The procedures must be followed to return back to normal operation as soon as possible. The interaction between the control centre and the technology will in many cases be necessary. |
| 17 | **Effectuate procedures for damaged technology or sensor fails:** The consequences of the fail/error must be understood before a decision is made. Guidelines and understanding of consequences must be evaluated and measures must be taken. Consider starting MRC approaches. |
| 18 | **Effectuate effective control of the extent of smoke / fire damage:** Start ventilation for diverting smoke away from vulnerable areas. This is to avoid smoke damage and inhalation of dangerous gases. First aid equipment for the treatment of burns should called for in case humans have been exposed. |
| 19 | **Activate features for emergency salvation:** In case a vessel has to be towed a towing line should be launched such that external rescue team can assist. |

(*continued on next page*)

**Table 15** (*continued*)

| # | Reactive barriers |
|---|---|
| | Similarly, it should be possible to use an autonomous vessel to tow external vessels in distress. |
| 20 | **Effectuate solutions for combating battery fire:** Activate battery fire procedures to limit damage / ensure continued propulsion (e.g., redundancy in engine compartment and battery compartment, short-circuit various cells to reduce fire in damaged cells). |
| 21 | **Call for human assistance:** In case the situation needs human intervention for awareness building or for operational control, the planned *hand-over* process between the operators and site personnel should be followed. |
| 22 | **Technological operational capabilities:** In case the situation requires a high pressure on the equipment in use, the capabilities should be understood, and the operations stopped when the limits have been reached. |
| 23 | **Reallocate ship to different terminal:** In case the situation cannot be mitigated soon enough |
| 24 | **Reallocate ship to different port:** In case the situation cannot be mitigated soon enough |

**Table 16**
Reactive barriers and measures for threats associated with external.

| # | Reactive barriers |
|---|---|
| **Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc.** | |
| 1 | **Initiate procedures and solutions for evacuation and rescue of vessel/ cargo/equipment:** Follow guidelines for evacuation and rescue, which could be to inform about the situation by information sharing (digital, voice, alarms), to call for assistance, and to start an MRC process. |
| 2 | **Call for external assistance to maintenance technology/vessel/ equipment:** Start the process of calling external assistance to handle the event, by providing them with data about the event and to order needed technology for maintenance purposes. |
| 3 | **Effectuate *procedures to start MRC:*** Start the procedures for an MRC. At the same time, if required, call for external assistance should be done, at the same time as a deeper situational awareness should be built. In a worst case the technology, as an example the vessel, should be navigated to an emergency ports/quays/zones/places of refuge, where it can be grounded to minimise consequences. |
| 4 | **Effectuate back-up plans:** In case the weather does not allow operation of cranes/vessel/equipment a back-up plan should be started, such as sailing a vessel to another terminal where the weather picture allows operations. The decisions could also be stay in the area until the weather allows operations, but likely there will be a deviation to original plan that should be announced. |
| 5 | **Call for extra terminal resources:** In case the weather does not allow crane operations, a plan for how to load or unload the vessel should be followed. This can be to call for extra terminal reach-stackers, or to allow both vessel cranes and terminal cranes to operate in parallel. It can also be to use another crane that have higher operational capabilities (certificated to operate in strong wind). This of course requires that the lashing is following the operations. |
| 6 | **Inform about deviation:** In case of a disruption because of the weather, this should be announced as early as possible such that new transport corridors can be booked for to minimise the consequences in the delays. |
| 7 | **Operation in low water or with heavy tide level:** In case there will be restrictions due to low water, or strong tide, either the schedule should be updated to allow expected operation, or a new transport corridor should be launched. |
| **Other external factors (e.g., other ship traffic, construction work)** | |
| 8 | **Collaboration with other traffic*:*** Send information to other traffic regards planned transport route, where information about vessel type (autonomous) and needed assistance should be notified. |
| 9 | Initiate reporting of incident or **damages*:*** Routines must be followed to report damages on cargo/load unit/infrastructure/vessel/crane/infrastructure. If possible, backup should be called for a replacement should be done. |
| 10 | **Effectuate new transport plan*:*** A new transport route/plan should be followed if planned route cannot be used for different reasons. |

- Effectuate effective cargo handling (Table 14- #3)
- Effectuate deviation management (Table 14- #4)

2 The reputation is decreasing:

- Effectuate effective cargo handling (Table 14- #3)
- Effectuate interaction with service providers (Table 14- #13)
- Allow involvement of external assistance by providing access to the technology (Table 15- #6)
- Send notification of deviations according to plan (Table 15- #10)

3 The cargo has to be rescheduled, cannot reach next transport means:

- Reallocate ship to different terminal (Table 15- #23)
- Reallocate ship to different port (Table 15- #24)
- Effectuate back-up plans (Table 16- #4)
- Inform about deviation (Table 16- #6)

It is important to note that certain factors, such as the statistical frequency of engine breakdowns, were not taken into account in assessing the AEGIS solution. This was because reliable data on these issues was unavailable then. However, it is acknowledged that this issue can be addressed and considered in future studies or assessments. By obtaining more reliable data in the future, it will be possible to incorporate and analyze these factors further to enhance the evaluation and understanding of the AEGIS solution.

## 7. Discussion and conclusion

To ensure a smooth green transition to autonomous vessels employing low-carbon emission propulsion systems, this study presents a way to assess potential risks in sustainable autonomous maritime transportation systems. This method is based on a well-known safety and security analysis technique called “bow-tie.” The paper describes how this method works by using examples related to various aspects of an autonomous transport chain, such as threats, preventive actions, unwanted incidents, reactive actions, and possible outcomes. For this purpose, by proposing the new methodology a comprehensive study has been conducted to identify top events as well as preventive and reactive measures to increase resiliency. The goal was to evaluate the impact of AEGIS solutions within the use case between Trondheim and Rotterdam, at the same time as the resilience assessment to the case was investigated.

The methodology also pointed to the importance of thinking about the whole transport system, and possible barriers that could be both human-oriented, technology-oriented, and external factors. The studies are also a valuable contribution to the technology providers when answering regulatorily questions to autonomous operation. It is also an important contribution when focusing on resilience, to prepare for unknown events and have some barriers to be launched when needed.

The analysis reveals that when it comes to minimizing the consequences of unwanted events, compared to conventional maritime transportation, autonomy changes the traditional safeguards that relate to human intervention. Therefore, it also creates new opportunities for processes, procedures, and operations that were not possible with human control. It is worth mentioning that when considering the outcomes of incidents, it is essential to differentiate between typical reliability-related consequences, like delays and business interruptions, and safety-related consequences. Autonomous systems can improve safety by eliminating human error but may introduce new safety challenges that could make the system vulnerable. However, according to the assessments, in terms of overall resilience, the consequences follow similar patterns as conventional shipping. This is because the primary goal of shipping, which is to transport goods from one place to another, remains the same, whether conventional or autonomous.

The methodology described in this paper has shown valuable when planning for autonomous technology to be implemented into a transport system. It can also be used for conventional and multimodal transport, and it is worth mentioning that it is necessary to tailor it to its own operations where possible new threats and barriers are identified and written into the methodology. But from the case study in AEGIS, we have described the value of using such a methodology, to understand

challenges and to understand how to avoid an event or minimize the consequences.

In closing, we believe that the results of this paper are important from both a managerial and a policy perspective. From a managerial perspective, establishing a credible business case for the AEGIS solution necessitates (as an important prerequisite) the analysis of system resilience. From a policy perspective, and at least in Europe, shifting cargoes from road to greener modes (such as short sea shipping and inland navigation) remains an important policy goal (Psaraftis and Zis, 2020). The recently adopted European Green Deal, of which the "Fit for 55" package (EC, 2021) is an important pillar, is expected to encourage transport solutions that are greener and at the same time resilient. We believe that the results of this paper can be useful for the realization of this goal.

## CRediT authorship contribution statement

**Kay Fjørtoft:** Writing – original draft, Writing – review & editing. **Seyed Parsa Parvasi: . Dag Atle Nesheim: . Lars Andreas Lien Wennerberg: . Odd Erik Mørkrid: . Harilaos N. Psaraftis:** Writing – original draft, Writing – review & editing.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

Data will be made available on request.

## Acknowledgments

Work on this paper has been funded in part by the EU H2020 AEGIS project, Grant No. 859992 (2020-2023). SINTEF OCEAN of Norway is the project leader. We want to thank the partners of the AEGIS consortium for their fruitful collaboration. We also acknowledge the two Norwegian Research Council projects MARMAN (324726 - FORSKER21).

## References

Abaei, M.M., Hekkenberg, R., BahooToroody, A., Banda, O.V., van Gelder, P., 2022. A probabilistic model to evaluate the resilience of unattended machinery plants in autonomous ships. Reliab. Eng. Syst. Saf. 219, 108176.

AEGIS 2023, https://aegis.autonomous-ship.org/.

Commission of the European Communities 2009, Strategic Goals and Recommendations for the EU's Maritime Transport Policy until 2018, COM/2009/0008 final, Brussels, January 2009.

Dagdilelis, D., Blanke, M., Andersen, R.H., Galeazzi, R., 2022. Cyber-resilience for marine navigation by information fusion and change detection. Ocean Eng. 266, 112605.

Deshmukh, R., Weber, P., Deschenes, O., Hernandez-Cortes, D., Kordell, T., Lee, R., Malloy, C., Mangin, T., Meng, M., Sum, S., Thivierge, V., 2023. Equitable low-carbon transition pathways for California's oil extraction. Nat. Energy 1–13.

Dui, H., Zheng, X., Wu, S., 2021. Resilience analysis of maritime transportation systems based on importance measures. Reliab. Eng. Syst. Saf. 209, 107461.

European Commission 2011, 'European Commission White Paper', available at: https://ec.europa.eu/transport/themes/strategies/2011_white_paper_en.

European Commission 2019, 'A European Green Deal', accessed 5th April 2021, available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.

European Commission 2021, 'Fit for 55 - delivering the EU's 2030 climate target on the way to climate neutrality', In: available at: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0550.

Evensen, M.H., 2020. Safety and security of autonomous vessels. Based on the Yara Birkeland project. The University of Bergen. Master's thesis.

Fjørtoft, K.E., Holte, E.A., 2022. Implementing operational envelopes for improved resilience of autonomous maritime transport. Human Fact. Transport.

Fjørtoft, K.E., Mørkrid, O.E., 2021. Resilience in autonomous shipping. Proceedings to the ESREL-21 Conference.

Gu, B., Liu, J., 2023. A systematic review of resilience in the maritime transport. Int. J. Log. Res. Appl. 1–22.

Hoem, Å.S., Johnsen, S.O., Rødseth, Ø.J., Fjørtoft, K.E., Jenssen, G. and Moen, T., 2021. Improving safety by learning from automation in transport systems with a focus on sensemaking and meaningful human control. Sensemaking in Safety Critical and Complex Situations: Human Factors and Design.

Hollnagel 2019, https://www.resilience-engineering-association.org/blog/2019/11/09/what-is-resilience-engineering/.

International Maritime Organization (IMO) 2021, IMO - MSC.1/Circ.1638 3 June 2021 – Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships (MASS), Circular 1638.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.H., 2022. Maritime cybersecurity: are onboard systems ready? Marit. Policy Manag. 1–19.

Koimtzoglou, A., Themelis, N., Ventikos, N.P., Louzis, K., Koimtzoglou, M., Giannakis, K., Panagiotidis, P., Moustogiannis, S., Ramiro, M., Peña, J., Gomez, D., 2022. Assessing the risk during mustering in large passenger vessels: A digital tool for real time decision support. In: Sustainable Development and Innovations in Marine Technologies. CRC Press, pp. 269–276.

Krause, S., Wurzler, L., Mørkrid, O.E., Fjørtoft, K., Psaraftis, H.N., Vilanova, M.R., Zis, T., Coelho, N.F., van Tatenhove, J., Raakjær, J., Kloch, K., 2022. Development of an advanced, efficient and green intermodal system with autonomous inland and short sea shipping-AEGIS. J. Phys. Conf. Series 2311 (1), 012031. IOP Publishing.

Mallam, S.C., Nazir, S., Sharma, A., 2020. The human element in future Maritime Operations–perceived impact of autonomous shipping. Ergonomics 63 (3), 334–345.

MUNIN 2016, 'MUNIN final brochure', http://www.unmanned-ship.org/munin/wp-content/uploads/2016/02/MUNIN-final-brochure.pdf.

OECD. 2022. OECD.Stat. Available at: https://stats.oecd.org.

Omer, M., Mostashari, A., Nilchiani, R., Mansouri, M., 2012. A framework for assessing resiliency of maritime transportation systems. Marit. Policy Manag. 39 (7), 685–703.

Onishchenko, O., Shumilova, K., Volyanskyy, S., Volyanskaya, Y., Volianskyi, Y., 2022. Ensuring cyber resilience of ship information systems. TransNav: International Journal on Marine Navigation and Safety of Sea. Transportation 16 (1), 43–50.

Park, H., Blanco, C.C., Bendoly, E., 2022. Vessel sharing and its impact on maritime operations and carbon emissions. Prod. Oper. Manag. 31 (7), 2925–2942.

Psaraftis, H.N., 2012. Formal safety assessment: an updated review. J. Mar. Sci. Technol. 17, 390–402.

Psaraftis, H.N., Zis, T., 2020. European policies for short sea shipping and intermodality. In: Short Sea Shipping in the Age of Sustainable Development and Information Technology, pp. 3–21.

Schröder-Hinrichs, J.U., Praetorius, G., Graziano, A., Kataria, A., Baldauf, M., 2016. Introducing the concept of resilience into maritime safety. In: 6th Symposium on Resilience Engineering, Lisbon, Portugal, June 22-25, 2015. Resilience Engineering Association, pp. 176–182.

Tunggal 2020. UpGuard eBook: Critical cybersecurity threats and KPIs for every business, and https://www.upguard.com/blog/cyber-attack.

UNCTAD 2020, Accelerating digitalization - Critical actions to strengthen the resilience of the maritime supply chain, Mobility and transport connectivity series, viewed [December 2022], https://unctad.org/system/files/non-official-document/tlb_20210304_report_wb.pdf.

Veitch, E., Alsos, O.A., 2022. A systematic review of human-AI interaction in autonomous ship systems. Saf. Sci. 152, 105778.

Verschuur, J., Koks, E.E., Hall, J.W., 2020. Port disruptions due to natural disasters: Insights into port and logistics resilience. Transp. Res. Part D: Transp. Environ. 85, 102393.

Woods, D.D., 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 141, 5–9.

Zavitsas, K., Zis, T., Bell, M.G., 2018. The impact of flexible environmental policy on maritime supply chain resilience. Transp. Policy 72, 116–128.

Zhou, Y., Wang, J., Yang, H., 2019. Resilience of transportation systems: concepts and comprehensive review. IEEE Trans. Intell. Transp. Syst. 20 (12), 4262–4276.

Zis, T.P., Psaraftis, H.N., Reche-Vilanova, M., 2023. Design and application of a key performance indicator (KPI) framework for autonomous shipping in Europe. Maritime Transport Research 5, 100095.